Statement of Carine Kanimba, July 27, 2022

Mr. Chairman, Members of the Committee, thank you for the invitation to speak before you today and the opportunity to share my story.

My name is Carine Kanimba. I am the youngest of six children of Taciana and Paul Rusesabagina. I am a naturalized American Citizen. As it has over the course of nearly 250 years, the United States welcomed my family as we were in search of her refuge. Finding safety and security within its borders, we are truly the beneficiaries of the American Dream. I am a proud graduate of Northwestern University. Until two years ago, I had a job I loved in finance based out of New York City.

In August of 2020, everything changed. Nearly 700 days ago, my father was lured from our family home in San Antonio, Texas, by an intelligence operation directed by the government of Rwanda. He was kidnapped in Dubai and then illegally rendered to Kigali via a private jet chartered directly by the office of the Rwandan President. My father was tortured, subjected to a sham trial, and sentenced to 25 years in prison. His crime? Using words to agitate for democracy and human rights.

Since that time, my family and I have become my father's full-time advocates, engaging with government officials and others in the United States and across Europe, all in an effort to secure his release.

In 2021, just as my father had been targeted in the U.S., I too became a victim of the government of Rwanda. This time, through Rwanda's use of NSO's Pegasus spyware. I have, sitting here today, lost all sense of security in my private actions and my physical surroundings.

This has all been perpetrated by a country which is supposed to be an ally of the United States and is the recipient of hundreds of millions of dollars in aid funded by U.S. taxpayers. That what happened to my family on U.S. soil was funded by our own tax dollars truly shocks the conscience. More on that in a moment. First, I'd like to tell you more about why I am here today.

I was born in Rwanda just prior to the horrific 1994 genocide that made me an orphan. My birth parents were among the first victims of the nearly 1 million people killed during the genocide, leaving my sister, Anaise, and I orphans. Anaise is here with me today.

My father, Paul Rusesabagina, is a hero of the genocide. In 1994, he was the manager of a hotel in Kigali. He gave refuge to 1,268 people in his hotel, risking his own life every day to push back the militia who were waiting outside. Not a single person in the hotel was killed during the many weeks the genocide continued.

Once the killing finally ended, my yet to be adoptive parents—Taciana and Paul-- searched for us, found us in a refugee camp, then raised and loved us as their own, along with my adoptive brothers and sisters Lys, Roger, Diane, and Tresor. My mother is also with me here today. I owe her and my father everything.

In 2004, this story was portrayed in the film Hotel Rwanda and my father's name became known all over the world. He was known as a man of peace and virtue. In 2005, he was awarded the U.S. Presidential Medal of Freedom by President George W. Bush. I'll never forget that moment.

My father was given a platform and he used it for good. He was critical of what he saw as an increasing violation of the human rights of Rwandans, calling loudly for democracy, freedom of speech and press, as well truth and reconciliation for all Rwandans, without regard to their ethnic origins. This criticism turned him into a target of Rwandan President Paul Kagame.

Due to my father's activism, elevated voice and continued belief in a better world, President Kagame launched a harassment campaign targeting him. Like a school yard bully, but with deadly consequences. There were assassination attempts against my father's life in Belgium, house break-ins, smears and lies printed daily against him. But my father was never intimidated into silence, he knew that he had a responsibility to use his platform and be the voice for the silenced victims of a 30-year Rwandan dictatorship.

It was in this context that President Kagame would call my father's kidnapping a "flawless" operation. It was flawless because Rwanda surveilled and tracked him in San Antonio, Texas. We know that the Rwandan government has surveilled my father for many years and in this case it publicly boasted, for example, about knowing precisely when my father got his required Covid test prior to departing the U.S.

With the passage of the Robert Levinson Act of 2020, we hope that the new authorities this legislation provides—including sanctions and denial of entry into the United States for persons engaged in this very conduct—will help prevent other American families from being victimized as we have been.

In February of 2021, I was contacted by a collective of journalists called Forbidden Stories, working with Amnesty International and Citizen Lab on the Pegasus project. They had reason to believe I was being spied on. They asked to conduct a forensics analysis on my phone and I agreed. It then was discovered that the Pegasus surveillance had been used to target me. I was mortified to learn that I was a victim of this powerful surveillance malware.

The forensic reports have been presented to this Committee and I understand will be made part of the public record. The reports show that the spyware triggered into operation as I walked with my mother into a meeting with the Belgian Minister of Foreign Affairs. It was active during calls with the US Presidential Envoy for Hostage Affairs team and the U.S. State Department, as well as when speaking with US human rights groups. This surveillance is illegal under U.S. law and allowed the Rwandan government to always stay a step ahead as we fought to keep our father alive and secure his release.

I don't know exactly how much my surveillance cost the government of Rwanda, but I am told it would run into millions of dollars. Rwanda is the third most aid dependent country in the world, with foreign aid constituting over 70% of national expenditures. The U.S. provided 160 million dollars in aid to Rwanda last year. All of you, members of Congress, and American taxpayers themselves deserve to know that the government of Rwanda is spending humanitarian aid to finance the kidnapping of a democracy activist from U.S. soil and using modern technology to surveil his 29-year-old daughter working to secure his release.

Just this past month, Citizen Lab also discovered that my cousin Jean Paul Nsonzerumpa's phone had also been infected. Jean-Paul and I live in the same house. Two phones in the same household, targeted by the same software, by the same repressive regime.

I am frightened by what the Rwandan government will do to me and my family next. It is horrifying to me that they knew everything I was doing, precisely where I was, who I was speaking with, my private thoughts and actions, at any moment they desired. Unless there are consequences for the countries and their enablers which abuse this technology to hurt innocent people, none of us are safe.

I am very grateful, once again, to share my story and the story of my father, Paul Rusesabagina. I hope you find it useful to consider how to regulate the types of tools used to target my family. We are also grateful that the House of Representatives has already twice passed Resolutions demanding my father's release and I promise you all that we will not stop advocating for him until he is home.

United States Department of State

Washington, D.C. 20520

www.state.gov

May 6, 2022

To Whom It May Concern:

This letter serves to summarize facts known by or reported to the U.S. Department of State concerning the Rwandan government's wrongful detention of U.S. Lawful Permanent Resident Paul Rusesabagina.

Pursuant to the Robert Levinson Hostage Recovery and Hostage-taking Accountability Act, Section 302(c) of the Consolidated Appropriations Act, 2021, Public Law 116-260, the U.S. Department of State has determined the government of Rwanda has wrongfully detained U.S. Lawful Permanent Resident Paul Rusesabagina. He was arrested on August 31, 2020, and has been detained in Rwanda since that time. He is currently held in Mageragere Prison, Kigali. Since his arrest, Mr. Rusesabagina has been unable to travel, freely communicate, or complete documentation necessary to manage his personal affairs. The U.S. Department of State has been engaged on Mr. Rusesabagina's case throughout and remains committed to assuring his welfare and securing his release.

If you have any questions, please contact Jennifer Harkins at the U.S. Department of State's Office of the Special Presidential Envoy for Hostage Affairs at 202-485-2128 or by email at HarkinsJ@State.gov.

Sincerely,

Roger D. Carstens

Special Presidential Envoy for Hostage Affairs

AMERICAN BAR ASSOCIATION

Center for Human Rights

The Case of Paul Rusesabagina

June 2021

TRIALWATCH FAIRNESS REPORT

A CLOONEY FOUNDATION FOR JUSTICE INITIATIVE

ABOUT THE AUTHORS:

Geoffrey Robertson AO, QC is the founder and head of Doughty Street Chambers, which is Europe's largest human rights practice. He has had a long and distinguished career as trial and appellate counsel in Britain and in international courts, and he served as first President of the UN war crimes court in Sierra Leone, and as a founding member of the UN's Internal Justice Council. In 2011 he received the New York Bar Association Award for distinction in international law and affairs and in 2018 he was awarded the Order of Australia for services to human rights. He is the author of Crimes against Humanity – The Struggle for Global Justice and other scholarly works on genocide and the use of targeted sanctions against human rights abusers. He is a Master of the Middle Temple and visiting professor at the New College of Humanities.

Staff at the American Bar Association Center for Human Rights helped to draft this report. The **American Bar Association** (ABA) is the largest voluntary association of lawyers and legal professionals in the world. As the national voice of the legal profession, the ABA works to improve the administration of justice, promotes programs that assist lawyers and judges in their work, accredits law schools, provides continuing legal education, and works to build public understanding around the world of the importance of the rule of law. The **ABA Center for Human Rights** has monitored trials and provided pro bono assistance to at-risk human rights defenders in over 60 countries. It is an implementing partner in the Clooney Foundation for Justice's TrialWatch initiative.

ABOUT THE CLOONEY FOUNDATION FOR JUSTICE'S TRIALWATCH INITIATIVE:

The **Clooney Foundation for Justice's TrialWatch initiative** is focused on monitoring and responding to trials around the world that pose a high risk of human rights violations. TrialWatch is global in scope and focused on trials targeting journalists, LGBTQ persons, women and girls, minorities, and human rights defenders. It works to expose injustice and rally support to secure justice for defendants whose rights have been violated.

The statements and analysis expressed have not been approved by the House of Delegates or the Board of Governors of the American Bar Association, and do not represent the position or policy of the American Bar Association. Furthermore, nothing in this report should be considered legal advice for specific cases. Additionally, the views expressed in this report are not necessarily those of the Clooney Foundation for Justice.

EXECUTIVE SUMMARY

The American Bar Association Center for Human Rights has been monitoring criminal proceedings against Paul Rusesabagina in Rwanda since September 2020 as part of the Clooney Foundation for Justice's TrialWatch initiative. This report, co-authored by TrialWatch expert Geoffrey Robertson QC and the ABA Center for Human Rights, details many aspects of the proceedings thus far which cause grave disquiet as to their fairness, and which may have irretrievably prejudiced the defense. Given the analysis below, which draws on standards established by the United Nations Human Rights Committee and African human rights bodies, the fairness of the proceedings appears to have been compromised such as to call into question any verdict convicting Mr. Rusesabagina.

Mr. Rusesabagina's trial opened on February 17. After the defendants were led into the courtroom, the first thing the judges did was to adjourn for five minutes to enable photographs to be taken, raising concerns that the trial was more public spectacle than judicial undertaking. These concerns persisted throughout the trial.

At a hearing on March 12, 2021, Mr. Rusesabagina, who is charged alongside 20 co-accused with various terrorism-related offenses, stated that he would no longer participate in his trial. Mr. Rusesabagina explained that his withdrawal was based on the court's rulings that the trial could proceed despite his transfer to Rwanda outside of any legal framework and despite restrictions on his access to case materials. Since that date, Mr. Rusesabagina and his lawyers have not attended the trial, which has consisted of prosecution and defense presentations.

While the continuation of the trial in Mr. Rusesabagina's absence may itself be consistent with international and regional human rights standards, the circumstances surrounding and subsequent to his withdrawal disclose severe violations of his fair trial rights. In particular, Mr. Rusesabagina has been denied his right to adequately prepare for trial and his right to confidential communication with counsel – potentially to the irreparable detriment of the defense.

Namely, the prison authorities, which are supervised by the Minister of Justice – the prosecuting authority in Mr. Rusesabagina's case – insisted on intercepting, reading, and, oftentimes, retaining all communications between counsel and Mr. Rusesabagina on the pretext that they were entitled to maintain security and check for any escape plans. Even after the Minister of Justice and court ordered the prison to take greater care in distinguishing between non-privileged and privileged materials, officials heightened restrictions, subjecting Mr. Rusesabagina's lawyers to intrusive searches for documents prior to entering the prison and, in one case, confiscating a document marked privileged and confidential. Any openness Mr. Rusesabagina might have felt in discussing the case and strategy with his lawyers has thus been extinguished.

The authorities further failed to effect simple reforms to address the lack of facilities available to Mr. Rusesabagina (which the court itself had deemed a problem), so that Mr. Rusesabagina could prepare for trial. On March 12, when the court ruled that the trial could proceed, the authorities had yet to return seized case documents to Mr. Rusesabagina or provide him with a computer (to review some 3,000 pages of court papers).

Where an accused withdraws from trial, courts are obligated to make all efforts to ensure that his or her fair trial rights are upheld. This often takes the form of appointing amicus counsel – an independent lawyer to probe the testimony of witnesses hostile to the defendant. Here, the court made no effort to this end: to the contrary, the court presiding over Mr. Rusesabagina's case failed to ask questions testing the motives or credibility of the two witnesses against Mr. Rusesabagina who testified in hearings immediately following his withdrawal from the trial. Of subsequent witnesses, the court went so far as to ask leading questions about Mr. Rusesabagina's guilt. This conduct strayed far from the principle that an accused's withdrawal from the proceedings necessitates ever vigilant protection of his fair trial rights. Further, the verdict will not have been based on evidence which has been properly tested and will thus lack credibility.

More broadly, there have been allegations that the authorities are attempting to pressure Mr. Rusesabagina to resume participation in the trial before the verdict. Notably, the trial has taken place against a backdrop in which President Paul Kagame has repeatedly made comments characterizing Mr. Rusesabagina as guilty, a severe violation of the presumption of innocence.

In this context, the overwhelming question is whether Mr. Rusesabagina's trial, both initially, and thereafter *in absentia*, can be considered fair. Taking into consideration the developments to date and noting that final conclusions on this matter will be issued after the verdict, it is doubtful that the court is prepared to offer the guarantees of fairness that these proceedings require in order to be credible if they are to result, as seems predetermined, in a conviction which may carry a sentence of life imprisonment.

Lastly, it appears that the Belgian authorities have assisted the Rwandan authorities in Mr. Rusesabagina's prosecution since his transfer to Rwanda. This assistance, repeatedly referenced by the prosecution in submissions to the court, raises serious questions for the government of Belgium, whose diplomats have been present at the trial. In light of the above analysis, Belgium should clarify the scope and nature of its previous assistance, whether and how it addressed the potential that its support might facilitate fair trial violations, and whether it plans on continuing such support.

The court heard from civil parties on June 16, and prosecution closing arguments have now commenced. Defense closing arguments are expected to begin the week of June 21. This report is being released now, before the conclusion of the trial, to underscore the continuing importance of fair trial guarantees and the severity of the concerns regarding what has transpired to date. A full report will be released after the verdict is issued.

PROCEDURAL HISTORY

This report covers events subsequent to the release of the Center's background briefing and TrialWatch Expert Geoffrey Robertson's accompanying statement in January 2021. Similarly, the present report is being released in conjunction with a statement from co-author and TrialWatch Expert Geoffrey Robertson, which raises additional concerns about the fairness of the proceedings that will be fully evaluated in the final report on the case.

A. PRETRIAL MOTIONS

Mr. Rusesabagina's trial was scheduled to start on January 26, 2021. It was subsequently postponed to February 17, 2021.[1]

In the period leading up to trial, the defense filed several motions alleging violations of Mr. Rusesabagina's rights. A motion filed on January 21, for example, requested that the court release Mr. Rusesabagina and permanently stay the proceedings on the basis of his "illegal and enforced disappearance and extraordinary rendition to Rwanda."[2] The motion further alleged that the prison authorities had been confiscating and not returning case-related materials delivered by defense counsel to Mr. Rusesabagina in prison, hindering his ability to prepare for trial.[3] As mentioned in the Center's background briefing, the authorities have reportedly confiscated not only case documents but also exchanges between counsel and Mr. Rusesabagina, such as defense strategy memoranda.[4] The January motion filed by defense counsel noted that even if confiscation had not occurred, Mr. Rusesabagina lacked the necessary tools (not "even paper and a pen") to review case-related documents.[5]

A second motion filed on February 12 stated that the aforementioned violations relating to prison officials' interception and retention of case-related materials had persisted and put forth additional arguments with respect to Mr. Rusesabagina's transfer to Rwanda.[6] The motion "request[ed]a postponement of the start of the trial until the issues raised by

[1] Prior to trial, there were certain hearings that were not held in public in in which Mr. Rusesabagina was interrogated by the prosecution and judges. This represents a serious violation of his rights and will be discussed in the final report issued after the verdict.

[2] Rusesabagina Defense Team, Motion Re Fundamental Rights, January 21, 2021.

[3] Id.

[4] American Bar Association Center for Human Rights, "Background Briefing on Proceedings Against Paul Rusesabagina", January 26, 2021. Available at https://www.americanbar.org/groups/human_rights/reports/background_briefing_rwanda_paul_rusesabagina/.

[5] Rusesabagina Defense Team, Motion Re Fundamental Rights, January 21, 2021.

[6] Rusesabagina Defense Team, Motion Re Fundamental Rights, February 12, 2021.

the Defendant have been adjudicated, and until adequate and reasonable time and facilities have been provided for his preparation for trial."[7]

B. START OF THE TRIAL

The trial commenced on February 17. As noted above, the defendants were led into the courtroom in handcuffs. The first thing the court did was to adjourn for 5 minutes to enable photographs to be taken.

As of the opening of trial, the court had not yet responded to defense motions. The prosecution notified the court that three defendants – Callixte Nsabimana (Sankara), Herman Nsengimana, and Jean-Damascene Nsabimana – had been joined to the case, making the total number of accused 21.[8] At the beginning of the hearing, Mr. Rusesabagina stepped forward and stated that he had been kidnapped.[9]
The remainder of the hearing consisted of defense and prosecution arguments on the issue of Mr. Rusesabagina's transfer to Rwanda. The court asked the parties to submit written pleadings regarding the circumstances of Mr. Rusesabagina's arrest and transfer to Rwanda and adjourned the hearing to February 26.[10]

On February 26, the court ruled that the discussion regarding Mr. Rusesabagina's arrest and detention was "irrelevant" and that the trial should proceed.[11] According to the court, "jurisdiction in the criminal codes [was] clear."[12] Mr. Rusesabagina's defense counsel, Gatera Gashabana, stated that in light of the ruling the defense required additional time to submit a new motion on the issue of adequate time and facilities (as noted above, the court had yet to rule on the defense's previous motions in this regard), particularly so as to consult with Mr. Rusesabagina on how to proceed.[13] Mr. Gashabana further raised the issue of the continuing seizure of documents by the prison authorities, which the presiding judge stated he was not familiar with (despite submitted defense motions stating as much).[14] Over the prosecution's objections, the court adjourned the hearing for the submission of pleadings on these two issues.[15] Mr. Gashabana additionally stated that he would appeal the court's ruling on jurisdiction and the relevance of the circumstances of Mr. Rusesabagina's transfer to Rwanda.[16]

[7] Id.
[8] Trial Monitor's Notes, February 17, 2021.
[9] Id.
[10] Id.
[11] Trial Monitor's Notes, February 26, 2021.
[12] Id.
[13] Id.
[14] Id.
[15] Id.
[16] Id.

C. MINISTER OF JUSTICE INTERVIEW AND THE PRISON VISIT

On February 26, Minister of Justice Johnston Busingye gave an interview with Al Jazeera in which he acknowledged that the Rwandan government had worked with an associate of Mr. Rusesabagina to lure him to Kigali.[17] He further stated that the confidentiality of Mr. Rusesabagina's communications with counsel had been protected and that the government had in no way intercepted any materials intended for Mr. Rusesabagina or otherwise violated his right to confidential communications with counsel.[18]

Mr. Busingye's public relations team, however, accidentally sent Al Jazeera a video of the team preparing Mr. Busingye for the interview.[19] During this conversation, Mr. Busingye stated that prisons insist on "finding out what is happening inside prisons … including legal documents" so as to maintain safety.[20] He indicated that the prison authorities had thus reviewed materials relayed to Mr. Rusesabagina in prison and that the authorities had found a document that contained escape plans[21] (the veracity of these allegations has been contested by the defense, which has asserted that the purported escape plan was a set-up to enable guards to kill Mr. Rusesabagina).[22]

Following the release of this video, Al Jazeera conducted a follow-up interview with Mr. Busingye, in which Mr. Busingye alternately stated that the confidentiality of communications between Mr. Rusesabagina and his counsel was protected by law and that the prison authorities were entitled to examine all documents entering the prison.[23] He additionally asserted that notwithstanding the fact that the Minister of Justice oversees the prison system, prison authorities act autonomously and would not normally inform him of the contents of any examined materials except where serious issues arose.[24]

Later on in the interview, Mr. Busingye appeared to contradict this statement. The interviewer asked: "When you looked at the communications of Rusesabagina and his

[17] Al Jazeera, "Rwanda Paid for the Flight that Led to Paul Rusesabagina Arrest", February 26, 2021. Available at https://www.aljazeera.com/program/upfront/2021/2/26/rwanda-paid-for-flight-that-led-to-paul-rusesabagina-arrest.
[18] Id.
[19] Id.
[20] Id.
[21] Id.
[22] Hotel Rwanda Rusesabagina Foundation, "Is the Escape Plan the Setup for Rwanda to Kill Paul Rusesabagina?", March 1, 2021. Available at https://hrrfoundation.com/2021/03/01/is-the-escape-plan-the-setup-for-rwanda-to-kill-paul-rusesabagina/.
[23] Al Jazeera, "Rwanda Paid for the Flight that Led to Paul Rusesabagina Arrest", February 26, 2021.
[24] Id.

attorney and found no security concerns you left it alone?”[25] Mr. Busingye responded: “Yes”, implying that he had looked at the communications in question.[26] With respect to the circumstances of Mr. Rusesabagina’s arrival in Kigali, Mr. Busingye stated that Rwanda had paid for the plane.[27]

The Rwandan Ministry of Justice subsequently released a statement on Twitter “clarify[ing]” its position on these issues.[28] Namely, the Ministry stated that communications between an accused and defense counsel were protected by law; that all other materials entering the prison were subjected to “routine safety checks”; that the Minister became aware of a potential violation of Mr. Rusesabagina’s right to confidential communications in December 2020; and that he subsequently instructed the prison authorities to return relevant documents to Mr. Rusesabagina and to take greater care in distinguishing between privileged and non-privileged materials.[29]

In light of these developments, the judges and all parties visited the prison on March 1. Mr. Rusesabagina restated points made at previous hearings, noting that the authorities were continuing to seize case related documents, and requesting that he be provided a computer so as to be able to review the case file, which was in excess of 3,000 pages.[30] Defense counsel asserted that Mr. Rusesabagina had been unable to contribute to the defense strategy given such obstacles.[31] The prison authorities responded that they had indeed confiscated documents pursuant to security regulations and that there had occasionally been delays in returning the documents (the defense in contrast stated that the materials had not just been delayed in reaching Mr. Rusesabagina, but were never returned at all).[32] The prison authorities further avowed that they would attempt to obtain a computer for Mr. Rusesabagina.[33] Upon viewing Mr. Rusesabagina’s cell the judges “found that he had a table and a shelf available, which could help him.”[34]

On March 5, the trial continued. The court summarized the prison visit and noted that Mr. Rusesabagina did not have adequate facilities to prepare for his defense, that case related documents had been confiscated and should not be confiscated going forward, and that “other things that people have sent to him through his defense lawyer” could be examined by prison management for compliance with safety regulations.[35] This

[25] Id.
[26] Id.
[27] Id.
[28] Twitter, Ministry of Justice of Rwanda Post, February 26,2021. Available at https://twitter.com/Rwanda_Justice/status/1365375804423561216/photo/1.
[29] Id.
[30] High Court Chamber for International Crimes, Report on the Prison Visit Following the Problems Raised by Paul Rusesabagina, March 1, 2021.
[31] Id.
[32] Id.
[33] Id.
[34] Id.
[35] Trial Monitor’s Notes, March 5, 2021.

pronouncement was reflected in a written ruling issued on March 9 in which the court declared, among other things, that:

> Paul Rusesabagina does not have sufficient means to allow him to prepare for his trial … The other thing that has been observed and that needs to be corrected is that there are documents from his trial, as well as other documents, that have been seized, and their return to his person is taking a long time. [T]he documents which form part of the case file which Rusesabagina Paul exchanges with his lawyers should not be seized. As regards other documents which are not part of the trial file, as well as various other objects which are sent to him through his lawyers, they should make a list (inventory) and hand them over to him through the prison administration.[36]

D. THE BISHOP'S TESTIMONY, RULING ON TRANSFER TO RWANDA, AND MR. RUSESABAGINA'S EXIT FROM THE TRIAL

At the hearing on March 5, following discussion of the prison visit, Mr. Rusesabagina again raised the issue of his transfer to Rwanda.[37] Defense counsel noted that the defense had submitted written pleadings but that it had not received the prosecution's response.[38] The prosecution stated that it was ready to make oral arguments and also wished to present a witness who could speak to the circumstances of Mr. Rusesabagina's arrest.[39] Over defense objections, the court ruled that oral arguments were sufficient and that the witness could make a statement.[40]

According to the court, the Bishop "w[ould] not testify as a witness under oath … [but would] only come as a witness to give information as to how Paul came to Rwanda, because he is the only one who has the full information."[41] The defence responded: "if he is not under oath, he will not be truthful."[42] The court restated that the Bishop would "speak as an informant, not as a witness," and the prosecution added "this is just information – we can come to his sworn testimony later."[43] As discussed below, there was

[36] High Court Chamber for International Crimes, Conclusions of the Visit to Mageragere Prison Following the Problems Raised by Paul Rusesabagina, March 1, 2021.
[37] Trial Monitor's Notes, March 5, 2021.
[38] Id.
[39] Id.
[40] Id.
[41] Id.
[42] Id.
[43] Id.

no such occasion as the court's response to the Bishop's statement (as well as other issues) provoked Mr. Rusesabagina to withdraw from the proceedings.

The Bishop stated that he had met Mr. Rusesabagina in 2017, at which point Mr. Rusesabagina told him that he led the FLN and asked the Bishop to introduce him to leaders in Burundi.[44] The Bishop claimed that as a "man of God" he despised the killing of women and children, which he alleged Mr. Rusesabagina had orchestrated as part of a plan to wage war on the Kagame government.[45] According to the Bishop, he "manipulated" Mr. Rusesabagina to persuade him that they were flying to Burundi and not Kigali, working with a member of Rwandan intelligence who arranged and paid for the charter flight.[46] The defense was not permitted to question the Bishop, as the court proceeded immediately to arguments on the merits of a so-called "luring" operation.

The prosecution argued that such an operation complied with international law.[47] The defense responded that bypassing extradition frameworks and luring Mr. Rusesabagina to a country to which he would never have returned voluntarily violated international law.[48] The court adjourned the trial to March 10 for a ruling on this issue.[49]

On March 10, the court ruled that Mr. Rusesabagina's transfer to Rwanda was legal and that the proceedings could continue, relying on the fact that Mr. Rusesabagina was allegedly tricked into boarding the plane, not brought to Rwanda by force.[50] At the subsequent hearing on March 11, Mr. Rusesabagina's lawyer was absent. Mr. Rusesabagina stated that his lawyer had chosen not to attend the hearing because the defense was appealing the March 10 ruling.[51] The court noted that an appeal could not justify counsel's absence and adjourned the trial to March 12, ordering all defense lawyers to appear in court.[52]

On March 12, Mr. Rusesabagina's counsel requested that the trial be put on hold for six months to allow his client time and facilities to prepare a defense.[53] Among other things, counsel referenced the court's March 9 ruling that Mr. Rusesabagina lacked the means to prepare his defense and order that seized case materials be returned to him, and also stated that private exchanges between counsel and Mr. Rusesabagina had been confiscated.[54] In response, the court noted that the case was initiated in November 2020

[44] Id.
[45] Id.
[46] Id.
[47] Id.
[48] Id.
[49] Id.
[50] See Associated Press, "Court: 'Hotel Rwanda' hero wasn't kidnapped, faces trial", March 10, 2021. Available at https://news.yahoo.com/court-hotel-rwanda-hero-wasnt-161200516.html.
[51] Trial Monitor's Notes, March 11, 2021.
[52] Id.
[53] Trial Monitor's Notes, March 12, 2021.
[54] Id.

and that "therefore the study of the file does not begin today"; that the other defendants named as accused in November 2020 had been able to adequately prepare for trial; and that in any event, Mr. Rusesabagina's lawyer "ha[d] access to the file."[55] Counsel for several other defendants and civil parties asserted that a delay of six months would be excessive, requesting that the trial begin.[56]

Over defense objections, the court ruled against granting a postponement. In support of this ruling, the court stated that Mr. Rusesabagina had access to certain parts of the file, that the court's decision on the prison visit should have been sufficient to allow him to prepare his case (the ruling was made only several days prior and Mr. Rusesabagina had yet to obtain a computer or all of the seized documents), that the court had to consider other defendants' right to a trial without undue delay, and that Mr. Rusesabagina could study the case file and prepare as the trial was ongoing, with Mr. Rusesabagina pleading last.[57]

Subsequently, the court resumed the trial and started to recount the evidence against one of Mr. Rusesabagina's co-accused, Sankara, including statements Sankara had made about Mr. Rusesabagina's role in founding and funding the National Liberation Front (FLN – an armed rebel group).[58] Mr. Rusesabagina interrupted, requesting the floor, and informed the court that he would no longer participate in the proceedings in light of what he alleged were violations of his right to defense.[59] The presiding judge returned to the charges and evidence against Sankara.[60]

E. HEARINGS AFTER MR. RUSESABAGINA'S EXIT

At the next hearing on March 24, neither Mr. Rusesabagina nor his lawyer showed up to court. The judge read a report from the prison director stating:

> we are notifying you that Paul is declining to come to court of his own will. He told the jail he will never again appear before the court. He will not show up to the court again because he expects no justice from this court.[61]

The court ruled that it was in Mr. Rusesabagina's discretion not to attend court and that the trial could proceed.[62]

[55] Id.
[56] Id.
[57] Id.
[58] Id.
[59] Id.
[60] Id.
[61] Trial Monitor's Notes, March 24, 2021.
[62] Id.

The remainder of the hearing consisted of the prosecution's questioning of its first witness, Michelle Martin, who previously served as a volunteer with the Hotel Rwanda Rusesabagina Foundation. Having gained access to the email account of one of Mr. Rusesabagina's associates, Providence Rubingisa, Ms. Martin copied and kept over 700 emails and downloaded over 1000 attachments.[63] Among other things, Ms. Martin testified about various email exchanges (stretching as far back as 2007) between Mr. Rubingisa and other individuals that allegedly entailed the discussion of plans to recruit and fund fighters.[64] Per Ms. Martin's testimony, some of these emails referenced Mr. Rusesabagina's direct involvement in such activities while others included Mr. Rusesabagina on cc.[65]

On March 25, Mr. Rusesabagina and defense counsel were again not in attendance. The prosecution questioned its second witness, Noel Habiyaremye, who testified that in 2008 Mr. Rusesabagina told him he was trying to create an armed wing of his political party, PDR-Ihumure, and asked him to help recruit fighters.[66] Mr. Habiyaremye further testified that Mr. Rusesabagina sent him money for this purpose on several occasions.[67] Notably, the prosecution characterized Ms. Martin and Mr. Habiyaremye as "context" witnesses providing background on the formation and progression of the armed movement against the Kagame government.[68] While the court asked both witnesses various questions, it never probed the credibility of Ms. Martin or Mr. Habiyaremye. such as by asking them about their potential motivations for testifying against Mr. Rusesabagina.

On March 31, Mr. Rusesabagina and defense counsel were not in attendance. The prosecution stated that it would explain the charges against each defendant and lay out the evidence supporting such charges, beginning with Herman Nsengimana and proceeding onward to Mr. Rusesabagina.[69] With respect to Mr. Rusesabagina, the prosecution went through the charges of forming an illegal armed group, being a member of an illegal armed group, and aiding terrorism.[70] On April 1, the prosecution continued reading out the charges and evidence against Mr. Rusesabagina, concluding its discussion of Mr. Rusesabagina's alleged actions in aiding terrorism and moving on to the charges of murder as an act of terrorism, abduction as a terrorist act, and armed robbery as a terrorist act.[71]

[63] Id.
[64] Id.
[65] Id.
[66] Trial Monitor's Notes, March 25, 2021.
[67] Id.
[68] Id; Trial Monitor's Notes, March 24, 2021.
[69] Trial Monitor's Notes, March 31, 2021.
[70] Id.
[71] Trial Monitor's Notes, April 1, 2021.

On April 21, Mr. Rusesabagina and defense counsel were again not in attendance. The clerk read aloud a report from the prison stating: “Paul Rusesabagina has made it known that he will not appear and that every time his case is called, he will not appear [because] he does not expect a fair trial.”[72] The prosecution proceeded to review the evidence for the remaining three charges against Mr. Rusesabagina; arson as a terrorist act, murder as a terrorist act (a second count), and assault and battery as a terrorist act.[73] The prosecution then moved on to its presentation of the cases against other defendants.[74]

On April 22 and April 28, Mr. Rusesabagina and defense counsel were again not in attendance. The prosecution continued with its recounting of the charges and evidence against Mr. Rusesabagina’s co-accused.[75] On April 29, co-accused Herman Nsengimana was questioned by the court and presented his defense.[76] When asked about his knowledge of Mr. Rusesabagina, Mr. Nsengimana stated that he had never had any dealings with him and knew of him only as a political leader.[77] Subsequently, co-accused Marc Nizeyimana was questioned by the court and presented his defense.[78] On May 6, Mr. Nizeyimana finished presenting his defense, followed by defense presentations from an additional two co-accused.[79] On May 7, another six co-accused presented their defenses.[80] On May 14, four co-accused presented their defenses.[81] At the final hearings in May – on May 19, 20, and 21 – the remaining defendants presented their cases.

On June 16, civil parties presented testimony and arguments. After the civil party presentation concluded, the prosecution commenced its closing arguments.

F. SUBMISSION TO UN SPECIAL PROCEDURES

On May 18, 2021, Mr. Rusesabagina’s international defense team submitted an urgent appeal to the UN Special Rapporteur on Torture[82] as well as a request for urgent action to the UN Working Group on Arbitrary Detention – both communications (henceforth referred to as “the UN appeals”) contained substantially the same information.[83] The UN appeals disclosed new allegations concerning the authorities’ treatment of Mr.

[72] Trial Monitor’s Notes, April 21, 2021.
[73] Id.
[74] Id.
[75] Trial Monitor’s Notes, April 22, 2021; Trial Monitor’s Notes, April 28, 2021.
[76] Trial Monitor’s Notes, April 29, 2021.
[77] Id.
[78] Id.
[79] Trial Monitor’s Notes, May 6, 2021.
[80] Trial Monitor’s Notes, May 7, 2021.
[81] Trial Monitor’s Notes, May 14, 2021.
[82] Communication to the UN Special Rapporteur on Torture, Urgent Appeal on behalf of Paul Rusesabagina, May 18, 2021.
[83] Communication to the UN Working Group on Arbitrary Detention, Request for Urgent Action on behalf of Paul Rusesabagina, May 18, 2021.

Rusesabagina in the period immediately following his arrest: namely, between August 27 and 31, when he was held in incommunicado detention.[84] Mr. Rusesabagina reportedly relayed this information to his lawyer during prison visits.[85] Among other things, he stated that he was kept in solitary confinement in a place akin to a "'slaughterhouse,'" where he "'could hear persons, women screaming, shouting, [and] calling for help.'"[86] During this time he was blindfolded, his hands and feet were bound, a gag was put on his mouth, and he was "deprived of food and at times deprived of sleep."[87] According to the UN appeals, at one point an agent from the Rwanda Investigation Bureau stepped on Mr. Rusesabagina's neck with "military boots" and stated "'we know how to torture you.'"[88] Mr. Rusesabagina further noted that the Prosecutor General of Rwanda and the Secretary General of the Rwanda Investigation Bureau visited him in detention and attempted to pressure him into making statements: "[t]hey told Mr. Rusesabagina that 'what we need from you is you to acknowledge that the President of Zambia gave you money for the FLN [National Liberation Front]. Other things are the matter of time, if you acknowledge that, we are going to release you.'"[89]

In addition to the above claims, the UN appeals contain new allegations regarding violations of confidential communications between Mr. Rusesabagina and counsel. The UN appeals report that since April 23 Mr. Rusesabagina's lawyers have been "subjected to searches of their possessions and persons" before prison visits and that they have been "prohibited from taking any documents, computers, or electronic devices into their meetings with Mr. Rusesabagina without first submitting them for inspection and review to the Prison Director of Nyarugenge Central Prison."[90] According to the UN appeals, when Mr. Rusesabagina's lawyers attempted to visit the prison on April 29, prison authorities confiscated certain documents, including documents marked privileged and confidential.[91]

On June 4, Mr. Rusesabagina's international defense team filed an update to the Working Group. The update stated that the prison authorities had stopped providing Mr. Rusesabagina with food, water, or medication and that phone calls from family members had been "discontinued."[92] According to defense counsel, the update was based on a short phone call between Mr. Rusesabagina and his family that took place on June 4. During the call, Mr. Rusesabagina reportedly stated that he was informed by

[84] Id.
[85] Id.
[86] Id.
[87] Id.
[88] Id.
[89] Id.
[90] Id.
[91] Id.
[92] Communication to the UN Working Group on Arbitrary Detention, Update to the UN Working Group on Arbitrary Detention, June 4, 2021.

prison officials that the aforementioned measures would soon be implemented and that he believed they were an attempt to coerce him into returning to the trial.

The Rwandan government has denied these claims, stating that the only change to Mr. Rusesabagina's previous conditions is that he is now given the same meals and water as other detainees, not "special meals."[93] Mr. Rusesabagina's counsel has since confirmed that Mr. Rusesabagina is receiving food but that his treatment has shifted as described above. In particular, counsel raised concerns that the standard one meal of corn and beans and one serving of water a day (Mr. Rusesabagina was prescribed three bottles of water a day by his Rwandan doctors) was insufficient in light of Mr. Rusesabagina's health condition and again noted the possibility that the change was intended to pressure Mr. Rusesabagina to resume participation in the trial.

G. COOPERATION BETWEEN THE BELGIAN AND RWANDAN AUTHORITIES

Throughout the hearings, the prosecution has continuously referenced Belgian cooperation in Mr. Rusesabagina's case. As stated by the prosecution, the present case against Mr. Rusesabagina commenced in 2018 and, upon the Rwandan authorities' request, the Belgian authorities started providing assistance shortly thereafter.[94] According to the prosecution, Belgian officials sent case materials to Rwanda at various points, including in May 2020[95] and December 2020 – after Mr. Rusesabagina's arrest.[96] Notably, the prosecution has referenced close cooperation with the Belgian authorities on investigations into Mr. Rusesabagina's activities since at least 2011.[97] This includes an extradition request in 2012 that was refused by Belgium, which has propelled the defense claim that Mr. Rusesabagina's transfer to Rwanda was an unlawful plot to circumvent the legal bar on Belgium handing him over (the prosecution has stated that the extradition request was for a different case, not the present one).

Thus far, evidence flagged by the prosecution as stemming from the Belgian investigation has included numerous WhatsApp chats from Mr. Rusesabagina's phone – which was seized by the Belgian police – in which Mr. Rusesabagina allegedly

[93] The New Times, "Rights Watchdog Clears Air Over Rusesabagina", June 11, 2021. Available at https://www.newtimes.co.rw/news/rights-watchdog-clears-air-over-rusesabagina.

[94] Trial Monitor's Notes, February 17, 2021. The indictment states that the Rwandan authorities asked the Belgian authorities for assistance with the investigation in May 2019. Documents of Complaint, Republic of Rwanda National Prosecuting Authority, November 16, 2020, para. 101.

[95] Trial Monitor's Notes, March 25, 2021; Documents of Complaint, Republic of Rwanda National Prosecuting Authority, November 16, 2020, para. 105.

[96] Trial Monitor's Notes, February 17, 2021; Trial Monitor's Notes, April 1, 2021.

[97] Documents of Complaint, Republic of Rwanda National Prosecuting Authority, November 16, 2020, paras. 70-71.

discussed FLN activities with various individuals;[98] documentation regarding alleged wire transfers from individuals involved with the Rwandan Movement for Democratic Change (MRCD – an opposition party co-founded by Mr. Rusesabagina) to individuals involved with the FLN;[99] various documents recovered from Mr. Rusesabagina's computer – seized by the Belgian police – such as an MRCD plan of action and an MRCD press release allegedly authored by Mr. Rusesabagina;[100]and statements from interviews conducted by the Belgian police with individuals such as Mr. Rusesabagina and the wife of the treasurer of the MRCD.[101]

According to a spokesperson for the Belgian Federal Prosecutor's Office, the investigation in Belgium is ongoing.[102] At a hearing on April 1, the Rwandan prosecution likewise noted that the Belgian investigation was ongoing and stated, "[i]f and when we find more evidence, we'll share it with the court", indicating that there might be further cooperation between Belgium and Rwanda on Mr. Rusesabagina's case. While the Rwandan prosecution has yet to clearly specify which branch of the Belgian government purportedly sent case file materials to Rwanda in December 2020,[103] the aforementioned spokesperson for the Belgian Federal Prosecutor's Office noted that the Office had not been in "contact with Rwandan authorities since Rusesabagina appeared in Kigali."[104]

[98] See Trial Monitor's Notes, March 31, 2021; Trial Monitor's Notes, April 1, 2021; Documents of Complaint, Republic of Rwanda National Prosecuting Authority, November 16, 2020, para. 103.
[99] See Trial Monitor's Notes, March 31, 2021; Trial Monitor's Notes, April 1, 2021; Documents of Complaint, Republic of Rwanda National Prosecuting Authority, November 16, 2020, para. 104.
[100] See Trial Monitor's Notes, March 31, 2021; Trial Monitor's Notes, April 1, 2021; Documents of Complaint, Republic of Rwanda National Prosecuting Authority, November 16, 2020, para. 103.
[101] See Trial Monitor's Notes, March 31, 2021; Documents of Complaint, Republic of Rwanda National Prosecuting Authority, November 16, 2020, para. 102.
[102] ABC News, "Paul Rusesabagina Was Called a Hero After 'Hotel Rwanda,' Now He's Accused of Terrorism", April 25, 2021. Available at https://abcnews.go.com/International/paul-rusesabagina-called-hero-hotel-rwanda-now-accused/story?id=76953569.
[103] The Rwandan prosecution has referred to the participation of the prosecution, a judge, and the Belgian embassy.
[104] ABC News, "Paul Rusesabagina Was Called a Hero After 'Hotel Rwanda,' Now He's Accused of Terrorism", April 25, 2021.

ANALYSIS

A. APPLICABLE LAW

This report draws upon the International Covenant on Civil and Political Rights (the "ICCPR"); jurisprudence from the United Nations Human Rights Committee, tasked with monitoring implementation of the ICCPR; the African Charter on Human and Peoples' Rights (the "African Charter"); jurisprudence from the African Commission on Human and Peoples' Rights (the "African Commission"), tasked with interpreting the Charter and considering individual complaints of Charter violations; jurisprudence from the African Court on Human and Peoples' Rights (the "African Court"), which – complementing the African Commission's work – is tasked with interpreting and applying the African Charter; and the African Commission's Principles and Guidelines on the Right to a Fair Trial and Legal Assistance in Africa (the "Fair Trial Guidelines").

The African Court has jurisdiction over "all cases and disputes submitted to it in respect of the interpretation and application of the African Charter on Human and Peoples' Rights (the Charter), the Protocol [on the Court's establishment] and any other relevant human rights instrument ratified by the States concerned."[105] Rwanda ratified the African Charter in 1983[106] and the Protocol in 2003.[107] Notably, the African Court has frequently relied on jurisprudence from both the European Court of Human Rights and the Inter-American Court of Human Rights, stating that the two bodies have analogous jurisdiction and are guided by instruments similar to the African Charter.[108] The Court has also stated that where the ICCPR provides for broader rights than those of the Charter, it can apply the ICCPR if the country under consideration has already acceded to or ratified it.[109] Rwanda acceded to the ICCPR in 1975.[110]

[105] African Court on Human and People's Rights, "Welcome to the African Court". Available at https://www.african-court.org/wpafc/welcome-to-the-african-court.

[106] African Union, "List of Countries which have signed, ratified/acceded to the African Charter on Human and Peoples' Rights". Available at https://au.int/sites/default/files/treaties/36390-sl-african_charter_on_human_and_peoples_rights_2.pdf.

[107] African Union, "List of Countries which have signed, ratified/acceded to the Protocol of the African Charter on Human and Peoples' Rights on the Establishment of an African Court on Human and Peoples' Rights". Available at https://au.int/sites/default/files/treaties/36393-sl-protocol_to_the_african_charter_on_human_and_peoplesrights_on_the_estab.pdf.

[108] See Jamil Ddamulira Mujuzi, "The African Court on Human and Peoples' Rights and Its Protection of the Right to a Fair Trial", The Law and Practice of International Courts and Tribunals, December 5, 2017, pg. 193. Available at https://brill.com/abstract/journals/lape/16/2/article-p187_187.xml.

[109] African Court on Human and Peoples' Rights, Alex Thomas v. Tanzania, App. No. 005/2013, November 20, 2015, para. 88; African Court on Human and Peoples' Rights, Wilfred Onyango Nganyi et al v. Tanzania, App. No. 006/2013, March 18, 2016, para. 165.

[110] United Nations Treaty Collection, "ICCPR Status as of May 5, 2021". Available at https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&clang=_en.

Additionally, the report draws on general principles concerning state responsibility for the conduct of third parties, which are summarized in the International Law Commission (ILC) Draft Articles on State Responsibility.

B. MR. RUSESABAGINA'S WITHDRAWAL FROM THE PROCEEDINGS: RIGHT TO BE PRESENT AT TRIAL AND RIGHT TO A DEFENSE

While it is within Mr. Rusesabagina's discretion to refrain from participating in the proceedings, it is more important than ever that the court protect his fair trial rights. The court's conduct since Mr. Rusesabagina's exit, however, indicates that it is more inclined to assist the prosecution in making its case against Mr. Rusesabagina than to safeguard Mr. Rusesabagina's rights.

International and Regional Standards

Article 14(3)(d) of the ICCPR provides for an accused's right to "be tried in his presence, and to defend himself in person or through legal assistance of his own choosing." Article 7 of the African Charter contains similar guarantees. These inter-related rights are waivable subject to stringent safeguards.

The African Commission, for example, has stated that "[t]he accused may voluntarily waive the right to appear at a hearing, but such a waiver shall be established in an unequivocal manner and preferably in writing."[111] The United Nations Human Rights Committee has likewise noted that proceedings "in the absence of the accused may in some circumstances be permissible."[112] According to the Committee, in order for such proceedings to comply with fair trial guarantees, the accused must be notified of the proceedings in a timely manner and decline to exercise his or right to be present:[113] "requirements of due process enshrined in article 14 cannot be construed as invariably rendering proceedings *in absentia* inadmissible irrespective of the reasons for the accused person's absence."[114]

The Committee has considered cases where the accused has declined to exercise both his or her right to be present and his or her right to a defense. In *Benhadj v. Algeria*, the accused was prosecuted before a military tribunal for, among other things, "crimes

[111] African Commission on Human and Peoples' Rights, Principles and Guidelines on the Right to a Fair Trial and Legal Assistance in Africa, 2003, Principle N(6)(c)(iii).
[112] Human Rights Committee, General Comment No. 32, U.N. Doc. CCPR/C/GC/32, August 23, 2017, para. 36.
[113] Id.
[114] Human Rights Committee, Mbenge v. Zaire, U.N. Doc. CCPR/C/18/D/16/1977, March 25, 1983, para. 14.1.

against state security."[115] He disputed the legitimacy of the court and the case against him, deeming it politically motivated.[116] Although he was notified sufficiently in advance of the proceedings, neither he nor his lawyer showed up to trial.[117] He was subsequently convicted. The Committee did not find a violation of Article 14(3)(d), citing the fact that the defendant "refused to attend" the proceedings.[118] This jurisprudence is consistent with that of the European Court of Human Rights, which has ruled that "[n]either the letter nor the spirit of Article 6 of the Convention prevents a person from waiving of his own free will, either expressly or tacitly, the entitlement to the guarantees of a fair trial."[119]

In contrast, some international criminal tribunals have assigned counsel to represent an accused person against his or her wishes where the accused has declined to attend hearings. In *Ferdinand Nahimana, Jean-Bosco Barayagwiza, and Hassan Ngeze v. The Prosecutor*, for example, an Appeals Chamber at the International Criminal Tribunal for Rwanda considered a case in which one of the accused, Mr. Barayagwiza, had proclaimed that he did not believe that the tribunal would afford him a fair trial and therefore would not participate.[120] He stopped attending hearings and ultimately terminated counsel's mandate.[121] The Trial Chamber assigned new counsel.[122] This ruling was subsequently upheld by the Appeals Chamber, which asserted that it was within the Trial Chamber's discretion to appoint counsel in the interests of justice as well as the interests of the accused, notwithstanding whether this contravened the accused's own wishes.[123]

In other cases, courts have chosen to appoint amicus counsel – an independent lawyer to probe the testimony of witnesses hostile to the defendant. For the trial of Slobodan Milosevic before the International Criminal Tribunal for the former Yugoslavia, for example, a team of international lawyers was appointed as amicus curiae not to represent Mr. Milosevic but to "assist in the proper determination of the case," including by "cross-examining witnesses as appropriate" and "acting in any other way which designated counsel considers appropriate in order to secure a fair trial."[124]

[115] Human Rights Committee, Benhadj v. Algeria, U.N. Doc. CCPR/C/90/D/1173/2003, July 20, 2007, para. 2.2.
[116] Id.
[117] Id. at para. 8.9.
[118] Id.
[119] European Court of Human Rights, Sejdovic v. Italy, App. No. 46221/99, May 12, 2005, para. 86.
[120] International Criminal Tribunal for Rwanda, Ferdinand Nahimana, Jean-Bosco Barayagwiza, Hassan Ngeze v. The Prosecutor, Case No. ICTR-99-52-A, Appeals Chamber Judgment, November 28, 2007, paras. 112–14.
[121] Id.at paras. 112-113, 120.
[122] Id. at para. 122.
[123] Id. at paras. 127–28.
[124] International Criminal Tribunal for the Former Yugoslavia, "Milosevic Case: The Registrar Appoints a Team of Experienced International Lawyers as Amicus Curiae to Assist the Trial Chamber", September 6, 2001. Available at https://www.icty.org/en/press/milosevic-case-registrar-appoints-team-experienced-international-lawyers-amicus-curiae-assist.

The Case Against Mr. Rusesabagina

In light of the above, it does not appear necessarily inconsistent with international and regional jurisprudence that the court has proceeded despite Mr. Rusesabagina's complete withdrawal from the proceedings.

However, whether an accused is permitted to withdraw entirely or is assigned counsel in his or her absence, it is incumbent on the court to ensure that fair trial guarantees are respected. The UN Human Rights Committee, for example, has stated that "when exceptionally for justified reasons trials *in absentia* are held, strict observance of the rights of the defence is all the more necessary."[125] The International Criminal Tribunal for the former Yugoslavia has likewise noted that where *in absentia* proceedings are conducted, "the fundamental rights pertaining to a fair trial would need to be safeguarded."[126]

In the present case, the judges have not "safeguarded" Mr. Rusesabagina's fair trial rights since his exit. With respect to prosecution witnesses Michelle Martin and Noel Habiyaremye, for example, the judges did not ask any questions about potential motivations for their testimony, such as financial incentives or connections with the Rwandan government, and did not otherwise attempt to test their credibility. Notably, Ms. Martin, as she acknowledged in her testimony, was previously employed by the Rwandan government[127] and Mr. Habiyaremye had previously provided testimony against government opponents.[128] The court's failure to probe their credibility or to appoint an amicus to do so was an indication of its reluctance to allow any action which might challenge the government's case.

Instead, the court undertook inquiries seemingly geared towards establishing Mr. Rusesabagina's guilt. The court posed questions to Ms. Martin, for example, such as whether Mr. Rusesabagina spoke to her about the FDLR (an armed rebel group) during their interactions, whether she had in her possession particular emails about Mr. Rusesabagina, and what she had heard about weapons exchanges with respect to Mr. Rusesabagina.[129]

This pattern continued throughout the proceedings. On April 29, co-accused Herman Nsengimana was testifying about his role in the FLN. Suddenly, a judge asked:

[125] Human Rights Committee, General Comment No. 13, April 13, 1984, para. 11.

[126] International Criminal Tribunal for the former Yugoslavia, Prosecutor v. Tihomir Blaskic, Case No. IT-95-14, Appeals Chamber Judgment, October 29, 1997, para. 59.

[127] Trial Monitor's Notes, March 24, 2021.

[128] Reuters, "Rwanda Rebels Admit Presidential Hopeful Link: Prosecutor", April 30, 2010. Available at https://www.reuters.com/article/us-rwanda-rebels/rwanda-rebels-admit-presidential-hopeful-link-prosecutor-idUSTRE63T3RG20100430. See also Human Rights Watch, "'We Will Force You to Confess': Torture and Unlawful Military Detention in Rwanda", 2017, pgs. 25-26. Available at https://www.hrw.org/sites/default/files/report_pdf/rwanda1017_web_0.pdf.

[129] Trial Monitor's Notes, March 24, 2021.

> Herman, in explaining, you said how you worked with Sankara from the beginning until you joined the army, but in your pleading there is nowhere where you talk about Rusesabagina, but as a president of the MRCD-FLN, *you should say something about him*, if you would have worked with him, if there would be any help which he brought to you in the function which you occupied (emphasis added).

This question was apparently designed to extract information inculpating Mr. Rusesabagina.[130] Mr. Nsengimana subsequently responded that he had never spoken to Mr. Rusesabagina and knew him only as a political leader.[131] Similarly, at a hearing on May 14, the judges repeatedly asked co-accused Marcel Niyirora whether Mr. Rusesabagina's party "had soldiers" and whether Mr. Rusesabagina provided help to soldiers and asked co-accused Emmanuel Nshimiyimana, who at the time was speaking on a different topic, "[d]uring your hearing, there is where you said that you heard that it was Rusesabagina who gave funding, that even one day he sent money for the military party. How did you get to know about this?"[132]

These actions were consistent with the court's conduct even prior to Mr. Rusesabagina's departure, such as allowing the Bishop to testify not under oath and without cross-examination by the defense about Mr. Rusesabagina's transfer to Rwanda. This contravened Article 14(3)(e) of the ICCPR and Article 7(c) of the African Charter,[133] which entitle defendants facing criminal charges to examine or have examined the witnesses against them. The court's refusal to follow this rule and to permit the Bishop to give evidence for the state without fear of contradiction raises serious concerns about its integrity.

Given the above, the judges have acted in a manner that suggests they are more invested in building the prosecution's case against Mr. Rusesabagina than endeavoring to protect his rights in his absence, as is their obligation. This contravenes the UN Human Rights Committee's directive that "when exceptionally for justified reasons trials *in absentia* are held, strict observance of the rights of the defence is all the more necessary."[134]

The severe violations of Mr. Rusesabagina's right to adequate facilities, right to communication with counsel, and right to presumption of innocence, described below, further call into question the fairness of the trial.

[130] Trial Monitor's Notes, April 29, 2021.

[131] Id.

[132] Trial Monitor's Notes, May 14, 2021.

[133] See also African Commission on Human and Peoples' Rights, Principles and Guidelines on the Right to a Fair Trial and Legal Assistance in Africa, 2003, Principle N(6)(f).

[134] Human Rights Committee, General Comment No. 13, April 13, 1984, para. 11.

C. RIGHT TO ADEQUATE FACILITIES TO PREPARE A DEFENSE

International and Regional Standards

Under Article 14(3)(b) of the ICCPR and Article 7 of the African Charter, accused persons are entitled to adequate time and facilities for the preparation of their defense. The proceedings against Mr. Rusesabagina to date disclose a violation of this guarantee.

As stated by the United Nations Human Rights Committee, "[w]hat counts as 'adequate time' depends on the circumstances of each case."[135] The African Commission has similarly noted that the issue of adequate time should be considered on a case-by-case basis, with reference to the "complexity of the case, the defendant's access to evidence, the length of time provided by rules of procedure prior to particular proceedings, and prejudice to the defence."[136] According to the UN Human Rights Committee, there "is an obligation to grant reasonable requests for adjournment, in particular, when the accused is charged with a serious criminal offence and additional time for preparation of the defence is needed."[137] Notably, the right to adequate time does not end with the commencement of trial: "since the course of trials cannot be fully charted in advance and may reveal elements which have not hitherto come to light and which require further preparation by the parties," trials generally necessitate preparation throughout the proceedings.[138]

The right to adequate time and right to adequate facilities are interconnected: where an accused does not have adequate facilities, he or she may require additional time both to obtain the required resources and to use said resources. The UN Human Rights Committee has stated that adequate facilities "must include access to documents and other evidence … that the prosecution plans to offer in court against the accused."[139] The African Commission has further noted that an accused person is entitled to "consult legal materials reasonably necessary for the preparation of his or her defence."[140]

[135] Human Rights Committee, General Comment No. 32, U.N. Doc. CCPR/C/GC/32, August 23, 2017, para. 32.

[136] African Commission on Human and Peoples' Rights, Principles and Guidelines on the Right to a Fair Trial and Legal Assistance in Africa, 2003, Principle N(3)(c).

[137] Human Rights Committee, General Comment No. 32, U.N. Doc. CCPR/C/GC/32, August 23, 2017, para. 32.

[138] European Court of Human Rights, Mattick v. Germany, App. No. 62116/00, March 31, 2005, Inadmissibility Decision.

[139] Human Rights Committee, General Comment No. 32, U.N. Doc. CCPR/C/GC/32, August 23, 2017, para. 33.

[140] African Commission on Human and Peoples' Rights, Principles and Guidelines on the Right to a Fair Trial and Legal Assistance in Africa, 2003, Principle N(3)(e)(v).

In terms of requirements regarding the accused's ability to examine evidence in the case file, European Court of Human Rights jurisprudence is instructive. In *Ocalan v. Turkey*, the Court ruled that the accused's right to adequate facilities had been violated where he was unable to gain access to a voluminous case file until after the proceedings had started and thereby was unable to be "involve[d] … in its examination or analysis."[141] As stated by the Court, "limitations on access by an accused or his lawyer to the court file must not prevent the evidence being made available to the accused before the trial and the accused being given an opportunity to comment on it through his lawyer in oral submissions."[142] The Court has highlighted the importance of a defendant's ability to instruct lawyers as to strategy and arguments based on inspection of the evidence: "the defence of the accused's interests may best be served by the contribution which the accused makes to his lawyer's conduct of the case before the accused is called to give evidence."[143]

The Case Against Mr. Rusesabagina

In the present case, prior to his decision not to participate in the trial, Mr. Rusesabagina did not have the opportunity to thoroughly inspect the case file, which reportedly encompasses more than 3,000 pages. The prison authorities routinely seized and read documents relayed by defense counsel to Mr. Rusesabagina and often did not return such materials to him. Further, Mr. Rusesabagina did not have access to paper or a pen with which to take notes, let alone a computer with which to efficiently examine case documents.

These facts have been corroborated by defense counsel; by Minister of Justice Busingye Johnston in the public relations preparation video accidentally sent to Al Jazeera, in which he admitted that prison authorities had been confiscating documents relayed to Mr. Rusesabagina; and by the court's oral pronouncement at the hearing on March 5 and written ruling on March 9, in which the court stated that Mr. Rusesabagina had been denied adequate facilities to prepare for trial and that certain case documents had been confiscated.

[141] European Court of Human Rights, Öcalan v. Turkey, App. No. 46221/99, May 12, 2005, paras. 147-148.
[142] Id. at para. 140.
[143] European Court of Human Rights, Moiseyev v. Russia, App. No. 62936/00, September 10, 2008, para. 214. See also European Court of Human Rights, Huseyn and others v. Azerbaijan, App. Nos. 35485/05, 45553/05, 35680/05 and 36085/05, July 26, 2011, para. 175 ("The accused must have the opportunity to organise his defence in an appropriate way and without restriction as to the possibility of putting all relevant defence arguments before the trial court and thus of influencing the outcome of the proceedings … The facilities which everyone charged with a criminal offence should enjoy include the opportunity to acquaint himself for the purposes of preparing his defence with the results of investigations carried out throughout the proceedings."); European Court of Human Rights, Gregacevic v. Croatia, App. No. 58331/09, July 10, 2012, para. 51. See Human Rights Committee, Esergepov v. Kazakhstan, U.N. Doc. CCPR/C/116/D/2129/2012, March 29, 2016, para. 11.4.

As detailed by the United Nations Human Rights Committee and African Commission, factors relevant to an assessment of the adequacy of time include whether the charges are severe and the case complex: the present case involves 21 defendants and an array of charges. If Mr. Rusesabagina is convicted, it is possible that he will spend the rest of his life in prison.

Taking these facts into account and in line with the UN Human Rights Committee's jurisprudence, the court was obligated to grant reasonable requests for adjournment (not necessarily the six months requested by defense counsel) so as to allow Mr. Rusesabagina adequate time and use of the recently ordered facilities to prepare his case. On March 12, however, the court rejected defense requests for an adjournment and ordered that the trial proceed immediately. At this point, Mr. Rusesabagina had yet to obtain access to the documents seized or to a computer. Even if all of these violations had been remedied, three days would not have been sufficient for him to review the voluminous case file.

Notably, the court stated that the trial could continue because Mr. Rusesabagina's lawyers had access to the documents and because the case against Mr. Rusesabagina could be reviewed last, after the cases against his 20 co-accused, meaning that Mr. Rusesabagina could prepare as the trial was in progress. The allegations against Mr. Rusesabagina's co-accused, however, are inextricably intertwined with the allegations against him. On March 12, for example, the court reviewed statements made by his co-accused Sankara about Mr. Rusesabagina's role in founding the FLN. On March 24 and 25, prosecution witnesses discussed numerous WhatsApp conversations, emails, and money transactions that allegedly inculpated Mr. Rusesabagina (ostensibly as "context" witnesses on the development of the armed movement against the Kagame government). These exchanges involved multiple parties and stretched back 15 years: only Mr. Rusesabagina himself was positioned to guide his lawyers regarding how to engage this evidence.

In light of the above, Mr. Rusesabagina's right to adequate time and facilities for a defense was violated.

D. RIGHT TO CONFIDENTIAL COMMUNICATIONS WITH COUNSEL

Mr. Rusesabagina's right to confidential communications with counsel has been violated. The nature of this violation raises concerns that his right to a defense has been irretrievably prejudiced. Further, this violation exacerbates the Rwandan authorities' continuing refusal to permit international counsel to assist Mr. Rusesabagina.[144]

[144] See American Bar Association Center for Human Rights, "Background Briefing on Proceedings

International and Regional Standards

In addition to the right to adequate facilities and time for preparation of a defense, Article 14(3(b) of the ICCPR protects the right to confidential communication with counsel.[145] As stated by the United Nations Human Rights Committee, "[c]ounsel should be able to meet their clients in private and to communicate with the accused in conditions that fully respect the confidentiality of their communications."[146] The Committee has thus found a violation of Article 14(3)(b) where all meetings between a detained accused and counsel were held in the presence of police.[147]

Article 7 of the African Charter likewise entitles an accused to confidential communications with his or her lawyer.[148] The African Commission has deemed the "right to confer privately with one's lawyer and exchange confidential information or instructions … a fundamental part of the preparation of a defence,"[149] stating that all persons in detention must be provided the facilities to communicate with counsel without "interception or censorship and in full confidentiality."[150] In *Egyptian Initiative for Personal Rights and Interights v. Arab Republic of Egypt*, the Commission considered a case where the accused were only able to speak to their lawyers in the courtroom in the presence of and "within earshot [of] security officials."[151] According to the Commission, this "restrictive access" to counsel violated Article 7.[152]

The UN Standard Minimum Rules for the Treatment of Prisoners (the Mandela Rules) echo the standards established by the ICCPR and African Charter. According to the Rules, "[p]risoners shall be provided with adequate opportunity, time and facilities to be visited by and to communicate and consult with a legal adviser of their own choice or a legal aid provider, without delay, interception or censorship and in full confidentiality, on any legal matter, in conformity with applicable domestic law."[153]

Against Paul Rusesabagina", January 26, 2021. Available at https://www.americanbar.org/groups/human_rights/reports/background_briefing_rwanda_paul_rusesabagina/.

[145] Human Rights Committee, General Comment No. 32, U.N. Doc. CCPR/C/GC/32, August 23, 2017, para. 34.

[146] Id.

[147] Human Rights Committee, Khomidova v. Tajikistan, U.N. Doc. CCPR/C/81/D/1117/2002, August 25, 2004, para. 6.4.

[148] African Commission on Human and Peoples' Rights, Principles and Guidelines on the Right to a Fair Trial and Legal Assistance in Africa, 2003, Principle N(3)(e)(i).

[149] Id. at Principle N(3)(e)(i).

[150] Id. at Principle N(3)(e).

[151] African Commission on Human and Peoples' Rights, Egyptian Initiative for Personal Rights and Interrights v. Arab Republic of Egypt, Communication No. 334/2006, March 2011, para. 211.

[152] Id.

[153] United Nations General Assembly, United Nations Standard Minimum Rules for the Treatment of Prisoners (Mandela Rules), U.N. Doc. A/RES/70/175, December 17, 2015, Rule 61(1).

The European Court of Human Rights has considered cases where state actors have intercepted correspondence between counsel and an accused, including case file materials and defense strategy documents. In *Moiseyev v. Russia*, for instance, authorities at the remand center where the accused was detained "routine[ly] read … all documents exchanged between the applicant and his defence team" pursuant to legislation that "provided for censorship of all correspondence by detainees in general terms, without exception for privileged correspondence, such as that with legal counsel."[154] The Court emphasized that interception of such correspondence could only be justified in exceptional circumstances, such as when "the authorities have reasonable cause to believe that the privilege is being abused, in that the contents of the letter endanger prison security or the safety of others or are otherwise of a criminal nature."[155] Given that there did not appear to be an exceptional circumstance that justified the "sweeping" review of all correspondence between the accused and his lawyer throughout the duration of the criminal proceedings, the Court found that the State had "encroached on the rights of the defence in an excessive and arbitrary fashion."[156] Notably, the remand center was operated by the "same authority" that was responsible for the accused's prosecution, meaning that the applicant was placed at "a disadvantage vis-à-vis his opponent."[157]

In evaluating cases concerning confidential communication, the Court has emphasized that "[i]f a lawyer were unable to confer with his client and receive confidential instructions from him without surveillance, his assistance would lose much of its usefulness."[158] As such, where communications between counsel and an accused have already been intercepted[159] or where communications have not in fact been intercepted but the accused has reasonable grounds to believe that confidentiality will be violated,[160] the Court has indicated that an accused's defense may be "irretrievably" compromised.[161] In *Zagaria v. Italy*, for example, a single conversation between the accused and counsel was wiretapped.[162] The State subsequently failed to discipline the official responsible for the wiretapping.[163] Consequently, the Court found that "there was

[154] European Court of Human Rights, Moiseyev v. Russia, App. No. 62396/00, October 9. 2008, paras. 210-211.
[155] Id. at para. 210. See also European Court of Human Rights, Khodorkovskiy and Lebedev v. Russia, App. nos. 11082/06 and 13772/05, July 25, 2013, para. 645.
[156] Id. at para. 211.
[157] Id.
[158] See id. at para. 209; European Court of Human Rights, S. v. Switzerland, App. Nos. 12629/87 and 13965/88, November 28, 1991, para. 48.
[159] European Court of Human Rights, Brennan v. United Kingdom, App. No. 39846/98, October 16, 2001, paras. 58-63.
[160] See European Court of Human Rights, Modarca v. Moldova, App. No. 14437/05, May 10, 2007, para. 89.
[161] European Court of Human Rights, Brennan v. United Kingdom, App. No. 39846/98, October 16, 2001, para. 62.
[162] European Court of Human Rights, Zagaria v. Italy, App. No. 58295/00, November 27, 2007, paras. 33-36.
[163] Id. at para. 35.

no guarantee to the applicant that the incident would not have been repeated. He could therefore reasonably fear that other conversations would be overheard, which may have given him grounds for hesitation before tackling questions which might be of importance to the prosecution."[164]

The Case Against Mr. Rusesabagina

In the present case, it is undisputed that materials relayed by defense counsel to Mr. Rusesabagina were confiscated and reviewed by the prison authorities. As noted in the Center's previous background briefing, defense counsel has stated that this seizure included documents from the case file as well as defense strategy memoranda. The confiscation of materials relayed by defense counsel to Mr. Rusesabagina has been corroborated by Minister of Justice Johnston Busingye in both the public relations video accidentally sent to Al Jazeera and his follow-on interview with Al Jazeera: Minister Busingye, while proclaiming that Mr. Rusesabagina's right to confidential communication with counsel had been preserved, stated that it was routine and consistent with international law for the prison authorities to review all correspondence sent to prisoners to ensure security.

The Ministry of Justice subsequently released a statement acknowledging that the Minister had learned of a potential violation of the right to confidential communication in December 2020 and had thus instructed the prison authorities to take greater care in distinguishing between privileged and non-privileged materials. But in a prison visit some three months later, the prison authorities stated that they were still examining materials relayed to Mr. Rusesabagina without exception. In oral rulings on March 5 and a written ruling on March 9, the court found that materials exchanged between Mr. Rusesabagina and his lawyer had been confiscated. According to the court:

> The other thing that has been observed and that needs to be corrected is that there are documents from his trial, as well as other documents, that have been seized, and their return to his person is taking a long time. … [D]ocuments which form part of the case file which Rusesabagina Paul exchanges with his lawyers should not be seized. As regards other documents which are not part of the trial file, as well as various other objects which are sent to him through his lawyers, they should make a list (inventory) and hand them over to him through the prison administration.

The ensuing UN appeals filed by the international defense team allege that violations have not only persisted but have worsened in the months since the court's ruling.

[164] Id.

According to the appeals, the prison authorities have searched Mr. Rusesabagina's lawyers prior to prison visits, insisting on examining all materials that the lawyers have brought for Mr. Rusesabagina and, on one instance, confiscating documents marked privileged and confidential. The most recent update to the UN appeals reports that the authorities stopped counsel from making a preapproved visit on June 4 – violating Mr. Rusesabagina's baseline right to receive legal assistance.

As a threshold matter, the facts confirmed by multiple actors in the leadup to the court's March 9 ruling reveal a violation of the right to confidential communication: as described above, the defense, the Minister of Justice, the prison authorities, and the court all stated at various points that the prison authorities have systematically confiscated and inspected materials relayed by defense counsel to Mr. Rusesabagina. Although Minister Busingye has asserted that international law permits prison authorities to review all incoming materials for security purposes, such a sweeping review contravenes the basic guarantee of Article 14(3)(b) of the ICCPR and Article 7 of the African Charter. Only for exceptional reasons may authorities intercept correspondence between an accused and defense counsel. While Minister Busingye cited an escape plan that had allegedly been discovered within the correspondence, the plan (the existence of which the defense has vigorously contested) appeared to have been discovered after interception had already commenced and, in any event, such interception had been authorized writ large, with no limiting factors or safeguards. Mr. Rusesabagina's right to confidential communication with his lawyers was thus violated.

The facts as alleged in the UN appeals filed by Mr. Rusesabagina's international defense team constitute a further violation of Mr. Rusesabagina's right to communicate with counsel.

Given the above, Mr. Rusesabagina would have reasonable grounds to believe that his right to confidential communications will continue to be compromised and that he should desist from open discussion with his lawyers about the case. Indeed, the prison authorities have yet to be subject to disciplinary measures (a key point raised by the European Court in *Zagaria v. Italy*): the Minister of Justice, which oversees both the prison system and the public prosecutor's office – responsible for the current proceedings against Mr. Rusesabagina – has defended the prison's conduct; the court has stated that the authorities may continue reviewing certain materials relayed to Mr. Rusesabagina by counsel and has not required the prison authorities to explain how they will screen for privileged materials; and prison officials have apparently disregarded the court's instruction to take greater care in distinguishing between privileged and non-privileged materials – to the contrary, subjecting lawyers visiting the prison to searches of all documents on their persons and confiscating documents marked privileged and confidential.

As such, Mr. Rusesabagina's defense has likely been "irreparably prejudiced."

E. RIGHT TO THE PRESUMPTION OF INNOCENCE

International and Regional Standards

Under Article 14(2) of the ICCPR and Article 7(1)(b) of the African Charter, individuals charged with criminal offenses are entitled to the presumption of innocence. The United Nations Human Rights Committee has stated that Article 14(2) "imposes on the prosecution the burden of proving the charge, guarantees that no guilt can be presumed until the charge has been proved beyond reasonable doubt, ensures that the accused has the benefit of doubt, and requires that persons accused of a criminal act must be treated in accordance with this principle."[165]

As specified by the Committee, the presumption can be violated where public authorities make statements pronouncing an accused's guilt.[166] The Committee, for example, has found violations where high ranking police officers publicly deemed a defendant guilty,[167] stating that the officers "failed to exercise the restraint that article 14, paragraph 2, requires," and where a documentary allegedly funded by the executive portrayed a defendant as guilty.[168] The African Commission has likewise noted of the presumption: "[p]ublic officials shall maintain a presumption of innocence. Public officials, including prosecutors, may inform the public about criminal investigations or charges, but shall not express a view as to the guilt of any suspect."[169]

The Case Against Mr. Rusesabagina

In the present case, President of Rwanda Paul Kagame has repeatedly made comments deeming Mr. Rusesabagina guilty, undermining the presumption of innocence and adding to the violations discussed above. Prior to Mr. Rusesabagina's trial, in a widely publicized interview with the press, President Kagame stated that Mr. Rusesabagina: "heads a group of terrorists that have killed Rwandans. He will have to pay for these crimes. Rusesabagina has the blood of Rwandans on his hands."[170]

[165] Human Rights Committee, General Comment 32, U.N. Doc. CCPR/C/GC/32, August 23, 2007, para. 30.
[166] Id.
[167] Human Rights Committee, Gridin v. Russian Federation, U.N. Doc. CCPR/C/69/D/770/1997, July 18, 2000, para. 8.3.
[168] Human Rights Committee, Kulov v. Kyrgyzstan, U.N. Doc. CCPR/C/99/D/1369/2005, August 19, 2010, paras. 3.7, 8.7.
[169] African Commission on Human and Peoples' Rights, Principles and Guidelines on the Right to a Fair Trial and Legal Assistance in Africa, 2003, Principle N(6)(e)(ii).
[170] Human Rights Watch, "Rwanda: Rusesabagina Was Forcibly Disappeared", September 10, 2020. [171] See ABC News, "Paul Rusesabagina Was Called a Hero After 'Hotel Rwanda': Now He's Accused of

In April 2021, after the trial was already underway, President Kagame spoke at a genocide commemoration ceremony, stating: “You heard the other day, when the person who was brought here, and the question is how he got here, and not that he led a group that was killing people here in Rwanda.”[171] The reference to “the person who was brought here” and who “led a group that was killing people here in Rwanda” is most likely a reference to Mr. Rusesabagina. In a subsequent interview with France24, President Kagame asked in response to a question about Mr. Rusesabagina’s arrest: “What’s wrong with tricking a criminal?”[172]

The repeated characterization of Mr. Rusesabagina as guilty by the country’s president constitutes a severe violation of the presumption of innocence.

F. STATE RESPONSIBILITY FOR THE CONDUCT OF THIRD PARTIES

Belgium’s facilitation of Mr. Rusesabagina’s prosecution raises significant questions that need to be answered. In particular, Belgium should explain what steps it took to ensure that assistance provided to Rwanda was not used to support a prosecution that violated Mr. Rusesabagina’s fair trial rights and whether the scope or nature of its assistance has changed over time as the circumstances of Mr. Rusesabagina’s transfer and treatment in Rwanda have become clear.

International Standards

General principles concerning state responsibility for the conduct of third parties are summarized by Article 16 of the International Law Commission’s (ILC) Draft Articles on State Responsibility, which the International Court of Justice has held reflects customary international law.[173] The Article provides that “[a] State which aids or assists another State in the commission of an internationally wrongful act by the latter is internationally responsible for doing so if: (a) that State does so with knowledge of the circumstances of the internationally wrongful act; and (b) the act would be internationally wrongful if

Terrorism”, April 25, 2021. Available at https://abcnews.go.com/International/paul-rusesabagina-called-hero-hotel-rwanda-now-accused/story?id=76953569.

[171] See ABC News, “Paul Rusesabagina Was Called a Hero After ‘Hotel Rwanda’: Now He’s Accused of Terrorism”, April 25, 2021. Available at https://abcnews.go.com/International/paul-rusesabagina-called-hero-hotel-rwanda-now-accused/story?id=76953569.

[172] Reuters, “Rwanda’s Kagame Says Relations Are on the Mend with France”, May 17, 2021. Available at https://www.reuters.com/world/africa/rwandas-kagame-says-relations-are-mend-with-france-2021-05-17/.

[173] International Court of Justice, Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. V. Serb. & Montenegro), Judgement, February 26, 2007, para. 420.

committed by that State."[174] In sum, a state may be responsible for aiding and abetting internationally wrongful acts when four conditions are met:

> (1) the state aids or assists another state in the commission of an internationally wrongful act;
> (2) such aid or assistance contributes to the commission of that act;
> (3) the assisting state has the intention to facilitate and/or knowledge of the circumstances of the internationally wrongful act; and
> (4) the recipient state's act would also be wrongful if committed by the assisting state.[175]

With respect to the first condition, any method of support is likely covered by the "aids or assists" phrasing: the ILC Commentary on the Draft Articles cites financial, logistical, and technical support. With respect to the second condition – the nexus between assistance and the principal wrong – the ILC Commentary provides that "the assisting State will only be responsible to the extent that its own conduct has caused or contributed to the internationally wrongful act."[176] The ILC Commentary further notes that while aid or assistance does not have to be essential to the performance of the internationally wrongful act, it must contribute significantly.[177]

The third prong, that of intent and knowledge, is the most debated condition. The confusion associated with this condition is due in part to the fact that the text of Article 16 refers to "knowledge of the circumstances of the internationally wrongful act," while the ILC's commentary specifies that no responsibility arises unless the assisting state provided support with "a view to facilitating the commission of the wrongful act."[178] As detailed by experts, although these requirements may appear inconsistent on "first glance"

> [t]hey can be reconciled … if the first element is understood to require knowledge that the aid or assistance facilitated an internationally wrongful act—that is, knowledge of the wrongfulness of the action to be taken by the assisted state. The second condition then would be understood to

[174] International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts with Commentaries, Part of Rep. on the Work of Its Fifty-Third Session, U.N. Doc. A/56/10., 2001, Article 16 (hereinafter "ILC Draft Articles").
[175] Ryan Goodman & Miles Jackson, "State Responsibility for Assistance to Foreign Forces (aka How to Assess US-UK Support for Saudi Ops in Yemen)", Just Security, August 31, 2016.
[176] ILC Draft Articles at pg. 66.
[177] Id.
[178] Id.

> require intent to facilitate the action taken by the state, even if the state did not specifically intend that act's wrongfulness.[179]

Moreover, in practice there may be little difference between a knowledge and intent standard. Under well-settled principles of international law, states are "supposed" to intend the foreseeable consequences of their actions.[180] Therefore, if a state has actual or near certain knowledge that its assistance will result in unlawful acts, it does not matter whether it has provided assistance with the specific purpose of aiding in the wrongful act.[181] This is consistent with examples cited by the ILC of state responsibility for passively supporting or tolerating wrongful acts of other states.[182]

Notably, many experts have argued that states may not evade responsibility through "willful blindness" – defined as "a deliberate effort by the assisting state to avoid knowledge of illegality on the part of the state being assisted, in the face of credible evidence of present or future illegality."[183] Credible evidence includes evidence from sources such as "fact-finding commissions, or independent monitors on the ground."[184]

The fourth element, that "the recipient state's act would also be wrongful if committed by the assisting state," requires that the act violate either peremptory international norms or a treaty to which both states are party.[185]

The Case Against Mr. Rusesabagina

As described above, the Belgian authorities have been helping the Rwandan authorities investigate the present case against Mr. Rusesabagina since 2019. Among other things, this assistance has entailed a raid on Mr. Rusesabagina's home, seizure of his phone and computer, acquisition of information regarding money transactions, and interviews with witnesses. According to the prosecution, since Mr. Rusesabagina's arrival in Rwanda the Belgian authorities have provided case-related documents to the Rwandan authorities on at least one occasion: in December 2020.

[179] Oona Hathaway, Alexandra Francis, Alyssa Yamamoto, Srinath Reddy Kethireddy and Aaron Haviland, "State Responsibility for U.S. Support of the Saudi-led Coalition in Yemen", Just Security, April 25, 2018. Available at https://www.justsecurity.org/55367/state-responsibility-u-s-support-saudi-led-coalition-yemen/.

[180] Ryan Goodman & Miles Jackson, "State Responsibility for Assistance to Foreign Forces (aka How to Assess US-UK Support for Saudi Ops in Yemen)", Just Security, August 31, 2016. See also Harriet Moynihan, "Aiding and Assisting: Challenges in Armed Conflict and Counterterrorism", Chatham House, November 2016, para. 74.

[181] Harriet Moynihan, "Aiding and Assisting: Challenges in Armed Conflict and Counterterrorism", Chatham House, November 2016, para. 70.

[182] Id. at para. 69

[183] Id. at para. 43.

[184] Id. at para. 45.

[185] Id. at paras. 28-29.

The proceedings against Mr. Rusesabagina have entailed both fair trial violations, as discussed above, and violations of his pretrial rights: among other things, an undisputed three days of incommunicado detention.

This raises the question of whether Belgium may bear any responsibility for wrongful acts committed by the Rwandan authorities. In particular, it would be important for Belgium to clarify whether it indeed provided materials to the Rwandan authorities in December 2020; if so, what was the nature of the materials provided; what other assistance if any has been provided since Mr. Rusesabagina's transfer to Rwanda; and how and whether Belgium addressed the potential that its support might facilitate international wrongful acts, including in light of documented patterns of unfair trials against government opponents in Rwanda.[186]

Further, it appears that the Belgian investigation is ongoing, with the corresponding possibility that cooperation between Belgium and Rwanda on Mr. Rusesabagina's case might continue. Given the violations that have come to light since the commencement of trial, such as the breach of Mr. Rusesabagina's right to confidential communication with counsel, it is all the more important that Belgium clarify the scope of its support and its assessment of this support's compatibility with international norms.

[186] See Amnesty International, "Rwanda: Paul Rusesabagina Must be Guaranteed a Fair Trial", September 14, 2020. Available at https://www.amnesty.org/en/latest/news/2020/09/rwanda-paul-rusesabagina-must-be-guaranteed-a-fair-trial/#:~:text=Paul%20Rusesabagina%20was%20allowed%20a,and%20critics%20of%20the%20government ("Amnesty has documented numerous violations of fair trial rights in previous cases involving opponents and critics of the government").

CONCLUSION

TrialWatch Expert Geoffrey Robertson's Findings:

Whatever the merits of the charges against Mr. Rusesabagina (and this report takes no position on those), it is clear that Mr. Rusesabagina's fair trial rights – in particular his right to confidential communication, his right to the presumption of innocence, and his right to prepare his defense – have been violated, potentially to the irreparable prejudice of the defense, calling into question the fairness of any potential convicting verdict. Further, by relying on the Bishop's untested statement to find that it had jurisdiction, by permitting two prosecution witnesses to present their allegations unchallenged, and by asking prosecution witnesses questions geared towards inculpating Mr. Rusesabagina, the court has evinced more concern for ensuring the prosecution's case is established than protecting Mr. Rusesabagina's rights.

Belgium, whose diplomats have been present for this trial, should explain how and why it has cooperated with Rwanda in the prosecution of a man to whom it had given asylum and citizenship. As described above, it appears that Belgium continued to provide assistance to the Rwandan investigation even after the proceedings' serious defects came to light. Complicity in an unfair trial should be a matter of international concern. Moreover, if the deception operation that brought Mr. Rusesabagina to Rwanda indeed amounts to circumvention of Belgian extradition law, Belgium should in fairness provide evidence to support Mr. Rusesabagina's argument to this effect.

Can the court regain credibility at this late stage? The court could sever Mr. Rusesabagina's trial from that of the co-defendants, and provide the adjournment that is necessary for him to prepare his defense. It could permit international counsel, representing him or invited as amici, to more fully make their case that the circumstances of Mr. Rusesabagina's transfer to Rwanda amount to an abuse of process, and rule upon it properly so that an adverse decision could be made the subject of appeal. It could recall the Bishop and the two vital witnesses and have their testimony subjected to cross examination.

Based on the course of the proceedings thus far, however, it may be doubted that the guarantees of fairness that these proceedings would require in order to be credible will be afforded Mr. Rusesabagina – especially if they are to result, as seems to be predetermined, in a conviction which may carry a sentence of life imprisonment.

Advance Edited Version

Distr.: General
18 March 2022

Original: English

Human Rights Council
Working Group on Arbitrary Detention

Opinions adopted by the Working Group on Arbitrary Detention at its ninety-second session, 15–19 November 2021

Opinion No. 81/2021 concerning Paul Rusesabagina (Rwanda)

1. The Working Group on Arbitrary Detention was established in resolution 1991/42 of the Commission on Human Rights. In its resolution 1997/50, the Commission extended and clarified the mandate of the Working Group. Pursuant to General Assembly resolution 60/251 and Human Rights Council decision 1/102, the Council assumed the mandate of the Commission. The Council most recently extended the mandate of the Working Group for a three-year period in its resolution 42/22.

2. In accordance with its methods of work,[1] on 3 June 2021 the Working Group transmitted to the Government of Rwanda a communication concerning Paul Rusesabagina. The Government has not replied to the communication. The State is a party to the International Covenant on Civil and Political Rights.

3. The Working Group regards deprivation of liberty as arbitrary in the following cases:

(a) When it is clearly impossible to invoke any legal basis justifying the deprivation of liberty (as when a person is kept in detention after the completion of his or her sentence or despite an amnesty law applicable to him or her) (category I);

(b) When the deprivation of liberty results from the exercise of the rights or freedoms guaranteed by articles 7, 13, 14, 18, 19, 20 and 21 of the Universal Declaration of Human Rights and, insofar as States parties are concerned, by articles 12, 18, 19, 21, 22, 25, 26 and 27 of the Covenant (category II);

(c) When the total or partial non-observance of the international norms relating to the right to a fair trial, established in the Universal Declaration of Human Rights and in the relevant international instruments accepted by the States concerned, is of such gravity as to give the deprivation of liberty an arbitrary character (category III);

(d) When asylum seekers, immigrants or refugees are subjected to prolonged administrative custody without the possibility of administrative or judicial review or remedy (category IV);

(e) When the deprivation of liberty constitutes a violation of international law on the grounds of discrimination based on birth, national, ethnic or social origin, language, religion, economic condition, political or other opinion, gender, sexual orientation, disability, or any other status, that aims towards or can result in ignoring the equality of human beings (category V).

[1] A/HRC/36/38.

Submissions

Communication from the source

4. Paul Rusesabagina, born in 1954, is a Rwandan and Belgian national and a permanent resident of the United States of America.

5. According to the information received, Mr. Rusesabagina has supported survivors and victims of genocide and oppression. In 1994, while he was serving as the manager of the Hôtel des Mille Collines in Kigali, he risked his life to shelter Hutus and Tutsis seeking refuge from genocide. The source refers to a movie, *Hotel Rwanda*, which contains a representation of those events. Mr. Rusesabagina has dedicated his life to speaking about the lessons learned from the genocide, addressing journalists, educators, students, policymakers, business leaders and human rights advocates.

6. Mr. Rusesabagina founded the Hotel Rwanda Rusesabagina Foundation to generate support for an internationally administered truth and reconciliation commission for Rwanda and the Great Lakes Region. The Foundation has worked on issues related to the ongoing conflicts. It campaigned for an end to military intervention and against the exploitation of conflict minerals. Mr. Rusesabagina has criticized the Government of Rwanda and openly discussed its responsibility for alleged war crimes, crimes against humanity and possible genocide.

7. The source reports that Mr. Rusesabagina became the target of public criticism by the Government of Rwanda because of his opinions and beliefs. After a failed assassination attempt in 1996, he left Rwanda to seek political asylum in Belgium, where he continued to voice criticism of the Government. In 2009, out of fear for his safety, he was forced to relocate to the United States.

8. In 2010, the Government of Rwanda allegedly began accusing Mr. Rusesabagina of funding a rebel group in the Democratic Republic of the Congo that is considered a terrorist organization. Mr. Rusesabagina has reportedly continued to face threats and attempts on his life, as well as the ransacking of his home in Belgium.

9. Mr. Rusesabagina has become a political opponent in the diaspora, serving for a time as the first head of a coalition of political parties when it was founded in 2018 and regularly criticizing the Government for its repression of political dissent and freedom.

a. Arrest and detention

10. According to the information received, in 2020 Mr. Rusesabagina was invited to travel to Burundi to speak at churches and public gatherings. On 26 August 2020, he left Chicago and flew to Dubai, United Arab Emirates. There, he planned to meet his host and fly on to Burundi. He arrived in Dubai at approximately 7 p.m. local time on 27 August 2020. The source claims that the Government of Rwanda arranged for a private jet to take Mr. Rusesabagina to Kigali without his knowledge and against his will, arriving in the early morning of 28 August 2020. The Justice Minister of Rwanda later admitted that the Government had paid for the flight. No application for Mr. Rusesabagina's arrest, extradition or deportation is known to have been made.

11. The source alleges that Mr. Rusesabagina was sedated in the aircraft while in Dubai. When he realized that the plane was landing in Kigali, he started screaming and tried to exit the plane, thinking he was going to be killed or harmed. He was then restrained by four agents from the Rwanda Investigation Bureau, who entered the plane and tied him up. They dragged him across the tarmac and into a car. He has never been provided with either a warrant of arrest or arrest documents, as required under Rwandan law.

12. From 28 to 31 August 2020, Mr. Rusesabagina was allegedly held in a facility described as a "slaughterhouse", where it was possible to "hear persons, women screaming, shouting and calling for help". During the morning of 28 August, Mr. Rusesabagina was allegedly tortured by an agent of the Rwanda Investigation Bureau wearing military boots, who stepped on his neck affirming "we know how to torture". While at the "slaughterhouse", Mr. Rusesabagina was restrained, blindfolded and held in solitary confinement. He was

deprived of food and at times of sleep. A 66-year-old cancer survivor with chronic medical issues, he was kept tied up, unable to stand up or walk, lacking strength and suffocating.

13. According to the information received, while he was held at the "slaughterhouse", Mr. Rusesabagina's blindfold was removed once, for an interrogation by the Prosecutor General of Rwanda and the Secretary-General of the Rwanda Investigation Bureau. They allegedly told him that they needed an acknowledgement falsely implicating a foreign leader in the charges that he was going to be accused of, including receiving money for a terrorist organization. They allegedly offered to release him if he accepted the accusation. Mr. Rusesabagina refused. He was then transferred to the Remera police station, where he was held until 17 September, and then transferred to Nyarugenge central prison in Mageragere. During the 22 days that he was kept in police stations, he lost approximately nine kilos, due to sleep and food deprivation.

14. On 31 August 2020, Mr. Rusesabagina was brought to the Remera metropolitan police station in Kigali, where he was registered as a prisoner and detained. At that point, the Rwandan authorities reportedly informed the Belgian authorities that a Belgian citizen had been detained.

15. The source claims that Mr. Rusesabagina was in a state of incommunicado detention from 27 and 31 August 2020 and was tortured during that period. It is not known where he was held during this time, or in what conditions. Despite inquiries, it has not been possible for his family or his lawyers to clarify what happened during this period, as they have not been able to raise the issue in public interviews or in proceedings before the courts.

16. From the evening of 27 August until 8 September, Mr. Rusesabagina had allegedly no direct contact with his family. He gave an interview to the New York Times on 17 September 2020, in which "he appeared to be speaking under duress".[2] In the interview, in which his account was at times muddled, he could not say what had happened to him for the three days between his flight from Dubai and his reappearance in Kigali, but said: "I do not know where I was. I was tied – the leg, the hands, the face. I could not see anything."

17. On 31 August 2020, the Rwanda Investigation Bureau reportedly announced a first version of the arrest in a tweet, stating that the authorities had arrested Mr. Rusesabagina "through international cooperation" and taken him into custody. The specifics of the "international cooperation" were not provided. That tweet was retweeted on the same day by the Minister of Justice and Attorney General, who praised the arrests taking place "thanks to international cooperation". The Bureau also announced that Mr. Rusesabagina was "suspected to be the founder, leader, sponsor and member of violent, armed, extremist terror outfits … operating out of various places in the region and abroad" and that he was the subject of an international arrest warrant. The source however has refuted this allegation.

18. On 6 September 2020, the President of Rwanda appeared on national television and indicated that Mr. Rusesabagina had been "lured", suggesting he had been tricked into boarding the flight. Reportedly, he said that: "There was no kidnap. There was not any wrongdoing in the process of his getting here. He got here on the basis of what he believed and wanted to do. ... It was actually flawless." The head of the National Intelligence and Security Services, reportedly commented that "it was quite flawless and I should say one of the best operations that any country can ever conduct".

19. The source claims that later in February 2021, when speaking with a reporter, the President again confirmed the operation. In an interview on 26 February 2021, the Minister of Justice affirmed that the Government of Rwanda had paid for the flight to Kigali. The Government admitted to deceiving Mr. Rusesabagina into leaving his home and going against his will to Rwanda, which he left after a failed assassination attempt in 1996 and where he would not voluntarily return out of fear for his life.

20. The source argues that the Government's versions of the arrest are contradictory. However, following criticism, the Government issued a third version, stating that Mr. Rusesabagina had boarded a private jet voluntarily, which then made a stopover in Kigali and the Rwandans took advantage of the situation to arrest him. That explanation allegedly

[2] See https://www.nytimes.com/2020/09/17/world/africa/paul-rusesabagina-rwanda-interview.html.

contradicts the version issued by the Rwanda Investigation Bureau and the Minister of Justice and Attorney General and the version put forward by the President and the head of the National Intelligence and Security Services.

21. On 1 September 2020, a spokesperson for the Rwanda Investigation Bureau indicated that Mr. Rusesabagina "has the right to a lawyer and the right to speak to his family". A newspaper published an interview with Mr. Rusesabagina, which he purportedly gave from his cell at Remera metropolitan police station. The journalist was given access to Mr. Rusesabagina before he had even had contact with legal counsel, consular officials or family. During the interview, Mr. Rusesabagina allegedly claimed that he was being "treated with kindness" and had been "offered an option to choose [his] defence team", that he expected to receive justice and a fair trial in Rwanda and that "he was choosing his defence team to prove his innocence". He confirmed, however, that he was not able to speak freely while in custody. It is unknown whether he willingly participated in the interview, if it was supervised, or the conditions under which he agreed to talk.

b. Judicial proceedings

22. According to the source, Mr. Rusesabagina's family engaged the services of a lawyer. He brought a letter to the Rwanda Investigation Bureau, confirming that the family had asked him to represent Mr. Rusesabagina.

23. On 2 September 2020, after hearing about his detention at Remera metropolitan police station, Mr. Rusesabagina's family called the police station and asked to speak to him. They were informed that the request would be passed on, but never received a response. On the same day, the lawyer they had retained visited the police station twice, but was denied access. He then informed the Bar Association that he had not been allowed to see his client.

24. On 5 September 2020, a different Rwandan lawyer gave a press conference, during which he claimed to have been selected by Mr. Rusesabagina from a list of public lawyers. The following day, Mr. Rusesabagina's family stated that the lawyer had not been appointed by them, but had been selected by the Government; Mr. Rusesabagina would never have engaged a lawyer who would hold a public press conference without first speaking with or consulting the family and who refused to address his kidnapping and arrest.

25. The source claims that the public lawyer represented Mr. Rusesabagina in a manner contrary to his interests, including by failing to challenge the jurisdiction of the Rwandan courts; failing to argue in support of a provisional release pending trial, given Mr. Rusesabagina's age, his medical condition and the coronavirus disease (COVID-19) pandemic; by holding a press conference to undermine the family's claim; and by failing to contact the family-appointed lawyer.

26. It is reported that on 9 September 2020, the President stated that: "Rusesabagina heads a group of terrorists that have killed Rwandans. He will have to pay for these crimes. Rusesabagina has the blood of Rwandans on his hands."

27. The source submits that 13 days after Mr. Rusesabagina's arrest, the Rwanda Investigation Bureau handed over its investigation case file to the National Public Prosecution Authority. On 14 September 2020, 18 days after his arrest, Mr. Rusesabagina was brought before the Kicukiro primary court in Kigali for a pretrial hearing, his first appearance before a judge. Mr. Rusesabagina's government-appointed lawyers requested his provisional release because of his poor health. On 17 September 2020, the court denied him bail, finding that the charges against him were "grave and serious" and that "the health concerns brought by Mr Rusesabagina are baseless".

28. On 25 September 2020, Mr. Rusesabagina reportedly appeared in front of the Nyarugenge intermediate court with his government-appointed lawyers, to appeal the denial of bail. Mr. Rusesabagina's government-appointed lawyers again failed to make any arguments that could challenge the Government, including failing to raise his kidnapping and incommunicado detention, or his susceptibility to serious illness. On 2 October 2020, the Nyarugenge intermediate court denied the appeal.

29. Mr. Rusesabagina remains in Mageragere prison, a local prison, where he cannot communicate freely and confidentially with his legal counsel. In an interview in February

2021, the Justice Minister specifically defended the right of the prison authorities to monitor the correspondence between Mr. Rusesabagina and his legal counsel, and acknowledged that they were intercepting and reading those communications.

30. The source claims that, after being represented by two government-appointed lawyers, who failed to put forward basic motions and objections, and only after extensive efforts by his family to permit Mr. Rusesabagina to select his own attorney, the family was able to engage a private lawyer.

31. On 16 November 2020, an indictment was issued, charging Mr. Rusesabagina with nine offences that carry a sentence of life imprisonment. The indictment listed 17 co-defendants, none of whom Mr. Rusesabagina had ever met.

32. Although the private lawyer was appointed in October 2020, he represented Mr. Rusesabagina in court for the first time on 27 November 2020, before the Nyarugenge intermediate court by videoconference. It was then, for the first time, that counsel for Mr. Rusesabagina raised the issue of his transfer to Rwanda from the United Arab Emirates. The trial was postponed until 17 February 2021, however his counsel had been unable to meet with Mr. Rusesabagina frequently enough to prepare his defence effectively.

33. In addition, the source claims that Mr. Rusesabagina continued to be denied access to his international lawyers. On 29 December 2020, Mr. Rusesabagina wrote a letter from prison to the Bar Association, designating his international legal team but the letter was subsequently confiscated. Finally, after several attempts to submit the request, on 26 January 2021 the Bar Association denied his request to be represented by international counsel.

34. The source argues that the prison restrictions deprive Mr. Rusesabagina of effective legal advocacy. It is not possible to receive calls where he is being held. His only option for communicating with counsel is to make calls out. However, as a detainee, he is limited to a five-minute phone call, which is not confidential. Court and other legal documents left by his lawyer have been confiscated by prison officials. The Director of the prison allegedly told him that they had been confiscated and would not be returned, despite being privileged documents.

35. The authorities have allegedly denied Mr. Rusesabagina access to the documents and materials needed to prepare his defence. He only received his indictment in early January 2021, a month after his trial date was set and more than four months after he was arrested. Prison officials have allegedly denied him access to pens and paper, let alone a computer.

36. According to the source, on 2 December 2020 the trial court dismissed his appeal against an order extending his pretrial detention. On 3 December 2020, the date of Mr. Rusesabagina’s criminal trial was set for 26 January 2021. Additionally, the Court approved merging the case of Mr. Rusesabagina and his 17 co-defendants with ongoing proceedings against a former spokesperson of a rebel group. On 26 January 2021, the trial was rescheduled for 17 February 2021.

37. On 13 January 2021, Mr. Rusesabagina’s private lawyer filed a letter to the presiding judge in the Rwandan court system, seeking remedies for ongoing fair trial violations. Further motions were filed with the court on 21 January and 12 February. On 26 February, the court ruled that it was not relevant to talk about how Mr. Rusesabagina was arrested or detained; none of the fair trial violations raised were addressed by the court.

38. On 10 March 2021, the court ruled on certain pretrial motions concerning due process violations. Despite permitting Mr. Rusesabagina a computer with his case file on it, the court ruled that, moving forward, privileged documents would be protected only after having been identified, without specifying by whom or whether copies would be shared with Ministry of Justice officials. Further, the court reportedly did not provide any remedy for the Government’s prior access to all privileged communications, including documents outlining his defence strategy. Mr. Rusesabagina appealed the ruling and the session ended without a date set for the next hearing. The criminal trial is currently ongoing.

39. Since 23 April 2021, Mr. Rusesabagina’s Rwandan lawyers have been prohibited from taking any documents, computers or electronic devices into their meetings with Mr. Rusesabagina without first submitting them for inspection and review to the Director of the

prison. Documents marked privileged and confidential sent by international lawyers were confiscated by the prison authorities on 29 April 2021. In addition, Mr. Rusesabagina's Rwandan lawyers have been subjected to invasive and extraordinary searches of their bodies and possessions.

40. The source claims that Mr. Rusesabagina's health has progressively and seriously deteriorated in detention. He is a 66-year-old cancer survivor who suffers from hypertension and cardiovascular disease. His medication for a heart disorder is being withheld. His treating physician in Belgium stated that interrupting and modifying his treatment, as well as inducing stress, risk causing him severe hypertensive attacks and even a stroke. Mr. Rusesabagina is experiencing worsening dizziness and very high blood pressure. Additionally, he has lost a significant amount of weight. He has not been able to disclose the full extent of his physical injuries to his lawyers or to an independent doctor whom he can trust.

41. On 17 February 2021, the day that the trial began, the President of Rwanda again reportedly affirmed Mr. Rusesabagina's guilt. No prospect of a free and fair trial exists because neither the Ministry of Justice nor the Rwandan judiciary could or would do anything to undermine the President's pronouncements.

42. The source reports that in early May 2021, after 260 days, Mr. Rusesabagina's solitary confinement finally ended. During that time, his only human contact was occasionally speaking to prison guards, sporadic visits from his attorneys and five minutes per week on a monitored phone call with his family. Mr. Rusesabagina's placement in solitary confinement early in his imprisonment and not as a last resort, the dire circumstances and length of time he has been in solitary confinement, as well as the lack of judicial oversight, allegedly constitute a violation of his rights.

i. Category I

43. According to the source, Mr. Rusesabagina's extrajudicial transfer to Rwanda had no legal basis. The source refers to articles 9 and 13 of the International Covenant on Civil and Political Rights, to article 6 of the African Charter on Human and Peoples' Rights and to article 68 of the Rwandan Code of Criminal Procedure. Mr. Rusesabagina's arrest and transfer to Rwanda allegedly lacked a legal basis and the due process of law, in violation of article 9 of the Universal Declaration of Human Rights and article 9 of the Covenant.

ii. Category II

44. The source argues that the detention of Mr. Rusesabagina is arbitrary because it resulted from the exercise of his fundamental right to freedom of expression.

45. The right to freedom of expression is protected under article 19 of the Covenant, which is of special importance for political opponents. Restrictions on the right to political free speech are strongly limited. The right to free expression is also protected by article 19 of the Universal Declaration of Human Rights, while article 38 of the Rwandan Constitution recognizes and guarantees the right to freedom of expression.

46. The protection of free expression "is broad enough to include the right of individuals to criticize or openly and publicly evaluate their Governments without fear of interference or punishment. Without such protection, members of political opposition and human rights activists will not be able to criticize, investigate, or expose corrupt and illegal practices by government officials".[3]

47. It is alleged that, despite international and national legal guarantees for the rights of individuals to freedom of expression, the Government arbitrarily detained Mr. Rusesabagina as a direct result of his public condemnation of the Government and his political opposition. Allegedly, the Government has a documented pattern of attacking and attempting to silence its opponents and critics through harassment and detention.

[3] Opinion No. 22/2013, para. 11.

48. The source recalls that "sharing of information and ideas through online media cannot reasonably qualify as posing threats against morality, public order and the general welfare in a democratic society".[4]

49. The source states that Mr. Rusesabagina's public criticisms of the President and the Government are protected under his right to freedom of expression. Whether in the form of a book, speaking on the radio, sharing his opinion online or in interviews, Mr. Rusesabagina has been an outspoken critic that the Government has wanted to silence for many years. His public criticisms constitute his exercise of a fundamental right and thus cannot be the basis for a deprivation of liberty.

iii. Category III

50. The source claims that the Government has violated Mr. Rusesabagina's right to be presented with a warrant, to counsel of his own choosing, to the presumption of innocence until proved guilty, to humane treatment, to prompt consular assistance and to be brought promptly before a tribunal.

51. The Rwandan authorities allegedly violated Mr. Rusesabagina's rights in the absence of a warrant or judicial order. Article 9 (1) of the Covenant and principle 2 of the Body of Principles for the Protection of All persons under Any Form of Detention or Imprisonment prohibit arbitrary arrest and require compliance with domestic rules that define procedures for arrest, such as specifying when a warrant is required and permitting access to counsel. Rwandan law reportedly stipulates that an arrest warrant must be shown to the person against whom it is issued, who shall be given a copy of it.

52. The source alleges that Mr. Rusesabagina was never presented with a warrant or other judicial order when he was arrested. While the Government has stated that there was an international arrest warrant, it has never produced one. It is alleged that, because Mr. Rusesabagina was arrested without a warrant when one is required by law, the authorities violated his legal rights and his subsequent detention is arbitrary.

53. The source also recalls that article 36 of the Vienna Convention on Consular Relations, to which both Rwanda and Belgium are parties, outlines the requirement to provide consular assistance for those detained in a foreign country.

54. Principle 16 (2) of the Body of Principles recognizes the right of a detained foreign national to "communicate by appropriate means with a consular post of the diplomatic mission of the State of which he is a national". Rule 62 of the United Nations Standard Minimum Rules for the Treatment of Prisoners (the Nelson Mandela Rules) also provides that: "Prisoners who are foreign nationals shall be allowed reasonable facilities to communicate with the diplomatic and consular representatives of the State to which they belong." Denial of consular rights is allegedly a deprivation of the right to a fair trial.

55. Mr. Rusesabagina is a Belgian citizen. However, the Government of Rwanda did not inform the Belgian authorities of his detention until three days after his arrest. In addition, the detaining authorities did not promptly provide Mr. Rusesabagina with an opportunity to communicate with the Belgian consulate.

56. Article 14 (3) (b) of the Covenant provides that a defendant is entitled to "have adequate time and facilities for the preparation of his defence and to communicate with counsel of his own choosing". In its general comment No. 32 (2007), the Human Rights Committee stated that defendants must have access to documents and other evidence, including "all materials that the prosecution plans to offer in court against the accused or that are exculpatory". Also, that counsel "be able to meet their clients in private and to communicate with the accused in conditions that fully respect the confidentiality of their communications" (paras. 33–34).

[4] Opinion No. 71/2019, para. 79.

57. The European Court of Human Rights has interpreted this as a non-derogable right and has found that restriction of an applicant’s access to a lawyer he or she has retained constitutes a violation of the right to legal representation of his or her choice.[5]

58. The source claims that the Government used its own legal aid system, designed for indigent defendants, to impose a lawyer on Mr. Rusesabagina, when it knew that his family had retained a lawyer to represent him. Allegedly, this could only have been done to deny Mr. Rusesabagina an independent counsel. The government-appointed lawyers never raised the issue of his transfer to Rwanda from the United Arab Emirates as a limit to the jurisdiction of the court, or as a reason why the court should decline to exercise its jurisdiction based on the abuse of process that brought Mr. Rusesabagina before it.

59. The lawyer appointed by Mr. Rusesabagina’s family brought a letter to the Rwanda Investigation Bureau confirming his representation shortly after the arrest. After the Bureau received the letter and the lawyer had visited the police station twice, the Government appointed a public defence lawyer. Over a month after the arrest, the private lawyer was finally permitted to visit Mr. Rusesabagina, although he was only able to represent him in court for the first time at the end of November 2020.

60. The source claims that Mr. Rusesabagina continues to be denied access to international lawyers. Even though Mr. Rusesabagina has finally been permitted counsel of his own choosing, he is still not allowed private phone conversations with his counsel, nor can his counsel share case files with him. In addition, because of COVID-19, his counsel was unable to confer with Mr. Rusesabagina for several weeks, despite the trial commencing. As a result, Mr. Rusesabagina was deprived of his ability to have counsel prepare for his trial.

61. The source claims that the inability of Mr. Rusesabagina to be assisted by counsel of his own choice for well over a month after his arrest; the continued denial of rightful international legal assistance, despite the international nature of his arrest and charges; and the practical restrictions that are depriving him of the ability to prepare an effective defence, amount to a violation of article 14 of the Covenant.

62. The source recalls that under article 14 (2) of the Covenant, article 11 (1) of the Universal Declaration of Human Rights and principle 36 of the Body of Principles, everyone has the right to be presumed innocent until proved guilty. Under the presumption of innocence, the burden of proof to establish the guilt of the accused lies with the prosecution. Public authorities must refrain from prejudging the outcome of the proceedings by making any official statements or using conclusory language that would portray an accused person as guilty.

63. On 6 September 2020, during a broadcast on national television, the President reportedly said: “Rusesabagina heads a group of terrorists that have killed Rwandans. He will have to pay for these crimes. Rusesabagina has the blood of Rwandans on his hands.” He also allegedly said that Mr. Rusesabagina became “an associate of these groups or even a leader of different groups” and that “these groups … that Rusesabagina was leading or is one of their leaders, killed people in the south-western part of our country in about three districts”. Mr. Rusesabagina was reportedly charged by a Rwandan court on 14 September 2020, a week after the President’s broadcast. Then, on 17 February 2020, the first day of Mr. Rusesabagina’s trial, the President supposedly made similar comments. The source claims that these were a violation of the presumption of innocence and constitute a de facto guilty verdict.

64. The source further recalls that article 10 (1) of the Covenant and principle 1 of the Body of Principles state that persons deprived of their liberty shall be treated with humanity and with respect for the inherent dignity of the human person. Article 7 of the Covenant, article 5 of the Universal Declaration of Human Rights, article 14 of the Rwandan Constitution and principle 6 of the Body of Principles contain a prohibition of torture or cruel or inhuman treatment. The source claims that in the present case, the violations further

[5] See, for example, *Croissant v. Germany* (application No. 13611/88), judgment of 25 September 1992, para. 29, and *Martin v. Estonia* (application No. 35985/09), judgment of 30 May 2013, para. 90.

amount to a contravention of the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment.

65. It is alleged that Rwandan government authorities violated the right of Mr. Rusesabagina to be free from torture, cruel, inhuman or degrading treatment or punishment, when they forcibly disappeared him and by their continued denial of proper medical care, including blood pressure medication, despite Mr. Rusesabagina's pre-existing and serious medical conditions.

66. An enforced disappearance is any form of deprivation of liberty by agents of the State or by persons or groups of persons acting with the authorization, support or acquiescence of the State, followed by a refusal to acknowledge the deprivation of liberty or by concealment of the fate or whereabouts of the disappeared person, which places such a person outside the protection of the law. Enforced disappearances violate numerous substantive and procedural provisions of the Covenant, including articles 9 and 14, and constitute a particularly aggravated form of arbitrary detention.

67. The source alleges that the authorities violated Mr. Rusesabagina's right to humane treatment when they kidnapped and subsequently imprisoned him, held him incommunicado for three days under circumstances that involved torture, interrogations and physical and mental abuse, and rendered him subject to an enforced disappearance. In addition, the subsequent 260 days of solitary confinement is allegedly a form of torture because of the severe psychological distress and physical toll that it created.

68. According to the Body of Principles, medical care and treatment shall be provided, whenever necessary, free of charge. In the present case, Mr. Rusesabagina is allegedly in extremely poor health and has taken prescribed medication since 1996.

69. The source claims that the Government is not providing adequate medical treatment for Mr. Rusesabagina's condition, as the authorities are not delivering the prescribed medication that has been provided to the prison guards. Mr. Rusesabagina has suffered rapid weight loss since his arrest. He suffers from constant high blood pressure, extreme headaches and dizziness. His health has deteriorated to the point that he is at risk of dying from a stroke. The source argues that the Government's denial of adequate medical treatment amounts to a violation of articles 7 and 10 of the Covenant and article 5 of the Universal Declaration of Human Rights.

70. Due process guarantees include the right of an arrested or detained person to be brought promptly before a judge or other officer authorized to exercise judicial power. The Human Rights Committee interprets the term "promptly" to be within about 48 hours, except in exceptional circumstances. The 2018 Rwandan Law on Counter-terrorism, which reportedly provides for the duration of arrest and provisional detention of a suspect of a terrorist act for 15 days, renewable, allegedly violates the country's obligations under the Covenant.

71. The source claims that the Government detained Mr. Rusesabagina for 18 days before allowing him to see a judge. Eighteen days of detention without being brought before a tribunal is 16 days more than international human rights law permits. The source argues that the treatment of Mr. Rusesabagina and the Government's failure to guarantee his rights under the Universal Declaration of Human Rights and the Covenant amount to an arbitrary deprivation of liberty under category III.

iv. Category V

72. The source alleges that the Government is targeting Mr. Rusesabagina because of his expression of political views and in particular for his association with a group politically opposed to the President, as well as for his criticism of the Government, his work with intergovernmental and civil society organizations and his anti-genocide advocacy.

73. Mr. Rusesabagina has criticized a broad range of human rights violations in Rwanda, including a lack of democracy and unfair elections. He has also challenged cases of arbitrary detention, torture and extrajudicial killings. He has publicly made allegations of war crimes and crimes against humanity. His criticisms are echoed by civil society organizations, government agencies and others.

74. The Government has allegedly threatened Mr. Rusesabagina since 2005. The President has called him a manufactured hero. During a genocide commemoration in 2007, the President called Mr. Rusesabagina a swindler, a gangster and someone who maligns the name of Rwanda. In 2010, leading up to the presidential elections, the harassment by the Government reportedly increased, as Mr. Rusesabagina became more active in his criticism. Mr. Rusesabagina has been active in organizing Rwandans in the diaspora. Fifteen years of these activities have allegedly led to his current kidnapping and detention. Accordingly, the source claims that his detention is arbitrary under category V.

Response from the Government

75. On 3 June 2021, the Working Group transmitted the allegations from the source to the Government under its regular communications procedure. The Working Group requested the Government to provide, by 3 August 2021, detailed information about the situation of Mr. Rusesabagina and to clarify the legal provisions justifying his continued detention, as well as its compatibility with the obligations of Rwanda under international human rights law, and in particular with regard to the treaties ratified by the State. The Working Group called upon the Government to ensure his physical and mental integrity.

76. The Working Group regrets that it received no reply from the Government.

Discussion

77. In the absence of a response from the Government, the Working Group has decided to render the present opinion, in conformity with paragraph 15 of its methods of work.

78. In determining whether a person's detention was arbitrary, the Working Group has regard to the principles established in its jurisprudence to deal with evidentiary issues. If the source has established a prima facie case for breach of international law constituting arbitrary detention, the burden of proof should be understood to rest upon the Government if it wishes to refute the allegations.[6] In the present case, the Government has chosen not to challenge the prima facie credible allegations made by the source.

79. The Working Group wishes to reaffirm that States have the obligation to respect, protect and fulfil all human rights and fundamental freedoms, including liberty of person, and that any national law allowing deprivation of liberty should be made and implemented in conformity with the relevant international standards set forth in the Universal Declaration of Human Rights, the Covenant and other applicable international and regional instruments. Consequently, even if the detention is in conformity with national legislation, regulations and practices, the mandate of the Working Group is to assess the circumstances of the detention, including the law itself, to determine whether such detention is also consistent with the relevant provisions of international human rights law.[7]

Category I

80. In arguing that Mr. Rusesabagina's transfer to and arrest in Rwanda had no legal basis, the source referred to articles 9 and 13 of the Covenant, to article 6 of the African Charter on Human and Peoples' Rights and to article 68 of the Rwandan Code of Criminal Procedure.

81. It is clear from the facts presented by the source that Mr. Rusesabagina's conveyance from Dubai to Kigali in a private jet was arranged by the Government of Rwanda, as admitted by the Minister of Justice, and was without his knowledge and consent. He was sedated while in the aircraft. The Working Group considers the whole process of getting Mr. Rusesabagina on board and transporting him to a destination he did not intend to go to as constituting an abduction, which also involves a detention.

82. In the present case, Mr. Rusesabagina was not informed of the grounds for his arrest at the time he was taken onto the private jet, which constitutes a violation of the prohibition of arbitrary arrest. When he later realized that the plane was landing in Kigali, he tried to exit

[6] A/HRC/19/57, para. 68.

[7] See, for example, opinions No. 36/2019, para. 33; No. 42/2019, para. 43; No. 51/2019, para. 53; and No. 56/2019, para. 74.

the plane, thinking he was going to be killed or otherwise harmed. He was then restrained by four Rwandan agents, who entered the plane and tied him up. They dragged him across the tarmac and into a car. He has never been provided with arrest documents, as required under Rwandan law.

83. International law concerning the right to personal liberty allows restrictions to this right in appropriate circumstances. The right however includes the guarantee of being presented with an arrest warrant, in cases that do not involve arrests made in flagrante delicto, to ensure the objectivity and fairness of the arrest. It is also required that the decision on whether the arrest is warranted be taken by an outside, competent, independent and impartial judicial authority. That is procedurally inherent in the right to personal liberty and security and the prohibition of arbitrary deprivation of liberty under articles 3 and 9 of the Universal Declaration of Human Rights.[8]

84. In consequence, the Working Group considers that Rwanda violated Mr. Rusesabagina's rights under article 9 of the Universal Declaration of Human Rights, article 9 of the Covenant and principles 2, 10, and 36 (2) of the Body of Principles.

85. The source claims that Mr. Rusesabagina was in a state of incommunicado detention from 27 and 31 August 2020 and was tortured during that period. It is not known where Mr. Rusesabagina was held during that time, or in what conditions.

86. Holding persons at secret, undisclosed locations and in circumstances undisclosed to the person's family violates their right to be brought promptly before a judge and to challenge the legality of their detention before a court or tribunal, under articles 9 (3) and (4) of the Covenant. Judicial oversight of any detention is a central safeguard for personal liberty and is critical in ensuring that detention has a legitimate basis. In the circumstances attending the incarceration of Mr. Rusesabagina, his disappearance led to him not being presented before a judge and unable to challenge his detention before a court for the first 18 days after his arrest. Consequently, his rights to an effective remedy under article 8 of the Universal Declaration of Human Rights and article 2 (3) of the Covenant were also violated. Mr. Rusesabagina was placed outside the protection of the law, in violation of his right to be recognized as a person before the law under article 6 of the Universal Declaration of Human Rights and article 16 of the Covenant.

87. Holding a detainee at a location unknown to their families and lawyers is a deprivation of liberty analogous to an enforced disappearance, which entails a wilful refusal to disclose the fate or whereabouts of the persons concerned or to acknowledge their detention. This lacks any valid legal basis under any circumstance. Enforced disappearances violate numerous substantive and procedural provisions of the Covenant and constitute a particularly aggravated form of arbitrary detention.[9] They are also inherently arbitrary, as they place the person outside the protection of the law.

88. For these reasons, the Working Group finds that Mr. Rusesabagina's detention has no legal basis and is therefore arbitrary under category I.

Category II

89. Freedom of opinion and expression and of peaceful assembly are fundamental human rights, enshrined in articles 19 and 20 of the Universal Declaration of Human Rights and articles 19 and 21 of the Covenant.[10] The Government must respect, protect and fulfil the right to hold and express opinions, including those that are not in accordance with its official policy, as well as the right to think and manifest personal convictions that can be at odds with its official ideology.[11]

90. Restrictions on the right to freedom of expression must not be overbroad; they must conform to the principle of proportionality, be appropriate to achieving their protective function, be the least intrusive instrument among those that might achieve their protective

[8] Opinion No. 32/2020, para. 33.

[9] Human Rights Committee, general comment No. 35 (2014), para. 17.

[10] *Yong Joo-Kang v. Republic of Korea* (CCPR/C/78/D/878/1999), para. 7.2.

[11] Opinions No. 76/2017, para. 62; No. 88/2017, para. 32; and No. 94/2017, para. 59.

function and be proportionate to the interest protected. It is worth noting that the value placed by the Covenant on uninhibited expression is particularly high in the circumstances of public debate in a democratic society concerning figures in the public and political domain.[12]

91. The source argues that Mr. Rusesabagina's detention is arbitrary because it resulted from the exercise of his fundamental right to freedom of expression. Since 1994, Mr. Rusesabagina has been supporting survivors and victims of genocide and oppression. He has dedicated his life to speaking about the lessons learned from the Rwandan genocide, addressing journalists, educators, students, policymakers, business leaders and human rights advocates. Through his Hotel Rwanda Rusesabagina Foundation, he aims to generate support for an internationally administered truth and reconciliation commission for Rwanda and the Great Lakes Region. He has criticized the Government and openly discussed its responsibility for alleged war crimes, crimes against humanity and possibly genocide. As a result, he has become the target of public criticism by the Government because of his opinions and beliefs. After a failed assassination attempt in 1996, he left Rwanda to seek asylum in Belgium, where he continued to voice criticism of the Government's policies. In 2009, out of fear for his safety, he was forced to relocate to the United States.

92. Mr. Rusesabagina became a political opponent in the diaspora, serving for a time as the first head of a coalition of political parties, when it was founded in 2018, regularly criticizing the Government for its repression of political dissent and freedom.

93. In this context, the Human Rights Committee has urged Rwanda to refrain from prosecuting "politicians, journalists and human rights defenders as a means of discouraging them from freely expressing their opinions and take immediate action to investigate attacks against them".[13] The Committee against Torture has also issued similar recommendations.[14]

94. The Working Group agrees with the source that Mr. Rusesabagina's public criticisms of the President and the Government are protected under his right to freedom of expression. Whether in the form of a book, speaking on the radio, sharing his opinion online or in interviews, Mr. Rusesabagina has been an outspoken critic that the Government has wanted to silence for many years. Mr. Rusesabagina's public criticisms constitute his exercise of a fundamental right and thus cannot be the basis for a deprivation of liberty.

95. The deprivation of liberty of Mr. Rusesabagina results from his exercise of universally recognized human rights, in particular the right to freedoms of opinion, expression and peaceful assembly. Mr. Rusesabagina's detention can be interpreted as a calculated move to curb his dissent by intimidating him and others associated with his work.

96. The Working Group concludes that Mr. Rusesabagina's detention resulted from the peaceful exercise of his right to freedom of opinion and expression and the right to take part in the conduct of public affairs, contrary to articles 19 and 21 of the Universal Declaration of Human Rights and 19 and 25 of the Covenant. His detention is arbitrary under category II.

Category III

97. Given its finding that Mr. Rusesabagina's deprivation of liberty is arbitrary under category II, the Working Group wishes to emphasize that, in such circumstances, no trial should take place. However, given that Mr. Rusesabagina is held in detention and considering the allegations made by the source, the Working Group will now examine the reported violations of the right to a fair trial and to the guarantees of due process.

98. The Working Group notes that the alleged violations of international human rights norms and standards in the arrest and detention of Mr. Rusesabagina include those in the minimum standards of due process relating to fair trial and treatment of detainees. The source recalls that Mr. Rusesabagina was arrested without a warrant and was not informed of the reasons for his arrest. This was contrary to articles 9 (2) and 14 (3) (a) of the Covenant, as well as principles 10 and 13 of the Body of Principles.

[12] Human Rights Committee, general comment No. 34, para. 34.

[13] CCPR/C/RWA/CO/4, para. 40.

[14] CAT/C/RWA/CO/2, paras. 52–53.

99. The source claims that Mr. Rusesabagina's rights to a fair trial were violated when he was not brought promptly before a tribunal, was denied the right to a counsel of his own choosing, was not granted prompt consular assistance, was not accorded the presumption of innocence and was subjected to inhumane treatment.

100. The source alleges that Mr. Rusesabagina was never presented with a warrant or other judicial order when he was arrested. While the Government claimed that there was an international arrest warrant for him, it has not produced one. It is alleged that, because Mr. Rusesabagina was arrested without a warrant while one was required by law, the authorities violated his legal rights and his subsequent detention is arbitrary.

101. The arrest in the absence of a warrant or judicial order violated Mr. Rusesabagina's right under article 9 (1) of the Covenant and principle 2 of the Body of Principles, which prohibit arbitrary arrest and require compliance with domestic rules that define such procedures, such as specifying when a warrant is required and permitting access to counsel. Rwandan law reportedly stipulates that an arrest warrant "must be shown to the persons against whom they are issued and such persons shall be given a copy of the warrant".

102. As regards the right to legal representation, the source claims that the Government imposed a public defence lawyer on Mr. Rusesabagina, when it was known that another lawyer had been privately appointed to represent him. Allegedly, this could only have been done to deny Mr. Rusesabagina an independent counsel.

103. The family requested a specific lawyer for Mr. Rusesabagina, who had a letter confirming his representation. Government officials received this letter and, after the lawyer had visited the police station twice, Mr. Rusesabagina had a public defence lawyer appointed for him. In October, over a month after the arrest, the private lawyer was finally permitted to visit Mr. Rusesabagina, although he was only able to represent him in court at the end of November 2020.

104. Legal representation is a core guarantee of the right to a fair trial. Legal assistance should be available at all stages of criminal proceedings, during the pretrial, trial and appellate stages. Denial of access to a lawyer substantially undermines and compromises the capacity to defend oneself from accusations in any judicial proceedings, which can enable further violations of due process guarantees.

105. Principle 18 (3) of the Body of Principles and rule 61 (1) of the Nelson Mandela Rules, stipulate that defendants must have access to legal counsel without delay. Persons deprived of their liberty have the right to legal assistance by a counsel of their choice at any time during their detention, including immediately after apprehension, and must be promptly informed of this right upon apprehension.[15]

106. Article 14 (3) (b) of the Covenant provides that a defendant is entitled to "have adequate time and facilities for the preparation of his defence and to communicate with counsel of his own choosing". Defendants must have access to documents and other evidence, including all materials that the prosecution plans to offer in court against the accused or that could assist the defence. It further requires that defendants "be able to meet their clients in private and to communicate with the accused in conditions that fully respect the confidentiality of their communications".[16]

107. In addition, the Working Group notes the allegations of the source concerning Mr. Rusesabagina being denied access to consular assistance. In terms of article 36 of the Vienna Convention on Consular Relations, to which both Rwanda and Belgium are parties, consular assistance ought to be provided for those detained in a foreign country. Additionally, principle 16 (2) of the Body of Principles recognizes the right of a detained foreign national to "communicate by appropriate means with a consular post of the diplomatic mission of the State of which he is a national" and rule 62 of the Nelson Mandela Rules provides that: "Prisoners who are foreign nationals shall be allowed reasonable facilities to communicate

[15] See also United Nations Basic Principles and Guidelines on Remedies and Procedures on the Right of Anyone Deprived of Their Liberty to Bring Proceedings Before a Court.

[16] Human Rights Committee, general comment No. 32 (2007), paras 33–34.

with the diplomatic and consular representatives of the State to which they belong." Denial of consular rights is alleged to be a deprivation of the right to a fair trial.

108. Mr. Rusesabagina has been a Belgian citizen since 1999. However, it appears that Rwanda did not inform the Belgian authorities of his detention until several days after his arrest, nor did Rwanda promptly inform Mr. Rusesabagina of his right to communicate with a Belgian consular officer, or facilitate such communication.

109. Concerning the presumption of innocence, the source recalls that on 6 September 2020, on national television, the President reportedly accused Mr. Rusesabagina of leading a terrorist organization that had killed Rwandans and that he had the blood of his compatriots on his hands. He also allegedly said that Mr. Rusesabagina had killed people in the south-west of the country. On 14 September 2020, a week after the President's broadcast, a Rwandan court reportedly charged Mr. Rusesabagina. Then, on 17 February 2020, the first day of Mr. Rusesabagina's trial, the President supposedly made similar comments.

110. Under articles 14 (2) of the Covenant and 11 (1) of the Universal Declaration of Human Rights and principle 36 of the Body of Principles, everyone has the right to be presumed innocent until proved guilty. This requires that to establish the guilt of the accused, the burden of proof lies with the prosecutor and public authorities must refrain from prejudging the outcome of the proceedings, make any official statements, or use conclusive language that would portray an accused person as guilty.

111. According to the source, from 28 to 31 August 2020, Mr. Rusesabagina was held in a facility described as a "slaughterhouse". During the morning of 28 August, Mr. Rusesabagina was allegedly tortured by a Government agent, wearing military boots, who stepped on his neck while affirming "we know how to torture". While at the "slaughterhouse", Mr. Rusesabagina was restrained, blindfolded and held in solitary confinement. He was deprived of food and at times of sleep. A 66-year-old cancer survivor with chronic medical issues, he was kept tied up, unable to stand up or walk, lacking strength and suffocating.

112. According to the information received, also while held at the "slaughterhouse", Mr. Rusesabagina's blindfold was removed once, for an interrogation by the Prosecutor General of Rwanda and the Secretary-General of the Rwanda Investigation Bureau. They allegedly told Mr. Rusesabagina that they needed an acknowledgement falsely implicating a foreign leader in the charges that he was going to be accused of, including receiving money for a terrorist organization. They allegedly offered to release him if he accepted the accusation. Mr. Rusesabagina refused. He was then transferred to the Remera police station, where he was held until 17 September, and then transferred to Nyarugenge central prison in Mageragere.

113. International human rights law requires that detainees be protected from any practices that violate their right to be free from any act that could cause severe pain or suffering, whether physical or mental, and which is inflicted intentionally on a person. The right to freedom from torture and other ill-treatment or punishment is absolute, it applies in all circumstances and it may never be restricted, including in times of war or states of emergency. No exceptional circumstances whatsoever, including threats of terrorism or other violent crime, may be invoked to justify torture or other ill-treatment. Such a prohibition applies irrespective of the offence allegedly committed by the accused person.

114. Article 10 (1) of the Covenant and principle 1 of the Body of Principles state that persons deprived of their liberty shall be treated with humanity and with respect for the inherent dignity of the human person. Article 7 of the Covenant, article 5 of the Universal Declaration of Human Rights, article 14 of the Rwandan Constitution and principle 6 of the Body of Principles contain a prohibition on torture, cruel or inhuman treatment. Article 14 (3) (g) of the Covenant further prohibits using methods of coercion or duress, including torture and ill-treatment, to extract and use incriminatory confessions. The source claims that, in the present case, the violations further amount to a contravention of the Convention against Torture. The Working Group therefore refers the present case to the Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment for appropriate action.

115. The source alleges that the authorities violated Mr. Rusesabagina's right to humane treatment when they kidnapped and subsequently imprisoned him, held him incommunicado

for three days under circumstances that involved torture, interrogations and physical and mental abuse, and rendered him subject to an enforced disappearance. In addition, the subsequent 260 days of solitary confinement, is allegedly a form of torture because of the severe psychological distress and physical toll that it created.

116. It is alleged that government authorities violated the right of Mr. Rusesabagina to be free from torture, cruel, inhuman or degrading treatment or punishment by their continued denial of proper medical care, including blood pressure medication, despite Mr. Rusesabagina's pre-existing and serious medical conditions.

117. According to the Body of Principles, medical care and treatment shall be provided, whenever necessary, free of charge. In the present case, Mr. Rusesabagina is allegedly in extremely poor health and has taken prescribed medication since 1996.

118. The source claims that the Government is not providing adequate medical treatment for Mr. Rusesabagina's condition, as the authorities are not delivering the prescribed medication, which the Belgian Embassy reportedly provided to the prison authorities. Mr. Rusesabagina has suffered rapid weight loss since his arrest. He suffers from constant high blood pressure, extreme headaches and dizziness. His health has deteriorated to the point that he is at risk of dying from a stroke. The source argues that the Government's denial of adequate medical treatment amounts to a violation of articles 7 and 10 of the Covenant and article 5 of the Universal Declaration of Human Rights. None of these allegations have been rebutted by the Government. The Working Group thus finds that the detention was arbitrary under category III.

Category V

119. The source alleges that the Government is targeting Mr. Rusesabagina because of his expression of political views and in particular for his association with a group politically opposed to the President, his widely published criticism of the Government, his work with intergovernmental and civil society organizations and his anti-genocide advocacy. Mr. Rusesabagina has supported calls for regime change and many opposition groups look to him as a leader.

120. It is clear on the facts that Mr. Rusesabagina has been targeted by the Government on account of his work as a human rights defender, because of his criticism of the Government on a broad range of human rights issues, including unfair elections and a lack of democracy, freedom of speech, freedom of association and freedom of the press. He has also challenged cases of arbitrary detention, torture and extrajudicial killings. He has publicly made allegations of war crimes and crimes against humanity since before the 1994 genocide and especially since 1998. Mr. Rusesabagina's criticisms are echoed on a regular basis by civil society organizations and government agencies, among others. As Mr. Rusesabagina has been targeted on account of his activism as a human rights defender and his political opposition to the Government, his detention is thus discriminatory, contrary to articles 2 (1) and 26 of the Covenant and 2 and 7 of the Universal Declaration of Human Rights, and is considered arbitrary under category V.

Concluding remarks

121. The Working Group has been informed that on 20 September 2021, a court in Kigali rendered a guilty verdict on eight of nine charges against Mr. Rusesabagina and sentenced him to imprisonment for 25 years. Allegedly, the violation of his guarantees of due process, necessary for the defence, continued during the trial, hearings and sentencing. For example, it is reported that the conviction relied upon a confession extracted under duress. Mr. Rusesabagina is now 67 years old and in poor health, so this sentence is allegedly tantamount to a death sentence.

122. The source stresses that the most urgent concern remains Mr. Rusesabagina's health, which requires his immediate humanitarian release. He suffers daily symptoms linked to the deprivation of his prescription heart medication and although he is in remission from cancer, he has not received a cancer screening since his incarceration began. He has recently suffered a swollen arm, which may be a result of a thrombosis. The European Parliament adopted a resolution on 7 October 2021 calling for Mr. Ruseabagina's immediate release.

123. The Working Group wishes to stress that every detainee has the right to the highest attainable standard of physical and mental health. That right extends not only to timely and appropriate health care, but also to underlying determinants of health, such as adequate food, water and sanitation. Moreover, sick prisoners whose health requires specialist treatment should be transferred to specialized institutions or to civil hospitals. The failure to provide access to adequate medical care violates the right to health and risks further human right violations, such as to the right to life.

124. Finally, the Working Group wishes to make it clear that the findings in the present opinion are without prejudice to the allegations that Mr. Rusesabagina was deprived of his liberty in the context of a flight that made a connection layover in the United Arab Emirates.

Disposition

125. In the light of the foregoing, the Working Group renders the following opinion:

> The deprivation of liberty of Paul Rusesabagina, being in contravention of articles 5, 6, 8, 9 and 11 of the Universal Declaration of Human Rights and articles 2, 7, 9, 10, 14, 16, 19 and 21 of the International Covenant on Civil and Political Rights, is arbitrary and falls within categories I, II, III and V.

126. The Working Group requests the Government of Rwanda to take the steps necessary to remedy the situation of Mr. Rusesabagina without delay and bring it into conformity with the relevant international norms, including those set out in the Universal Declaration of Human Rights and the Covenant.

127. The Working Group considers that, taking into account all the circumstances of the case, the appropriate remedy would be to release Mr. Rusesabagina immediately and accord him an enforceable right to compensation and other reparations, in accordance with international law. In the current context of the COVID-19 pandemic and the threat that it poses in places of detention, the Working Group calls upon the Government to take urgent action to ensure the immediate unconditional release of Mr. Rusesabagina.

128. The Working Group urges the Government to ensure a full and independent investigation of the circumstances surrounding the arbitrary deprivation of liberty of Mr. Rusesabagina and to take appropriate measures against those responsible for the violation of his rights.

129. In accordance with paragraph 33 (a) of its methods of work, the Working Group refers the present case to the Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment for appropriate action.

130. The Working Group requests the Government to disseminate the present opinion through all available means and as widely as possible.

Follow-up procedure

131. In accordance with paragraph 20 of its methods of work, the Working Group requests the source and the Government to provide it with information on action taken in follow-up to the recommendations made in the present opinion, including:

(a) Whether Mr. Rusesabagina has been released and, if so, on what date;

(b) Whether compensation or other reparations have been made to Mr. Rusesabagina;

(c) Whether an investigation has been conducted into the violation of Mr. Rusesabagina’s rights and, if so, the outcome of the investigation;

(d) Whether any legislative amendments or changes in practice have been made to harmonize the laws and practices of Rwanda with its international obligations in line with the present opinion;

(e) Whether any other action has been taken to implement the present opinion.

132. The Government is invited to inform the Working Group of any difficulties it may have encountered in implementing the recommendations made in the present opinion and

whether further technical assistance is required, for example through a visit by the Working Group.

133. The Working Group requests the source and the Government to provide the above-mentioned information within six months of the date of transmission of the present opinion. However, the Working Group reserves the right to take its own action in follow-up to the opinion if new concerns in relation to the case are brought to its attention. Such action would enable the Working Group to inform the Human Rights Council of progress made in implementing its recommendations, as well as any failure to take action.

134. The Working Group recalls that the Human Rights Council has encouraged all States to cooperate with the Working Group and has requested them to take account of its views and, where necessary, to take appropriate steps to remedy the situation of persons arbitrarily deprived of their liberty, and to inform the Working Group of the steps they have taken.[17]

[*Adopted on 19 November 2021*]

[17] See Human Rights Council resolution 42/22, paras. 3 and 7.

UNIVERSITY OF TORONTO

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

CID# 9703

Date: 17 June, 2022
Memo: The targeting of Carine Kanimba with Pegasus spyware
Prepared by: The Citizen Lab
Prepared for: Carine Kanimba

This memorandum is prepared for Carine Kanimba at her request and with her consent. It confirms that our forensic analysis of digital artifacts on Carine Kanimba's Apple device ("Carine Kanimba's device")[1] *indicates that at least one of her devices was compromised with Pegasus spyware. Pegasus spyware is made by NSO Group.*

Background

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

The Citizen Lab's research mandate includes tracking digital threats against civil society actors, as well as tracking the proliferation of the mercenary spyware industry. As part of the Citizen Lab's investigations into the mercenary spyware industry, the Citizen Lab has developed the ability to identify evidence of device compromise with Pegasus spyware.

Confirming the infection of Carine Kanimba with NSO Group's Pegasus spyware

Citizen Lab researchers analyzed forensic artifacts from Carine Kanimba's device and obtained a positive result, which indicates that at least one device belonging to her was targeted and infected with NSO Group's Pegasus spyware. Our analysis indicates that she was infected with Pegasus spyware in the following approximate time periods:

1. Sometime 2020-09-12 - 2020-09-20

[1] The device with serial number ******EN72Q

2. Sometime 2020-09-20 - 2020-09-28
3. Sometime 2020-09-29 - 2020-10-02
4. Sometime 2020-10-02 - 2020-10-06
5. Sometime 2020-10-06 - 2020-10-12
6. On or around 2020-10-12
7. Sometime 2020-10-12 - 2020-10-21
8. Sometime 2020-10-21 - 2020-10-26
9. On or around 2020-10-29
10. Sometime 2020-11-04 - 2020-11-11
11. Sometime 2020-11-11 - 2020-11-17
12. Sometime 2020-11-17 - 2020-11-20
13. Sometime 2020-11-20 - 2020-11-22
14. Sometime 2021-01-29 - 2021-02-02
15. Sometime 2021-02-10 - 2021-02-15
16. Sometime 2021-03-16 - 2021-03-24
17. Sometime 2021-03-24 - 2021-03-30
18. Sometime 2021-03-30 - 2021-04-02
19. Sometime 2021-04-06 - 2021-04-10
20. Sometime 2021-04-22 - 2021-04-25
21. On or around 2021-04-25
22. On or around 2021-04-26
23. On or around 2021-04-27

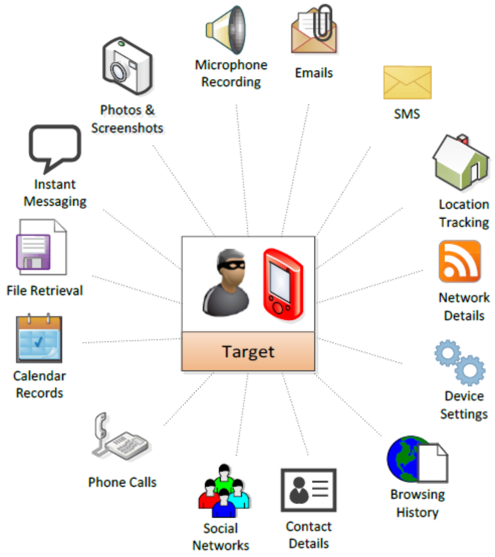
This does not preclude the possibility of other infections.

What a successful infection with Pegasus spyware can do

Pegasus is a surveillance tool that provides its operator complete access to a target's mobile device. Pegasus allows the operator to extract passwords, files, photos, web history, contacts, as well as identity data (such as information about the mobile device).

Pegasus can take screen captures, and monitor user inputs, as well as activating a telephone's microphone and camera. This enables attackers to monitor all activity on the device and in the vicinity of the device, such as conversations conducted in a room.

Pegasus also allows the operator to record chat messages as they are sent and received (including messages sent through "encrypted" / disappearing-message-enabled texting apps like WhatsApp or Telegram), as well as phone and VoIP calls (including calls through "encrypted" calling apps).



NSO marketing material showing some of what Pegasus can monitor on a target's device.
Source: NSO Marketing Materials

For some chat programs, Pegasus also supports the extraction of past message logs. Pegasus also allows the operator to track the target's location. As with any infection, spyware may also allow for the modification or manipulation of data on a device.

Additionally, Pegasus spyware may be used to steal tokens allowing for persistent access to popular cloud accounts.

CID# 9703

More information about NSO Group and its Pegasus spyware

Pegasus spyware is sold and marketed by NSO Group (which goes by the name Q Cyber Technologies, as well as other names). NSO Group is an Israeli-based company which develops and sells spyware technology, including Pegasus.[2] NSO Group is majority-owned by Novalpina Capital, a European private equity firm based in London.[3]

NSO Group claims it sells its spyware strictly to government clients only and that all of its exports are undertaken in accordance with Israeli government export laws and oversight mechanisms. NSO Group also claims to abide by a human rights policy. However, the number of documented cases in which their technology is used abusively to target civil society continues to grow.

You can review Citizen Lab research into NSO Group at this website: https://citizenlab.ca/tag/nso-group/

[2] Note that in specific transactions for this technology, the Pegasus spyware may be given other codenames.
[3] For more information on NSO Group, you can find a summary of key public reporting here. Further, exhibits filed in the ongoing litigation between WhatsApp/Facebook and NSO Group in the United States provide insight into Pegasus' functions and NSO Group's operations (see, in particular, Exhibit 10 of the complaint).

FORENSIC METHODOLOGY REPORT

HOW TO CATCH NSO GROUP'S PEGASUS

INTRODUCTION

NSO Group claims that its Pegasus spyware is only used to "investigate terrorism and crime" and "leaves no traces whatsoever". This Forensic Methodology Report shows that neither of these statements are true. This report accompanies the release of the Pegasus Project, a collaborative investigation that involves more than 80 journalists from 17 media organizations in 10 countries coordinated by Forbidden Stories with technical support of Amnesty International's Security Lab.[1]

Amnesty International's Security Lab has performed in-depth forensic analysis of numerous mobile devices from human rights defenders (HRDs) and journalists around the world. This research has uncovered widespread, persistent and ongoing unlawful surveillance and human rights abuses perpetrated using NSO Group's Pegasus spyware.

As laid out in the UN Guiding Principles on Business and Human Rights, NSO Group should urgently take pro-active steps to ensure that it does not cause or contribute to human rights abuses within its global operations, and to respond to any human rights abuses when they do occur. In order to meet that responsibility, NSO Group must carry out adequate human rights due diligence and take steps to ensure that HRDs and journalists do not continue to become targets of unlawful surveillance.

In this Forensic Methodology Report, Amnesty International is sharing its methodology and publishing an open-source mobile forensics tool and detailed technical indicators, in order to assist information security researchers and civil society with detecting and responding to these serious threats.

This report documents the forensic traces left on iOS and Android devices following targeting with the Pegasus spyware. This includes forensic records linking recent Pegasus infections back to the 2016 Pegasus payload used to target the HRD Ahmed Mansoor.

The Pegasus attacks detailed in this report and accompanying appendices are from 2014 up to as recently as July 2021. These also include so-called "zero-click" attacks which do not require any interaction from the target. Zero-click attacks have been observed since May 2018 and continue until now. Most recently, a successful "zero-click" attack has been observed

[1] The technical evidence provided in the report includes the forensic research carried out as part of the Pegasus Project as well as additional Amnesty International Security Lab research carried out since the establishment of the Security Lab in 2018.

exploiting multiple zero-days to attack a fully patched iPhone 12 running iOS 14.6 in July 2021.
Sections 1 to 8 of this report outline the forensic traces left on mobile devices following a Pegasus infection. This evidence has been collected from the phones of HRDs and journalists in multiple countries.

Finally, in section 9 the report documents the evolution of the Pegasus network infrastructure since 2016. NSO Group has redesigned their attack infrastructure by employing multiple layers of domains and servers. Repeated operational security mistakes have allowed the Amnesty International Security Lab to maintain continued visibility into this infrastructure. We are publishing a set of 700 Pegasus-related domains.

Names of several of the civil society targets in the report have been anonymized for safety and security reasons. Individuals who have been anonymized have been assigned an alphanumeric code name in this report.

1. DISCOVERING PEGASUS NETWORK INJECTION ATTACKS

Amnesty International's technical investigation into NSO Group's Pegasus intensified following our discovery of the targeting of an Amnesty International staffer and a Saudi activist, Yahya Assiri, in 2018. Amnesty International's Security Lab began refining its forensics methodology through the discovery of attacks against HRDs in Morocco in 2019, which were further corroborated by attacks we discovered against a Moroccan journalist in 2020. In this first section we detail the process which led to the discovery of these compromises.
Numerous public reports had identified NSO Group's customers using SMS messages with Pegasus exploit domains over the years. As a result, similar messages emerged from our analysis of the phone of Moroccan activist Maati Monjib, who was one of the activists targeted as documented in Amnesty International's 2019 report.

However, on further analysis we also noticed suspicious redirects recorded in Safari's browsing history. For example, in one case we noticed a redirect to an odd-looking URL after Maati Monjib attempted to visit Yahoo:

Visit ID	Date (UTC)	URL	Redirect Source	Redirect Destination
16119	2019-07-22 17:42:32.475	http://yahoo.fr/	null	16120
16120	2019-07-22 17:42:32.478	https://bun54l2b67.get1tn0w.free247downloads[.]com:30495/szev4hz	16119	null

(**Please note**: throughout this document we escaped malicious domains with the marking *[.]* to prevent accidental clicks and visits.)

The URL **https://bun54l2b67.get1tn0w.free247downloads[.]com:30495/szev4hz** immediately appeared suspicious, particularly because of the presence of a 4th level subdomain, a non-standard high port number, and a random URI similar to links contained in SMS messages previously documented in connection to NSO Group's Pegasus. As you can see in the table above, the visit to Yahoo was immediately redirected to this suspicious URL with database ID 16120.

In our October 2019 report, we detail how we determined these redirections to be the result of network injection attacks performed either through tactical devices, such as rogue cell towers, or through dedicated equipment placed at the mobile operator. When months later we analysed the iPhone of Moroccan independent journalist Omar Radi, who as documented in our 2020 report was targeted, we found similar records involving the **free247downloads[.]com** domain as well.

In November 2019, after Amnesty International's initial report, a new domain **urlpush[.]net** was registered. We found it subsequently involved in similar redirects to the URL **https://gnyjv1xltx.info8fvhgl3.urlpush[.]net:30875/zrnv5revj.**

Although Safari history records are typically short lived and are lost after a few months (as well as potentially intentionally purged by malware), we have been able to nevertheless find NSO Group's infection domains in other databases of Omar Radi's phone that did not appear in Safari's History. For example, we could identify visits through Safari's **Favicon.db** database, which was left intact by Pegasus:

Date (UTC)	URL	Icon URL
2019-02-11 14:45:53	https://d9z3sz93x5ueidq3.get1tn0w.free247downloads[.]com:30897/rdEN5YP	https://d9z3sz93x5ueidq3.get1tn0w.free247downloads[.]com:30897/favicon.ico
2019-09-13 17:01:38	https://2far1v4lv8.get1tn0w.free247downloads[.]com:31052/meunsnyse#011356570257117296834845704022338973133022433397236	https://2far1v4lv8.get1tn0w.free247downloads[.]com:31052/favicon.ico
2019-09-13 17:01:56	https://2far1v4lv8.get1tn0w.free247downloads[.]com:31052/meunsnyse#068099561614626278519925358638789161572427833645389	https://2far1v4lv8.get1tn0w.free247downloads[.]com:31052/favicon.ico
2020-01-17 11:06:32	https://gnyjv1xltx.info8fvhgl3.urlpush[.]net:30875/zrnv5revj#074196419827987919274001548622738919835556748325946%2324	https://gnyjv1xltx.info8fvhgl3.urlpush[.]net:30875/favicon.ico
2020-01-27 11:06:24	https://gnyjv1xltx.info8fvhgl3.urlpush[.]net:30875/zrnv5revj#074196419827987919274001548622738919835556748325946	https://gnyjv1xltx.info8fvhgl3.urlpush[.]net:30875/favicon.ico

As explained in the Technical Appendix of our 2020 report on Pegasus attacks in Morocco, these redirects do not only happen when the target is navigating the Internet with the browser app, but also when using other apps. For example, in one case Amnesty International identified a network injection while Omar Radi was using the Twitter app. When previewing a link shared in his timeline, the service com.apple.SafariViewService was invoked to load a Safari WebView, and a redirect occurred.

Because of this, we can find additional records involving the domains free247downloads[.]com and urlpush[.]net in app-specific WebKit local storage, IndexedDB folders, and more. In multiple cases IndexedDB files were created by Safari shortly after the network injection redirect to the Pegasus Installation Server.

In addition, Safari's Session Resource logs provide additional traces that do not consistently appear in Safari's browsing history. It appears Safari does not record full redirect chains, and might only keep history records showing the final page that was loaded. Session Resource logs recovered from the analysed phones demonstrate that additional staging domains are used as trampolines eventually leading to the infection servers. In fact, these logs reveal that the very first network injection against Maati Monjib we describe at the beginning of this post also involved the domain documentpro[.]org:

Redirect Source	Origin	Redirect Destination
yahoo.fr	documentpro[.]org	free247downloads[.]com

Maati Monjib visited http://yahoo.fr, and a network injection forcefully redirected the browser to documentpro[.]org before further redirecting to free247downloads[.]com and proceed with the exploitation.

Similarly, on a different occasion Omar Radi visited the website of French newspaper Le Parisien, and a network injection redirected him through the staging domain tahmilmilafate[.]com and then eventually to free247downloads[.]com as well. We also saw tahmilmilafate[.]info used in the same way:

Redirect Source	Origin	Redirect Destination
leparisien.fr	tahmilmilafate[.]com	free247downloads[.]com

In the most recent attempts Amnesty International observed against Omar Radi in January 2020, his phone was redirected to an exploitation page at gnyjv1xltx.info8fvhgl3.urlpush[.]net passing through the domain baramije[.]net. The domain baramije[.]net was registered one day before urlpush[.]net, and a decoy website was set up using the open source Textpattern CMS.

Traces of network activity were not the only available indicators of compromise, and further inspection of the iPhones revealed executed processes which eventually led to the establishment of a consistent pattern unique to all subsequent iPhones that Amnesty International analysed and found to be infected.

2. PEGASUS' BRIDGEHEAD AND OTHER MALICIOUS PROCESSES APPEAR

Amnesty International, Citizen Lab, and others have primarily attributed Pegasus spyware attacks based on the domain names and other network infrastructure used to deliver the attacks. However, forensic evidence left behind by the Pegasus spyware provides another independent way to attribute these attacks to NSO Group's technology.

iOS maintains records of process executions and their respective network usage in two SQLite database files called "*DataUsage.sqlite*" and "*netusage.sqlite*" which are stored on the device. It is worth noting that while the former is available in iTunes backup, the latter is not. Additionally, it should be noted that only processes that performed network activity will appear in these databases.

Both Maati Monjib's and Omar Radi's network usage databases contained records of a suspicious process called "**bh**". This "bh" process was observed on multiple occasions immediately following visits to Pegasus Installation domains.

Maati Monjib's phone has records of execution of "bh" from April 2018 until March 2019:

Fist date (UTC)	Last date (UTC)	Process Name	WWAN IN	WWAN OUT	Process ID
2018-04-29 00:25:12	2019-03-27 22:45:10	bh	3319875.0	144443.0	59472

Amnesty International found similar records on Omar Radi's phone between February and September 2019:

Fist date (UTC)	Last date (UTC)	Process Name	WWAN IN	WWAN OUT	Process ID
2019-02-11 14:45:56	2019-09-13 17:02:11	bh	3019409.0	147684.0	50465

The last recorded execution of "bh" occurred a few seconds after a successful network injection (as seen in the favicon records listed earlier at 2019-09-13 17:01:56).

Crucially, we find references to "bh" in the Pegasus iOS sample recovered from the 2016 attacks against UAE human rights defender Ahmed Mansoor, discovered by Citizen Lab and analysed in depth by cybersecurity firm Lookout.

As described in Lookout's analysis, in 2016 NSO Group leveraged a vulnerability in the iOS JavaScriptCore Binary (jsc) to achieve code execution on the device. This same vulnerability was also used to maintain persistence on the device after reboot. We find references to "bh" throughout the exploit code:

```
var compressed_bh_addr =  shellcode_addr_aligned + shellcode32.byteLength;
replacePEMagics(shellcode32, dlsym_addr, compressed_bh_addr,
bundle.bhCompressedByteLength);
storeU32Array(shellcode32, shellcode_addr);
storeU32Array(bundle.bhCompressed32, compressed_bh_addr);
```

This module is described in Lookout's analysis as follows:

"bh.c - Loads API functions that relate to the decompression of next stage payloads and their proper placement on the victim's iPhone by using functions such as BZ2_bzDecompress, chmod, and malloc"

Lookout further explains that a configuration file located at /var/tmp/jb_cfg is dropped alongside the binary. Interestingly, we find the path to this file exported as **_kBridgeHeadConfigurationFilePath** in the libaudio.dylib file part of the Pegasus bundle:

```
__const:0001AFCC                EXPORT _kBridgeHeadConfigurationFilePath
__const:0001AFCC _kBridgeHeadConfigurationFilePath DCD cfstr_VarTmpJb_cfg ;
"/var/tmp/jb_cfg"
```

Therefore, we suspect that **"bh" might stand for "BridgeHead"**, which is likely the internal name assigned by NSO Group to this component of their toolkit.

The appearance of the "bh" process right after the successful network injection of Omar Radi's phone is consistent with the evident purpose of the BridgeHead module. It completes the browser exploitation, roots the device and prepares for its infection with the full Pegasus suite.

2.1 ADDITIONAL SUSPICIOUS PROCESSES FOLLOWING BRIDGEHEAD

The **bh** process first appeared on Omar Radi's phone on 11 February 2019. This occurred 10 seconds after an IndexedDB file was created by the Pegasus Installation Server and a favicon entry was recorded by Safari. At around the same time the file *com.apple.CrashReporter.plist file* was written in */private/var/root/Library/Preferences/*, likely to disable reporting of crash logs back to Apple. The exploit chain had obtained root permission at this stage.

Less than a minute later a "**roleaboutd**" process first appears.

Date (UTC)	Event
2019-02-11 14:45:45	IndexedDB record for URL https_d9z3sz93x5ueidq3.get1tn0w.free247downloads.com_30897/
2019-02-11 14:45:53	Safari Favicon record for URL hxxps//d9z3sz93x5ueidq3.get1tn0w.**free247downloads[.]com**:30897/rdEN5YP
2019-02-11 14:45:54	Crash reporter disabled by writing ***com.apple.CrashReporter.plist***
2019-02-11 14:45:56	Process: **bh**
2019-02-11 14:46:23	Process: **roleaboutd** first
2019-02-11 17:05:24	Process: **roleaboutd** last

Omar Radi's device was exploited again on the 13 September 2019. Again a "**bh**" process started shortly afterwards. Around this time the *com.apple.softwareupdateservicesd.plist* file was modified. A "**msgacntd**" process was also launched.

Date (UTC)	Event

2019-09-13 17:01:38	Safari Favicon record for URL hxxps://2far1v4lv8.get1tn0w.**free247downloads[.]com**:31052/meunsnyse
2019-09-13 17:02:11	Process: **bh**
2019-09-13 17:02:33	Process: **msgacntd** first
2019-09-13 17:02:35	File modified: **com.apple.softwareupdateservicesd.plist**
2019-09-14 20:51:54	Process: **msgacntd** last

Based on the timing and context of exploitation, Amnesty International believes the **roleaboutd** and **msgacntd** processes are a later stage of the Pegasus spyware which was loaded after a successful exploitation and privilege escalation with the **BridgeHead payload**.
Similarly, the forensic analysis of Maati Monjib's phone revealed the execution of more suspicious processes in addition to **bh**. A process named **pcsd** and one named **fmld** appeared in 2018:

Fist date	Last date	Process Name	WWAN IN	WWAN OUT	Process ID
2018-05-04 23:30:45	2018-05-04 23:30:45	pcsd	12305.0	10173.0	14946
2018-05-21 23:46:06	2018-06-4 13:05:43	fmld	0.0	188326.0	21207

Amnesty International verified that no legitimate binaries of the same names were distributed in recent versions of iOS.

The discovery of these processes on Omar Radi's and Maati Monjib's phones later became instrumental for Amnesty International's continued investigations, as we found processes with the same names on devices of targeted individuals from around the world.

3. PEGASUS PROCESSES FOLLOWING POTENTIAL APPLE PHOTOS EXPLOITATION

During Amnesty International's investigations as part of The Pegasus Project we discovered additional cases where the above mentioned "bh" process was recorded on devices compromised through different attack vectors.

In one instance, the phone of a French human rights lawyer (CODE: FRHRL1) was compromised and the "bh" process was executed seconds after network traffic for the iOS Photos app (*com.apple.mobileslideshow*) was recorded for the first time. Again, after a successful exploitation, crash reporting was disabled by writing a *com.apple.CrashReporter.plist* file to the device.

2019-10-29 09:04:32	Process: mobileslideshow/com.apple.mobileslideshow first
2019-10-29 09:04:58	Process: **bh**
2019-10-29 09:05:08	com.apple.CrashReporter.plist dropped
2019-10-29 09:05:53	Process: **mptbd**

The next and last time network activity for the iOS Photos app was recorded was on 18 December 2019, again preceding the execution of malicious processes on the device.

2019-12-18 08:13:33	Process: mobileslideshow/com.apple.mobileslideshow last
2019-12-18 08:13:47	Process: bh
2019-12-18 11:50:15	Process: ckeblld

In a separate case, we identified a similar pattern with the "mobileslideshow" and "bh" processes on the iPhone of a French journalist (CODE: FRJRN1) in May 2020:

2020-05-24 15:44:21	Process: mobileslideshow/com.apple.mobileslideshow first
2020-05-24 15:44:39	Process: bh
2020-05-24 15:46:51	Process: fservernetd
	...
2020-05-27 16:58:31	Process: mobileslideshow/com.apple.mobileslideshow last
2020-05-27 16:58:52	Process: bh
2020-05-27 18:00:50	Process: ckkeyrollfd

Amnesty International was not able to capture payloads related this exploitation but suspects that the iOS Photos app or the Photostream service were used as part of an exploit chain to deploy Pegasus. The apps themselves may have been exploited or their functionality misused to deliver a more traditional JavaScript or browser exploit to the device.

As you can see from the tables above, additional process names such as mptbd, ckeblld, fservernetd, and ckkeyrollfd appear right after bh. As with fmld and pcsd, Amnesty International believes these to be additional payloads downloaded and executed after a successful compromise. As our investigations progressed, we identified dozens of malicious process names involved in Pegasus infections.

Additionally, Amnesty International found the same iCloud account bogaardlisa803[@]gmail.com recorded as linked to the "com.apple.private.alloy.photostream" service on both devices. Purposefully created iCloud accounts seem to be central to the delivery of multiple "zero-click" attack vectors in many recent cases of compromised devices analysed by Amnesty International.

4. AN iMESSAGE ZERO-CLICK 0DAY USED WIDELY IN 2019

While SMS messages carrying malicious links were the tactic of choice for NSO Group's customers between 2016 and 2018, in more recent years they appear to have become increasingly rare. The discovery of network injection attacks in Morocco signalled that the attackers' tactics were indeed changing. Network injection is an effective and cost-efficient attack vector for domestic use especially in countries with leverage over mobile operators. However, while it is only effective on domestic networks, the targeting of foreign targets or of individuals in diaspora communities also changed.

From 2019 an increasing amount of vulnerabilities in iOS, especially iMessage and FaceTime, started getting patched thanks to their discoveries by vulnerability researchers, or to cybersecurity vendors reporting exploits discovered in-the-wild.

In response, Amnesty International extended its forensic methodology to collect any relevant traces by iMessage and FaceTime. iOS keeps a record of Apple IDs seen by each installed application in a plist file located at */private/var/mobile/Library/Preferences/com.apple.identityservices.*idstatuscache*.plist*. This file is also typically available in a regular iTunes backup, so it can be easily extracted without the need of a jailbreak.

These records played critical role in later investigations. In many cases we discovered suspected Pegasus processes executed on devices immediately following suspicious iMessage account lookups. For example, the following records were extracted from the phone of a French journalist (CODE FRJRN2):

2019-06-16 12:08:44	Lookup of bergers.o79@gmail.com by com.apple.madrid (iMessage)
2019-08-16 12:33:52	Lookup of bergers.o79@gmail\x00\x00om by com.apple.madrid (iMessage)
2019-08-16 12:37:55	The file *Library/Preferences/com.apple.CrashReporter.plist* is created within RootDomain
2019-08-16 12:41:25	The file *Library/Preferences/roleaccountd.plist* is created within RootDomain
2019-08-16 12:41:36	Process: roleaccountd
2019-08-16 12:41:52	Process: stagingd
2019-08-16 12:49:21	Process: aggregatenotd

Amnesty International's forensic analysis of multiple devices found similar records. In many cases the same iMessage account reoccurs across multiple targeted devices, potentially indicating that those devices have been targeted by the same operator. Additionally, the processes roleaccountd and stagingd occur consistently, along with others.

For example, the iPhone of a Hungarian journalist (CODE HUJRN1) subsequent the following records:

2019-09-24 13:26:15	Lookup of jessicadavies1345@outlook.com by com.apple.madrid (iMessage)
2019-09-24 13:26:51	Lookup of emmadavies8266@gmail.com by com.apple.madrid (iMessage)
2019-09-24 13:32:10	Process: roleaccountd
2019-09-24 13:32:13	Process: stagingd

In this case, the first suspicious processes performing some network activity were recorded 5 minutes after the first lookup. The *com.apple.CrashReporter.plist* file was already present on this device after a previous successful infection and was not written again.

The iPhone of yet another Hungarian journalist (CODE HUJRN2) show lookups for the same iMessage accounts along with numerous other processes along with roleaccountd and stagingd:

2019-07-15 12:01:37	Lookup of mailto:e\x00\x00adavies8266@gmail.com by com.apple.madrid (iMessage)
2019-07-15 14:21:40	Process: accountpfd
2019-08-29 10:57:43	Process: roleaccountd
2019-08-29 10:57:44	Process: stagingd
2019-08-29 10:58:35	Process: launchrexd
2019-09-03 07:54:26	Process: roleaccountd
2019-09-03 07:54:28	Process: stagingd
2019-09-03 07:54:51	Process: seraccountd
2019-09-05 13:26:38	Process: seraccountd
2019-09-05 13:26:55	Process: misbrigd
2019-09-10 06:09:04	Lookup of emmadavies8266@gmail.com by com.apple.madrid (iMessage)
2019-09-10 06:09:47	Lookup of jessicadavies1345@outlook.com by com.apple.madrid (iMessage)
2019-10-30 14:09:51	Process: nehelprd

It is interesting to note that in the traces Amnesty International recovered from 2019, the iMessage lookups that immediately preceded the execution of suspicious processes often contained two-bytes 0x00 padding in the email address recorded by the ID Status Cache file.

5. APPLE MUSIC LEVERAGED TO DELIVER PEGASUS IN 2020

In mid-2021 Amnesty International identified yet another case of a prominent investigative journalist from Azerbaijan (CODE AZJRN1) who was repeatedly targeted using Pegasus zero-click attacks from 2019 until mid-2021.

Yet again, we found a similar pattern of forensic traces on the device following the first recorded successful exploitation:

2019-03-28 07:43:14	File: Library/Preferences/com.apple.CrashReporter.plist from RootDomain
2019-03-28 07:44:03	File: Library/Preferences/roleaccountd.plist from RootDomain
2019-03-28 07:44:14	Process: roleaccountd
2019-03-28 07:44:14	Process: stagingd

Interestingly we found signs of a new iOS infection technique being used to compromise this device. A successful infection occurred on 10th July 2020:

2020-07-06 05:22:21	Lookup of f\x00\x00ip.bl82@gmail.com by iMessage (com.apple.madrid)
2020-07-10 14:12:09	Pegasus request by Apple Music app: https://x1znqjo0x8b8j.php78mp9v.opposedarrangement[.]net:37271/afAVt89Wq/stadium/pop2.html?key=501_4&n=7

2020-07-10 14:12:21	Process: roleaccountd
2020-07-10 14:12:53	Process: stagingd
2020-07-13 05:05:17	Pegasus request by Apple Music app: https://4n3d9ca2st.php78mp9v.opposedarrangement[.]net:37891/w58Xp5Z/stadium/pop2.html?key=501_4&n=7

Shortly before Pegasus was launched on the device, we saw network traffic recorded for the Apple Music service. These HTTP requests were recovered from a network cache file located at */private/var/mobile/Containers/Data/Application/D6A69566-55F7-4757-96DE-EBA612685272/Library/Caches/com.apple.Music/Cache*.db which we retrieved by jailbreaking the device.

Amnesty International cannot determine from forensics if Apple Music was itself exploited to deliver the initial infection or if instead, the app was abused as part of a sandbox escape and privilege escalation chain. Recent research has shown that built-in apps such as the iTunes Store app can be abused to run a browser exploit while escaping the restrictive Safari application sandbox.

Most importantly however, the HTTP request performed by the Apple Music app points to the domain opposedarrangement[.]net, which we had previously identified as belonging to NSO Group's Pegasus network infrastructure. This domain matched a distinctive fingerprint we devised while conducting Internet-wide scans following our discovery of the network injection attacks in Morocco (see section 9).

In addition, these URLs show peculiar characteristics typical of other URLs we found involved in Pegasus attacks through the years, as explained in the next section.

6. MEGALODON: IMESSAGE ZERO-CLICK 0-DAYS RETURN IN 2021

The analysis Amnesty International conducted of several devices reveal traces of attacks similar to those we observed in 2019. These attacks have been observed as recently as July 2021. Amnesty International believes Pegasus is currently being delivered through zero-click exploits which remain functional through the latest available version of iOS at the time of writing (July 2021).

On the iPhone of a French human rights lawyer (CODE FRHRL2), we observed a lookup of a suspicious iMessage account unknown to the victim, followed by an HTTP request performed by the com.apple.coretelephony process. This is a component of iOS involved in all telephony-related tasks and likely among those exploited in this attack. We found traces of this HTTP request in a cache file stored on disk at */private/var/wireless/Library/Caches/com.apple.coretelephony/Cache.db* containing metadata on the request and the response. The phone sent information on the device including the model 9,1 (iPhone 7) and iOS build number 18C66 (version 14.3) to a service fronted by Amazon CloudFront, suggesting NSO Group has switched to using AWS services in recent months. At the time of this attack, the newer iOS version 14.4 had only been released for a couple of weeks.

Date (UTC)	Event
2021-02-08 10:42:40	Lookup of linakeller2203@gmail.com by iMessage (com.apple.madrid)
2021-02-08 11:27:10	com.apple.coretelephony performs an HTTP request to https://d38j2563clgblt.cloudfront[.]net/fV2GsPXgW//stadium/megalodon?m=iPhone9,1&v=18C66
2021-02-08 11:27:21	Process: gatekeeperd
2021-02-08 11:27:22	gatekeeperd performs an HTTP request to https://d38j2563clgblt.cloudfront.net/fV2GsPXgW//stadium/wizard/01-00000000
2021-02-08 11:27:23	Process: gatekeeperd

The *Cache.db* file for com.apple.coretelephony contains details about the HTTP response which appeared to have been a download of ~250kb of binary data. Indeed, we found the downloaded binary in the *fsCachedData* sub-folder, but it was unfortunately encrypted. Amnesty International believes this to be the payload launched as gatekeeperd.

Amnesty International subsequently analysed the iPhone of a journalist (CODE MOJRN1), which contained very similar records. This device was exploited repeatedly on numerous times between February and April 2021 and across iOS releases. The most recent attempt showed the following indicators of compromise:

Date (UTC)	Event
2021-04-02 10:15:38	Lookup of linakeller2203@gmail.com by iMessage (com.apple.madrid)
2021-04-02 10:36:00	com.apple.coretelephony performs an HTTP request to https://d38j2563clgblt.cloudfront[.]net/dMx1hpK//stadium/megalodon?m=iPhone8,1&v=18D52&u=[REDACTED]
2021-04-02 10:36:08	Process PDPDialogs performs an HTTP request to https://d38j2563clgblt.cloudfront[.]net/dMx1hpK//stadium/wizard/ttjuk
2021-04-02 10:36:16	Process PDPDialogs performs an HTTP request to https://d38j2563clgblt.cloudfront[.]net/dMx1hpK//stadium/wizard/01-00000000
2021-04-02 10:36:16	com.apple.coretelephony performs an HTTP request to https://d38j2563clgblt.cloudfront[.]net/dMx1hpK//stadium/wizard/cszjcft=frzaslm
2021-04-02 10:36:35	Process: gatekeeperd
2021-04-02 10:36:45	Process: rolexd

As is evident, the same iMessage account observed in the previous separate case was involved in this exploitation and compromise months later. The same CloudFront website was contacted by *com.apple.coretelephony* and the additional processes executed, downloaded and launched additional malicious components.

The initial check-in indicates the compromised iPhone 6s was running iOS 14.4 (build number 18D52) at the time of the attack. Although versions 14.4.1 and 14.4.2 were already available then, they only addressed vulnerabilities in WebKit, so it is safe to assume the vulnerability leveraged in these iMessage attacks was exploited as a 0-day.

It is worth noting that among the many other malicious process names observed executed on this phone we see msgacntd, which we also found running on Omar Radi’s phone in 2019, as documented earlier.

In addition, it should be noted that the URLs we have observed used in attacks throughout the last three years show a consistent set of patterns. This supports Amnesty International’s analysis that all three URLs are in fact components of Pegasus customer attack infrastructure. The Apple Music attack from 2020 shows the same 4th level domain structure and non-standard high port number as the 2019 network injection attack. Both the free247downloads[.]com and opposedarrangements[.]net domains matched our Pegasus V4 domain fingerprint.

Additionally, the Apple Music attack URL and the 2021 Megaladon attack URLs share a distinctive pattern. Both URL paths start with a random identifier tied to the attack attempt followed by the word "stadium".

Attack	URL
Network injection (2019)	https://2far1v4lv8.get1tn0w.free247downloads[.]com:31052/meunsnyse
Apple Music attack (2020)	https://4n3d9ca2st.php78mp9v.opposedarrangement[.]net:37891/w58Xp5Z/stadium/pop2.html?key=501_4&n=7
iMessage zero-click (2021)	https://d38j2563clgblt.cloudfront[.]net/dMx1hpK//stadium/wizard/ttjuk

Amnesty International reported this information to Amazon, who informed us they *“acted quickly to shut down the implicated infrastructure and accounts”*.[2]

The iPhone 11 of a French human rights activist (CODE FRHRD1) also showed an iMessage look-up for the account linakeller2203[@]gmail.com on June 11th 2021 and malicious processes afterwards. The phone was running iOS 14.4.2 and was upgraded to 14.6 the following day.

Most recently, Amnesty International has observed evidence of compromise of the iPhone XR of an Indian journalist (CODE INJRN1) running iOS 14.6 (latest available at the time of writing) as recently as 16th June 2021. Lastly, Amnesty International has confirmed an active infection of the iPhone X of an activist (CODE RWHRD1) on June 24th 2021, also running iOS 14.6. While we have not been able to extract records from Cache.db databases due to the inability to jailbreak these two devices, additional diagnostic data extracted from these iPhones show numerous iMessage push notifications immediately preceding the execution of Pegasus processes.

[2] Email to Amnesty International, May 2021

The device of a Rwandan activist (CODE RWHRD1) shows evidence of multiple successful zero-click infections in May and June 2021. We can see one example of this on 17 May 2021. An unfamiliar iMessage account is recorded and in the following minutes at least 20 iMessage attachment chunks are created on disk.

Date (UTC)	Event
2021-05-17 13:39:16	Lookup for iCloud account **benjiburns8[@]gmail.com** (iMessage)
2021-05-17 13:40:12	File: /private/var/mobile/Library/SMS/Attachments/dc/12/DEAE6789-0AC4-41A9-A91C-5A9086E406A5/.eBDOuIN1wq.gif-2hN9
2021-05-17 13:40:21	File: /private/var/mobile/Library/SMS/Attachments/41/01/D146B32E-CA53-41C5-BF61-55E0FA6F5FF3/.TJi3fIbHYN.gif-bMJq
...	...
2021-05-17 13:44:19	File: /private/var/mobile/Library/SMS/Attachments/42/02/45F922B7-E819-4B88-B79A-0FEE289701EE/.v74ViRNkCG.gif-V678

Amnesty International found no evidence that the 17 May attack was successful. Later attacks on the 18 June and 23 June were successful and led to Pegasus payloads being deployed on the device.
Initially, many iMessage (com.apple.madrid) push notifications were received, and attachment chunks were written to disk. The following table show a sample of the 48 attachment files found on the filesystem.

Date (UTC)	Event
2021-06-23 20:45:00	8 push notifications for topic com.apple.madrid (iMessage)
2021-06-23 20:46:00	46 push notifications for topic com.apple.madrid (iMessage)
2021-06-23 20:46:19	File: /private/var/tmp/com.apple.messages/F803EEC3-AB3A-4DC2-A5F1-9E39D7A509BB/.cs/ChunkStoreDatabase
2021-06-23 20:46:20	File: /private/var/mobile/Library/SMS/Attachments/77/07/4DFA8939-EE64-4CB5-A111-B75733F603A2/.8HfhwBP5qJ.gif-u0zD
...	...
2021-06-23 20:53:00	17 push notifications for topic com.apple.madrid (iMessage)
2021-06-23 20:53:54	File: /private/var/tmp/com.apple.messages/50439EF9-750C-4449-B7FC-851F28BD3BD3/.cs/ChunkStoreDatabase
2021-06-23 20:53:54	File: /private/var/mobile/Library/SMS/Attachments/36/06/AA10C840-1776-4A51-A547-BE78A3754773/.7bb9OMWUa8.gif-UAPo
2021-06-23 20:54:00	54 push notifications for topic com.apple.madrid (iMessage)

A process crash occurred at 20:48:56 which resulted in the **ReportCrash** process starting followed by restarts of multiple processes related to iMessage processing:

Date (UTC)	Event
2021-06-23 20:48:56	Process with PID 1192 and name ReportCrash
2021-06-23 20:48:56	Process with PID 1190 and name IMTransferAgent

2021-06-23 20:48:56	Process with PID 1153 and name SCHelper
2021-06-23 20:48:56	Process with PID 1151 and name CategoriesService
2021-06-23 20:48:56	Process with PID 1147 and name MessagesBlastDoorService
2021-06-23 20:48:56	Process with PID 1145 and name NotificationService

A second set of crashes and restarts happened five minutes later. The **ReportCrash** process was started along with processes related to parsing of iMessage content and iMessage custom avatars.

Date (UTC)	Event
2021-06-23 20:54:16	Process with PID 1280 and name ReportCrash
2021-06-23 20:54:16	Process with PID 1278 and name IMTransferAgent
2021-06-23 20:54:16	Process with PID 1266 and name com.apple.WebKit.WebContent
2021-06-23 20:54:16	Process with PID 1263 and name com.apple.accessibility.mediaac
2021-06-23 20:54:16	Process with PID 1262 and name CategoriesService
2021-06-23 20:54:16	Process with PID 1261 and name com.apple.WebKit.Networking
2021-06-23 20:54:16	Process with PID 1239 and name avatarsd

Shortly afterwards at 20:54 the exploitation succeeded, and we observe that a network request was made by the **com.apple.coretelephony** process causing the Cache.db file to be modified. This matches the behaviour Amnesty International hasseen in the other Pegasus zero-click attacks in 2021.

Date (UTC)	Event
2021-06-23 20:54:35	File: /private/var/wireless/Library/Caches/com.apple.coretelephony/Cache.db-shm
2021-06-23 20:54:35	File: /private/var/wireless/Library/Caches/com.apple.coretelephony/fsCachedData/3C73213F-73E5-4429-AAD9-0D7AD9AE83D1
2021-06-23 20:54:47	File: /private/var/root/Library/Caches/**appccntd**/Cache.db
2021-06-23 20:54:53	File: /private/var/tmp/XtYaXXY
2021-06-23 20:55:08	File: /private/var/tmp/CFNetworkDownload_JQeZFF.tmp
2021-06-23 20:55:09	File: /private/var/tmp/PWg6ueAldsvV8vZ8CYpkp53D
2021-06-23 20:55:10	File: /private/var/db/com.apple.xpc.roleaccountd.staging/**otpgrefd**
2021-06-23 20:55:10	File: /private/var/tmp/vditcfwheovjf/kk
2021-06-23 20:59:35	Process: **appccntd**
2021-06-23 20:59:35	Process: **otpgrefd**

Lastly, the analysis of a fully patched iPhone 12 running iOS 14.6 of an Indian journalist (CODE INJRN2) also revealed signs of successful compromise. **These most recent discoveries indicate NSO Group's customers are currently able to remotely compromise all recent iPhone models and versions of iOS.**

We have reported this information to Apple, who informed us they are investigating the matter.[3]

[3] Email to Amnesty International, July 2021.

7. INCOMPLETE ATTEMPTS TO HIDE EVIDENCE OF COMPROMISE

Several iPhones Amnesty International has inspected indicate that Pegasus has recently started to manipulate system databases and records on infected devices to hide its traces and and impede the research efforts of Amnesty International and other investigators.

Interestingly, this manipulation becomes evident when verifying the consistency of leftover records in the *DataUsage.sqlite* and *netusage.sqlite* SQLite databases. Pegasus has deleted the names of malicious processes from the ZPROCESS table in DataUsage database but not the corresponding entries from the ZLIVEUSAGE table. The ZPROCESS table stores rows containing a process ID and the process name. The ZLIVEUSAGE table contains a row for each running process including data transfer volume and the process ID corresponding to the ZPROCESS entry. These inconsistencies can be useful in identifying times when infections may have occurred. Additional Pegasus indicators of compromise were observed on all devices where this anomaly was observed. No similar inconsistencies were found on any clean iPhones analysed by Amnesty International.

Although most recent records are now being deleted from these databases, traces of recent process executions can also be recovered also from additional diagnostic logs from the system.

For example, the following records were recovered from the phone of an HRD (CODE RWHRD1):

Date (UTC)	Event
2021-01-31 23:59:02	Process: libtouchregd (PID 7354)
2021-02-21 23:10:09	Process: mptbd (PID 5663)
2021-02-21 23:10:09	Process: launchrexd (PID 4634)
2021-03-21 06:06:45	Process: roleaboutd (PID 12645)
2021-03-28 00:36:43	Process: otpgrefd (PID 2786)
2021-04-06 21:29:56	Process: locserviced (PID 5492)
2021-04-23 01:48:56	Process: eventfssd (PID 4276)
2021-04-23 23:01:44	Process: aggregatenotd (PID 1900)
2021-04-28 16:08:40	Process: xpccfd (PID 1218)
2021-06-14 00:17:12	Process: faskeepd (PID 4427)
2021-06-14 00:17:12	Process: lobbrogd (PID 4426)
2021-06-14 00:17:12	Process: neagentd (PID 4423)
2021-06-14 00:17:12	Process: com.apple.rapports.events (PID 4421)
2021-06-18 08:13:35	Process: faskeepd (PID 4427)
2021-06-18 15:31:12	Process: launchrexd (PID 1169)
2021-06-18 15:31:12	Process: frtipd (PID 1168)
2021-06-18 15:31:12	Process: ReminderIntentsUIExtension (PID 1165)
2021-06-23 14:31:39	Process: launchrexd (PID 1169)
2021-06-23 20:59:35	Process: otpgrefd (PID 1301)
2021-06-23 20:59:35	Process: launchafd (PID 1300)
2021-06-23 20:59:35	Process: vm_stats (PID 1294)

2021-06-24 12:24:29	Process: **otpgrefd** (PID 1301)

System log files also reveal the location of Pegasus binaries on disk. These file names match those we have consistently observed in the process execution logs presented earlier. The binaries are located inside the folder ***/private/var/db/com.apple.xpc.roleaccountd.staging/*** which is consistent with the findings by Citizen Lab in a December 2020 report.

```
/private/var/db/com.apple.xpc.roleaccountd.staging/launchrexd/EACA3532-7D15-32EE-A88A-
96989F9F558A
```

Amnesty International’s investigations, corroborated by secondary information we have received, seem to suggest that Pegasus is no longer maintaining persistence on iOS devices. Therefore, binary payloads associated with these processes are not recoverable from the non-volatile filesystem. Instead, one would need to be able to jailbreak the device without reboot, and attempt to extract payloads from memory.

8. PEGASUS PROCESSES DISGUISED AS IOS SYSTEM SERVICES

Across the numerous forensic analyses conducted by Amnesty International on devices around the world, we found a consistent set of malicious process names executed on compromised phones. While some processes, for example **bh**, seem to be unique to a particular attack vector, most Pegasus process names seem to be simply disguised to appear as legitimate iOS system processes, perhaps to fool forensic investigators inspecting logs. Several of these process names spoof legitimate iOS binaries:

Pegasus Process Name	Spoofed iOS Binary
ABSCarryLog	ASPCarryLog
aggregatenotd	aggregated
ckkeyrollfd	ckkeyrolld
com.apple.Mappit.SnapshotService	com.apple.MapKit.SnapshotService
com.apple.rapports.events	com.apple.rapport.events
CommsCenterRootHelper	CommCenterRootHelper
Diagnostic-2543	Diagnostic-2532
Diagnosticd	Diagnostics
eventsfssd	fseventsd
fmld	fmfd
JarvisPluginMgr	JarvisPlugin
launchafd	launchd
MobileSMSd	MobileSMS
nehelprd	nehelper
pcsd	com.apple.pcs
PDPDialogs	PPPDialogs
ReminderIntentsUIExtension	RemindersIntentsUIExtension
rlaccountd	xpcroleaccountd
roleaccountd	xpcroleaccountd

The list of process names we associate with Pegasus infections is available among all other indicators of compromise on our GitHub page.

9. UNRAVELLING THE PEGASUS ATTACK INFRASTRUCTURE OVER THE YEARS

The set of domain names, servers and infrastructure used to deliver and collect data from NSO Group's Pegasus spyware has evolved several times since first publicly disclosed by Citizen Lab in 2016.

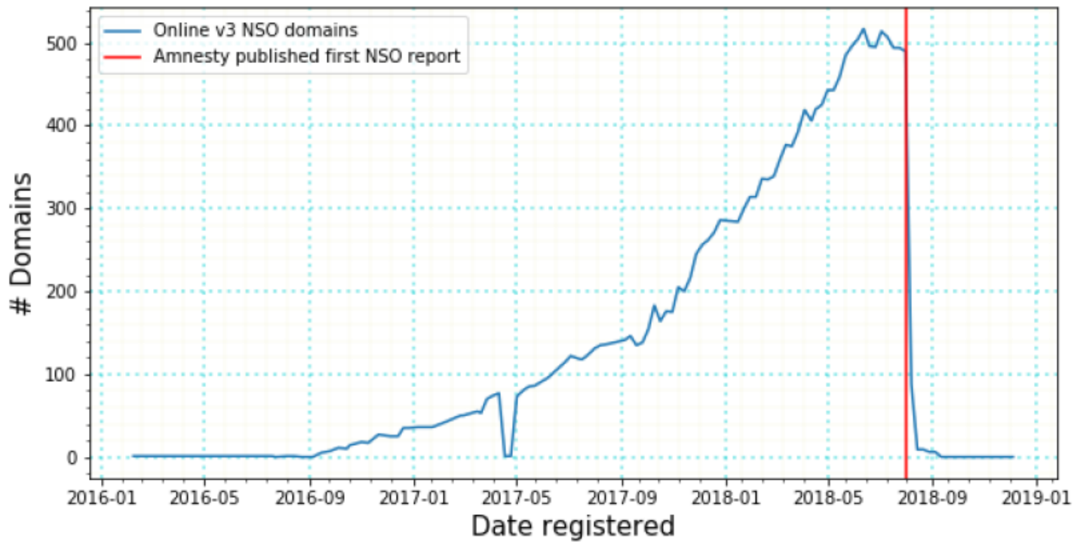
In August 2018, Amnesty International published a report *"Amnesty International Among Targets of NSO-powered Campaign"* which described the targeting of an Amnesty International staff member and a Saudi human rights defender. In this report, Amnesty International presented an excerpt of more than 600 domain names tied to NSO Group's attack infrastructure. Amnesty International published the full list of domains in October 2018. In this report, we refer to these domains as Pegasus network **Version 3 (V3)**.

The **Version 3** infrastructure used a network of VPS's and dedicated servers. Each Pegasus Installation server or Command-and-Control (C&C) server hosted a web server on port 443 with a unique domain and TLS certificate. These edge servers would then proxy connections through a chain of servers, referred to by NSO Group as the **"Pegasus Anonymizing Transmission Network" (PATN).**

It was possible to create a pair of fingerprints for the distinctive set of TLS cipher suites supported by these servers. The fingerprint technique is conceptually similar to the JA3S fingerprint technique published by Salesforce in 2019. With that fingerprint, Amnesty International's Security Lab performed Internet-wide scans to identify Pegasus Installation/infection and C&C servers active in the summer of 2018.

NSO Group made critical operational security mistakes when setting up their Version 3 infrastructure. Two domains of the previous Version 2 network were reused in their Version 3 network. These two Version 2 domains, **pine-sales[.]com** and **ecommerce-ads[.]org** had previously been identified by Citizen Lab. These mistakes allowed Amnesty International to link the attempted attack on our colleague to NSO Group's Pegasus product. These links were independently confirmed by Citizen Lab in a 2018 report.

NSO Group rapidly shutdown many of their Version 3 servers shortly after the Amnesty International and Citizen Lab's publications on 1 August 2018.



9.1 FURTHER ATTEMPTS BY NSO GROUP TO HIDE THEIR INFRASTRUCTURE

In August 2019, the Amnesty International identified another case of NSO Group's tools being used to target a human rights defender, this time in Morocco. Maati Monjib was targeted with SMS messages containing Version 3 Pegasus links.

Amnesty performed a forensic analysis of his iPhone as described previously. This forensic analysis showed redirects to a new domain name **free247downloads.com**. These links looked suspiciously similar to infection links previously used by NSO.

Amnesty International confirmed this domain was tied to NSO Group by observing distinctive Pegasus artefacts created on the device shortly after the infection URL was opened. With this new domain in hand, we were able to begin mapping the Pegasus **Version 4 (V4)** infrastructure.
NSO Group re-factored their infrastructure to introduce additional layers, which complicated discovery. Nevertheless, we could now observe at least 4 servers used in each infection chain.

Validation domain: https://baramije[.]net/[ALPHANUMERIC STRING]
Exploit domain: https://[REDACTED].info8fvhgl3.urlpush[.]net:30827/[SAME ALPHANUMERIC STRING]

1. **A validation server:** The first step was a website which we have seen hosted on shared hosting providers. Frequently this website was running a random and sometimes obscure PHP application or CMS. Amnesty International believes this was an effort to make the domains look less distinguishable.

   The validation server would check the incoming request. If a request had a valid and still active URL the validation server would redirect the victim to the newly generated exploit server domain. If the URL or device was not valid it would redirect to a legitimate decoy website. Any passer-by or Internet crawler would only see the decoy PHP CMS.

2. **Infection DNS server:** NSO now appears to be using a unique subdomain for every exploit attempt. Each subdomain was generated and only active for a short period of time. This prevented researchers from finding the location of the exploit server based on historic device logs.

   To dynamically resolve these subdomains NSO Group ran a custom DNS server under a subdomain for every infection domain. It also obtained a wildcard TLS certificate which would be valid for each generated subdomain such as ***.info8fvhgl3.urlpush[.]net** or ***.get1tn0w.free247downloads[.]com**.

3. **Pegasus Installation Server:** To serve the actual infection payload NSO Group needs to run a web server somewhere on the Internet. Again, NSO Group took steps to avoid internet scanning by running the web server on a random high port number.

   We assume that each infection webserver is part of the new generation **"Pegasus Anonymizing Transmission Network"**. Connections to the infection server are likely proxied back to the customer's Pegasus infrastructure.

4. **Command and Control server**: In previous generations of the PATN, NSO Group used separate domains for the initial infection and later communication with the spyware. The iPwn report from Citizen Lab provided evidence that Pegasus is again using separate domains for command and control. To avoid network-based discovery, the Pegasus spyware made direct connections the Pegasus C&C servers without first performing a DNS lookup or sending the domain name in the TLS SNI field.

9.2 IDENTIFYING OTHER NSO ATTACK DOMAINS

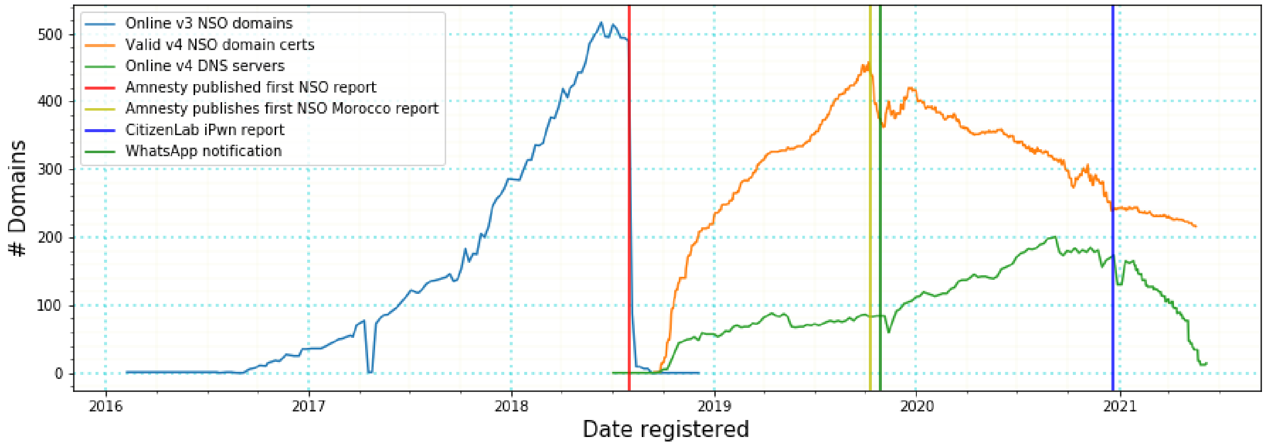
Amnesty International began by analysing the configuration of the infection domains and DNS servers used in the attacks against Moroccan journalists and human rights defenders. Based on our knowledge of the domains used in Morocco we developed a fingerprint which identified 201 Pegasus Installation domains which had infrastructure active at the time of the initial scan. This set of 201 domains included both **urlpush[.]net** and **free247downloads[.]com**.

Amnesty International identified an additional 500 domains with subsequent network scanning and by clustering patterns of domain registration, TLS certificate issuance and domain composition which matched the initial set of 201 domains.

Amnesty International believes that this represents a significant portion of the Version 4 NSO Group attack infrastructure. We are publishing these 700 domains today. We recommend the civil society and media organisations check their network telemetry and/or DNS logs for traces of these indicators of compromise.

9.3 WHAT CAN BE LEARNED FROM NSO GROUP'S INFRASTRUCTURE

The following chart shows the evolution of NSO Group Pegasus infrastructure over a 4-year period from 2016 until mid-2021. Much of the **Version 3** infrastructure was abruptly shut down in August 2018 following our report on an Amnesty International staff member targeted with Pegasus. The **Version 4** infrastructure was then gradually rolled out beginning in September and October 2018.



A significant number of new domains were registered in November 2019 shortly after WhatsApp notified their users about alleged targeting with Pegasus. This may reflect NSO rotating domains due to perceived risk of discovery, or because of disruption to their existing hosting infrastructure.

The V4 DNS server infrastructure began going offline in early 2021 following the Citizen Lab iPwn report which disclosed multiple Pegasus V4 domains.
Amnesty International suspects the shutting down of the V4 infrastructure coincided with NSO Group's shift to using cloud services such as Amazon CloudFront to deliver the earlier stages of their attacks. The use of cloud services protects NSO Group from some Internet scanning techniques.

9.4 ATTACK INFRASTRUCTURE HOSTED PRIMARILY IN EUROPE AND NORTH AMERICA

NSO Group's Pegasus infrastructure primarily consists of servers hosted at datacentres located in European countries. The countries hosting the most infection domain DNS servers included Germany, the United Kingdom, Switzerland, France, and the United States (US).

Country	Servers per country
Germany	212
United Kingdom	79
Switzerland	36
France	35
United States	28
Finland	9

Netherlands	5
Canada	4
Ukraine	4
Singapore	3
India	3
Austria	3
Japan	1
Bulgaria	1
Lithuania	1
Bahrain	1

The following table shows the number of DNS servers hosted with each hosting provider. Most identified servers are assigned to the US-owned hosting companies Digital Ocean, Linode and Amazon Web Services (AWS).
Many hosting providers offer server hosting in multiple physical locations. Based on these two tables it appears that NSO Group is primarily using the European datacentres run by American hosting companies to run much of the attack infrastructure for its customers.

Network	Servers per network
DIGITALOCEAN-ASN	142
Linode, LLC	114
AMAZON-02	73
Akenes SA	60
UpCloud Ltd	9
Choopa	7
OVH SAS	6
Virtual Systems LLC	2
ASN-QUADRANET-GLOBAL	1
combahton GmbH	1
UAB Rakrejus	1
HZ Hosting Ltd	1
PE Brezhnev Daniil	1
Neterra Ltd.	1
Kyiv Optic Networks Ltd	1

Amnesty International's research identified 28 DNS servers linked to the infection infrastructure which were hosted in the US.

Domain name	DNS server IP	Network
drp32k77.todoinfonet.com	104.223.76.216	ASN-QUADRANET-GLOBAL
imgi64kf5so6k.transferlights.com	165.227.52.184	DIGITALOCEAN-ASN
pc43v65k.alignmentdisabled.net	167.172.215.114	DIGITALOCEAN-ASN
img54fsd3267h.prioritytrail.net	157.245.228.71	DIGITALOCEAN-ASN
jsfk3d43.netvisualizer.com	104.248.126.210	DIGITALOCEAN-ASN
cdn42js666.manydnsnow.com	138.197.223.170	DIGITALOCEAN-ASN
css1833iv.handcraftedformat.com	134.209.172.164	DIGITALOCEAN-ASN
js43fsf7v.opera-van.com	159.203.87.42	DIGITALOCEAN-ASN
pypip36z19.myfundsdns.com	167.99.105.68	DIGITALOCEAN-ASN

css912jy6.reception-desk.net	68.183.105.242	DIGITALOCEAN-ASN
imgi64kf5so6k.transferlights.com	206.189.214.74	DIGITALOCEAN-ASN
js85mail.preferenceviews.com	142.93.80.134	DIGITALOCEAN-ASN
css3218i.quota-reader.net	165.227.17.53	DIGITALOCEAN-ASN
mongo87a.sweet-water.org	142.93.113.166	DIGITALOCEAN-ASN
react12x2.towebsite.net	3.13.132.96	AMAZON-02
jsb8dmc5z4.gettingurl.com	13.59.79.240	AMAZON-02
react12x2.towebsite.net	3.16.75.157	AMAZON-02
cssgahs5j.redirigir.net	18.217.13.50	AMAZON-02
jsm3zsn5kewlmk9q.dns-analytics.com	18.225.12.72	AMAZON-02
imgcss35d.domain-routing.com	13.58.85.100	AMAZON-02
jsb8dmc5z4.gettingurl.com	18.191.63.125	AMAZON-02
js9dj1xzc8d.beanbounce.net	199.247.15.15	CHOOPA
jsid76api.buildyourdata.com	108.61.158.97	CHOOPA
cdn19be2.reloadinput.com	95.179.177.18	CHOOPA
srva9awf.syncingprocess.com	66.175.211.107	Linode
jsfk3d43.netvisualizer.com	172.105.148.64	Linode
imgdsg4f35.permalinking.com	23.239.16.143	Linode
srva9awf.syncingprocess.com	45.79.190.38	Linode

9.5 INFECTION DOMAIN RESOLUTIONS OBSERVED IN PASSIVE DNS DATABASE

Based on forensic analysis of compromised devices, Amnesty International determined that NSO Group was using a unique and randomly generated subdomain for each attempt to deliver the Pegasus spyware.

Amnesty International searched passive DNS datasets for each of the Pegasus Version 4 domains we have identified. Passive DNS databases record historic DNS resolution for a domain and often included subdomains and the corresponding historic IP address.

A subdomain will only be recorded in passive DNS records if the subdomain was successfully resolved and the resolution transited a network which was running a passive DNS probe. This probe data is collected based on agreements between network operators and passive DNS data providers. Many networks will not be covered by such data collection agreements. For example, no passive DNS resolutions were recorded for either Pegasus infection domains used in Morocco.

As such, these resolutions represent only a small subset of overall NSO Group Pegasus activity.

Infection domain	Unique infection subdomains
mongo77usr.urlredirect.net	417
str1089.mailappzone.com	410
apiweb248.theappanalytics.com	391
dist564.htmlstats.net	245
css235gr.apigraphs.net	147
nodesj44s.unusualneighbor.com	38

jsonapi2.linksnew.info	30
img9fo658tlsuh.securisurf.com	19
pc25f01dw.loading-url.net	12
dbm4kl5d3faqlk6.healthyguess.com	8
img359axw1z.reload-url.net	5
css2307.cssgraphics.net	5
info2638dg43.newip-info.com	3
img87xp8m.catbrushcable.com	2
img108jkn42.av-scanner.com	2
mongom5sxk8fr6.extractsight.com	2
img776cg3.webprotector.co	1
tv54d2ml1.topadblocker.net	1
drp2j4sdi.safecrusade.com	1
api1r3f4.redirectweburl.com	1
pc41g20bm.redirectconnection.net	1
jsj8sd9nf.randomlane.net	1
php78mp9v.opposedarrangement.net	1

The domain urlredirect.net had the highest number of observed unique subdomains. In total 417 resolutions were recorded between 4 October 2018, and 17 September 2019. The second highest was mailappzone.com which has 410 resolutions in a 3-month period between 23 July 2020, and 15 October 2020.

Amnesty International believes that each of these subdomain resolutions, 1748 in total, represent an attempt to compromise a device with Pegasus. These 23 domains represent less than 7% of the 379 Pegasus Installation Server domains we have identified. Based on this small subset, Pegasus may have been used in thousands of attacks over the past three years.

10. MOBILE DEVICES, SECURITY AND AUDITABILITY

Much of the targeting outlined in this report involves Pegasus attacks targeting iOS devices. It is important to note that this does not necessarily reflect the relative security of iOS devices compared to Android devices, or other operating systems and phone manufacturers.

In Amnesty International's experience there are significantly more forensic traces accessible to investigators on Apple iOS devices than on stock Android devices, therefore our methodology is focused on the former. As a result, most recent cases of confirmed Pegasus infections have involved iPhones.

This and all previous investigations demonstrate how attacks against mobile devices are a significant threat to civil society globally. The difficulty to not only prevent, but posthumously detect attacks is the result of an unsustainable asymmetry between the capabilities readily available to attackers and the inadequate protections that individuals at risk enjoy.

While iOS devices provide at least some useful diagnostics, historical records are scarce and easily tampered with. Other devices provide little to no help conducting consensual forensics analysis. Although much can be done to improve the security posture of mobile devices and mitigate the risks of attacks such as those documented in this report, even more could be achieved by improving the ability for device owners and technical experts to perform regular checks of the system's integrity.

Therefore, Amnesty International strongly encourages device vendors to explore options to make their devices more auditable, without of course sacrificing any security and privacy protections already in place. Platform developers and phone manufacturers should regularly engage in conversations with civil society to better understand the challenges faced by HRDs, who are often under-represented in cybersecurity debates.

11. WITH OUR METHODOLOGY, WE RELEASE OUR TOOLS AND INDICATORS

For a long time, triaging the state of a suspected compromised mobile device has been considered a near-impossible task, particularly within the human rights communities we work in. Through the work of Amnesty International's Security Lab we have built important capabilities that may benefit our peers and colleagues supporting activists, journalists, and lawyers who are at risk.

Therefore, through this report, **we are not only sharing the methodology we have built over years of research but also the tools we created to facilitate this work, as well as the Pegasus indicators of compromise we have collected.**

All indicators of compromise are available on our GitHub , including domain names of Pegasus infrastructure, email addresses recovered from iMessage account lookups involved in the attacks, and all process names Amnesty International has identified as associated with Pegasus.

Amnesty International is also releasing a tool we have created, called Mobile Verification Toolkit **(MVT)**. MVT is a modular tool that simplifies the process of acquiring and analysing data from Android devices, and the analysis of records from iOS backups and filesystem dumps, specifically to identify potential traces of compromise.

MVT can be provided with indicators of compromise in STIX2 format and will identify any matching indicators found on the device. In conjunction with Pegasus indicators, MVT can help identify if an iPhone have been compromised.

Among others, some of the features MVT has include:

- Decrypt encrypted iOS backups.

- Process and parse records from numerous iOS system and apps databases and system logs.
- Extract installed applications from Android devices.
- Extract diagnostic information from Android devices through the adb protocol.
- Compare extracted records to a provided list of malicious indicators in STIX2 format. Automatically identify malicious SMS messages, visited websites, malicious processes, and more.
- Generate JSON logs of extracted records, and separate JSON logs of all detected malicious traces.
- Generate a unified chronological timeline of extracted records, along with a timeline all detected malicious traces.

ACKNOWLEDGEMENTS

The Amnesty International Security Lab wishes to acknowledge all those who have supported this research. Tools released by the iOS security research community including libimobiledevice and checkra1n were used extensively as part of this research. We would also like to thank Censys and RiskIQ for providing access to their internet scan and passive DNS data.

Amnesty International wishes to acknowledge Citizen Lab for its important and extensive research on NSO Group and other actors contributing to the unlawful surveillance of civil society. Amnesty International thanks Citizen Lab for its peer-review of this research report.

Finally Amnesty International wishes to thank the numerous journalists and human rights defenders who bravely collaborated to make this research possible.

APPENDIX A: PEER REVIEW OF METHODOLOGY REPORT BY CITIZEN LAB

The Citizen Lab at the University of Toronto has independently peer-reviewed a draft of the forensic methodology outlined in this report. Their review can be found here.

APPENDIX B: SUSPICIOUS ICLOUD ACCOUNT LOOKUPS

This Appendix shows the overlap of iCloud accounts found looked-up on the mobile devices of different targets. This list will be progressively updated.

iCloud Account	Target
emmaholm575[@]gmail.com	• AZJRN1 - Khadija Ismayilova
filip.bl82[@]gmail.com	• AZJRN1 - Khadija Ismayilova
kleinleon1987[@]gmail.com	• AZJRN1 - Khadija Ismayilova
bergers.o79[@]gmail.com	• Omar Radi • FRHRL1 - Joseph Breham • FRHRL2 • FRJRN1 - Lenaig Bredoux • FRJRN2 • FRPOI1 • FRPOI2 - François de Rugy
naomiwerff772[@]gmail.com	• Omar Radi • FRHRL1 - Joseph Breham • FRPOI1
bogaardlisa803[@]gmail.com	• FRHRL1 - Joseph Breham • FRJRN1 - Lenaig Bredoux • FRJRN2
linakeller2203[@]gmail.com	• FRHRD1 - Claude Mangin • FRPOI3 - Philippe Bouyssou • FRPOI4 • FRPOI5 - Oubi Buchraya Bachir • MOJRN1 – Hicham Mansouri
jessicadavies1345[@]outlook.com	• HUJRN1 - András Szabó • HUJRN2 - Szabolcs Panyi
emmadavies8266[@]gmail.com	• HUJRN1 - András Szabó • HUJRN2 - Szabolcs Panyi
k.williams.enny74[@]gmail.com	• HUPOI1 • HUPOI2 - Adrien Beauduin • HUPOI3
taylorjade0303[@]gmail.com	• INHRD1 - SAR Geelani • INJRN6 - Smita Sharma • INPOI1 - Prashant Kishor

lee.85.holland[@]gmail.com	• INHRD1 - SAR Geelani • INJRN6 - Smita Sharma • INPOI1 - Prashant Kishor
bekkerfredi[@]gmail.com	• INHRD1 - SAR Geelani • INPOI2
herbruud2[@]gmail.com	• INJRN1 - Mangalam Kesavan Venu • INJRN2 - Sushant Singh • INPOI1 - Prashant Kishor
vincent.dahl76[@]gmail.com	• KASH01 - Hatice Cengiz • KASH02 - Rodney Dixon
oskarschalcher[@]outlook.com	• KASH03 - Wadah Khanfar
benjiburns8[@]gmail.com	• RWHRD1 - Carine Kanimba

APPENDIX C: DETAILED TRACES PER TARGET

This Appendix contains detailed breakdowns of forensic traces recovered for each target. This Appendix will be progressively updated.

C.1 FORENSIC TRACES OVERVIEW FOR MAATI MONJIB

Date (UTC)	Event
2017-11-02 12:29:33	Pegasus SMS with link to hxxps://tinyurl[.]com/y73qr7mb redirecting to hxxps://**revolution-news[.]co**/ikXFZ34ca
2017-11-02 16:42:34	Pegasus SMS with link to hxxps://**stopsms[.]biz**/vi78ELI
2017-11-02 16:44:00	Pegasus SMS with link to hxxps://**stopsms[.]biz**/vi78ELI from +212766090491
2017-11-02 16:45:10	Pegasus SMS with link to Hxxps://**stopsms[.]biz**/bi78ELI from +212766090491
2017-11-02 16:57:00	Pegasus SMS with link to Hxxps://**stopsms[.]biz**/bi78ELI from +212766090491
2017-11-02 17:13:45	Pegasus SMS with link to Hxxps://**stopsms[.]biz**/bi78ELI from +212766090491
2017-11-02 17:21:57	Pegasus SMS with link to Hxxps://**stopsms[.]biz**/bi78ELI from +212766090491
2017-11-02 17:30:49	Pegasus SMS with link to Hxxps://**stopsms[.]biz**/bi78ELI from +212766090491
2017-11-02 17:40:46	Pegasus SMS with link to Hxxps://**stopsms[.]biz**/bi78ELI from +212766090491
2017-11-15 17:05:17	Pegasus SMS with link to hxxps://**videosdownload[.]co**/nBBJBIP
2017-11-20 18:22:03	Pegasus SMS with link to hxxps://**infospress[.]com**/LqoHgMCEE
2017-11-24 13:43:17	Pegasus SMS with link to hxxps://tinyurl[.]com/y9hbdqm5 redirecting to hxxps://**hmizat[.]co**/JaCTkfEp
2017-11-24 17:26:09	Pegasus SMS with link to hxxps://**stopsms[.]biz**/2Kj2ik6
2017-11-27 15:56:10	Pegasus SMS with link to hxxps://**stopsms[.]biz**/yTnWt1Ct
2017-11-27 17:32:37	Pegasus SMS with link to hxxps://**hmizat[.]co**/ronEKDVaf
2017-12-07 18:21:57	Pegasus SMS with link to hxxp://tinyurl[.]com/y7wdcd8z redirecting to hxxps://**infospress[.]com**/Ln3HYK4C

2018-01-08 12:58:14	Pegasus SMS with link to hxxp://tinyurl[.]com/y87hnl3o redirecting to hxxps://**infospress[.]com**/asjmXqiS
2018-02-09 21:12:49	Process: **pcsd**
2018-03-16 08:24:20	Process: **pcsd**
2018-04-28 22:25:12	Process: **bh**
2018-05-04 21:30:45	Process: **pcsd**
2018-05-21 21:46:06	Process: **fmld**
2018-05-22 17:36:51	Process: **bh**
2018-06-04 11:05:43	Process: **fmld**
2019-03-27 21:45:10	Process: **bh**
2019-04-14 23:02:41	Safari favicon from URL hxxps://c7r8x8f6zecd8j.get1tn0w**.free247downloads[.]com**:30352/Ld3xuuW5
2019-06-27 20:13:10	Safari favicon from URL hxxps://3hdxu4446c49s.get1tn0w**.free247downloads[.]com**:30497/pczrccr#052045871202826837337308184750023238630846883009852
2019-07-22 15:42:32	Safari visit to hxxps://bun54l2b67.get1tn0w**.free247downloads[.]com**:30495/szev4hz
2019-07 22 15:42:32	Safari visit to hxxps://bun54l2b67.get1tn0w**.free247downloads[.]com**:30495/szev4hz#048634787343287485982474853012724998054718494423286
2019-07-22 15:43:06	Safari favicon from URL hxxps://bun54l2b67.get1tn0w**.free247downloads[.]com**:30495/szev4hz#048634787343287485982474853012724998054718494423286
n/a	WebKit IndexedDB file for URL hxxps://c7r8x8f6zecd8j.get1tn0w**.free247downloads[.]com**
n/a	WebKit IndexedDB file for URL hxxps://bun54l2b67.get1tn0w**.free247downloads[.]com**
n/a	WebKit IndexedDB file for URL hxxps://keewrq9z.get1tn0w**.free247downloads[.]com**
n/a	WebKit IndexedDB file for URL hxxps://3hdxu4446c49s.get1tn0w**.free247downloads[.]com**

C.2 FORENSIC TRACES OVERVIEW FOR OMAR RADI

Date (UTC)	Event
2019-02-11 14:45:45	Webkit IndexedDB file for URL hxxps://d9z3sz93x5ueidq3.get1tn0w**.free247downloads[.]com**
2019-02-11 13:45:53	Safari favicon from URL hxxps://d9z3sz93x5ueidq3.get1tn0w**.free247downloads[.]com**:30897/rdEN5YP
2019-02-11 13:45:56	Process: **bh**
2019-02-11 13:46:16	Process: **roleaboutd**
2019-02-11 13:46:23	Process: **roleaboutd**
2019-02-11 16:05:24	Process: **roleaboutd**
2019-08-16 17:41:06	iMessage lookup for account **bergers.o79[@]gmail.com**
2019-09-13 15:01:38	Safari favicon for URL hxxps://2far1v4lv8.get1tn0w**.free247downloads[.]com**:31052/meunsnyse#011356570257117296834845704022338973133022433397236

2019-09-13 15:01:56	Safari favicon for URL hxxps://2far1v4lv8.get1tn0w**.free247downloads[.]com**:31052/meunsnyse#068099561614626278519925358638789161572427833645389
2019-09-13 15:02:11	Process: **bh**
2019-09-13 15:02:20	Process: **msgacntd**
2019-09-13 15:02:33	Process: **msgacntd**
2019-09-14 15:02:57	Process: **msgacntd**
2019-09-14 18:51:54	Process: **msgacntd**
2019-10-29 12:21:18	iMessage lookup for account **naomiwerff772[@]gmail.com**
2020-01-27 10:06:24	Safari favicon for URL hxxps://gnyjv1xltx.info8fvhgl3**.urlpush[.]net**:30875/zrnv5revj#074196419827987919274001548622738919835556748325946
2020-01-27 10:06:26	Safari visit to hxxps://gnyjv1xltx.info8fvhgl3**.urlpush[.]net**:30875/zrnv5revj#074196419827987919274001548622738919835556748325946#2
2020-01-27 10:06:26	Safari visit to hxxps://gnyjv1xltx.info8fvhgl3**.urlpush[.]net**:30875/zrnv5revj#074196419827987919274001548622738919835556748325946#24
2020-01-27 10:06:32	Safari favicon for URL hxxps://gnyjv1xltx.info8fvhgl3**.urlpush[.]net**:30875/zrnv5revj#074196419827987919274001548622738919835556748325946%2324

APPENDIX D: PEGASUS FORENSIC TRACES PER TARGET

All individuals have been assigned a code name for safety and privacy reasons. Only individuals who have given consent will be named publicly.

The occurrence of a known malicious iCloud account may be a result of actions made by a Pegasus customer against a potential target device. It does not by itself signify that an attack was attempted or succeeded.

FORENSIC TRACES FOR AZJRN1 – KHADIJA ISMAYILOVA

Date (UTC)	Event
2019-03-28 07:44:14	Process: **roleaccountd**
2019-03-28 07:44:14	Process: **stagingd**
2019-03-28 07:44:15	File: Library/Preferences/***roleaccountd.plist***
2019-04-02 09:17:55	Process record deleted from ZPROCESS
2019-04-12 07:42:38	Process record deleted from ZPROCESS
2019-05-01 10:48:06	Process record deleted from ZPROCESS
2019-05-03 07:42:27	Process record deleted from ZPROCESS
2019-05-18 11:03:21	Process record deleted from ZPROCESS
2019-06-17 05:10:02	Process record deleted from ZPROCESS
2019-06-18 05:25:41	Process record deleted from ZPROCESS
2019-06-25 17:03:13	Process record deleted from ZPROCESS
2019-07-08 05:39:13	Process record deleted from ZPROCESS
2019-07-12 11:10:51	Process record deleted from ZPROCESS
2019-07-18 13:40:01	Process record deleted from ZPROCESS

2019-08-22 08:41:02	Process record deleted from ZPROCESS
2019-08-26 05:04:19	Process record deleted from ZPROCESS
2019-08-27 15:02:15	Process record deleted from ZPROCESS
2019-09-06 05:52:30	Process record deleted from ZPROCESS
2019-09-07 07:19:31	Process record deleted from ZPROCESS
2019-09-15 06:11:31	Process record deleted from ZPROCESS
2019-09-17 14:11:51	Process record deleted from ZPROCESS
2019-09-28 12:25:15	Process: libtouchregd
2019-10-01 19:42:17	Process record deleted from ZPROCESS
2019-10-14 05:11:06	Process record deleted from ZPROCESS
2019-10-14 16:08:43	Process: libbmanaged
2019-10-14 16:08:43	Process: mobileargd
2019-10-14 16:08:43	Process: brstaged
2019-10-14 16:08:43	Process: libtouchregd
2019-10-14 16:08:43	Process: launchrexd
2019-10-15 14:21:44	Process: faskeepd
2019-10-16 22:17:17	Process: bundpwrd
2019-10-22 15:42:40	Process: seraccountd
2019-10-22 15:42:40	Process: comnetd
2019-11-25 09:06:49	Process: confinstalld
2019-11-25 09:06:49	Process: msgacntd
2019-11-25 09:06:49	Process: launchrexd
2019-11-25 09:06:49	Process: accountpfd
2019-11-25 09:06:49	Process: xpccfd
2019-11-25 09:06:49	Process: setframed
2019-11-25 09:06:49	Process: natgd
2019-11-25 09:06:49	Process: aggregatenotd
2019-12-09 05:28:20	Process record deleted from ZPROCESS
2019-12-22 16:10:27	Process record deleted from ZPROCESS
2019-12-26 06:01:46	Process record deleted from ZPROCESS
2020-01-09 05:43:20	Process record deleted from ZPROCESS
2020-01-14 06:56:05	Process record deleted from ZPROCESS
2020-01-27 05:44:27	Process record deleted from ZPROCESS
2020-01-31 11:41:04	Process record deleted from ZPROCESS
2020-02-07 05:00:03	Process record deleted from ZPROCESS
2020-02-09 07:03:56	Process record deleted from ZPROCESS
2020-02-13 05:00:59	iMessage lookup for account e\x00\x00aholm575[@]gmail.com (emmaholm575[@]gmail.com)
2020-02-23 07:39:00	Process record deleted from ZPROCESS
2020-02-26 04:57:01	Process record deleted from ZPROCESS
2020-03-09 05:33:30	Process record deleted from ZPROCESS
2020-03-13 06:45:19	Process record deleted from ZPROCESS
2020-03-24 07:27:42	Process record deleted from ZPROCESS

2020-03-30 06:08:44	Process record deleted from ZPROCESS
2020-04-21 12:04:31	Process record deleted from ZPROCESS
2020-04-23 06:26:56	iMessage lookup for account filip.bl82[@]gmail.\x00\x00m (filip.bl82[@]gmail.com)
2020-04-23 07:24:11	Process record deleted from ZPROCESS
2020-04-29 07:31:57	Process record deleted from ZPROCESS
2020-04-30 07:58:32	Process record deleted from ZPROCESS
2020-05-11 14:25:28	Process record deleted from ZPROCESS
2020-05-15 11:31:09	Process record deleted from ZPROCESS
2020-05-17 07:03:29	Process record deleted from ZPROCESS
2020-05-20 21:10:16	Process: logseld
2020-05-20 21:10:16	Process: brstaged
2020-05-20 21:10:16	Process: pstid
2020-05-20 21:10:16	Process: roleaboutd
2020-05-20 21:10:16	Process: libtouchregd
2020-05-20 21:10:16	Process: brstaged
2020-05-29 07:11:37	Process record deleted from ZPROCESS
2020-05-31 07:32:56	Process record deleted from ZPROCESS
2020-05-31 15:28:11	Process: bfrgbd
2020-05-31 15:28:11	Process: xpccfd
2020-05-31 15:28:11	Process: nehelprd
2020-06-01 09:07:27	iMessage lookup for account kleinleon1987[@]gma\x00\x00.com (kleinleon1987[@]gmail.com)
2020-06-05 13:07:16	Process record deleted from ZPROCESS
2020-06-08 08:13:02	Process record deleted from ZPROCESS
2020-06-08 18:22:45	Process: comnetd
2020-06-08 18:22:45	Process: fservernetd
2020-06-08 18:22:45	Process: rolexd
2020-06-12 08:45:08	Process record deleted from ZPROCESS
2020-06-22 05:29:22	Process: roleaccountd
2020-06-22 05:29:23	Process: stagingd
2020-06-27 11:23:05	Process record deleted from ZPROCESS
2020-06-27 11:23:09	Process record deleted from ZPROCESS
2020-06-29 05:13:04	Process record deleted from ZPROCESS
2020-06-29 05:13:04	Process record deleted from ZPROCESS
2020-06-30 05:59:08	iMessage lookup for account k\x00\x00inleon1987[@]gmail.com (kleinleon1987[@]gmail.com)
2020-07-01 13:04:43	Process: nehelprd
2020-07-01 13:04:43	Process: aggregatenotd
2020-07-01 13:04:43	Process: fservernetd
2020-07-01 13:04:43	Process: msgacntd
2020-07-02 06:29:48	Process record deleted from ZPROCESS
2020-07-02 06:29:48	Process record deleted from ZPROCESS

2020-07-03 06:51:47	Process record deleted from ZPROCESS
2020-07-03 06:51:53	Process record deleted from ZPROCESS
2020-07-04 07:20:57	Process record deleted from ZPROCESS
2020-07-04 07:20:58	Process record deleted from ZPROCESS
2020-07-05 07:23:50	Process record deleted from ZPROCESS
2020-07-06 05:22:21	iMessage lookup for account f\x00\x00ip.bl82[@]gmail.com (filip.bl82[@]gmail.com)
2020-07-10 14:12:09	Cache file /private/var/mobile/Containers/Data/Application/D6A69566-55F7-4757-96DE-EBA612685272/Library/Caches/com.apple.Music/Cache.db recorded visit to URL hxxps://x1znqjo0x8b8j.php78mp9v.opposedarrangement[.]net:37271/afAVt89Wq/stadium/pop2.html?key=501_4&n=7
2020-07-10 14:12:15	Cache file /private/var/mobile/Containers/Data/Application/D6A69566-55F7-4757-96DE-EBA612685272/Library/Caches/com.apple.Music/Cache.db recorded visit to URL hxxps://x1znqjo0x8b8j.php78mp9v.opposedarrangement[.]net:37271/afAVt89Wq/stadium/pop2.html?key=501_4&n=1
2020-07-10 14:12:21	Process: roleaccountd
2020-07-10 14:12:26	Process: stagingd
2020-07-11 19:34:04	Process: confinstalld
2020-07-11 19:34:04	Process: roleaboutd
2020-07-11 19:34:04	Process: lobbrogd
2020-07-11 19:34:04	Process: fservernetd
2020-07-11 19:34:04	Process: launchafd
2020-07-13 05:05:17	Cache file /private/var/mobile/Containers/Data/Application/D6A69566-55F7-4757-96DE-EBA612685272/Library/Caches/com.apple.Music/Cache.db recorded visit to URL hxxps://4n3d9ca2st.php78mp9v.opposedarrangement[.]net:37891/w58Xp5Z/stadium/pop2.html?key=501_4&n=7
2020-12-07 07:23:23	iMessage lookup for account kleinleon1987[@]gmail.com
2021-04-20 17:53:51	iMessage lookup for account filip.bl82[@]gmail.com
2021-05-06 08:34:43	iMessage lookup for account emmaholm575[@]gmail.com

FORENSIC TRACES FOR AZJRN2 – SEVINC VAQIFQIZI

Date (UTC)	Event
2019-04-17 10:53:04	File created: Library/Preferences/com.apple.CrashReporter.plist from RootDomain
2019-04-17 10:53:45	Process: roleaccountd
2019-04-17 10:53:45	File created: Library/Preferences/roleaccountd.plist from RootDomain
2019-04-24 12:13:29	Process: roleaccountd

2019-04-24 12:13:31	Process: stagingd
2019-07-18 09:35:17	Process: rolexd
2019-08-02 11:45:12	Process: actmanaged
2019-10-08 15:22:29	Process: libbmanaged
2019-10-12 08:17:28	Process: xpccfd
2019-10-14 05:05:09	Process: setframed
2019-10-18 06:16:16	Process: natgd
2019-10-21 05:23:50	Process: libtouchregd
2019-10-29 05:28:54	Process: frtipd
2019-11-08 07:01:25	Process: brstaged
2019-11-11 10:46:47	Process: boardframed
2019-11-17 07:15:36	Process: ckkeyrollfd
2019-11-19 11:50:37	Process: mptbd
2019-12-02 05:18:49	Process: mobileargd
2019-12-03 13:15:03	Process: nehelprd
2019-12-12 14:38:31	Process: corecomnetd
2020-02-10 05:15:54	Process: pstid
2020-02-12 10:10:30	Process: stagingd (IN: 63.17 MB, OUT: 2.76 MB)
2020-02-13 15:32:49	Process: roleaccountd (IN: 0.25 MB, OUT: 0.13 MB)
2020-03-02 08:57:41	Process: roleaccountd
2020-03-02 08:57:48	Process: stagingd
2020-03-02 08:58:07	Process: seraccountd
2020-12-15 10:55:58	Process: comsercvd
2020-12-24 08:45:03	Process: comsercvd (IN: 17.63 MB, OUT: 64.19 MB)
2020-12-24 16:47:45	Process: comsercvd
2021-02-09 09:42:00	Attack related push notifications over iMessage
2021-02-09 10:06:50	Process: ctrlfs
2021-02-09 10:06:50	Process: ctrlfs
2021-05-20 05:46:42	Process: com.apple.rapports.events

FORENSIC TRACES FOR FRHRD1 – CLAUDE MANGIN

Phone 1

Date (UTC)	Event
2020-10-08 08:40:42	File created: Library/Preferences/com.apple.softwareupdateservicesd.plist from HomeDomain
2020-10-08 10:25:29	Process record deleted from ZPROCESS (IN: 5.46 MB, OUT: 45.62 MB)
2020-10-09 16:17:22	Process record deleted from ZPROCESS (IN: 0.71 MB, OUT: 1.33 MB)
2020-10-10 16:17:24	Process record deleted from ZPROCESS (IN: 0.30 MB, OUT: 0.82 MB)
2020-10-11 16:17:32	Process record deleted from ZPROCESS (IN: 2.25 MB, OUT: 4.88 MB)
2020-10-12 16:51:34	Process record deleted from ZPROCESS (IN: 0.98 MB, OUT: 1.31 MB)
2020-10-13 17:55:23	Process record deleted from ZPROCESS (IN: 1.20 MB, OUT: 5.40 MB)
2020-10-15 17:30:29	Process record deleted from ZPROCESS (IN: 1.56 MB, OUT: 1.92 MB)

2020-10-17 17:08:00	Process record deleted from ZPROCESS (IN: 1.80 MB, OUT: 0.23 MB)
2020-11-18 13:32:24	Process record deleted from ZPROCESS (IN: 1.83 MB, OUT: 0.21 MB)
2020-12-14 15:29:59	Process record deleted from ZPROCESS (IN: 1.83 MB, OUT: 0.25 MB)
2020-12-14 15:31:13	Process record deleted from ZPROCESS (IN: 0.02 MB, OUT: 0.05 MB)
2020-12-15 14:36:59	Process record deleted from ZPROCESS (IN: 1.83 MB, OUT: 0.25 MB)
2021-01-12 14:33:11	Process record deleted from ZPROCESS (IN: 6.99 MB, OUT: 22.26 MB)
2021-01-15 13:39:12	Process record deleted from ZPROCESS (IN: 0.06 MB, OUT: 0.07 MB)
2021-01-16 13:43:10	Process record deleted from ZPROCESS (IN: 2.00 MB, OUT: 1.88 MB)
2021-01-17 15:48:01	Process record deleted from ZPROCESS (IN: 1.25 MB, OUT: 4.43 MB)
2021-01-19 13:58:33	Process record deleted from ZPROCESS (IN: 2.94 MB, OUT: 3.59 MB)
2021-01-21 08:40:52	Process record deleted from ZPROCESS (IN: 1.69 MB, OUT: 1.64 MB)
2021-01-22 08:41:08	Process record deleted from ZPROCESS (IN: 2.50 MB, OUT: 4.70 MB)
2021-03-16 12:33:20	Process record deleted from ZPROCESS (IN: 292.83 MB, OUT: 353.60 MB)
2021-03-17 12:40:45	Process record deleted from ZPROCESS (IN: 0.63 MB, OUT: 0.37 MB)
2021-03-19 10:55:06	Process record deleted from ZPROCESS (IN: 2.74 MB, OUT: 1.72 MB)
2021-03-20 10:57:33	Process record deleted from ZPROCESS (IN: 9.34 MB, OUT: 8.15 MB)
2021-03-21 10:59:08	Process record deleted from ZPROCESS (IN: 12.38 MB, OUT: 19.65 MB)
2021-03-22 11:02:54	Process record deleted from ZPROCESS (IN: 2.54 MB, OUT: 5.11 MB)
2021-03-23 11:34:43	Process record deleted from ZPROCESS (IN: 0.35 MB, OUT: 0.21 MB)
2021-03-24 11:51:11	Process record deleted from ZPROCESS (IN: 2.69 MB, OUT: 1.72 MB)
2021-03-25 12:44:15	Process record deleted from ZPROCESS (IN: 3.74 MB, OUT: 3.94 MB)
2021-03-27 14:43:42	Process record deleted from ZPROCESS (IN: 1.72 MB, OUT: 1.06 MB)
2021-03-27 22:52:14	Process: brstaged
2021-03-31 14:18:42	Process record deleted from ZPROCESS (IN: 0.02 MB, OUT: 0.01 MB)
2021-03-31 14:19:03	Process record deleted from ZPROCESS (IN: 1.87 MB, OUT: 0.28 MB)
2021-04-01 05:50:40	Process: accountpfd
2021-04-30 12:25:15	Process record deleted from ZPROCESS (IN: 77.19 MB, OUT: 49.49 MB)
2021-05-01 16:35:25	Process record deleted from ZPROCESS (IN: 5.86 MB, OUT: 3.63 MB)
2021-05-03 07:27:01	Process record deleted from ZPROCESS (IN: 1.70 MB, OUT: 0.97 MB)
2021-05-04 07:59:24	Process record deleted from ZPROCESS (IN: 2.66 MB, OUT: 1.77 MB)
2021-05-05 09:09:40	Process record deleted from ZPROCESS (IN: 11.23 MB, OUT: 7.73 MB)
2021-05-07 13:13:51	Process record deleted from ZPROCESS (IN: 5.51 MB, OUT: 3.57 MB)
2021-05-08 13:15:26	Process record deleted from ZPROCESS (IN: 13.65 MB, OUT: 9.88 MB)
2021-05-09 13:18:40	Process record deleted from ZPROCESS (IN: 15.42 MB, OUT: 9.87 MB)
2021-05-10 13:20:46	Process record deleted from ZPROCESS (IN: 0.31 MB, OUT: 0.19 MB)
2021-05-12 09:25:23	Process record deleted from ZPROCESS (IN: 3.87 MB, OUT: 2.33 MB)
2021-05-13 09:26:19	Process record deleted from ZPROCESS (IN: 1.79 MB, OUT: 1.15 MB)
2021-05-14 00:32:59	Process: comsercvd
2021-05-15 12:51:46	Process: com.apple.Mappit.SnapshotService (IN: 0.03 MB, OUT: 0.01 MB)

2021-05-15 12:56:04	Process record deleted from ZPROCESS (IN: 1.87 MB, OUT: 0.28 MB)
2021-05-15 13:04:10	Process: roleaboutd
2021-05-15 13:04:10	Process: confinstalld
2021-05-15 13:04:10	Process: gssdp
2021-05-15 20:58:34	Process: roleaboutd
2021-05-15 20:58:34	Process: confinstalld
2021-05-15 20:58:34	Process: gssdp
2021-05-16 21:46:58	Process: roleaboutd
2021-05-16 21:46:58	Process: confinstalld
2021-05-16 21:46:58	Process: gssdp
2021-05-17 21:46:13	Process: roleaboutd
2021-05-17 21:46:13	Process: confinstalld
2021-05-17 21:46:13	Process: gssdp
2021-05-18 21:47:13	Process: roleaboutd
2021-05-18 21:47:13	Process: confinstalld
2021-05-18 21:47:13	Process: gssdp
2021-05-19 22:30:36	Process: roleaboutd
2021-05-19 22:30:36	Process: confinstalld
2021-05-19 22:30:36	Process: gssdp
2021-05-21 21:09:59	Process: roleaboutd
2021-05-21 21:09:59	Process: confinstalld
2021-05-21 21:09:59	Process: gssdp
2021-05-22 21:12:51	Process: roleaboutd
2021-05-22 21:12:51	Process: confinstalld
2021-05-22 21:12:51	Process: gssdp
2021-05-23 21:13:37	Process: roleaboutd
2021-05-23 21:13:37	Process: confinstalld
2021-05-23 21:13:37	Process: gssdp
2021-05-23 21:14:55	Process: roleaboutd
2021-05-23 21:14:55	Process: confinstalld
2021-05-23 21:14:55	Process: gssdp
2021-05-25 10:51:16	Process: roleaboutd
2021-05-25 10:51:16	Process: confinstalld
2021-05-25 10:51:16	Process: gssdp
2021-05-26 19:31:58	Process: roleaboutd
2021-05-26 19:31:58	Process: confinstalld
2021-05-26 19:31:58	Process: gssdp
2021-05-27 19:35:21	Process: roleaboutd
2021-05-27 19:35:21	Process: confinstalld
2021-05-27 19:35:21	Process: gssdp
2021-05-28 19:50:06	Process: roleaboutd
2021-05-28 19:50:06	Process: confinstalld
2021-05-28 19:50:06	Process: gssdp

2021-05-29 19:51:18	Process: roleaboutd
2021-05-29 19:51:18	Process: confinstalld
2021-05-29 19:51:18	Process: gssdp
2021-05-31 04:52:47	Process: roleaboutd
2021-05-31 04:52:47	Process: confinstalld
2021-05-31 04:52:47	Process: gssdp
2021-05-31 04:53:49	Process: roleaboutd
2021-05-31 04:53:49	Process: confinstalld
2021-05-31 04:53:49	Process: gssdp
2021-06-01 05:13:25	Process: roleaboutd
2021-06-01 05:13:25	Process: confinstalld
2021-06-01 05:13:25	Process: gssdp
2021-06-01 14:12:05	Process: PDPDialogs
2021-06-02 05:14:44	Process: roleaboutd
2021-06-02 05:14:44	Process: confinstalld
2021-06-02 05:14:44	Process: gssdp
2021-06-03 05:23:42	Process: roleaboutd
2021-06-03 05:23:42	Process: confinstalld
2021-06-03 05:23:42	Process: gssdp
2021-06-04 14:38:54	Process: roleaboutd
2021-06-04 14:38:54	Process: confinstalld
2021-06-04 14:38:54	Process: gssdp
2021-06-05 20:26:58	Process: confinstalld
2021-06-06 20:33:20	Process: confinstalld
2021-06-07 20:31:57	Process: confinstalld
2021-06-09 14:42:29	Process: confinstalld
2021-06-10 20:09:26	Process: confinstalld
2021-06-11 09:34:00	Attack related push notifications over iMessage
2021-06-11 09:35:00	Attack related push notifications over iMessage
2021-06-11 09:36:00	Attack related push notifications over iMessage
2021-06-11 09:37:00	Attack related push notifications over iMessage
2021-06-11 09:37:52	iMessage lookup for account linakeller2203[@]gmail.com
2021-06-11 09:38:00	Attack related push notifications over iMessage
2021-06-11 09:40:00	Attack related push notifications over iMessage
2021-06-11 09:41:00	Attack related push notifications over iMessage
2021-06-11 09:43:00	Attack related push notifications over iMessage
2021-06-11 09:48:37	Process: com.apple.Mappit.SnapshotService (IN: 0.02 MB, OUT: 0.01 MB)
2021-06-11 09:48:49	Process: com.apple.Mappit.SnapshotService
2021-06-11 09:51:28	Process: cfprefssd
2021-06-11 20:25:58	Process: confinstalld
2021-06-12 19:30:30	Process: confinstalld

Phone 2

Date (UTC)	Event
2021-07-06 12:39:42	iMessage lookup for account **linakeller2203[@]gmail.com**
2021-07-06 12:40:30	Traces from zero-click attack attempt over iMessage

FORENSIC TRACES FOR FRHRD2

Date (UTC)	Event
2019-01-03 11:32	Suspicious SMS with fake Facebook link: **https://web-facebook[.]com/[REDACTED]**

FORENSIC TRACES FOR FRHRL1 - JOSEPH BREHAM

Date (UTC)	Event
2019-09-20 10:27:41	iMessage lookup for account **bergers.o79[@]gmail.com**
2019-09-20 10:29:47	iMessage lookup for account **naomiwerff772[@]gmail.com**
2019-10-29 09:04:58	Process: **bh** (IN: 2.86 MB, OUT: 0.21 MB)
2019-10-29 09:05:08	File created: *Library/Preferences/**com.apple.CrashReporter.plist*** from RootDomain
2019-10-29 09:05:52	Process: **mptbd** (IN: 18.31 MB, OUT: 106.70 MB)
2019-11-01 12:09:05	Process: **mptbd**
2019-11-01 19:03:23	Process: **mptbd**
2019-11-04 09:35:34	Process: **corecomnetd** (IN: 62.45 MB, OUT: 157.21 MB)
2019-11-07 11:53:06	Process: **corecomnetd**
2019-11-07 19:41:45	Process: **corecomnetd**
2019-11-08 15:27:30	Process: **actmanaged** (IN: 90.27 MB, OUT: 139.34 MB)
2019-11-13 19:09:16	Process: **actmanaged**
2019-11-15 17:07:06	Process: **actmanaged**
2019-11-20 11:15:13	Process: **pstid** (IN: 13.85 MB, WWAN OUT: 1.83 MB)
2019-11-20 11:17:40	Process: **pstid**
2019-11-22 09:17:27	Process: **bh**
2019-11-22 09:22:00	Process: **logseld** (IN: 0.01 MB, WWAN OUT: 0.01 MB)
2019-11-26 09:23:57	Process: **ckeblld** (IN: 0.02 MB, WWAN OUT: 0.01 MB)
2019-11-29 09:38:05	Process: **libbmanaged** (IN: 77.70 MB, OUT: 128.32 MB)
2019-12-05 10:45:44	Process: **libbmanaged**
2019-12-06 08:25:23	Process: **libbmanaged**
2019-12-06 12:02:25	Process: **natgd**
2019-12-09 10:44:59	Process: **launchrexd** (IN: 22.50 MB, OUT: 86.92 MB)
2019-12-15 17:17:59	Process: **launchrexd**
2019-12-16 01:37:31	Process: **launchrexd**
2019-12-18 08:13:29	Process: **bh**
2019-12-18 08:14:05	Process: **ckeblld**
2019-12-18 11:50:15	Process: **ckeblld**
2019-12-22 15:13:04	Process: **natgd** (IN: 5.39 MB, OUT: 35.72 MB)
2019-12-25 08:57:28	iMessage lookup for account **bogaardlisa803[@]gmail.com**

FORENSIC TRACES FOR FRHRL2

Date (UTC)	Event
2019-06-13 14:03:23	File created: Library/Preferences/**com.apple.CrashReporter.plist** from RootDomain
2019-06-13 14:03:42	File created: Library/Preferences/**roleaccountd.plist** from RootDomain
2019-06-13 14:04:00	Process: **roleaccountd** (IN: 0.01 MB, OUT: 0.00 MB)
2019-06-13 14:04:00	Process: **stagingd** (IN: 1.47 MB, OUT: 0.08 MB)
2019-06-13 14:04:30	Process: **launchafd** (IN: 0.01 MB, OUT: 0.01 MB)
2019-06-13 14:04:31	Process: **launchafd**
2019-06-13 16:03:43	Process: **roleaccountd**
2019-06-17 17:22:00	Process: **corecomnetd**
2019-06-24 08:58:25	Process: **corecomnetd** (IN: 0.51 MB, OUT: 0.88 MB)
2019-07-01 14:44:29	iMessage lookup for account **b\x00\x00gers.o79[@]gmail.com** (bergers.o79[@]gmail.com)
2019-07-04 09:01:19	Process: **fdlibframed**
2019-07-08 10:14:53	Process: **fdlibframed** (IN: 25.19 MB, OUT: 209.25 MB)
2019-07-10 08:44:54	Process: **fdlibframed**
2019-07-12 13:58:16	iMessage lookup for account **bergers.o79[@]gmail\x00\x00om** (bergers.o79[@]gmail.com)
2019-07-18 18:22:47	Process: **corecomnetd** (IN: 64.69 MB, OUT: 401.88 MB)
2019-07-18 19:53:44	Process: **corecomnetd**
2019-07-22 15:13:11	Process: **roleaboutd**
2019-07-25 18:29:47	Process: **roleaboutd** (IN: 4.62 MB, OUT: 10.40 MB)
2019-07-28 20:24:31	Process: **roleaboutd** (IN: 27.80 MB, OUT: 261.17 MB)
2019-07-29 04:02:57	Process: **roleaboutd**
2019-08-02 15:34:08	Process: **roleaccountd** (IN: 0.02 MB, OUT: 0.01 MB)
2019-08-02 15:34:11	Process: **stagingd** (IN: 2.95 MB, OUT: 0.12 MB)
2019-08-02 15:34:19	Process: **stagingd**
2019-08-02 15:34:36	Process: **pstid** (IN: 10.20 MB, OUT: 68.77 MB)
2019-08-03 13:58:01	Process: **pstid**
2019-08-07 10:40:04	iMessage lookup for account **bergers.o79[@]gmail.com**
2020-02-06 14:52:22	Photostream lookup for account **bogaardlisa803[@]gmail.com**
2021-02-08 10:42:40	iMessage lookup for account **linakeller2203[@]gmail.com**
2021-02-08 11:27:23	Process: **gatekeeperd** (IN: 0.01 MB, OUT: 0.00 MB)
2021-02-08 11:27:25	Process: **bluetoothfs**
2021-02-08 12:27:21	Process: **gatekeeperd**

FORENSIC TRACES FOR FRJRN1 - LÉNAÏG BREDOUX

Date (UTC)	Event
2019-07-08 05:22:05	iMessage lookup for account **bergers.o79[@]gmail.com**
2019-10-10 12:39:17	File: *Library/Preferences/**com.apple.CrashReporter.plist*** from RootDomain

2020-03-12 15:06:23	Process: frtipd (IN: 0.05 MB, OUT: 0.43 MB)
2020-03-13 02:20:34	Process: frtipd
2020-03-16 10:46:55	Process: comnetd (IN: 0.58 MB, OUT: 4.92 MB)
2020-03-20 09:48:10	Process: comnetd
2020-03-21 20:09:49	Process: comnetd
2020-03-23 13:57:42	Process: netservcomd (IN: 0.01 MB, OUT: 0.06 MB)
2020-03-23 21:10:16	Process: netservcomd
2020-04-19 12:25:41	Process: setframed (IN: 0.23 MB, OUT: 2.00 MB)
2020-04-20 21:32:18	Process: setframed
2020-04-22 16:43:22	Process: launchrexd (IN: 0.50 MB, OUT: 4.14 MB)
2020-04-27 20:01:46	Process: launchrexd
2020-05-01 14:18:15	Process: nehelprd (IN: 4.24 MB, OUT: 52.75 MB)
2020-05-03 00:57:11	Process: nehelprd
2020-05-04 11:39:47	Process: msgacntd (IN: 3.21 MB, OUT: 34.59 MB)
2020-05-06 12:52:13	Process: msgacntd
2020-05-06 20:29:07	Process: msgacntd
2020-07-07 15:04:34	Process: aggregatenotd (IN: 1.10 MB, OUT: 10.69 MB)
2020-05-08 17:56:58	Process: aggregatenotd
2020-05-09 10:21:18	Process: bundpwrd (IN: 1.37 MB, OUT: 9.63 MB)
2020-05-09 16:52:05	Process: bundpwrd
2020-05-12 05:27:20	Process: seraccountd (IN: 0.06 MB, OUT: 0.42 MB)
2020-05-12 19:29:17	Process: seraccountd
2020-05-13 16:06:41	Process: otpgrefd (IN: 1.28 MB, OUT: 13.78 MB)
2020-05-13 17:19:07	Process: otpgrefd
2020-05-15 12:23:30	Process: eventstorpd (IN: 0.01 MB, OUT: 0.06 MB)
2020-05-16 18:00:50	Process: eventstorpd
2020-05-16 18:12:29	Process: eventstorpd
2020-05-17 14:42:23	Process: roleaboutd (IN: 6.54 MB, OUT: 69.61 MB)
2020-05-20 11:38:45	Process: roleaboutd
2020-05-20 21:01:24	Process: roleaboutd
2020-05-21 14:54:20	Process: mptbd (IN: 0.70 MB, OUT: 8.14 MB)
2020-05-23 16:05:30	Process: mptbd
2020-05-23 22:58:10	Process: bh (IN: 4.93 MB, OUT: 0.61 MB)
2020-05-24 15:44:39	Process: bh
2020-05-24 15:46:51	Process: fservernetd (IN: 0.00 MB, OUT: 0.04 MB)
2020-05-24 17:36:36	Process: fservernetd
2020-05-26 12:28:34	Process: brstaged (IN: 2.56 MB, OUT: 22.61 MB)
2020-05-27 04:33:50	Process: brstaged
2020-05-27 14:55:06	Process: ckkeyrollfd (IN: 0.01 MB, OUT: 0.09 MB)
2020-05-27 16:58:52	Process: bh
2020-05-27 18:00:50	Process: ckkeyrollfd
2020-07-10 11:12:35	iMessage account lookup: bogaardlisa803[@]gmail.com

FORENSIC TRACES FOR FRJRN2

Date (UTC)	Event
2019-08-16 12:08:44	iMessage lookup for account **bergers.o79[@]gmail.com**
2019-08-16 12:33:52	iMessage lookup for account **bergers.o79[@]gmail\x00\x00om**
2019-08-16 12:37:55	File created: **Library/Preferences/com.apple.CrashReporter.plist** from RootDomain
2019-08-16 12:41:25	File created: **Library/Preferences/roleaccountd.plist** from RootDomain
2019-08-16 12:41:36	Process: **roleaccountd** (IN: 0.01 MB, OUT: 0.01 MB)
2019-08-16 12:41:52	Process: **stagingd** (IN: 1.46 MB, OUT: 0.09 MB)
2019-08-16 12:49:21	Process: **aggregatenotd**
2019-08-20 13:35:23	Process: **aggregatenotd** (IN: 11.07 MB, OUT: 45.52 MB)
2019-08-21 14:10:48	Process: **aggregatenotd**

FORENSIC TRACES FOR FRJRN3 – EDWY PLENEL

Date (UTC)	Event
2019-07-05 11:23:29	File: *Library/Preferences/**com.apple.CrashReporter.plist*** from RootDomain
2019-07-05 11:23:45	File created: *Library/Preferences/**roleaccountd.plist*** from RootDomain
2019-07-05 11:23:51	Process: **stagingd**
2019-07-05 11:24:19	Process: **eventfssd**
2019-07-07 11:28:15	Process: **eventfssd**
2019-07-09 10:39:41	Process: **fservernetd**
2019-07-09 11:49:48	Process: **fservernetd**
2019-07-12 11:12:24	Process: **nehelprd**
2019-07-14 14:01:26	Process: **nehelprd**
2019-07-20 12:18:30	Process: **libbmanaged**
2019-08-11 14:03:11	Process: **rlaccountd**
2019-08-13 17:34:40	Process: **rlaccountd**
2019-08-19 13:21:02	Process: **libbmanaged**
2019-08-19 14:48:42	Process: **libbmanaged**
2019-08-19 21:51:00	Process: **libbmanaged**
2019-08-28 09:12:33	Process: **roleaccountd**
2019-08-28 09:12:34	Process: **stagingd**
2019-08-28 09:12:49	Process: **stagingd**
2019-08-28 09:13:10	Process: **boardframed**
2019-08-29 09:15:05	Process: **boardframed**
2019-08-31 09:04:17	Process: **boardframed**
2019-08-31 09:49:33	Process: **boardframed**
2019-09-03 10:59:31	Process: **launchafd**
2019-09-05 11:02:43	Process: **launchafd**
2019-09-05 20:32:02	Process: **launchafd**

FORENSIC TRACES FOR FRJRN4 – BRUNO DELPORT

Date (UTC)	Event
2019-07-05 13:21:47	File created *Library/Preferences/com.apple.CrashReporter.plist* from RootDomain
2019-07-05 13:21:53	File modified *Library/Preferences/com.apple.CrashReporter.plist* from RootDomain

FORENSIC TRACES FOR FRPOI1

Date (UTC)	Event
2019-03-16 10:42:56	iMessage lookup for account bergers.o79[@]gmail.com
2020-08-02 20:03:19	iMessage lookup for account naomiwerff772[@]gmail.com

FORENSIC TRACES FOR FRPOI2 - FRANÇOIS DE RUGY

Date (UTC)	Event
2019-07-XX	iMessage lookup for account bergers.o79[@]gmail.com

FORENSIC TRACES FOR FRPOI3 – PHILIPPE BOUYSSOU

Date (UTC)	Event
2021-07-06 12:20:01	iMessage lookup for account linakeller2203[@]gmail.com

FORENSIC TRACES FOR FRPOI4

Date (UTC)	Event
2021-XX-XX	iMessage lookup for account linakeller2203[@]gmail.com

FORENSIC TRACES FOR FRPOI5 - OUBI BUCHRAYA BACHIR

Date (UTC)	Event
2021-03-15 12:08:27	iMessage lookup for account linakeller2203[@]gmail.com
2021-03-15 12:12:49	Traces related to iMessage exploitation
2021-03-15 12:16:02c	File modified: *Library/Caches* from RootDomain

FORENSIC TRACES FOR HUJRN1 - ANDRÁS SZABÓ

Date (UTC)	Event
2019-06-13 11:15:40	File created: *Library/Preferences/com.apple.CrashReporter.plist* from RootDomain
2019-06-13 11:15:53	File created: *Library/Preferences/roleaccountd.plist* from RootDomain
2019-06-13 12:39:40	Process record deleted from ZPROCESS (IN: 3.69 MB, OUT: 27.39 MB)
2019-06-15 08:06:27	Process record deleted from ZPROCESS (IN: 0.32 MB, OUT: 0.56 MB)
2019-07-25 09:31:09	Process record deleted from ZPROCESS (IN: 7.80 MB, OUT: 6.43 MB)

2019-08-16 10:13:19	Process record deleted from ZPROCESS (IN: 18 MB, OUT: 29.81 MB)
2019-09-15 15:30:44	Process record deleted from ZPROCESS (IN: 1.27 MB, OUT: 3.34 MB)
2019-09-17 06:33:24	Process record deleted from ZPROCESS (IN: 2.00 MB, OUT: 5.57 MB)
2019-09-24 13:26:15	iMessage lookup for account jessicadavies1345[@]outlook.com
2019-09-24 13:26:51	iMessage lookup for account emmadavies8266[@]gmail.com
2019-09-24 13:32:10	Process: roleaccountd (IN: 0.02 MB, OUT: 0.003 MB)
2019-09-24 13:32:11	Process: roleaccountd
2019-09-24 13:32:13	Process: stagingd (IN: 4.03 MB, OUT: 0.19 MB)
2019-09-24 13:32:23	Process: stagingd
2019-09-26 14:32:25	Process record deleted from ZPROCESS (IN: 1.16 MB, OUT: 2.81 MB)
2019-10-24 05:40:33	Process record deleted from ZPROCESS (IN: 12.81 MB, OUT: 46 MB)

FORENSIC TRACES FOR HUJRN2 - SZABOLCS PANYI

Date (UTC)	Event
2019-04-04 05:33:02	File created: *Library/Preferences/com.apple.CrashReporter.plist* from RootDomain
2019-04-04 05:33:12	File created: *Library/Preferences/roleaccountd.plist* from RootDomain
2019-04-04 06:02:26	Process: libbmanaged (IN: 23.29 MB, OUT: 21.39 MB)
2019-04-06 21:47:45	Process: libbmanaged
2019-07-05 08:35:28	Process: ckeblld (IN: 45.44 MB, OUT: 118.06 MB)
2019-07-12 20:49:11	Process: ckeblld
2019-07-13 20:32:28	Process: ckeblld
2019-07-15 12:02:37	iMessage lookup for account e\x00\x00adavies8266[@]gmail.com (emmadavies8266[@]gmail.com)
2019-07-15 14:21:40	Process: accountpfd (IN: 0.88 MB, OUT: 1.77 MB)
2019-07-16 14:25:11	Process: accountpfd
2019-08-29 10:57:43	Process: roleaccountd (IN: 0.01 MB, OUT: 0.003 MB)
2019-08-29 10:57:44	Process: stagingd (IN: 4.05 MB, OUT: 0.20 MB)
2019-08-29 10:58:35	Process: launchrexd (IN: 0.03 MB, OUT: 0.01 MB)
2019-09-03 07:54:26	Process: roleaccountd
2019-09-03 07:54:28	Process: stagingd
2019-09-03 07:54:51	Process: seraccountd (IN: 20.94 MB, OUT: 7.52 MB)
2019-09-05 08:00:15	Process: seraccountd
2019-09-05 13:26:38	Process: seraccountd
2019-09-05 13:26:55	Process: misbrigd (IN: 10.12 MB, OUT: 8.13 MB)
2019-09-06 13:27:04	Process: misbrigd
2019-09-06 22:04:12	Process: misbrigd
2019-09-10 06:09:04	iMessage lookup for account emmadavies8266[@]gmail.com
2019-09-10 06:09:49	iMessage lookup for account jessicadavies1345[@]outlook.com
2019-10-30 14:09:51	Process: nehelprd (IN: 23.45 MB, OUT: 8.64 MB)
2019-11-04 14:27:48	Process: nehelprd
2019-11-07 01:58:52	Process: nehelprd

FORENSIC TRACES FOR HUPOI1

Date (UTC)	Event
2018-06-01 12:33:08	Process: stagingd
2018-06-01 12:33:08	Process: roleaccountd
2018-06-01 12:35:55	Process: fmld
2018-06-05 18:21:35	Process: stagingd (IN: 7.17 MB, OUT: 0.01 MB)
2018-06-08 14:42:05	Process: fmld (IN: 3.52 MB, OUT: 0.07 MB)
2018-06-21 07:02:55	File created: Library/Preferences/com.apple.CrashReporter.plist from RootDomain
2018-06-21 07:03:19	Process: roleaccountd (IN: 0.05 MB, OUT: 0.00 MB)
2018-06-21 07:03:31	Process: stagingd
2018-06-27 05:04:19	Thumper lookup for account k.williams.enny74[@]gmail.com
2018-06-27 08:09:04	Process: bh (IN: 4.42 MB, OUT: 0.29 MB)
2018-07-09 08:30:34	Process: bh
2018-07-10 08:31:19	Process: fmld (IN: 22.54 MB, OUT: 64.62 MB)
2018-07-10 09:40:37	Process: fmld

FORENSIC TRACES FOR HUPOI2 - ADRIEN BEAUDUIN

Date (UTC)	Event
2018-12-19 09:13:48	File created: Library/Preferences/com.apple.CrashReporter.plist from RootDomain
2018-12-19 09:15:57	File modified: Library/Caches from RootDomain
2018-12-20 11:06:49	Thumper lookup for account k.williams.enny74[@]gmail.com

FORENSIC TRACES FOR HUPOI3

Date (UTC)	Event
2018-06-01 10:12:49	IMessage lookup for k.williams.enny74[@]gmail.com

FORENSIC TRACES FOR INHRD1 - SAR GEELANI

Date (UTC)	Event
2017-07-05 15:01:28	Process: pcsd
2017-11-30 09:26:33	Process: pcsd (IN: 24.09 MB, OUT: 211.43 MB)
2017-12-19 06:48:00	Process: pcsd
2018-02-13 12:46:10	SMS from +447797801009: United Nations launches online portal for the independence of Kashmir. To cast your online vote click here http://bit[.]ly/2o487h1 (https://signpetition[.]co/vU1zwaqFh)
2018-02-15 12:06:01	SMS from +447797801009: BJP hatches conspiracy for a muslim free Jammu region through medical poisoning of muslims. http://bit[.]ly/2o95TNh (https://news-alert[.]org/TfteZB6wK)
2018-02-16 09:44:46	SMS from +447797801009: Another incident showing Indian army beating librandu Kashmiri youth mercilessly to chant Pakistan Murdabad. http://bit[.]ly/2ob9QkO (https://news-alert[.]org/K9pAkFk3R)

2018-04-12 14:10:57	SMS from +447797801009: Organization of Islamic countries(OIC) launches online portal for the independence of Kashmir from India. For the detailed article, click here http://bit[.]ly/2Hk1UJE (https://news-alert[.]org/WW7G1EW2)
2018-04-13 13:13:30	SMS from +447797801009: Global powers urge Indian leadership to concede the entire Jammu & Kashmir to Pakistan for regional peace and stability. For the detailed article, click here. https://news-alert[.]org/T1q4YjltT
2018-04-16 10:52:26	SMS from +447797801009: Hot & sexy male & female escorts available at 60% discount. To avail the service, please click on https://my-privacy[.]co/Ooboe7u
2018-04-17 12:39:36	SMS from +447797801009: European Union leads its unconditional support to India over the issue of Kashmir during the current visit of PM Modi. For more details, click https://my-privacy[.]co/j2xgK558
2018-04-20 13:36:02	SMS from +447797801009: India & America strategically conspiring for the failure of China Pakistan Economic Corridor(CPEC). For the detailed article, click here. https://my-privacy[.]co/ZOubFbXW
2018-04-23 12:58:31	SMS from +447797801009: Syed Ali Shah Geelani comes out with 5 point proposal for India, Pak. http://bit[.]ly/2HkhW2L (https://news-alert[.]org/1M2VbKPeB)
2018-04-27 08:17:38	SMS from +447797801009: Pakistan always stood like a rock guarding Kashmir cause says Geelani. http://bit[.]ly/2Fl7Dtq (https://news-alert.org/xdwWVvCP)
2018-04-27 12:02:13	SMS from +447797801009: Yasin Malik to address press conference at UN.For detail news click at http://bit[.]ly/2FlNjIC (https://news-alert[.]org/CyCX97BO)
2018-05-01 11:57:38	SMS from +447797801009: Pakistan strategically preparing to put the issue of Kashmir in International Court of Justice. Read full storey here http://bit[.]ly/2Fwg2dH (https://news-alert[.]org/AXJ1n6e)
2018-05-02 12:36:16	SMS from +447797801009: Pakistan in all probability will become the next province of China through China Pakistan Economic Corridor (CPEC). For the detailed article, click here. https://news-alert[.]org/KYz4FG6
2018-05-18 04:37:42	Process: fmld
2018-05-24 04:18:31	Process: roleaccountd
2018-05-24 04:18:41	Process: stagingd
2018-07-20 14:05:14	Thumper lookup for account taylorjade0303[@]gmail.com
2018-10-24 08:48:04	Process: fmld (IN: 208.63 MB, OUT: 3591.56 MB)
2018-10-27 07:05:42	Process: roleaccountd (IN: 0.28 MB, OUT: 0.04 MB)
2018-10-27 07:05:50	Process: stagingd (IN: 53.02 MB, OUT: 0.15 MB)
2018-10-28 07:09:14	Process: fmld (IN: 1.84 MB, OUT: 110.30 MB)
2018-10-29 07:16:51	Process: fmld (IN: 1.70 MB, OUT: 69.41 MB)
2018-10-30 07:25:43	Process: fmld (IN: 1.25 MB, OUT: 4.15 MB)
2018-10-31 07:29:37	Process: fmld (IN: 0.63 MB, OUT: 19.51 MB)

2018-12-08 07:24:18	Process: **fmld** (IN: 9.88 MB, OUT: 150.38 MB)
2018-12-10 06:23:11	Process: **fmld**
2018-12-27 09:44:30	Process: **otpgrefd** (IN: 1.66 MB, OUT: 20.07 MB)
2018-12-28 09:08:32	Process: **otpgrefd**
2018-12-31 06:37:59	Process: **bfrgbd**
2019-01-02 06:45:14	Process: **bfrgbd** (IN: 3.02 MB, OUT: 59.12 MB)
2019-01-02 15:34:37	Process: **bfrgbd**
2019-01-03 07:13:41	Process: **stagingd** (IN: 12.96 MB, OUT: 0.05 MB)
2019-01-03 07:20:50	Process: **fservernetd** (IN: 0.58 MB, OUT: 15.90 MB)
2019-01-03 08:35:44	Process: **fservernetd**
2019-01-05 05:28:58	Process: **libtouchregd** (IN: 1.04 MB, OUT: 41.43 MB)
2019-01-05 05:33:02	Process: **libtouchregd** (IN: 0.00 MB, OUT: 0.38 MB)
2019-01-07 06:06:22	Process: **roleaccountd** (IN: 0.05 MB, OUT: 0.01 MB)
2019-01-07 06:09:43	Process: **stagingd**
2019-01-07 06:11:34	Process: **accountpfd** (IN: 1.41 MB, OUT: 9.05 MB)
2019-01-07 18:13:34	Process: **accountpfd**
2019-01-25 07:26:52	Thumper lookup for account **lee.85.holland[@]gmail.com**
2019-01-25 07:33:59	File created: *Library/Preferences/com.apple.CrashReporter.plist* from RootDomain
2019-01-25 07:34:08	File created: *Library/Preferences/com.apple.CrashReporter.plist* from RootDomain
2019-01-26 14:16:19	File created: *Library/Preferences/com.apple.CrashReporter.plist* from RootDomain
2019-09-22 05:14:27	iMessage lookup for account **bekkerfredi[@]gmail.com**
2019-09-27 09:20:58	SMS from +9159039000: Trump to mediate between India and Pakistan on Kashmir **https://bit[.]ly/ecICPjk**
2019-09-27 09:32:59	Process: **bh** (IN: 1.47 MB, OUT: 0.09 MB)
2019-09-27 09:33:49	Process: **natgd** (IN: 19.95 MB, OUT: 171.65 MB)
2019-09-28 13:49:07	Process: **natgd**
2019-10-15 08:40:38	SMS from +9156161940: Get Rs 100 off on recharge of your Tata Sky Id 1093453759 **https://todaysdeals4u[.]com/n7V7uA4X5**
2019-10-18 10:34:49	SMS from +9156161940: Avail extra benefits on recharge of your Tata Sky Id 1093453759 **https://todaysdeals4u[.]com/KjtvDBA**
2019-10-23 17:07:15	Process: **frtipd** (IN: 2.24 MB, OUT: 2.87 MB)
2019-10-24 19:27:51	Process: **frtipd**

FORENSIC TRACES FOR INJRN1 - MANGALAM KESAVAN VENU

Date (UTC)	Event
2021-02-16 18:40:27	Process: **frtipd**
2021-02-22 21:34:35	Process: **otpgrefd**
2021-03-25 08:11:28	Process: **boardframed**
2021-03-25 08:11:28	Process: **comsercvd**
2021-05-15 05:06:16	Process: **llmdwatchd**

2021-05-15 05:06:16	Process: aggregatenotd
2021-05-21 19:17:37	Process: setframed
2021-06-03 19:15:52	Process: seraccountd
2021-06-07 07:09:16	Upgrade from iOS 14.4.2 to 14.6
2021-06-11 14:02:14	Process: comsercvd
2021-06-11 14:02:14	Process: Diagnostics-2543
2021-06-16 05:53:28	Process: actmanaged
2021-06-16 05:53:28	Process: nehelprd
2021-06-16 05:53:29	Process: cfprefssd
2021-06-16 05:58:43	Process: actmanaged
2021-06-16 06:18:04	Process: actmanaged
2021-06-16 07:01:03	Process: actmanaged
2021-06-16 07:16:45	Process: cfprefssd
2021-06-16 07:16:45	Process: nehelprd
2021-06-23 13:39:51	Process record deleted from ZPROCESS (IN: 0.20 MB, OUT: 2.04 MB)
2021-06-27 03:27:12	iMessage lookup for account herbruud2[@]gmail.com
2021-06-27 03:49:51	Process: corecomnetd (IN: 1.25 MB, OUT: 13.20 MB)
2021-06-28 11:11:36	Process: corecomnetd (IN: 0.03, OUT: 0.04 MB)
2021-06-29 07:26:55	Process: corecomnetd

FORENSIC TRACES FOR INJRN2 - SUSHANT SINGH

Date (UTC)	Event
2021-03-31 13:45:32	Process: CommsCenterRootHelper (IN: 0.01 MB, OUT: 4.41 KB)
2021-03-31 13:45:46	Process: CommsCenterRootHelper
2021-04-07 09:34:40	Process: eventfssd
2021-04-07 09:34:40	Process: locserviced
2021-04-13 08:52:18	Process: accountpfd
2021-04-13 08:52:18	Process: fservernetd
2021-04-19 15:49:38	Process: otpgrefd
2021-04-19 15:49:38	Process: ckeblld
2021-04-26 13:54:30	Process record deleted from ZPROCESS (IN: 4.24 MB, OUT: 2.19 MB)
2021-04-27 03:34:16	Process: comsercvd
2021-06-05 13:36:54	Process record deleted from ZPROCESS (IN: 0.11 MB, OUT:
2021-06-06 13:38:51	Process record deleted from ZPROCESS (IN: 0.10 MB, OUT: 0.11 MB)
2021-06-07 13:41:51	Process record deleted from ZPROCESS (IN: 0.16 MB, OUT: 0.17 MB)
2021-06-08 13:42:25	Process record deleted from ZPROCESS (IN: 0.11MB, OUT: 0.13 MB)
2021-06-10 13:42:35	Process record deleted from ZPROCESS (IN: 0.10 MB, OUT: 0.11 MB)
2021-06-12 19:09:37	Process: faskeepd
2021-06-12 19:09:37	Process: logseld
2021-06-18 09:40:45	Process record deleted from ZPROCESS (IN: 0.20 MB, OUT: 0.23 MB)
2021-06-19 14:25:16	Process record deleted from ZPROCESS (IN: 0.04 MB, OUT:
2021-06-19 17:05:21	Process: xpccfd

2021-06-19 17:05:21	Process: pstid
2021-06-21 05:29:38	iMessage lookup for account herbruud2[@]gmail.com
2021-06-21 05:56:55	Process: bfrgbd
2021-06-21 05:56:55	Process: msgacntd
2021-06-21 05:56:55	Process: CommsCenterRootHelper
2021-06-21 06:29:13	Process: bfrgbd
2021-06-21 06:59:25	Process: bfrgbd
2021-06-21 08:22:27	Process: bfrgbd (IN: 1.02 MB, OUT: 2.25 MB)
2021-06-21 13:33:03	Process: bfrgbd
2021-06-21 13:33:03	Process: msgacntd
2021-06-21 13:33:03	Process: CommsCenterRootHelper
2021-06-21 13:34:01	Process: bfrgbd
2021-06-21 13:34:01	Process: msgacntd
2021-06-21 13:34:01	Process: CommsCenterRootHelper
2021-06-22 09:47:01	Process: bfrgbd (IN: 0.50 MB, OUT: 0.65 MB)
2021-06-22 14:06:24	Process: bfrgbd
2021-06-22 14:06:24	Process: msgacntd
2021-06-22 14:06:24	Process: CommsCenterRootHelper
2021-06-23 09:50:46	Process: bfrgbd (IN: 0.86 MB, OUT: 1.05 MB)
2021-06-23 15:02:35	Process: bfrgbd
2021-06-23 15:02:35	Process: msgacntd
2021-06-23 15:02:35	Process: CommsCenterRootHelper
2021-06-24 09:50:51	Process: bfrgbd (IN: 0.44 MB, OUT: 60.72 MB)
2021-06-24 15:02:23	Process: bfrgbd
2021-06-24 15:02:23	Process: msgacntd
2021-06-24 15:02:23	Process: CommsCenterRootHelper
2021-06-25 09:59:00	Process: bfrgbd (IN: 0.74 MN, OUT: 5.53 MB)
2021-06-25 15:03:09	Process: bfrgbd
2021-06-25 15:03:09	Process: msgacntd
2021-06-25 15:03:09	Process: CommsCenterRootHelper
2021-06-26 13:04:37	Process: bfrgbd (IN: 0.08 MB, OUT: 0.09 MB)
2021-06-26 16:18:41	Process: bfrgbd
2021-06-26 16:18:41	Process: msgacntd
2021-06-26 16:18:41	Process: CommsCenterRootHelper
2021-06-26 16:22:12	Process: bfrgbd
2021-06-26 16:22:12	Process: msgacntd
2021-06-26 16:22:12	Process: CommsCenterRootHelper
2021-06-27 13:34:07	Process: bfrgbd (IN: 0.91 MB, OUT: 1.29 MB)
2021-06-28 00:04:15	Process: bfrgbd
2021-06-28 00:04:15	Process: msgacntd
2021-06-28 00:04:15	Process: CommsCenterRootHelper
2021-06-28 13:37:38	Process: bfrgbd (IN: 0.43 MB, OUT: 0.60 MB)
2021-06-29 06:39:31	Process: bfrgbd

2021-06-29 06:39:31	Process: **msgacntd**
2021-06-29 06:39:31	Process: **CommsCenterRootHelper**
2021-06-29 06:40:42	Process: **bfrgbd**
2021-06-29 06:40:42	Process: **msgacntd**
2021-06-29 06:40:42	Process: **CommsCenterRootHelper**
2021-06-29 14:12:36	Process: **bfrgbd** (IN: 0.14 MB, OUT: 0.17 MB)
2021-06-30 07:15:33	Process: **bfrgbd**
2021-06-30 07:15:33	Process: **msgacntd**
2021-06-30 07:15:33	Process: **CommsCenterRootHelper**
2021-06-30 14:15:33	Process: **bfrgbd** (IN: 0.61 MB, OUT: 1.90 MB)
2021-07-01 14:19:26	Process: **bfrgbd** (IN: 0.30 MB, OUT: 0.46 MB)
2021-07-01 14:33:08	Process: **bfrgbd**
2021-07-01 14:33:08	Process: **msgacntd**
2021-07-01 14:33:08	Process: **CommsCenterRootHelper**
2021-07-02 14:20:32	Process: **bfrgbd** (IN: 0.43 MB, OUT: 0.50 MB)
2021-07-03 04:14:29	Process: **bfrgbd**
2021-07-03 04:14:29	Process: **msgacntd**
2021-07-03 04:14:29	Process: **CommsCenterRootHelper**
2021-07-03 14:27:24	Process: **bfrgbd** (IN: 0.03 MB, OUT: 0.02 MB)
2021-07-04 05:34:57	Process: **bfrgbd**
2021-07-04 05:34:57	Process: **msgacntd**
2021-07-04 05:34:57	Process: **CommsCenterRootHelper**
2021-07-04 14:39:00	Process: **bfrgbd** (IN: 0.77 MB, OUT: 0.91 MB)
2021-07-05 09:40:02	Process: **bfrgbd**
2021-07-05 12:12:01	Process: **bfrgbd**
2021-07-05 12:12:01	Process: **msgacntd**
2021-07-05 12:12:01	Process: **CommsCenterRootHelper**
2021-07-05 12:13:31	Process: **bfrgbd**
2021-07-05 12:13:31	Process: **msgacntd**
2021-07-05 12:13:31	Process: **CommsCenterRootHelper**
2021-07-05 12:50:32	Process: **msgacntd**
2021-07-05 12:50:32	Process: **bfrgbd**

FORENSIC TRACES FOR INJRN3 - SNM ABDI

Date (UTC)	Event
2019-04-02 04:51:19	File created: *Library/Preferences/**com.apple.CrashReporter.plist*** from RootDomain
2019-04-02 04:51:40	File created *Library/Preferences/**roleaccountd.plist*** from RootDomain
2019-04-02 04:51:45	Process: **roleaccountd**
2019-04-02 04:51:50	Process: **stagingd**
2019-04-26 03:27:40	Process: **fdlibframed**
2019-04-28 04:00:46	Process: **fdlibframed** (IN: 7.90 MB, OUT: 25.36 MB)
2019-04-29 12:56:34	Process: **fdlibframed**

2019-05-27 04:46:07	Process: xpccfd
2019-05-28 04:48:01	Process: xpccfd (IN: 5.24 MB, OUT: 15.32 MB)
2019-07-04 03:33:11	Process: ckeblld (IN: 7.91 MB, OUT: 33.05 MB)
2019-07-05 01:22:18	Process: ckeblld
2019-07-05 09:22:54	Process: lobbrogd (IN: 3.76 MB, OUT: 15.59 MB)
2019-07-06 03:20:03	Process: lobbrogd
2019-07-08 05:56:52	Process: xpccfd (IN: 5.69 MB, OUT: 16.14 MB)
2019-07-10 01:24:04	Process: xpccfd
2019-07-11 06:46:37	Process: pstid (IN: 3.59 MN, OUT: 12.08 MB)
2019-07-11 13:41:50	Process: pstid
2019-07-12 09:07:18	Process: roleaccountd (IN: 0.03 MB, OUT: 0.02 MB)
2019-07-12 09:08:07	Process: boardframed (IN: 6.24 MB, OUT: 32.14 MB)
2019-07-12 14:15:01	Process: boardframed
2019-07-15 06:07:28	Process: stagingd (IN: 8.49 MB, OUT: 0.5 MB)
2019-07-15 18:08:57	Process: ckkeyrollfd
2019-10-19 04:32:33	Process: roleaccountd (IN: 0.04 MB, OUT: 0.02 MB)
2019-10-19 04:33:46	Process: launchafd (IN: 1.28 MB, OUT: 6.48 MB)
2019-10-19 06:10:04	Process: launchafd
2019-10-21 07:07:16	Process: netservcomd (IN: 0.22 MB, OUT: 1.26 MB)
2019-10-21 07:31:16	Process: netservcomd
2019-10-23 03:48:40	Process: roleaccountd
2019-10-23 03:48:47	Process: stagingd (IN: 7.03 MB, OUT: 0.41 MB)
2019-10-23 03:49:02	Process: stagingd
2019-10-23 03:49:24	Process: misbrigd
2019-10-24 03:50:28	Process: misbrigd (IN: 15.79 MB, OUT: 99.28 MB)
2019-12-22 11:15:30	Process: netservcomd
2019-12-22 11:15:30	Process: launchafd
2019-12-22 11:15:30	Process: misbrigd

FORENSIC TRACES FOR INJRN4 - SIDDHARTH VARADARAJAN

Date (UTC)	Event
2018-04-06 08:17:14	Process: roleaccountd (IN: 0.03 MB, OUT: 0.01 MB)
2018-04-06 08:17:22	Process: stagingd
2018-04-06 08:18:47	Process: pcsd
2018-04-24 07:57:53	Process: stagingd (IN: 4.15 MB, OUT: 0.02 MB)
2018-04-24 07:57:56	Process: roleaccountd
2018-04-24 07:58:16	Process: stagingd
2018-04-26 05:35:12	Process: pcsd (IN: 16.30 MB, OUT: 329.17 MB)
2018-04-26 12:24:42	Process: pcsd
2018-04-27 04:41:37	File created Library/Preferences/com.apple.CrashReporter.plist in RootDomain

FORENSIC TRACES FOR INJRN5 - PARANJOY GUHA THAKURTA

Date (UTC)	Event
2018-04-04 05:33:47	Process: roleaccountd
2018-04-04 05:33:49	Process: stagingd
2018-05-15 07:46:30	Process: pcsd
2018-05-22 04:17:46	Process: roleaccountd (IN: 0.04 MB, OUT: 0.01 MB)
2018-05-22 04:17:59	Process: stagingd (IN: 5.18 MB, OUT: 0.02 MB)
2018-05-22 04:18:08	Process: pcsd (IN: 3.25 MB, OUT: 20.54 MB)
2018-05-22 04:18:17	Process: pcsd
2018-05-22 04:18:48	Process: fmld
2018-06-20 10:44:14	Process: roleaccountd
2018-06-20 10:44:31	Process: stagingd
2018-07-25 03:58:42	File created Library/Preferences/com.apple.CrashReporter.plist from RootDomain
2018-07-29 13:07:51	Process: fmld (IN: 55.21 MB, OUT: 417.58 MB)
2018-07-30 11:07:56	Process: fmld

FORENSIC TRACES FOR INJRN6 - SMITA SHARMA

Date (UTC)	Event
2018-06-25 17:31:37	iMessage lookup for taylorjade0303[@]gmail.com
2018-07-20 11:11:49	iMessage lookup for lee.85.holland[@]gmail.com

FORENSIC TRACES FOR INJRN7

Date (UTC)	Event
2019-06-12 08:48:04	SMS "R&AW and IB chief to get three months extension. Read full story https://globalnews247[.]net/3BMw9Zj"

FORENSIC TRACES FOR INPOI1 - PRASHANT KISHOR

Date (UTC)	Event

2018-06-21 13:23:30	Thumper lookup for account taylorjade0303[@]gmail.com
2018-09-06 09:11:49	Thumper lookup for account lee.85.holland[@]gmail.com
2021-04-28 03:31:39	Process: ReminderIntentsUIExtension (IN: 0.01 MB, OUT: 0.00 MB)
2021-04-28 03:31:39	Process: ReminderIntentsUIExtension
2021-04-28 03:31:45	Process: ReminderIntentsUIExtension
2021-06-11 12:45:48	Process record deleted from ZPROCESS (IN: 0.01 MB, OUT: 0.00 MB)
2021-06-11 12:46:22	Process record deleted from ZPROCESS (IN: 1.79 MB, OUT: 0.31 MB)
2021-06-11 12:46:47	Process record deleted from ZPROCESS (IN: 12.94 MB, OUT: 145.88 MB)
2021-06-14 06:17:10	Process record deleted from ZPROCESS (IN: 2.36 MB, OUT: 2.76 MB)
2021-06-15 06:21:28	Process record deleted from ZPROCESS (IN: 1.05 MB, OUT: 1.29 MB)
2021-06-16 13:47:51	Process record deleted from ZPROCESS (IN: 0.16 MB, OUT: 0.16 MB)
2021-06-18 13:52:14	Process record deleted from ZPROCESS (IN: 0.01 MB, OUT: 0.00 MB)
2021-06-18 13:53:37	Process record deleted from ZPROCESS (IN: 1.79 MB, OUT: 0.31 MB)
2021-06-18 13:58:41	Process record deleted from ZPROCESS (IN: 13.63 MB, OUT: 172.99 MB)
2021-06-19 14:16:20	Process record deleted from ZPROCESS (IN: 0.87 MB, OUT: 1.02 MB)
2021-06-21 05:44:29	Process record deleted from ZPROCESS (IN: 1.81 MB, OUT: 2.58 MB)
2021-06-22 05:45:29	Process record deleted from ZPROCESS (IN: 1.19 MB, OUT: 1.38 MB)
2021-06-23 05:49:37	Process record deleted from ZPROCESS (IN: 0.98 MB, OUT: 1.19 MB)
2021-06-24 05:57:02	Process record deleted from ZPROCESS (IN: 2.66 MB, OUT: 24.15 MB)
2021-06-25 05:57:03	Process record deleted from ZPROCESS (IN: 1.98 MB, OUT: 2.77 MB)
2021-06-26 06:01:26	Process record deleted from ZPROCESS (IN: 0.35 MB, OUT: 0.47 MB)
2021-06-27 06:06:59	Process record deleted from ZPROCESS (IN: 0.42 MB, OUT: 0.49 MB)
2021-06-28 13:19:57	Process record deleted from ZPROCESS (IN: 1.12 MB, OUT: 7.33 MB)
2021-06-30 04:50:04	Process record deleted from ZPROCESS (IN: 1.51 MB, OUT: 6.50 MB)

2021-07-01 04:50:49	Process record deleted from ZPROCESS (IN: 0.52 MB, OUT: 0.60 MB)
2021-07-02 05:08:42	Process record deleted from ZPROCESS (IN: 1.48 MB, OUT: 1.73 MB)
2021-07-03 05:33:23	Process record deleted from ZPROCESS (IN: 1.00 MB, OUT: 2.03 MB)
2021-07-05 11:44:29	Traces related to iMessage attack
2021-07-05 11:48:34	File created: Library/Caches from RootDomain
2021-07-05 11:48:35	Process record deleted from ZPROCESS (IN: 0.01 MB, OUT: 0.00 MB)
2021-07-05 11:49:27	Process: CommsCenterRootHelper (IN: 1.88 MB, OUT: 0.31 MB)
2021-07-05 11:49:27	Process: CommsCenterRootHelper
2021-07-05 11:50:19	Process record deleted from ZPROCESS (IN: 7.57 MB, OUT: 90.71 MB)
2021-07-07 04:11:55	Process record deleted from ZPROCESS (IN: 0.62 MB, OUT: 0.77 MB)
2021-07-08 12:21:05	iMessage lookup for account herbruud2[@]gmail.com
2021-07-08 12:27:04	Process record deleted from ZPROCESS (IN: 0.01 MB, OUT: 0.00 MB)
2021-07-08 12:27:18	Process record deleted from ZPROCESS (IN: 1.88 MB, OUT: 0.23 MB)
2021-07-08 12:28:14	Process: smmsgingd (IN: 6.94 MB, OUT: 82.77 MB)
2021-07-09 12:59:49	Process: smmsgingd (IN: 0.45 MB, OUT: 0.51 MB)
2021-07-12 08:45:26	Process: smmsgingd (IN: 2.69 MB, OUT: 7.99 MB)
2021-07-13 08:47:45	Process: smmsgingd (IN: 1.23 MB, OUT: 8.63 MB)
2021-07-14 09:26:50	Process: smmsgingd (IN: 0.77 MB, OUT: 2.28 MB)
2021-07-14 13:17:15	Process: smmsgingd

FORENSIC TRACES FOR INPOI2

Date (UTC)	Event
2019-10-18 03:59:01	iMessage lookup for bekkerfredi[@]gmail.com

FORENSIC TRACES FOR KASH01 - HATICE CENGIZ

Date (UTC)	Event
2018-10-06 00:33:28	File created: *Library/Preferences/com.apple.CrashReporter.plist* from RootDomain
2018-10-06 07:30:13	Process: fmld (IN: 33.27 MB, OUT: 324.72 MB)
2018-10-09 07:12:39	Process: bh (IN: 1.49 MB, OUT: 0.95 MB)
2018-10-09 07:13:07	Process: bh
2018-10-12 08:30:33	Process: fmld
2018-10-12 21:23:23	Process: fmld
2019-06-02 16:05:23	iMessage lookup for account vincent.dahl76[@]gmail.com

FORENSIC TRACES FOR KASH02 - RODNEY DIXON

Date (UTC)	Event
2019-04-29 10:50:44	iMessage lookup for account vincent.dahl76[@]gmail.com

FORENSIC TRACES FOR KASH03 - WADAH KHANFAR

Phone 1:

Date (UTC)	Event
2019-11-02 17:19:22	Process record deleted from ZPROCESS
2019-11-02 17:19:29	File created *Library/Preferences/com.apple.CrashReporter.plist* by RootDomain
2019-11-02 17:20:23	Process record deleted from ZPROCESS
2021-04-11 08:35:25	Process: ReminderIntentsUIExtension (IN: 0.01 MB, OUT: 0.00 MB)
2021-04-11 08:35:33	Process: ReminderIntentsUIExtension
2021-06-30 08:58:04	iMessage lookup for account oskarschalcher[@]outlook.com
2021-06-30 09:34:34	Process: com.apple.Mappit.SnapshotService (IN: 0.02 MB, OUT: 0.01 MB)
2021-06-30 09:34:40	Process: com.apple.Mappit.SnapshotService

Phone 2:

Date (UTC)	Event
2021-04-02 10:43:27	iMessage lookup for oskarschalcher[@]outlook.com

FORENSIC TRACES FOR KASH04 – HANAN EL ATR

Date (UTC)	Event
2017-11-08 10:22	Malicious SMS from VERIFY: WhatsApp Web for [REDACTED] is now active on CHROME in ABU DHABI. Not you? Click here: hxxps://noonstore[.]sale/tkYHFbE
2017-11-15 09:01	Malicious SMS from VERIFY: Emirates AIrline changing the game in first class travel: hxxp://bit[.]ly/2A00EI7
2017-11-19	Malicious SMS from VERIFY: Dear Hanan Elatr, Nada shared a photo with you on Photobucket! Click here to view it and download our app. hxxp://bit[.]ly/AbzvEMS
2018-11-26 17:16:48	Malicious link in browsing history: https://done[.]events/TajbxOGh5

2017-11-27 08:48	Malicious SMS: Dear HANA you have a package from CAIRO via Aramex, enter PIN 3483 and choose delivery location on our map: https://bit[.]ly/2zxnwOF
2018-04-15 09:33	Malicious SMS from SMSINFO: MONA ELATR shared a photo with you on Photobucket! Click here to view it and download our app: https://myfiles[.]photo/sVIKHJE

FORENSIC TRACES FOR MOJRN1 – HICHAM MANSOURI

Date (UTC)	Event
2021-02-04 10:31:36	Process: CommsCenterRootHelper (IN: 0.01 MB, OUT: 0.00 MB)
2021-02-11 13:45:07	Process: CommsCenterRootHelper
2021-04-02 10:15:38	iMessage lookup for account linakeller2203[@]gmail.com

Forensic traces for MXJRN1

Date (UTC)	Event
2016-08-03 21:52:00	SMS: Hola Alvaro unicamente paso a saludarte y enviarte esta nota de the guardian que parece importante retomar: http://bit[.]ly/2ayGnMm (https://smsmensaje[.]mx/5901888s/)

FORENSIC TRACES FOR MXJRN2 – CARMEN ARISTEGUI

These Pegasus attack messages were original discovered and published as part of collaborative investigation between Citizen Lab, R3D, SocialTic and Article 19.

Date (UTC)	Event
2014-11-20 03:10:04	SMS from +525536438524: El siguiente mensaje esta marcado como urgente y no se recibio correctamente. http://smsmensaje[.]mx/5103285s/
2014-12-17 19:32:13	SMS from +525511393977: El siguiente mensaje no ha sido enviado http://smscentro[.]com/7984947s/
2015-01-06 18:29:53	SMS from +525512350872: El siguiente mensaje no ha sido enviado http://smscentro[.]com/4064303s/
2015-01-09 19:45:57	SMS from +525512350872: El siguiente mensaje no ha sido enviado http://tinyurl[.]com/l8cwcc5 (http://smscentro[.]com/1097486s/)
2015-01-13 01:59:19	SMS from +525511393877: El siguiente mensaje no ha sido enviado http://bit[.]ly/1z2NQdh (http://smscentro[.]com/9480260s/)
2015-03-26 18:15:59	SMS from +525585292665: El numero 5535606234 le ha enviado un mensaje de texto que no se recibio. Entre a http://iusacell-movil[.]com[.]mx/6731340s/ para ver el sms
2015-04-12 22:41:24	SMS from +525525715066: Notificacion de compra con tarjeta **** monto $3,500.00 M.N, ver detalles en: http://smsmensaje[.]mx/1493024s/
2015-05-08 19:49:23	SMS from +525525715066: Aviso de vencimiento de pago asociado a tu servicio con cargo a tu tarjeta ****, ver mas detalles: http://smsmensaje[.]mx/6445761s/

2015-05-08 23:19:14	SMS from +525585292665: El siguiente mensaje esta marcado como urgente y no se recibio correctamente, recuperalo en .. http://smsmensaje[.]mx/3863925s/
2015-05-09 01:24:29	SMS from +525525715066: Haz realizado un Retiro/Compra en tienda departamental **** monto $2,500.00 M.N, ver detalles http://smsmensaje[.]mx/9936510s/
2015-05-09 02:42:26	SMS from +525585292665: Haz realizado un Retiro/Compra en tienda departamental **** monto $2,500.00 M.N, ver detalles http://smsmensaje[.]mx/1796758s/
2015-05-10 00:09:55	SMS from +525585292665: UNOTV[.]com/ AUDI ENTRE LOS PRINCIPALES AUTOS CON PROBLEMAS EN LA TRANSMICION VERIFICA LA LISTA DE ELLOS: http://unonoticias[.]net/1291412s/
2015-05-11 20:19:20	SMS from +525585292665: El siguiente mensaje esta marcado como urgente y no se recibio correctamente, recuperalo en .. http://smsmensaje[.]mx/6713776s/
2015-05-12 02:05:06	SMS from +525585292665: El siguiente mensaje esta marcado como urgente y no se recibio correctamente, recuperalo en .. http://smsmensaje[.]mx/6318147s/
2015-05-12 04:03:33	SMS from +525525715066: Estimado cliente informamos que presentas un problema de pago asociado a tu servicio, ver detalles.. http://smsmensaje[.]mx/8884678s/
2015-05-12 22:42:53	SMS from +525585292665: Alcanzaste la tarifa premium de IUSACELL $0.30 Min a Celular y $0.10 Nacional, codigo 2207 y activalo ya... http://smsmensaje[.]mx/3432773s/
2015-05-14 00:37:27	SMS from +525585292665: Alcanzaste la tarifa premium de IUSACELL $0.30 Min a Celular y $0.10 Nacional, codigo 2207 activalo ya... http://smsmensaje[.]mx/7534402s/
2015-05-14 02:55:35	SMS from +525525715066: UNONOTICIAS. En encuesta revelan las 3 posiciones sexuales favoritas de las mujeres, ver nota en: http://unonoticias[.]net/6218095s/
2015-05-14 03:24:41	SMS from +525585292665: Retiro/Compra en tienda departamental $4,000.00 M.N 13/05/2015 20:10 hrs ,ver detalles en: http://smsmensaje[.]mx/9550014s/
2015-05-14 19:56:23	SMS from +525585292665: El numero +525541337879 le ha mandado un mensaje de texto que ser ecibio incompleto. Ver mensaje en: http://smsmensaje[.]mx/5670989s/
2015-05-15 01:18:30	SMS from +525585292665: UNOTV. Detectan irregularidades en caso Aristegui, ver nota completa.. http://unonoticias[.]net/4347580s/
2015-06-05 01:56:27	SMS from +525585292665: UNOTV. Que depara el futuro para MVS y cual es el camino de Carmen Aristegui? ver nota completa.. http://unonoticias[.]net/9275690s/
2015-07-26 03:05:05	SMS from +525585292665: TELCEL[.]com/ RECIBISTE CORRECTAMENTE TU FACTURA ELECTRONICA VERIFICA DETALLES DE TU COMPRA: http://ideas-telcel.com[.]mx/9872742s/

2015-07-26 12:34:59	SMS from +525525715066: has realizado un Retiro/Compra Tarjeta**** M.N monto $3,500.00 verifica detalles de operacion: http://smsmensaje[.]mx/6156234s/
2015-07-26 15:23:35	SMS from +525525715066: UNOTV.com/ ANONYMUS ANUNCIA QUE ATACARA PAGINA DE ARISTEGUI VER DETALLES: http://unonoticias[.]net/9250302s/
2015-08-20 19:20:46	SMS from +525525715066: IUSACELL/ Estimado cliente su factura esta lista, agradeceremos pago puntual por $17401.25 Detalles: http://iusacell-movil[.]com[.]mx/8595070s/
2015-08-20 19:34:05	SMS from +525525715066: USEMBASSY.GOV/ DETECTAMOS UN PROBLEMA CON TU VISA POR FAVOR ACUDE PRONTAMENTE A LA EMBAJADA. VER DETALLES: http://bit[.]ly/1MAAWrO (http://smsmensaje[.]mx/9439115s/)
2015-08-23 04:58:47	SMS from +525525715066: IUSACELL.com/ EL SIGUIENTE MENSAJE ESTA MARCADO COMO URGENTE REVISALO DESDE NUESTRO PORTAL VER http://iusacell-movil[.]com[.]mx/7918310s/
2015-08-24 03:03:48	SMS from +525585292665: UNOTV[.]com/ FAMILIA DE CHAPO SE REFUGIA EN GRANDES RESIDENCIAS EN DF ENTRE ELLAS SN JERONIMO VER DONDE: http://unonoticias[.]net/6353793s/
2015-08-24 15:31:38	SMS from +525525715066: ALERTA AMBER DF/ COOPERACION PARA LOCALIZAR A NINO DE 9 ANOS, DESAPARECIDO EN LA COLONIA SAN JERONIMO. DETALLES: http://bit[.]ly/1EQYOkG (http://mymensaje-sms[.]com/6649365s/)
2015-08-24 15:31:59	SMS from +525585292665: ALERTA AMBER DF/ COOPERACION PARA LOCALIZAR A NINO DE 9 ANOS, DESAPARECIDO EN LA COLONIA SAN JERONIMO. DETALLES: http://bit[.]ly/1EQYSB1 (http://mymensaje-sms[.]com/5186565s/)
2015-09-02 18:43:23	SMS from +525585292665: Hola Carmen, solo para desearte una excelente tarde y compartirte la nota que publica proceso sobre el 3er informe: http://bit[.]ly/1JNTfox (http://twiitter[.]com.mx/8527373s/)
2015-09-05 15:39:41	SMS from +525585292665: IUSACELL[.]com / DESCUBRE LA NUEVA TELEFONIA Y CONOCE LAS APLICACIONES MAS SEGURAS PARA TU SMARTPHONE SEGUN EL PENTAGONO http://bit[.]ly/1IQhzFw (http://iusacell-movil[.]com.mx/5726967s/)
2015-09-25 18:47:50	SMS from +525585292665: Queridisima Carmen en la madrugada fallecio mi padre, estamos muy devastados. Mando datos del funeral ojala puedas ir: http://bit[.]ly/1KDGbSR (http://smsmensaje[.]mx/4966295s/)
2015-10-17 18:12:07	SMS from +525585292665: chatita como estas, espero que bien este mi numero nuevo checa esta noticia la subi a drive checala para borrarla urge http://tinyurl[.]com/pfwmr88 (https://googleplay-store[.]com/7863372s/)
2015-10-25 23:39:29	SMS from +525525715066: Hola te envio invitacion electronica con detalles por motivo de mi fiesta de disfraces espero contar contigo

	alonso: http://tinyurl[.]com/o2tq8rl (https://smsmensaje[.]mx/8623600s/)
2016-02-09 17:46:42	SMS from +525552899427: Carmen hace 5 dias que no aparece mi hija te agradecere mucho que compartas su foto, estamos desesperados: http://bit[.]ly/1KDekJ9 (https://smsmensaje[.]mx/5957475s/)
2016-02-10 23:10:59	SMS from +525552899427: Querida Carmen fallecio mi hermano en un accidente, estoy devastada, envio datos del velorio, espero asistas: http://bit[.]ly/1TTjm6D (https://smsmensaje[.]mx/6056487s)
2016-02-11 22:30:48	SMS from +525568850176: Hace 7 dias desaparecio mi hija de 8 a?os en ecatepec, por favor ayudame a compartir su foto, estamos desesperados: https://smsmensaje[.]mx/7430255t/
2016-02-11 22:32:15	SMS from +525568850176: Hace 7 dias desaparecio mi hija de 8 a?os en ecatepec, por favor ayudame a compartir su foto, estamos desesperados: https://smsmensaje[.]mx/7430255t/
2016-02-11 23:58:10	SMS from +525568850176: Perdon en el sms anterior no se veia la foto, la reenvio, por favor compartela queremos a nuestra ni?a de vuelta: https://smsmensaje[.]mx/7430255t/
2016-02-15 04:02:23	SMS from +525547311580: Vinieron unas personas a extorsionarnos si no les dabamos 100mil pesos saben quienes somos tome fotos mira https://fb-accounts[.]com/1324052s/
2016-02-24 15:45:04	SMS from +525552899427: UNOTV[.]com/ LANZA TELEVISA DESPLEGADOS EN TODOS SUS MEDIOS;CRITICA POSTURA DE ORGANIZACION ARTICULO 19. VER: http://bit[.]ly/1SU5N7q (https://unonoticias[.]net/6809853s/)
2016-02-25 15:27:59	SMS from +525552899427: has realizado un Retiro/Compra Tarjeta**** M.N monto $3,500.00 verifica detalles de operacion: http://bit[.]ly/21jxVFW (https://unonoticias[.]net/2250072s/)
2016-03-10 16:09:38	SMS from +529993190183: ARISTEGUI NOTICIAS ESTRENA SERVICIO DE SMS. SUSCRIBASE Y RECIBIRA RESUMEN DE LAS NOTICIAS MAS IMPORTANTES: http://bit[.]ly/225VXRR (https://smsmensaje[.]mx/8807734s/)
2016-03-11 16:19:14	SMS from +529993190183: ARISTEGUI NOTICIAS ESTRENA SERVICIO DE SMS. SUSCRIBASE Y RECIBIRA RESUMEN DE LAS NOTICIAS MAS IMPORTANTES: https://smsmensaje[.]mx/4701759s/
2016-04-05 14:42:23	SMS from +528120754135: ARISTEGUINOTICIASONLINE[.]mx ESTRENA SERVICIO DE SMS. SUSCRIBASE Y RECIBIRA LAS NOTICIAS MAS IMPORTANTES: http://bit[.]ly/1q3n16a (https://smsmensaje[.]mx/7974159s/)
2016-04-07 20:54:12	SMS from +528120953203: ARISTEGUINOTICIASONLINE[.]mx ESTRENA SERVICIO DE SMS. SUSCRIBASE Y RECIBIRA LAS NOTICIAS MAS IMPORTANTES: https://smsmensaje[.]mx/1119786s/

2016-04-12 21:42:40	SMS from +528120943682: ARISTEGUINOTICIASONLINE[.]mx ESTRENA SERVICIO DE SMS. SUSCRIBASE Y RECIBIRA LAS NOTICIAS MAS IMPORTANTES: https://smsmensaje[.]mx/2365691s/
2016-05-11 18:30:07	SMS from +525585401284: UNOTV[.]com/ CONFIRMA PGR QUE HIJO MAYOR DE AMLO LLEVA 48 HRS DESAPARECIDO. DETALLES: http://bit[.]ly/1QYVKaM (https://unonoticias[.]net/5911276s/)
2016-05-13 15:19:47	SMS from +528120531318: Perdon x molestarte pero hace 3 dias que no aparece mi hija te agradecere que me ayudes a compartir su foto: http://bit[.]ly/1Oo7cSS (https://smsmensaje[.]mx/8984621s/)
2016-06-03 18:03:24	SMS from +525585401299: Carmen la pagina esta intermitente, esta apareciendo este error al intentar ingresar: http://bit[.]ly/1WzrZ8T (https://smsmensaje[.]mx/9371877s/)
2016-06-09 19:19:10	SMS from +528120990524: Eres mierda porque yo me ando cojiendo a tu pareja mientras tu pendejeas y de prueba te mando esta foto: http://bit[.]ly/1rfaNHR (https://smsmensaje[.]mx/9449190s/)
2016-06-13 17:38:35	SMS from +525585401299: Hace 3 dias que no aparece mi hija, estamos desesperados, te agradecere que me ayudes a compartir su foto: http://bit[.]ly/235giae (https://smsmensaje[.]mx/1239663s/)
2016-06-15 21:21:29	SMS from +528122090316: Buenas tardes Carmen, unicamente paso a saludarte y enviarte esta nota de Proceso que es importante retomar: http://bit[.]ly/1twXSDI (https://smsmensaje[.]mx/1911343s/)
2016-06-22 21:35:59	SMS from +529993190053: UNOTV[.]com/ REVELAN VIDEO DONDE CRISTIANO RONALDO SE ENFADA Y AVIENTA MICROFONO DE REPORTERO. VIDEO EN: https://unonoticias[.]net/2068822s/
2016-06-28 21:32:09	SMS from +528120696998: UNOTV[.]com/ ATENTADO TERRORISTA EN ESTAMBUL DEJA 30 MUERTOS/SECUESTRAN REPORTERO DE TELEVISA/FALLECE CHACHITA http://bit[.]ly/295RNq7 (https://smsmensaje[.]mx/1656017s/)
2016-07-01 16:45:44	SMS from +528122090348: UNOTV[.]com/ CARMEN ARISTEGUI YA FIRMO CONTRATO PARA REGRESAR A LA RADIO. DETALLES: https://unonoticias[.]net/3423165s/
2016-07-04 20:32:34	SMS from +528121050415: UNOTV[.]com/ AMARILLISMO DE ARISTEGUI VS REALIDAD/ VAN 30 DETENIDOS EN ATENTADO DE ESTAMBUL/ CHILE CAMPEON http://bit[.]ly/29eWzzv (https://unonoticias[.]net/9436744s/)
2016-07-05 18:42:59	SMS from +525536438524: https://fb-accounts[.]com/2102272t/
2016-07-06 21:56:08	SMS from +528122090257: Hace 5 dias q no aparece mi hija te agradecere mucho q compartan su foto, estamos destrozados es un infierno: http://bit[.]ly/29rnk6c (https://smsmensaje[.]mx/7960742s/)
2016-07-12 21:20:25	SMS from +528120697015: UNOTV[.]com/ FILMAN A REPORTERO Y PERIODISTA CUANDO SON LEVANTADOS POR COMANDO ARMADO EN TAMAULIPAS. VIDEO: https://unonoticias[.]net/1887451s/

2016-07-14 20:29:40	SMS from +528122090358: ESTIMADO USUARIO ha realizado un Retiro/Compra Tarjeta M.N de ****** el 14/07/16 10:52:00 AM. Ver DETALLES: https://banca-movil[.]com/4982255s/
2016-07-15 23:56:16	SMS from +528122090286: Mi rey te mando mis fotos encueradita y abiertita asi como te gusta, las ves y las borras eh: http://bit[.]ly/29IQvyh (https://smsmensaje[.]mx/3376811s/)
2016-07-18 17:50:57	SMS from +523319983437: Hola oye abriste nuevo facebook? Me llego una solicitud de un face con tus fotos pero con otro nombre mira: https://fb-accounts[.]com/1607422s/
2016-07-19 17:55:54	SMS from +528113788852: Hola buen martes. Oye que pedo con el puto Lopez Doriga? Mira lo que escribio sobre ti hoy, urge desmentirlo: http://bit[.]ly/29LfZfD (https://smsmensaje[.]mx/9093723s/)
2016-07-22 21:33:26	SMS from +525576169290: Estimado cliente Unefon te informa su saldo vencido al de la lInea 5539290869, es por $4,278. DETALLES: https://ideas-telcel[.]com[.]mx/4729605s/
2016-07-23 17:51:28	SMS from +525576169290: Amigo,hay una pseudo cuenta de fb y twitter identica a la tuya checala para que la denuncies mira checala: https://fb-accounts[.]com/9543697s/
2016-07-25 21:01:24	SMS from +528122090359: Bienvenido Club CHICAS CALIENTES, se ha aplicado un cargo de $875.85 a su linea, si desea cancelar ingrese a: http://bit[.]ly/2a0hZ2I (https://smsmensaje[.]mx/6881768s/)
2016-07-28 22:47:46	SMS from +528120990542: UNOTV[.]com/ VIRAL EL VIDEO DE FUERTE GOLPE QUE RECIBE EN LA CARA OSORIO CHONG PROPINADO POR MAESTRO. VIDEO: https://unonoticias[.]net/6328951s/

FORENSIC TRACES FOR MXJRN3

No timestamps are available as these SMS messages where found in previous screenshots.

Date (UTC)	Event
	SMS from +523332078807: Buenas noches Sandra, unicamente paso a saludarte y enviarte esta nota de Proceso que es importante retomar: http://bit[.]ly/25JHLDm (https://smsmensaje[.]mx/5727775s/)
	SMS from +525546613611: Sandra amiga acaba de morir mi esposo, estamos devastadas, te envio los datos del velatorio espero asistas: http://bit[.]ly/28hMScw (https://smsmensaje[.]mx/6050864s/)
	SMS from +524446613611: Hace 3 dias quo no aparence mi hija, estamos desesperados, te agradecere que me ayudes a compartit su foto: http://bit[.]ly/235hzhv (https://smsmensaje[.]mx/4159043s/)
	SMS from +518122090332: Sandra, mi mama esta muy grave, tal vez no pase la noche te envio datos de donde esta internada ojala

	vengas: http://bit[.]ly/1PQsLvX (https://smsmensaje[.]mx/6395084s/)

FORENSIC TRACES FOR MXJRN4

This Pegasus attack message was original discovered and published as part of collaborative investigation between Citizen Lab, R3D, SocialTic and Article 19.

Date (UTC)	Event
2016-05-12 19:06:04	SMS from + 528112889362: Tengo pruebas clave y fidedignas en contra de servidores publicos, ayudame tiene que ver con este asunto http://bit[.]ly/1s2eguc (https://secure-access10[.]mx/2618844s/)

FORENSIC TRACES FOR RWHRD1 - CARINE KANIMBA

Date (UTC)	Event
2020-11-24 13:26:03	Process record deleted from ZPROCESS (IN: 12.86 MB, OUT: 168.99 MB)
2021-01-28 22:42:56	Process: Diagnosticd
2021-01-31 18:28:39	Process: dhcp4d
2021-01-31 23:59:02	Process: libtouchregd
2021-02-02 13:54:23	Process: MobileSMSd
2021-02-13 19:44:12	Process: vm_stats
2021-02-21 23:10:09	Process: launchrexd
2021-02-21 23:10:09	Process: mptbd
2021-02-22 15:39:00	Process: PDPDialogs
2021-03-16 13:33:22	Process: neagentd
2021-03-17 15:27:06	Process: CommsCenterRootHelper
2021-03-21 06:06:45	Process: roleaboutd
2021-03-23 17:37:31	Process: contextstoremgrd
2021-03-28 00:36:43	Process: otpgrefd

2021-03-31 13:57:01	Process: vm_stats
2021-04-06 21:29:56	Process: locserviced
2021-04-09 19:09:18	Process: bluetoothfs
2021-04-23 01:48:56	Process: eventfssd
2021-04-23 20:43:14	Process: com.apple.Mappit.SnapshotService
2021-04-23 23:01:44	Process: aggregatenotd
2021-04-24 22:01:47	Process: ReminderIntentsUIExtension
2021-04-24 22:01:54	Process: ReminderIntentsUIExtension
2021-04-28 13:34:53	Process: com.apple.rapports.events
2021-04-28 13:34:57	Process: com.apple.rapports.events (IN: 0.01 MB, OUT: 0.00 MB)
2021-04-28 13:34:57	Process: com.apple.rapports.events
2021-04-28 13:35:40	Process: com.apple.rapports.events
2021-04-28 16:08:40	Process: xpccfd
2021-05-03 08:07:38	Traces from zero-click attack attempt over iMessage
2021-05-08 07:28:40	Traces from zero-click attack attempt over iMessage
2021-05-16 12:30:10	Traces from zero-click attack attempt over iMessage
2021-05-17 13:39:16	iMessage lookup for account benjiburns8[@]gmail.com
2021-05-17 13:40:12	Traces from zero-click attack attempt over iMessage
2021-06-14 00:06:00	Attack related push notifications over iMessage
2021-06-14 00:09:33	Process crash detected
2021-06-14 00:12:57	Process: com.apple.rapports.events
2021-06-14 00:17:12	Process: faskeepd

2021-06-14 00:17:12	Process: lobbrogd
2021-06-14 00:17:12	Process: neagentd
2021-06-14 00:17:12	Process: com.apple.rapports.events
2021-06-14 17:38:44	Process: faskeepd
2021-06-14 17:38:44	Process: lobbrogd
2021-06-14 17:38:44	Process: neagentd
2021-06-14 17:39:59	Process: faskeepd
2021-06-14 17:39:59	Process: lobbrogd
2021-06-14 17:39:59	Process: neagentd
2021-06-15 18:26:22	Process: faskeepd
2021-06-15 18:26:22	Process: lobbrogd
2021-06-15 18:26:22	Process: neagentd
2021-06-15 18:28:16	Process: faskeepd
2021-06-15 18:28:16	Process: lobbrogd
2021-06-15 18:28:16	Process: neagentd
2021-06-15 18:30:12	Process: faskeepd
2021-06-15 18:30:12	Process: lobbrogd
2021-06-15 18:30:12	Process: neagentd
2021-06-16 00:04:37	Process: faskeepd
2021-06-16 00:04:37	Process: lobbrogd
2021-06-16 00:04:37	Process: neagentd
2021-06-16 18:49:50	Process: faskeepd

2021-06-16 18:49:50	Process: lobbrogd
2021-06-16 18:49:50	Process: neagentd
2021-06-16 21:54:15	Process: faskeepd
2021-06-16 21:54:15	Process: lobbrogd
2021-06-16 21:54:15	Process: neagentd
2021-06-18 08:13:35	Process: faskeepd
2021-06-18 15:21:00	Attack related push notifications over iMessage
2021-06-18 15:26:04	Process crash detected
2021-06-18 15:26:08	Process: com.apple.Mappit.SnapshotService
2021-06-18 15:26:16	Process: com.apple.Mappit.SnapshotService
2021-06-18 15:31:12	Process: launchrexd
2021-06-18 15:31:12	Process: frtipd
2021-06-18 15:31:12	Process: ReminderIntentsUIExtension
2021-06-19 16:00:16	Process: launchrexd
2021-06-19 16:00:16	Process: frtipd
2021-06-19 16:00:16	Process: ReminderIntentsUIExtension
2021-06-20 00:06:25	Process: launchrexd
2021-06-20 00:06:25	Process: frtipd
2021-06-20 00:06:25	Process: ReminderIntentsUIExtension
2021-06-20 19:52:25	Process: launchrexd
2021-06-20 19:52:25	Process: frtipd
2021-06-20 19:52:26	Process: ReminderIntentsUIExtension

2021-06-20 19:53:58	Process: launchrexd
2021-06-20 19:53:58	Process: frtipd
2021-06-20 19:53:58	Process: ReminderIntentsUIExtension
2021-06-22 03:57:10	Process: launchrexd
2021-06-22 03:57:10	Process: frtipd
2021-06-22 03:57:10	Process: ReminderIntentsUIExtension
2021-06-22 04:06:51	Process: launchrexd
2021-06-22 04:06:51	Process: frtipd
2021-06-22 04:06:51	Process: ReminderIntentsUIExtension
2021-06-23 00:01:02	Process: launchrexd
2021-06-23 00:01:02	Process: frtipd
2021-06-23 00:01:02	Process: ReminderIntentsUIExtension
2021-06-23 14:31:39	Process: launchrexd
2021-06-23 20:46:00	Attack related push notifications over iMessage
2021-06-23 20:48:56	Process crash detected
2021-06-23 20:54:16	Process crash detected
2021-06-23 20:55:10	Process: otpgrefd
2021-06-23 20:59:35	Process: otpgrefd
2021-06-23 20:59:35	Process: launchafd
2021-06-23 20:59:35	Process: vm_stats
2021-06-23 22:21:13	Attack artifact on disk: /private/var/tmp/vditcfwheovjf/cc/otpgrefd/
2021-06-24 12:16:22	Process: otpgrefd

2021-06-24 12:16:22	Process: launchafd
2021-06-24 12:16:22	Process: vm_stats
2021-06-24 12:24:29	Process: otpgrefd
2021-06-26 21:56:00	Attack related push notifications over iMessage
2021-06-26 23:25:32	Process: smmsgingd
2021-06-29 22:26:00	Attack related push notifications over iMessage
2021-06-29 22:30:46	Process crash detected
2021-06-29 22:36:01	Process: launchafd
2021-06-29 22:36:01	Process: otpgrefd
2021-06-29 22:36:01	Process: dhcp4d
2021-06-29 22:36:01	Process: ctrlfs
2021-06-30 00:09:19	Process: launchafd
2021-06-30 00:09:19	Process: otpgrefd
2021-06-30 00:09:19	Process: dhcp4d
2021-07-01 00:09:32	Process: launchafd
2021-07-01 00:09:32	Process: otpgrefd
2021-07-01 00:09:32	Process: dhcp4d
2021-07-01 12:16:43	Process: launchafd
2021-07-01 12:16:43	Process: otpgrefd
2021-07-01 12:16:43	Process: dhcp4d
2021-07-01 21:42:19	Process: launchafd
2021-07-03 06:06:37	iMessage lookup for account benjiburns8[@]gmail.com

2021-07-03 06:07:00	Attack related push notifications over iMessage
2021-07-03 06:22:16	Process crash detected
2021-07-03 06:32:56	Process: actmanaged
2021-07-03 06:32:56	Process: misbrigd
2021-07-03 06:32:56	Process: Diagnostics-2543
2021-07-03 06:32:56	Process: gssdp
2021-07-03 15:23:18	Process: actmanaged

BEPERKTE VERSPREIDING/DIFFUSION RESTREINTE
K.B. van/A.R. du 24 Mar 2000

LA DÉFENSE

Service Général du Renseignement et de la Sécurité

Evere, le 08 décembre 2021
Notre référence: DocID
Page(s): - 1 -

Madame Carine Izere KANIMBA
Avenue baron Albert d'Huart, 124
1950 KRAAINEM

Chère Madame,

Présence d'indicateurs de compromission au logiciel espion PEGASUS

En vertu de la loi du 30 novembre 1998, Art 11. premier alinéa, Art. 13, deuxième alinéa et Art. 19, relatifs aux missions du SGRS et aux menaces dont les citoyens belges peuvent faire l'objet, nous souhaitons vous faire parvenir une note d'information traitant de l'analyse de votre téléphone mobile (Iphone X, Device serial number : G6WVXYXJJCL9, IOS 14.6).

Le SGRS souhaiterait vous informer de la découverte d'éléments liés au logiciel espion PEGASUS, présents sur votre téléphone pendant une période de 07 mois, entre janvier et juillet 2021. Les éléments identifiés font partie de la liste d'indicateurs établie par AMNESTY INTERNATIONAL et qui a trait à l'entreprise israélienne NSO.

Au cours de l'analyse, 03 indicateurs de compromission ont été identifiés pour la période évoquée. Bien qu'en accord avec les observations mises en avant par l'enquête d'AMNESTY, et malgré la présence de preuves circonstancielles, notre service ne peut attribuer avec certitude l'initiateur de l'attaque.

Toutefois, dans le cadre de l'article 19 de la loi sur les services de renseignement du 30 novembre 1998, le SGRS communiquera les résultats de l'analyse technique de votre téléphone mobile aux autorités compétentes. Dans le cadre d'éventuelles poursuites judiciaires visant l'initiateur de l'attaque, notre service se tiendra à la disposition des institutions désignées et s'engage à partager son expertise si cela s'avère nécessaire.

Veuillez agréer, Madame, l'assurance de notre considération très distinguée.

Belgian Intelligence Findings of Pegasus on Carine Kanimba's Phone

TRANSLATIONS FROM FRENCH:

December 8, 2021

Service General du Renseignment et de la Securite (SGRS)

Dear Madam,

Presence of indicators of compromise to the PEGASUS spyware

In accordance with the law of November 30, 1998, Art. 11, first paragraph, Art. 13, second paragraph and Art. 19, relating to the missions of the SGRS and the threats to which Belgian citizens may be subject, we would like to send you an information note concerning the analysis of your cell phone (Iphone X, Device serial number : G6WVXYXJJCL9, IOS 14.6).

The SGRS would like to inform you of the discovery of elements related to the PEGASUS spyware, present on your phone for a period of 07 months, between January and July 2021. The identified elements are part of the list of indicators established by AMNESTY INTERNATIONAL and related to the Israeli company NSO. During the analysis, 03 indicators of compromise were identified for the period mentioned. Although in agreement with the observations put forward by the AMNESTY investigation, and despite the presence of circumstantial evidence, our service could not attribute with certainty the initiator of the attack.

However, within the framework of 'article 19 of the law on the intelligence services of November 30, 1998. The SGRS will communicate the results of the technical analysis of your cell phone to the competent authorities. Within the framework of possible legal proceedings against the initiator of the attack, our service will be at the disposal of the designated institutions and will share its expertise if necessary.

Please accept, Madam, the assurance of our most distinguished consideration.

CID# 9530

Date: 17 June, 2022
Memo: The targeting of Jean Paul Nsonzerumpa with Pegasus spyware
Prepared by: The Citizen Lab
Prepared for: Jean Paul Nsonzerumpa

This memorandum is prepared for Jean Paul Nsonzerumpa at his request and with his consent. It confirms that our forensic analysis of digital artifacts on Jean Paul Nsonzerumpa's Apple device ("Jean Paul Nsonzerumpa's device")[1] *indicates that at least one of his devices was compromised with Pegasus spyware. Pegasus spyware is made by NSO Group.*

Background

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

The Citizen Lab's research mandate includes tracking digital threats against civil society actors, as well as tracking the proliferation of the mercenary spyware industry. As part of the Citizen Lab's investigations into the mercenary spyware industry, the Citizen Lab has developed the ability to identify evidence of device compromise with Pegasus spyware.

Confirming the infection of Jean Paul Nsonzerumpa with NSO Group's Pegasus spyware

Citizen Lab researchers analyzed forensic artifacts from Jean Paul Nsonzerumpa's device and obtained a positive result, which indicates that at least one device belonging to him was targeted and infected with NSO Group's Pegasus spyware. Our analysis indicates that he was infected with Pegasus spyware in the following approximate time periods:

1. On or around 2020-10-04

[1] The device with serial number ******YTN1YV

2. On or around 2020-10-12
3. On or around 2020-10-15
4. On or around 2020-10-21
5. On or around 2020-10-24
6. On or around 2020-10-27
7. On or around 2020-10-31
8. On or around 2020-11-12
9. On or around 2020-11-14
10. On or around 2020-11-17

This does not preclude the possibility of other infections.

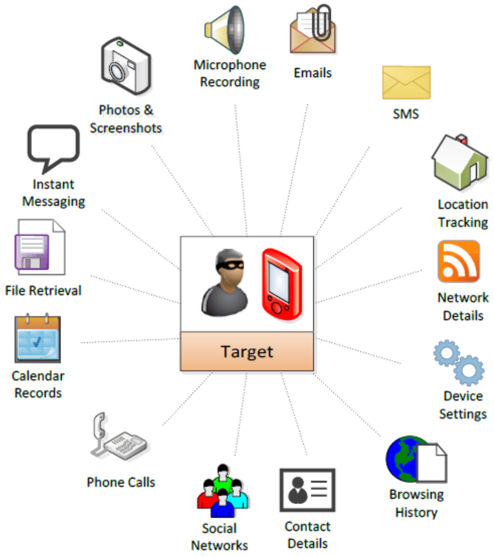
What a successful infection with Pegasus spyware can do

Pegasus is a surveillance tool that provides its operator complete access to a target's mobile device. Pegasus allows the operator to extract passwords, files, photos, web history, contacts, as well as identity data (such as information about the mobile device).

Pegasus can take screen captures, and monitor user inputs, as well as activating a telephone's microphone and camera. This enables attackers to monitor all activity on the device and in the vicinity of the device, such as conversations conducted in a room.

Pegasus also allows the operator to record chat messages as they are sent and received (including messages sent through "encrypted" / disappearing-message-enabled texting apps like WhatsApp or Telegram), as well as phone and VoIP calls (including calls through "encrypted" calling apps).

CID# 9530



NSO marketing material showing some of what Pegasus can monitor on a target's device.
Source: NSO Marketing Materials

For some chat programs, Pegasus also supports the extraction of past message logs. Pegasus also allows the operator to track the target's location. As with any infection, spyware may also allow for the modification or manipulation of data on a device.

Additionally, Pegasus spyware may be used to steal tokens allowing for persistent access to popular cloud accounts.

More information about NSO Group and its Pegasus spyware

Pegasus spyware is sold and marketed by NSO Group (which goes by the name Q Cyber Technologies, as well as other names). NSO Group is an Israeli-based company which develops and sells spyware technology, including Pegasus.[2] NSO Group is majority-owned by Novalpina Capital, a European private equity firm based in London.[3]

NSO Group claims it sells its spyware strictly to government clients only and that all of its exports are undertaken in accordance with Israeli government export laws and oversight mechanisms. NSO Group also claims to abide by a human rights policy. However, the number of documented cases in which their technology is used abusively to target civil society continues to grow.

You can review Citizen Lab research into NSO Group at this website:
https://citizenlab.ca/tag/nso-group/

[2] Note that in specific transactions for this technology, the Pegasus spyware may be given other codenames.

[3] For more information on NSO Group, you can find a summary of key public reporting here. Further, exhibits filed in the ongoing litigation between WhatsApp/Facebook and NSO Group in the United States provide insight into Pegasus' functions and NSO Group's operations (see, in particular, Exhibit 10 of the complaint).