UNCOVERING THE CITIZEN LAB –AN ANALYTICAL AND TECHNICAL REVIEW DISPROVING CATALANGATE

Technical Report · July 2022

DOI: 10.13140/RG.2.2.11352.16647

1 author:

Jonathan Scott
Northcentral University
1 PUBLICATION **0** CITATIONS

SEE PROFILE

UNCOVERING THE CITIZEN LAB

An Analytical & Technical Review

DISPROVING CATALANGATE

Prepared By :
Jonathan Boyd Scott, MSCS

Peer Reviewed
Dr. Gregorio Martin, PhD

UNCOVERING THE CITIZEN LAB AN ANALYTICAL AND TECHNICAL REVIEW DISPROVING CATALANGATE

Jonathan Boyd Scott, MSCS
PhD Student, Computer Science
Northcentral University

Peer Reviewed : Dr. Gregorio Martin, PhD Computer Science

Table of Contents

Author Overview

My name is Jonathan Scott, I am an American computer scientist focusing on mobile, IOT, and crypto security. I am a computer science PhD student attending Northcentral University, and my research focus is mobile malware and spyware. I have a masters degree from Colorado Tech in computer science with a concentration in cybersecurity engineering. My most recent professional employment experience was Lead Mobile Security Engineer and Mobile Threat Hunter for Celo.org and cLabs, Inc.

In 2022, I have been assigned 2 CVEs directly related to mobile device exploitation; CVE-2022-23728[1], and CVE-2022-23729[2] are respectively critical and high vulnerabilities affecting Android OS devices. These CVEs address chipset and application layer vulnerabilities that live in LG mobile devices. CVE-2022-23729 is a backdoor into all LG Mobile devices with Android OS 1.0 – 10.0. The backdoor allows a threat actor to act in stealth mode bypassing ADB (Android Debug Bridge) authentication. Exploitation of this mobile vulnerability can allow a device to unknowingly be remote controlled. Applications can be installed by plugging in the mobile device to a seemingly harmless usb "charging cable." I have recently discovered similar vulnerabilities in Samsung Mobile devices. After reporting, Samsung has confirmed the vulnerabilities I found and is actively patching the issues.

Q3 of 2021, I was the #1 Security Researcher[3] in The United States, and #4 globally. I responsibly reported 738 mobile, and web vulnerabilities that were validated and remediated on hackerone.com. I currently maintain the largest Pegasus spyware repository with decompiled Android OS samples. I started this GitHub project[4] July, 2021 to provide a centralized resource for mobile security researchers to study these samples in a way that has never been available before. I have taught iOS and Android OS mobile forensics methodologies to human rights defenders around the world.

My intention for pursuing mobile spyware and malware research is to raise awareness about the truth of our mobile device state of security. I would like to share my knowledge so that we can develop solutions to detect, remove, and combat mobile device threats more effectively.

[1] https://www.cvedetails.com/cve/CVE-2022-23728/
[2] https://www.opencve.io/cve/CVE-2022-23729

[3] https://jonathandata1.medium.com/true-life-recovering-bug-bounty-hacker-chapter-1-goodrx-3707f517a3fa
[4] https://github.com/jonathandata1/pegasus_spyware

Abstract

The Citizen Lab has become one of the most "trusted", and "credible" sources in the niche discipline of mobile spyware research. Globally known for their Pegasus spyware investigations, this Toronto University organization was founded in 2001. For years The Citizen Lab has been publishing research about high value individuals that have been infected with Pegasus spyware, but similarly for years they have never provided any samples for the general public to view, research, or challenge their claims. Citizen Lab's report on the hacking of human rights defender Ahmed Mansoor, concludes that they have been researching, and "confirming spyware infections" since 2011[5].

In the past 11 years, reproducible evidence to corroborate attribution of The Citizen Lab's mobile spyware research cannot be found. There have not been any in-depth technical documents written by The Citizen Lab that confirm conclusively, The NSO Group is the alleged spyware product owner frequently targeted by The Citizen Lab. Furthermore, The Citizen Lab has not produced any evidence to affirm the accusation that multiple nations around the world have been deploying Pegasus spyware, and targeting human rights defenders, politicians, journalists, and public figures.

The purpose of this whitepaper is to analyze the limited technical research Citizen Lab has provided, and present a working proof of concept that contests their claims of never receiving false positive results in their research. I will focus on the details related to their recent report "Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru," or, "CatalanGate," published April 18th, 2022. I will be reviewing key findings, assessing mobile forensic methodologies, conducting an analysis of the indicators of compromise, highlighting test results submitted by research participants, and raising questions about unknown quantitative data. I will not go into forensics details about Candiru spyware as it is Windows OS based and not mobile. Lastly, I will be discussing the ethical considerations that could impact technical results involving The Citizen Lab[6], and Amnesty International as their primary source of validation for their findings.

[5]https://tspace.library.utoronto.ca/bitstream/1807/96976/1/Report%2378--Million-Dollar-Dissident.pdf

[6] The Citizen Lab may be referred to as Citizen Lab or CL

A Brief Overview

The entirety of the CatalanGate report is based on events that occurred **April-May, 2019**. CVE-2019-3568 was issued for a vulnerability that affected 1,400 of WhatsApp users. WhatsApp released a statement saying, "*We stopped a highly sophisticated cyber-attack that exploited our video calling system in order to send malware to the mobile devices of a number of WhatsApp users. The nature of the attack did not require targeted users to answer the calls they received. We quickly added new protections to our systems and issued an update to WhatsApp to help keep people safe. We are now taking additional action, based on what we have learned to date. We sent a special WhatsApp message to approximately 1,400 users that we have reason to believe were impacted by this attack to directly inform them about what happened (WhatsApp, 2019).*"

WhatsApp further states The Citizen Lab volunteered to look into how this vulnerability could impact civil society. On **October 29th, 2019**, The Citizen Lab published a blog directly referencing the WhatsApp vulnerability, and how it could be exploited. The blog post references screenshots of an android mobile device that was "infected" with Pegasus spyware after the attacker initiated a voice call via WhatsApp mobile application.

Almost a year after the WhatsApp vulnerability was patched, new information about those affected by the WhatsApp vulnerability began to be released. In an article written by The Guardian **July 13th, 2020**, Citizen Lab Senior Researcher John Scott-Railton (JSR) comments about the alleged hacking of former Catalonian parliament president Roger Torrent. "*Given the nature of this attack and the limited information collected by WhatsApp on its users, we can confirm that the telephone was* ***targeted****. However, additional investigation would be necessary to confirm that the phone was hacked.* ***At this time, we have no reason to believe that it wasn't*** *(Kirchgaessner & Jones, 2020 July 13th)."* Citizen Lab in the same article then confirms Roger Torrent's phone to be *"****successfully infected*** *(Kirchgaessner & Jones, 2020 July 13th)*" in a memo to the former parliament president. The successful infection confirmation is based on Torrent's claims of "suspicious behavior" he noticed on his mobile device.

How WhatsApp obtained information about spyware targeted users is vague, and the specific "*limited information*" Scott-Railton speaks about, has never been released. The most known about how WhatsApp came to identify a vulnerability in their application comes from an article written by The New Yorker, which says unusual signaling messages[7] were captured. A civil complaint that was filed by WhatsApp against NSO Group Technologies Ltd. ("NSO Group") and Q Cyber Technologies Ltd does not offer any specific details as to how WhatsApp was able to identify malicious encrypted packets of data, and identify encrypted phone calls made to its users and attribute them to NSO Pegasus spyware. No one thought to ask the question of how WhatsApp was able to view user data that is said to be fully encrypted.

The lawsuit that WhatsApp filled against the NSO Group for their alleged hacking of mobile devices in 2019 made headlines around the world, but the civil complaint does not reference the WhatsApp CVE-2019-3568 vulnerability at all. The lawsuit references CVE-2016-4657[8], as one of the exploits used to hack into 1,400 mobile devices. This CVE referenced in the complaint is completely unrelated to the vulnerability patched in 2019 by WhatsApp, and dates back to 2016. The following is a description of the vulnerability WhatsApp references in their civil complaint against NSO Group "*WebKit in Apple iOS before 9.3.5 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site (CVE Details, 2016).*" The civil complaint alleges, "*Between approximately January 2018 and May 2019, Defendants created WhatsApp accounts that they used and caused to be used to send malicious code to Target Devices in April and May 2019. For example, on May 9, 2019, Defendants used WhatsApp servers to route malicious code, which masqueraded as a series of legitimate calls and call settings, to a Target Device using telephone number (202) XXX-XXXX. (WhatsApp Complaint, 2019).*"

Citizen Lab acknowledges and promotes the civil complaint against NSO Group in their blog post, "NSO Group / Q Cyber Technologies Over One Hundred New Abuse Cases.[9]" Citizen Lab disregards the fact that the civil complaint WhatsApp filed is trying to attribute a vulnerability found in 2016 affecting Safari in iOS 9.3.5, to a vulnerability found in 2019 that affects

[7]https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens

[8] https://www.cvedetails.com/cve/CVE-2016-4657/

[9]https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/

the WhatsApp mobile application. Regardless of the facts, Citizen Lab releases statements to the media citing WhatsApp as their source for claims that among the 1,400 targeted by the WhatsApp vulnerability were Catalonians.

In a statement from WhatsApp to The Guardian **July 28th, 2020**, director of public policy Niamh Sweeney said this regarding the alleged phone hacking of Roger Torrent, "*Based on the information available to us, we are not in a position to confirm whether Mr. Torrent's device was compromised as this could only be achieved through an exhaustive forensic analysis of the device (Kirchgaessner, 2020 July 28th).*"

The WhatsApp team concluded that exhaustive forensics analysis needed to be conducted in order to determine if in fact the mobile device of former Catalonian parliament president Roger Torrent's phone had been compromised. The July 28th, 2020 statement from WhatsApp to The Guardian is contrary to the statement made by John Scott-Railton. JSR's previous confidence in saying that there was no reason to believe Roger Torrent's phone was *not* hacked, and then confirming the successful infection is met with caution by the WhatsApp team.

14 days prior, on **July, 14th 2020**, Citizen Lab had spoken to Vice News' Motherboard about the Catalan spyware infections saying, "*It could not definitively confirm who actually deployed the NSO spyware (Franceschi-Bicchierai & Cox, 2020)*". **July, 13th 2020** in an interview with The Guardian; news came forth stating that The Citizen Lab had already alerted pro-independence activists Jordi Domingo, and Anna Gabriel in **early 2019** saying "*it seemed clear the Spanish state [was behind the attacks.](Kirchgaessner & Jones, 2020).*"

April 18th, 2022 The Citizen Lab released their research publication titled "Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru." In a section titled "Documented Surveillance Abuses in Spain and Catalonia," a new narrative is presented as to how Citizen Lab attributes the Spanish government to the deployment of spyware. "*The Spanish prime minister's office claimed that it was not aware of this spying. Nonetheless, in 2020, Spanish media El País, confirmed that the Spanish government was an NSO Group customer, and that the CNI actively used Pegasus spyware. A former NSO employee commented to Motherboard that they* [NSO Group] *"were actually very proud of them as a customer ... Finally, a European state (Scott-Railton et*

al., 2022)." The Citizen Lab adopted the 2020 publication by El País which attributes the Spanish government as being the ones who deployed the NSO spyware. This narrative adoption shifted the origin of accusations and *confirmations*, onto El País. The full impact of the CatalanGate report is yet to be seen, but thus far it has increased tensions around the world, created a larger divide amongst Catalonians and the Spanish government, and it has also raised alarms about the validity of The Citizen Lab's work.

Targeting The NSO Group

Spokesperson for NSO Group shared the corporation's derision towards The Citizen Lab and their close allies Amnesty International in regards to the incessant defamation. The spokesperson stated to The Guardian, "*NSO continues to be targeted by a number of politically motivated advocacy organizations like Citizen Labs and Amnesty to produce inaccurate and unsubstantiated reports based on vague and incomplete information (Jones, 2022).*"

There are many well known spyware firms around the world, but the NSO Group and Pegasus spyware seem to always be on Citizen Lab's radar. Allegations have been made that suggest Quadream, an Israeli NSO competitor, has developed zero-click exploits that can take over mobile devices. Quadream was founded in 2016 by former NSO employees, and the Saudi Arabian government is one of their clients[10]. The Citizen Lab has remarked that the zero-click exploits developed by Quadream are on the same level as those of NSO's, "*Citizen Lab security researcher Bill Marczak, who's been studying both companies' tools, told Reuters that the zero-click capability of QuaDream's flagship product seems "on par" with NSO's Pegasus spyware (Vaas, 2022).*"

Bill Marczak is a researcher with Citizen Lab, and admission that Quadream exploits are on par or the same as NSO Group's raise legit concerns as to how CL is able to properly distinguish exploits. The European Parliament questioned the reliability of Citizen Lab's methodology for attribution by posing the following question, "*Can Citizen Lab reliably distinguish Pegasus infection attempts from other spywares attacks?*" Director of The Citizen Lab Ron Deibert responded crassly to the European Parliament saying, "T*he Citizen Lab's technical methods for identifying Pegasus infections or infection attempts are supported by six years of published*

[10]https://www.haaretz.com/israel-news/tech-news/2021-06-08/ty-article/.highlight/the-secret-israeli-cyber-firm-selling-spy-tech-to-saudia-arabia/0000017f-df07-d856-a37f-ffc724f80000

research, as well as independent validations (Ronald Deibert - Response To European Parliament 2022)."

Unfortunately 6 years of published research by The Citizen Lab fails to provide facts sufficient to support their claims. Any claim of peer review or independent validation should not be conducted in bad faith by knowingly employing both the researcher and the validator as Citizen Lab had done. The conflict of interest in this bad faith situation presents itself as a hammer and NSO Group as the nail.

Targeting The Spanish Government

Placing crosshairs on NSO Group without proof of claim is not something new for Citizen Lab, nor is placing the blame on governments for hacking into cellular phones. March 4th, 2014 documentary filmmaker Alan Snitow in an email asked Director of The Citizen Lab Ron Deibert why he and his team are always placing blame on governments for deploying spyware, and in part asks where the evidence is[11]. Snitow writes, "Excellent report, but a question: why always the caveat that the spyware is "sold exclusively to governments?" Is there no evidence that companies, detective agencies and other entities could be using similar means to track their own critics? Or that some governments pass the technology onto semi-governmental agencies or private companies allied closely with regimes? Is there a wall that would prevent this from happening (Snitow, 2014)?" Ron Deibert replies to Snitow with an unrelated report and an OPED from the Washington Post, and in true form dismisses the valid questions. NSO Group has publicly stated that "*it only sells its products to government law enforcement and intelligence clients (Person & Christopher Bing, 2021),*" but this is not the case with all spyware firms, thus bringing validity to Snitow's question of why Deibert and CL are always placing blame on governments.

The Citizen Lab has been targeting the Spanish government and had aligned with the Catalan pro-independence movement years prior to the WhatsApp vulnerability. September 25th, 2017, before the Catalan independence referendum,[12] The Citizen Lab worked with pro-independence supporters and compiled a list of domains framed as being censored by the Spanish government. Censorship claims vs. lawful

[11]https://mailman.stanford.edu/pipermail/liberationtech/2014-March.txt

[12]https://en.wikipedia.org/wiki/2017_Catalan_independence_referendum

seizure are significantly different and the former paints the Spanish government in a negative and totalitarian light. Citizen Lab released the list of domains accusing the Spanish government of illegally censoring websites, violating human rights, and categorized them as "Political Criticism" with notes directly citing "referendum in Catalonia.[13]" Media quickly responded and spread the narrative that the Spanish government was actively engaged in human rights abuses as it pertains to monitoring and censoring.

The CatalanGate website has a modern user interface, and fluid user experience that mimics that of apple.com. The impressive design, and graphics are presented in a way that captures your attention, and keeps you engaged. This visually impressive web design was developed by Barcelona based creative studio Domestic Data Streamers.[14] Toutting The Citizen Lab as one of their clients, as seen in the footer of their website, this pro-independence organization led by founder and Catalonian Pau Garcia has a mission to trigger change[15].

CatalanGate is a twist of narratives, false positives, fabrications, collusion, and none of the research presented is backed by scientific evidence. Uncovering The Citizen Lab and their lack of integrity, honesty, and academic rigor is something that has been long overdue. Technical and factual data show that as early as 2017 Citizen Lab has been trying to frame a scenario in which the Spanish government has been spying on the citizens of Catalonia.

[13]https://github.com/citizenlab/test-lists/commit/902d7cd069f252249e96c28b9c8d15cf437b63ea

[14] https://domesticstreamers.com/

[15] https://www.linkedin.com/company/domestic-streamers/

The CatalanGate Researchers

I will begin with an overview of a few of the authors credited for their contribution to the CatalanGate publication, and offer professional insight into one of the most overlooked and rarely challenged issues in information security. How do you validate the qualifications of the researchers publishing their work? Media, journalists, bloggers, and many professionals in the infosec community believe that if you are a malware researcher, you are qualified to assess any operating system, and any application. The idea that someone would have an expertise in every OS is not logical and can cast doubt on any and all claims the researcher makes. The figure of speech, "Jack of all trades, master of none," does not fare well in this niche industry of mobile malware and spyware research.

I wrote an article Jan, 2022 entitled "Integrity and Validation in Mobile Spyware and Malware Research." In this article I emphasize the importance of understanding the differences and similarities between malware and spyware. Furthermore, I write about the critical distinctions that need to be made when referencing malware researchers.

This whitepaper is challenging the CatalanGate technical analysis, and it would only be reasonable to assume that the credited authors are qualified to deliver such an important and globally impactful report - claiming that the Spanish government has been spying on Catalonians. It would also be reasonable to assume all of the researchers are well trained in the modalities of mobile malware and spyware forensic analysis, but my research did not find this to be true.

John Scott-Railton

Senior Researcher at The Citizen Lab, John Scott-Railton claims to research malware.[16] Questions immediately start to form such as, if JSR researches malware what kind of malware research does he focus on? Where did he receive his training, and has he been employed as a malware researcher in any other company or institution? Claiming to be a malware researcher can be compared to saying you are an engineer. Logically, one should ask, what kind of engineer are you? I could not find any relevant experience of mobile malware research in any of Scott-Railton's

[16] https://www.johnscottrailton.com/

public accounts. At the time of the publication, JSR's LinkedIn profile does not have any endorsements for malware analysis, information security, or cyber warfare. I began to wonder what it is that John Scott-Railton actually does? It seems as though political science is his specialty, but why is he claiming "malware research" as his primary focus? I could not find any CVE (Common Vulnerabilities and Exposures) assignments that can corroborate his claims of being a "malware" or information security researcher. An argument can be made that you do not need to have any CVE assignments to be considered a "malware." or security researcher, but this then raises the question of what constitutes a "malware/security researcher," in the eyes of Citizen Lab? In 2018 JSR presented a keynote hosted by Virus Bulletin, and described how Citizen Lab "*used a really cool technique, DNS cache probing, to come up with a map where at least one NSO Pegasus victim was located (Virus Bulletin, 2018).*" JSR's nonchalant admission of The Citizen Lab exploiting servers by performing DNS cache poisoning attacks shows that CL is not concerned with ethics or integrity. "*DNS cache poisoning is a highly deceptive attack that not only diverts traffic from legitimate websites, but also leaves users vulnerable to many risks, including malware infections and data theft. In web cache poisoning, an attacker exploits a web server and cache to serve a malicious Hypertext Transfer Protocol (HTTP) response to users (Awati, 2021).*" I have found that the unethical process in which data is collected, is a shared commonality amongst Citizen Lab researchers and their cohorts.

Elies Campo

Another credited CatalanGate author is Elies Campo. Campo has previous experience in business development, and as of **January, 2022** he has become a fellow at The Citizen Lab. It is clear that special exceptions were granted to Elies Campo in order for him to be a fellow at CL. Campo does not meet the requirements of having completed a PhD. Requirements for a fellowship with CL are specific, and the date for fellowship consideration was set for **Feb 15th, 2022**[17]. Knowing Campo's deceptive past, the validity ethicacy of Campo acting as a forensics auditor was raised by the European Parliament. In response to questions sent to The Citizen Lab by the European Parliament, director of The

[17]https://munkschool.utoronto.ca/opportunity/fellow-in-residence-munk-school-of-global-affairs-public-policy/

Citizen Lab Ron Deibert stated, "*All researchers with the Citizen Lab are required to follow applicable research ethics protocols (Deibert, 2022).*" The research ethics protocols mentioned by Deibert align with The University of Toronto's Academic Integrity Policy, and according to section 4.2 Academic Offenses, falsification of information to gain entry into the academic institution is considered concocting. "Concocting – using false data, or providing false references (University of Toronto, 2019)." It has come to light that Elies Campo falsified his employment with Telegram, and in a request for information sent by publication El Espanol, Telegram spokesman Remi Vaughn confirmed that Elies Campo has ***never*** been employed and was ***never*** the head of business development (El Espanol, 2022). Campo is a key figure in the CatalanGate report as he has close personal relationships to the alleged hacking victims including former Catalonian president Carles Puigemont. Campo was part of the team that helped Citizen Lab in "*identifying potential cases (Deibert, 2022).*" Campo conducted mobile forensic field work in Catalonia from 2020-2022 as stated by Director Ron Deibert. Deibert states in his responses to the European Parliament that all field work Campo conducted remotely were under his supervision. Ron Deibert is not a mobile forensics analyst, computer scientist, or security engineer, and similarly Elies Campo does not have any professional experience in conducting, operating, or performing a mobile forensics analysis, audit, or acquisition. How Elies Campo came to be involved in the identification of potential cases of hacked Catalonians before ever being employed by The Citizen Lab, is unknown. The New Yorker published an article citing Elies Campo as a digital-security researcher and gives specific details as to how Elies Campo conducted the forensics investigation. The article further describes how a business relations manager Elies Campo affirmed a positive confirmation of a mobile spyware infection on Catalonian Politician Jordi Solé's iPhone 8 Plus. "*Campo collected records of Solé's phone's activity, including crashes it had experienced, then ran specialized software to search for spyware designed to operate invisibly. As they waited, Campo looked through the phone for evidence of attacks. Campo identified an apparent notification from the Spanish government's social-security agency which used the same format as links to malware that the Citizen Lab had found on other phones. "With this*

message, we have the proof that at some point you were attacked," Campo explained. Campo told Solé, "There's two confirmed infections," from June 2020. "In those days, your device was infected—they took control of it and were on it probably for some hours. Downloading, listening, recording." (Farrow, 2022)." Campo is listed in the CatalanGate report to have been "targeted" by spyware, and his father is listed as "infected." Campo's close business associates Pau Escrich, and Xavier Vives are also referenced in CatalanGate as being targeted with spyware.

Ron Deibert

Ron Deibert is the director of The Citizen Lab, and is actively involved with many projects. Deibert was the "*Co-founder and principal investigator of the OpenNet Initiative* [or ONI] *(Center for International Governance Innovation, 2020)*." ONI is an organization that was funded by The Open Society Foundation, and the Ford Institute among others[18]. Diebert has cross funded his projects by receiving contributions from the same aforementioned institutions.[19]

The Open Society Foundation[20] who's founder and chair is George Soros is a large donor to The Citizen Lab. Since 2014 The Open Society Foundation has been funding the Catalan independence movement as reported by La Vanguardia (Sallés Barcelona, 2016).

The Ford Foundation has also been supporting the Catalan independence movement for many years. The Foundation funded a French documentary titled, "Catalogne: l'Espagne au bord de la crise de nerfs (Catalonia: Spain on the Verge of a Nervous Breakdown.[21]" The documentary features alleged hacking victim and former Catalonian president Carles Puigdemont.

In an article written by El National, Amnesty International[22] is also another organization that has funded the Catalan independence documentary. Amnesty International is the organization The Citizen Lab leans on for technical validation and verification of their "research." Contributing further to questionable research bias, and nefarious activity, Deibert was also a member of the technical advisory group for Amnesty International as declared in a document he prepared for "THE MINISTER OF PUBLIC SAFETY AND

[18] https://opennet.net/funding-institutions
[19] https://citizenlab.ca/about/
[20] https://www.opensocietyfoundations.org/who-we-are/leadership
[21] https://www.imdb.com/title/tt8149754/?ref_=ttexst_exst_tt
[22]https://www.elnacional.cat/en/news/catalonia-international-film-festival-human-rights_232122_102.html

EMERGENCY PREPAREDNESS[23].” A job description that has now been removed by Amnesty shows that the Salary for a technical advisor is £52,241per year[24]. My research continued to surface more evidence of Citizen Lab’s lack of ethics and integrity. I found that these attributes are being passed down and encouraged by director Ron Diebert.

The Toronto Star wrote an article about Citizen Lab, Diebert, Psiphon VPN (A company owned by Diebert), and other fellows. The article reveals Diebert as the source of unethical practices within The Citizen Lab, and shows a side of Diebert that should raise alarms. "*The Citizen Lab uses the techniques of spies to secretly deploy software it developed that automatically checks for censored websites inside various countries. Sometimes the lab performs tests remotely, taking control of unprotected computers inside the censoring country without permission. This poses an ethical controversy, but Deibert says it’s for the greater good: ‘We don’t worry about that too much.”*”

Diebert admits that The Citizen Lab hacks into computers, installs spyware, and a remote access terminal, but states its for the greater good. Diebert continues by saying, “*The Lab even has “black boxes,” mini-sized computers that can be “planted” discreetly inside these countries to run the tests. “This kind of research is illegal in almost every country we do it in,” he adds (Toronto Star, 2009).*”

Diebert encourages illegal activities by planting spyware enabled hardware devices around the world. These devices are capable of infecting networks, devices, and computers. For Diebert, these types of illegal activities are nothing he worries about, but his actions are something that should concern the entire world. Planting espionage devices around the world for the greater good suggests clear political motivations, and starting an investigation into Diebert, and The Citizen Lab is an action that needs to be commenced.

After researching all contributors’ positions, and their experience, I did not find any qualified individual that would be able to professionally identify iOS mobile spyware, nor would they be able to conduct a qualified and quantifiable iOS mobile forensics audit. The initial public screening of The Citizen Lab authors reveals a lack of necessary mobile forensics skills, which is a critical issue especially in such a sensitive

[23] https://citizenlab.ca/wp-content/uploads/2021/10/Statement-of-Ronald-J-Deibert.pdf

[24] https://web.archive.org/web/20220615174336/https://careers.amnesty.org/vacancy/researcher-adviser-technology-and-human-rights---sabbatical-cover-3410/3438/description/

and controversial topic such as the CatalanGate.

Table 1 Represents all individuals affiliated with The Citizen Lab credited for their contribution to the CatalanGate report.

Table 1

Researcher	Position	Experience
John Scott-Railton	Senior Researcher	Research on electronic attacks[25] Threats civil society, including targeted malware operations, cyber militias, and online disinformation[26]
Elies Campo	Research Fellow	Business Development[27] Business Development and Growth[28]
Bill Marczak	Research Fellow	Internet scanning and conducting digital investigations[29]
Bahr Abdul Razzak	Security Researcher	Malware Analysis, Android Development[30]
Siena Anstis	Senior Legal Advisor	Senior legal advisor with the Citizen Lab at the Munk School of Global Affairs & Public Policy[31]
Gözde Böcü	Fellow, Trudeau Center for Peace	Comparative Politics and International Relations[32]
Salvatore Solimano	Research Assistant	Disinformation, cybersecurity, and platform governance in Latin America[33]
Ron Deibert	Director	Foreign Policy, Information Warfare, Qualitative Research, Data Analysis[34]

Conflict of interest is a serious ethical consideration and more detailed information about the research ethics violations can be found in a publication written by Dr. Jose Javier Olivas, entitled "Methodological and ethical issues in Citizen Lab's spyware investigation in Catalonia

[25] https://www.linkedin.com/in/johnscottrailton/
[26] https://citizenlab.ca/author/jsrailton/
[27] https://www.linkedin.com/in/eliescampo/
[28] https://www.crunchbase.com/person/elies-campo
[29] https://citizenlab.ca/author/bmarczak/
[30] https://www.linkedin.com/in/bahrabd/details/skills/
[31] https://www.law.utoronto.ca/faculty-staff/adjunct-visiting-faculty/siena-anstis
[32] https://munkschool.utoronto.ca/profile/bocu-gozde/
[33] https://www.linkedin.com/in/salvatore-solimano-a31b53190/
[34] https://www.linkedin.com/in/ronald-deibert-8b93171/details/skills/

(Olivas, 2022).” Clear research and ethical issues exist in all of these associations, but none is more evident than that of the relationship between The Citizen Lab and Amnesty International.

Technical Research Ethics

ISO/IEC 17020:2012 describes Conformity assessment — Requirements for the operation of various types of bodies performing inspection, **section 3.8** “Impartiality,” **Note 1 to entry:** Objectivity means that conflicts of interest do not exist or are resolved so as not to adversely influence subsequent activities of the inspection body. **Note 2 to entry:** Other terms that are useful in conveying the element of impartiality are: independence, freedom from conflict of interests, freedom from bias, lack of prejudice, neutrality, fairness, open-mindedness, even-handedness, detachment, balance (ISO, 2012).

I reference ISO because they set the international standards that are applicable to various industries around the world. After deliberation, drafts, revisions, and a consensus via a panel of experts in their respective field, international standards are adopted. In the event that an organization, firm, or research institution does not have a formally recognized ISO certification, the ISO standards can still be and should be applied as they are widely accepted reference points to follow.

Etienne “tek” Maynier

Research into The Citizen Lab, and Amnesty International provide concerning information that raise questions into the ethical nature of their professional relationships. The institutions worked very closely on the CatalanGate report. Etienne “tek” Maynier is a technologist employed by Amnesty International, and was also employed by The Citizen Lab as a fellow during the CatalanGate investigations. April 30th, 2022 Maynier’s personal website[35] had stated he was still employed by Citizen Lab, but shortly after questions into CL’s ethical practices began, he changed his website to say he was only employed by Citizen Lab until 2021.

Claudio Guarnieri

Claudio Guarnieri is the Head of Security Lab at AmnestyTech.[36] Claudio

[35] https://randhome.io/about/
[36] https://twitter.com/botherder

shares a commonality between him and Etienne Maynier, and the commonality is they both were research fellows with The Citizen Lab, and employed by Amnesty International during the time of the CatalanGate investigations. In a blog post written August 10th, 2019, Guarnieri was quoted as being "*a researcher at the University of Toronto's Citizen Lab (Invar Technologies, 2019).*"

Guarnieri also has strong ties to the Catalan pro-independence movement as he sits on the board of a project known as Barcelona Now.[37]

The revelation of facts showing director Ron Diebert, and fellows Etienne Maynier's, and Claudio Guarnieri were all employed by The Citizen Lab, and Amnesty International at the time research and forensics were conducted for the CatalanGate report provides valid reasoning for an unaffiliated 3rd party to conduct a thorough analysis on all of the samples that have been said to "independently" confirmed by Amnesty International.

[37] https://elaragon.net/2020/02/20/decode-final-review-meeting/

Indicators of Compromise

Verified indicators of compromise or IOCs are integral to the information security community. Virus and malware scanners, internet service providers, firewalls, and more rely on IOCs in order to help protect users and customers from becoming potential victims of a malicious cyber-attack.

In a blog post prominent security firm Crowdstrike says, "Identifying IOCs is a job handled almost exclusively by trained infosec professionals. Often these individuals leverage advanced technology to scan and analyze tremendous amounts of network traffic, as well as isolate suspicious activity (Crowdstrike, 2021)."

Citizen Lab frequently "identifies" IOCs, but they have never shared their methodology for acquisition. In 2021 Amnesty released a publication endorsing The Citizen Lab, and provided information stating that they share the same methods and tools to identify Pegasus spyware indicators of compromise. The primary tool used by both Citizen Lab and Amnesty International is called the MVT-Tool. The publication Entitled: ***Forensic Methodology Report: How to catch NSO Group's Pegasus,*** corroborates the integration of the alleged IOCs found by Citizen Lab. "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 (Amnesty International, 2021)."

Director Ron Deibert speaks about how critical the indicators of compromise are, to the extent that "antivirus company ESET draws on the Citizen Lab's indicators (Deibert, 2022)." Moreover, Diebert encourages experts to validate their findings based on the IOCs they provide, and says that "no reputable technical analysis has contradicted our findings[38]." The word *fingerprint* is mentioned many times in the CatalanGate report, it is referencing a set of identifying characteristics that can confirm a website URL is an NSO Group command and control server. There are not any technical documents that address what Versions 1-4.5 of Citizen Lab's fingerprints look like. CL later states that adsmetrics.co did not match their fingerprint, and they did not detect any "Version 4" domains because they contained SSL certificates issued by cPanel. Citizen Lab says they do not scan

[38]https://deibert.citizenlab.ca/wp-content/uploads/2022/05/2022.05.13-L-Ferris-to-J-Canas.pdf

for SSL Certificates issued by cPanel, and therefore any domain with a cPanel would not be attributed to their indicators of compromise.

Citizen Lab claims that 123tramites.com and nnews.co were complete matches for their fingerprint. Their "fingerprint," leads us down a rabbit hole they call "Athena[39]." Athena is alleged to be a "*novel technique to cluster some of our matches into 36 distinct Pegasus systems, each one which appears to be run by a separate operator (Marczak et al., 2020).*" Citizen Lab declines to share what exactly Athena does, and how or what a fingerprint is, but scientists, researchers, AV vendors, media, students and more are taking their research to be factual and accurate.

CL states, "*As we have done in the past when reporting on vendors of targeted malware, we have chosen to withhold publication of specific fingerprints and techniques to prevent harm that may result from external parties generating a list of NSO Group domains using these methods (Marczak et al., 2020).*"

Citizen Lab does not want external parties generating lists of NSO Group Domains because it may cause harm, or in other words they are the only research institution that is allowed to generate a list of NSO Group domains and distribute it. The frustration and vehement disagreement with Citizen Lab, and their research practices extend globally.

Dr. Uraz Yavanoglu, Professor of Computer Science at Gazi University in Turkey wrote a very detailed white paper titled, "**Citizen Lab Deep Packet Inspection Scam.**" The white paper disproves all of Citizen Labs's claims that the Turkish government was redirecting Turkish citizens to websites that would install spyware on their Windows based computers[40]. It is relevant to note that the same issues I raised about the qualifications of the Citizen Lab researchers are raised by Dr. Yavanoglu. Dr. Yavanoglu explicitly calls to point, the director of Citizen Lab Ron Diebert is not a computer scientist, yet claims to be the principal "controlling and monitoring the network traffic (Yavanoglu, 2018)" within the organization.

Moreover, Dr. Yavanoglu's white paper shares the conviction of many PhD computer scientists around the world by remarking, "It is not easy to understand why these people have created such a research group in Canada and have been writing technical reports on computer sciences

[39]https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

[40]https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/

although they are qualified in politics, public administration, etc. Certainly, disciplinary studies can be carried out but it is difficult to understand why 1 computer scientist and 5 social based people have come together for a report including technical data and specific libelous expressions. **It cannot be accepted as a disciplinary research under no circumstances** (Yavanoglu, 2018)."

In the summation of "**Citizen Lab Deep Packet Inspection Scam,**" Dr. Yavanoglu emphatically speaks about the baseless claims Citizen Lab continuously makes, and wants it to be known that the only Computer Scientist on staff at The Citizen Lab, Bill Marczak, does not follow any academic, or technical writing standards that would allow those reading to reproduce results that claim to be indicators of compromise.

IOC Data Commit

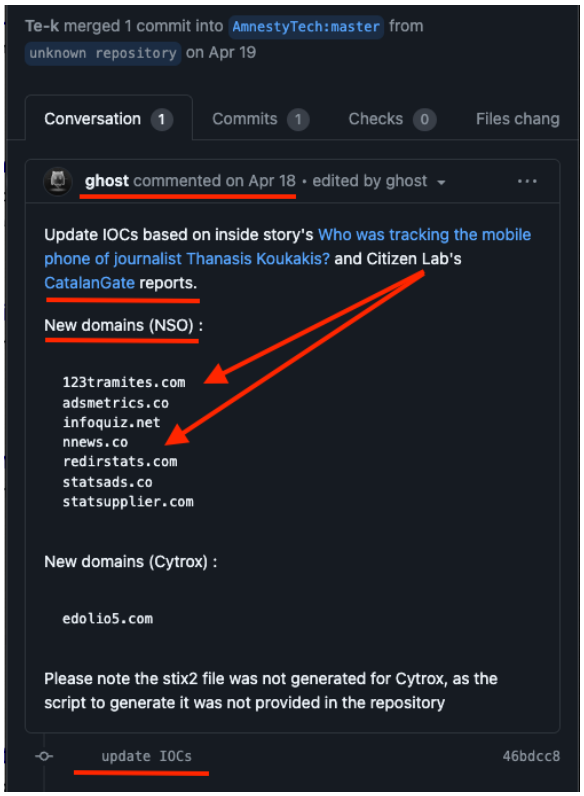
CatalanGate was published April 18th, 2022, and in the publication, the authors definitively confirm the following, "*Of these domains, only nnews[.]co and 123tramites[.]com were complete matches for our fingerprint, and statsads[.]co was a partial fingerprint match. Some of the domains appear to have customized behaviour or setup, perhaps in order to make them less visible to our Internet scanning. (Scott-Railton et al., 2022).*" The domains nnews.com and 123tramites.com among others are said to be indicators of compromise and can be attributed to the NSO Group, and Pegasus spyware according to Citizen Lab.

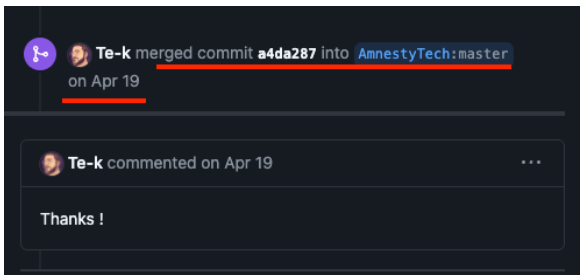
April 18th, 2022 an anonymous GitHub account creates a pull request to have Amnesty International update their IOCs, or in other words an unknown entity submitted a request to add information into a dataset, and titled part of the list "New domains (NSO).[41]

[41] https://github.com/AmnestyTech/investigations/pull26

April 19th, 2022 Etienne "tek" Maynier commits these domains to Amnesty International's Github Repository. This code repository contains the tools that Citizen Lab uses in order to identify spyware on mobile devices. Developed jointly by Citizen Lab and Amnesty international, the MVT-Tool or Mobile Verification Toolkit is an open-source program that is available for anyone to download and use. The MVT-Tool uses the IOC's provided by Citizen Lab and Amnesty as a keyword search utility. For example, if any of the keywords that are on the IOC lists are found on your device, you are determined by their software to be infected with a specific brand of spyware.

When the European Parliament asked Citizen Lab director Ron Diebert if Etienne Maynier conducted the external validation at Amnesty Tech, Diebert replied, "*Mr. Maynier was not involved in the Citizen Lab investigation of these cases at any time (Deibert, 2022).*" Blatantly lying to the European Parliament is right on par with the ethics of The Citizen Lab. The hard proof that Etienne Maynier committed and confirmed the indicators of compromise listed by Citizen Lab can be viewed here https://github.com/AmnestyTech/investigations/pull26.





Disproving Domain IOCs

It is easy to be caught up in The Citizen Labs's narratives. Timelines become crossed, statements shift into political anagrams, but I want to remind the readers of this white paper that the basis of the claims that Catalonians were hacked with Pegasus spyware come from a vulnerability found by WhatsApp. After this vulnerability was patched in May, 13th 2019 users were forced through the mobile software application to update the app version installed on their device (Morelli, 2019). In short, if a user tried to open the unpatched/older version of WhatsApp they would be prompted to update the app in order to continue usage.

October 29th, 2019 WhatsApp posted a now deleted webpage speaking about the WhatsApp vulnerability and the targeting of "at least 100 members of civil society (WhatsApp, Archive.org 2019)." On the same day Whatsapp released this public statement, Citizen Lab released their research and involvement in the May 2019 WhatsApp spyware incident[42].

Considering the factual timelines presented, and the claim that 123tramites.com is a 100% match for CL's indicator of compromise fingerprint, an analysis of the claims made by Citizen Lab requires proper attribution.

I performed a historical WHOIS domain search using the WHOIS API[43]. The entry in the WHOIS database dated **November 19th, 2018** shows that the domain 123tramites.com expired as of October 8th, 2018, and there was no current owner. **February 12th, 2019** the WHOIS database still reflects 123tramites as expired, and it is still not owned or registered. Over 6 months after the WhatsApp vulnerability was patched on **November 21st, 2019,** 123tramites.com is registered with NameSilo, LLC. The following data leaves the time frame for the alleged dates of compromise, but the data is relevant to the overall dispute of Citizen Lab's claims.

The name servers associated to the aforementioned date of registration for 123tramites.com were the following:

- NS11.HOSTPLAX.COM
- NS12.HOSTPLAX.COM

[42]https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/

[43] https://tools.whoisxmlapi.com/whois-history-search

Hostplax.com is now branded as Hostmines.com. A historical search on archive.org shows that Hostplax.com was a reseller of Namesilo.com domains. The terms of service on October 19th, 2019 state, "*HostPlax is not a domain registrar. We are a domain reseller for NameSilo so all HostPlax customers who purchase a domain or transfer a domain to us are bound by the terms and conditions set forth by NameSilo (hostplax.com, 2019).*"

November 20th, 2019 when 123tramites.com was registered, hostplax.com was running a promotion that included domain hosting services for $.95/month when you purchase a domain. The hosting services included cPanel shared hosting access. Citizen Lab says Version 4 of their fingerprints detection do not consider cPanel issued SSL certificates as part of their IOC attributions[44].

DNS TXT records history from securitytrails.com[45] show a TXT entry first seen **November 21st, 2019**.

v=spf1 +a +mx +ip4:69.16.209.146 ~all

IP Address 69.16.209.146 is seen to be managed by cPanel historically, and even to the date of this publication the cPanel attribution can be made.[46] According to CL's logic 123tramites.com should appear as a negative result for their Version 4 fingerprint, and alas CL assigns 123tamites.com to their version 4.5 fingerprint. A source provided for their fingerprint 4.5 directs to a January 12, 2022 publication written by The Citizen Lab called "Project Torogoz.[47]" The publication does not have any information about fingerprint 4.5, and the only mentions of the word fingerprint say, "*We fingerprinted Pegaus URL shortener websites…we saw SMS messages…matching our Pegasus fingerprint (Project Torogoz Scott-Railton et al., 2022).*" This is another example of CL's misdirection and deception published and accepted globally.

November 20th, 2021 123tramites.com had again expired, according to information from the WHOIS database. A search on archive.org confirms the expired domain and shows a landing page clearly marked as "expired[48]." It is not until May 21st, 2022 that 123tramites.com will have a new owner, and that owner is me, Jonathan Scott. I purchased

[44]https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/
[45] https://securitytrails.com/domain/123tramites.com/history/txt

[46] http://69.16.209.146/cgi-sys/defaultwebpage.cgi
[47]https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/
[48]https://web.archive.org/web/20211123031936/http://123tramites.com/

123tramites.com after starting to research the CatalanGate report. At the time the CatalanGate report was published, 123tramites.com had been expired for 6 months, yet Citizen Lab with the help of Amnesty International, Etienne Maynier and Claudio Guarnieri published 123tramites.com as an active indicator of compromise that is blacklisted around the world.

Ron Diebert told the European Parliament that Amnesty did not conduct their independent review until March-April 2022. CatalanGate has several references to 123tramites.com, but the following statement is the coup de grâce. "*We further believe that 123tramites[.]com was operated by the same customer, because an SMS with a link to 123tramites[.]com used identical bait content to an SMS with a link to statsupplier[.]com…These attacks involved operators sending text messages containing malicious links designed to trick targets into clicking. In this approach, once a victim clicks on a link, the device is infected via a Pegasus exploit server (Scott-Railton et al., 2022).*"

The verification by Amnesty of 123tramites.com would not have been possible because it had already been expired for 6 months, and there was no Pegasus exploit server to verify as Citizen Lab claims in their report. The same issue of credible verification by Amnesty International arises for all other alleged domain name indicators of compromise.

Domain IOC Data Analysis

April - May, 2019 Citizen Lab informed Catalonians such as Jordi Domingo, Anna Gabriel, and Roger Torrent that they were successfully infected with Pegasus spyware. Citizen Lab released a list of 7 indicators of compromise that confirmed their claims for infection. **2 of 7** domains confirmed by Citizen Lab to be indicators of compromise were expired April - May 2019. **2 of 7** indicators of compromise did not exist, and had never been registered. **1 of 7** domains was registered 11 days after WhatsApp patched the vulnerability claiming to have infected Catalonians with Pegasus. **1 of 7** domains was active and owned by security analytics firm NeuStar, Inc[49]. NeuStar, Inc. is owned by consumer credit service TransUnion. As part of NeuStar's services offered, advertisement metrics (admetrics), help serve relevant data to the clients. "*We help marketers send timely and relevant*

[49] https://securitytrails.com/domain/adsmetrics.co/history/ns

messages to the right people at the right time, using state of the art data analytics and modeling software. We can tell them what ads to serve, and to who and when they should serve them (Neustar, Inc. , 2019)." NeuStar Inc. also had a domain registry division. This business was acquired by Godaddy Inc in 2020 (GoDaddy Inc., 2020).

1 of 7 domains was active and the name servers are pointing to thorniancloud.com. Thorniancloud.com is accused of being "Anti-Tor," a project in which Citizen Lab has a significant interest in[50]. Etienne Maynier, and John Scott-Railton share a stage as participants in the Tor Project PrivChat[51]. Thorniancloud.com attribution for being "Anti-Tor," comes from crimeflare.[52] A full list of "Anti-Tor" domains can be found on https://git.safemobile.org/crimeflare/cloudflare-tor/raw/commit/bd10bef21277ae1b7fe909bff8f49dd5f265f02b/anti-tor_users/fqdn/attd.txt.

Domain IOC Data Results

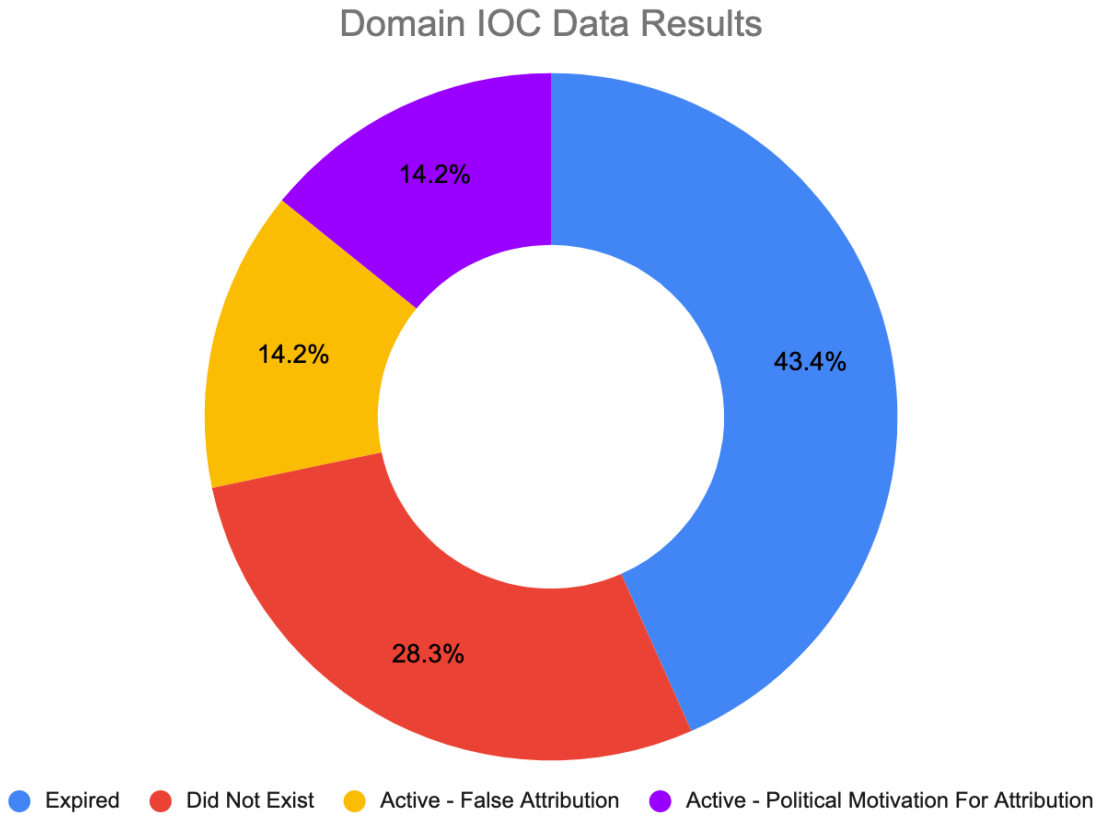
The claim that 7 domains are IOCs that are attributed to spyware fail. **Over 42%** of the alleged IOCs (domains) were expired during the attack time frame. **Over 28%** of the domains did not exist. **14%** were active and have false attributions. **14%** of the domains were active and attribution may be politically motivated. Servers associated point to an "anti-tor" domain, a project in which Amnesty International and Citizen Lab jointly collaborate in.

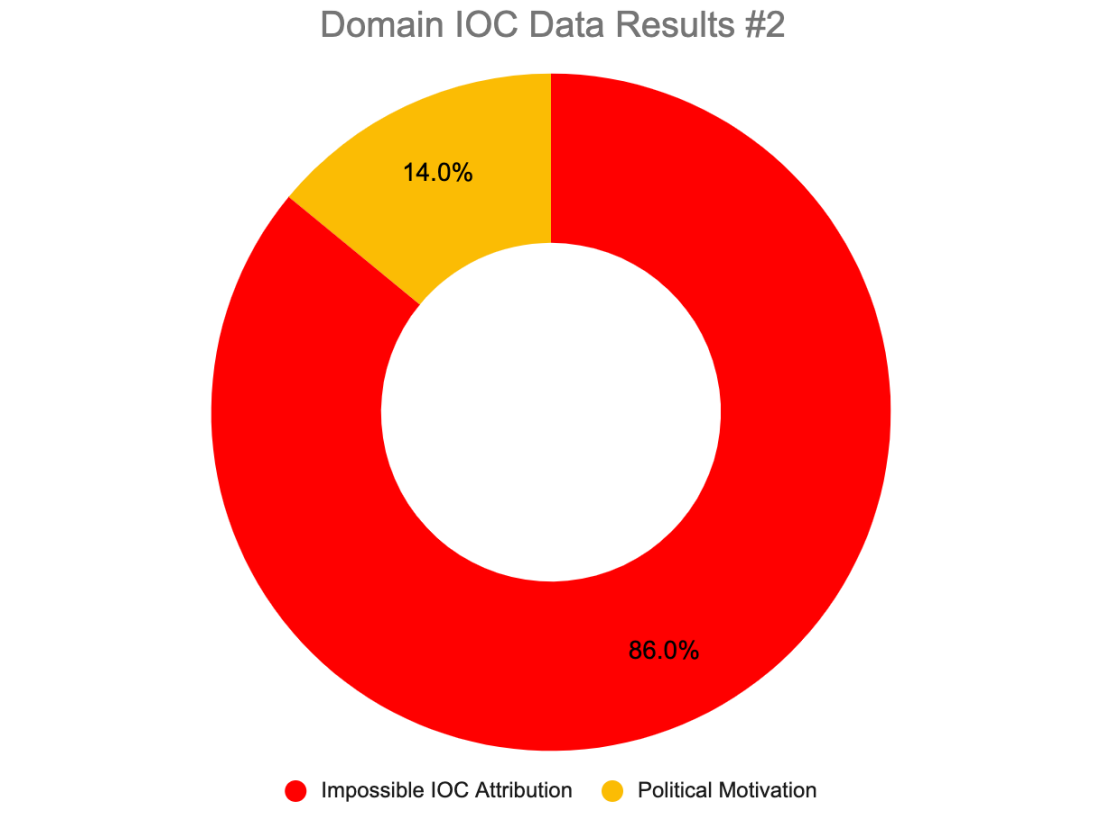
Combining expired domains, domains that did not exist, and false attribution domains yield **86%** of the alleged IOCs to be impossible to attribute.

100% of the domains were expired during the validation and verification alleged by Amnesty International. Citizen Lab failed to present valid data, and falsified their claims the IOCs listed were used to hack Catalonian citizens.

[50] https://www.torproject.org/privchat/chapter-5/
[51] https://www.youtube.com/watch?v=4ovmcZtaacY
[52]https://gitlab.com/crimeflare/cloudflare-tor/-/tree/master/anti-tor_users/fqdn

Alleged IOCs	Domain Status April - May 2019	Domain Status March - April 2022
123tramites.com	Expired	Expired
nnews.co	Active - Political motivation. Name servers thorniancloud.com accused of being Anti-Tor	Expired
statsads.co	Expired	Expired
adsmetrics.co	Active, False Attribution, domain was owned and operated by Security Analytics firm NeuStar, Inc. a TransUnion Company	
redirstats.com	Expired - Registered May 24th, 2019 - 11 day after WhatsApp Vuln. patch	Expired
statsupplier.com	Did not exist	Expired
infoquiz.net	Did not exist	Expired


Domain IOC Data Results
14.2%
43.4%
14.2%
28.3%
Expired
Did Not Exist
Active - False Attribution
Active - Political Motivation For Attribution


Domain IOC Data Results #2
14.0%
86.0%
Impossible IOC Attribution
Political Motivation

False Positives

One of the primary methods that Citizen Labs uses to detect spyware on a mobile device is by using the MVT-Tool. This method can be traced back to 2021. "*Our investigation began in September 2021 when a group of independent journalists contacted Access Now's Digital Security Helpline after testing their devices using the Amnesty International Security Lab's Mobile Verification Toolkit (MVT) tool to detect Pegasus spyware (Project Torogoz: Extensive hacking of Media & Civil Society in El Salvador with pegasus spyware 2022).*"

After reading through the code in the MVT-Tool it was easy to determine that the tool used to detect if a mobile device is infected with spyware is nothing more than a search for keywords. The keywords used to search for the infection are derived from the indicators of compromise published by Citizen Lab and Amnesty International. After reading which applications on an iOS device the MVT-Tool data parses, I hypothesized that I would be able to yield a false positive result of infection by simply accessing an IOC domain via Safari mobile web browser, and sending a WhatsApp message with the IOC URL. I was set out to prove that I could "infect" my own mobile device by sending a WhatsApp message with one of the IOCs to another WhatsApp user. I would never receive a message at all.

My first experiment and tests were conducted May 16th, 2022. Steps for setting up the experiment and my detailed results can be found on my Github repository https://github.com/jonathandata1/Pegasus-CatalanGate-False-Positives. My results did yield false positive results as expected, and I was able to successfully *infect* myself with Pegasus spyware, and Predator.

Next, I knew that if sending a message with an IOC to another device yielded a false positive, it seemed logical that I would be able to send myself a WhatsApp message, and I could not see anywhere in the code to dispute my logic. I sent out a tweet asking for 50 volunteers to help in a "Pegasus Spyware Detection Controlled Test" research project. 9 of 50 I hoped to participate responded to my open call.

I wrote a 14 page document detailing who I was, the type of research the volunteer would be participating in, and I gave

instructions on how to perform the test, and how to deliver their results[53].

Research Participants

9 different countries were represented in this experiment. All participants agreed to have their first name and last initial and their email address publicly published and partially redacted. Researchers also agreed to sharing their unredacted information with journalists, researchers and scientists for validation if requested.

First	Last	Email	Country
Isaac	A	[redact]@gmail.com	Ghana
Khaukha	A	[redact]@gmail.com	Uganda
Patrik	D	[redact]@live.co.uk	Norway
Marcin	G	[redact]@gmail.com	United Kingdom
Raymond	S	[redact]@protonmail.com	Republic of Benin
Shuaib	O	[redact]@yahoo.com	Nigeria
Al	L	[redact]@gmail.com	Israel
Emeka	O	[redact]@gmail.com	Nigeria
Susanna	P	[redact]@gmail.com	USA

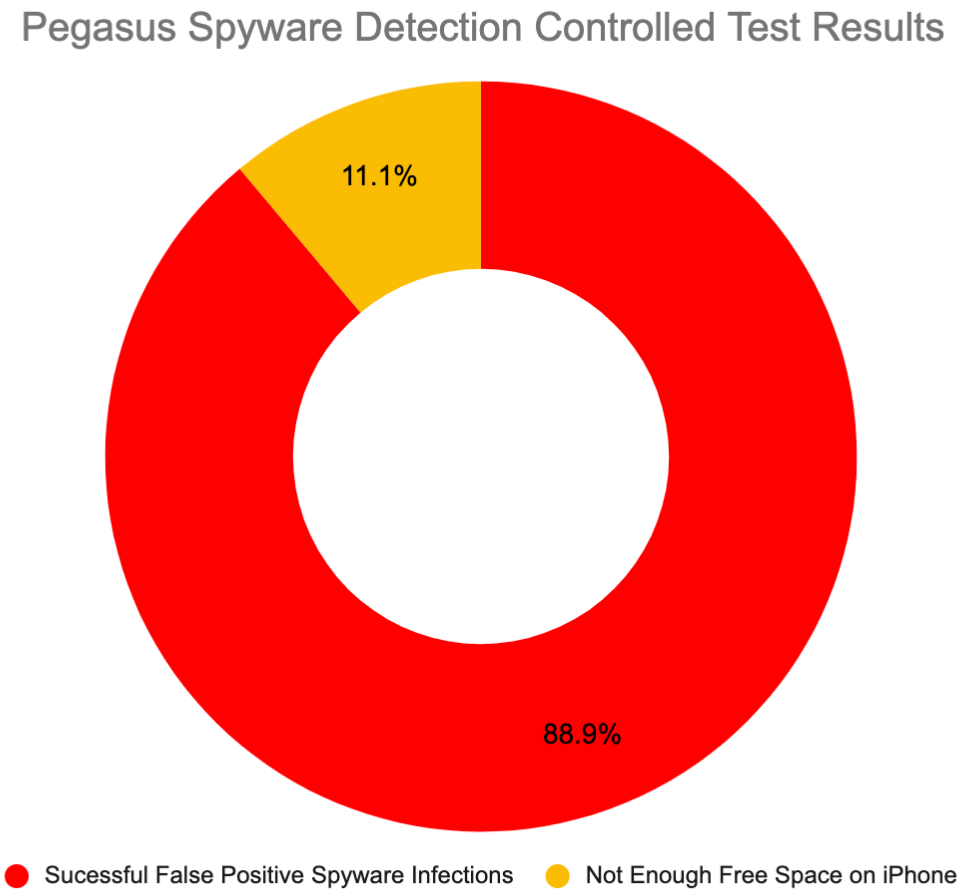
[53]https://github.com/jonathandata1/Pegasus-CatalanGate-False-Positives/wiki/Pegasus-Spyware-Detection-Test---Open-Call

Participants Results

7 of 9 Participants in the test yielded false positive results by sending a WhatsApp message to themselves. 1 of 9 participants did not have enough space on their iPhone 6s Plus to complete the iOS backup needed by the MVT-Tool. 1 of 9 did not follow the instructions and sent an SMS message to themselves with the IOC included. Although they failed to send a WhatsApp message to themselves, the MVT-Tool detected the SMS message and still yielded a false positive result for a spyware infection. Detailed Logs for each of the participants have been available for review since May 21st, 2022, and can be found in the Wiki section of my Github Repository - Pegasus CatalanGate False Positives https://github.com/jonathandata1/Pegasus-CatalanGate-False-Positives/wiki.

First	Last	Email	Country	False Positive Pegasus	False Positive Predator	Results
Isaac	A	[redact]@gmail.com	Ghana	Yes	Yes	Click For Detailed Results
Khaukha	A	[redact]@gmail.com	Uganda	Yes	Yes	Click For Detailed Results
Patrik	D	[redact]@live.co.uk	Norway	Yes	Yes	Click For Detailed Results
Marcin	G	[redact]@gmail.com	United Kingdom	Yes	Yes	Click For Detailed Results
Raymond	S	[redact]@protonmail.com	Republic of Benin	Yes	Yes	Click For Detailed Results
Shuaib	O	[redact]@yahoo.com	Nigeria	Yes	Yes	Click For Detailed Results
Al	L	[redact]@gmail.com	Israel	Yes	Yes	Click For Detailed Results
Emeka	O	[redact]@gmail.com	Nigeria	Not enough space to complete backup	Not enough space to complete backup	Click For Detailed Results
Susanna	P	[redact]@gmail.com	USA	Yes	Yes	Click For Detailed Results

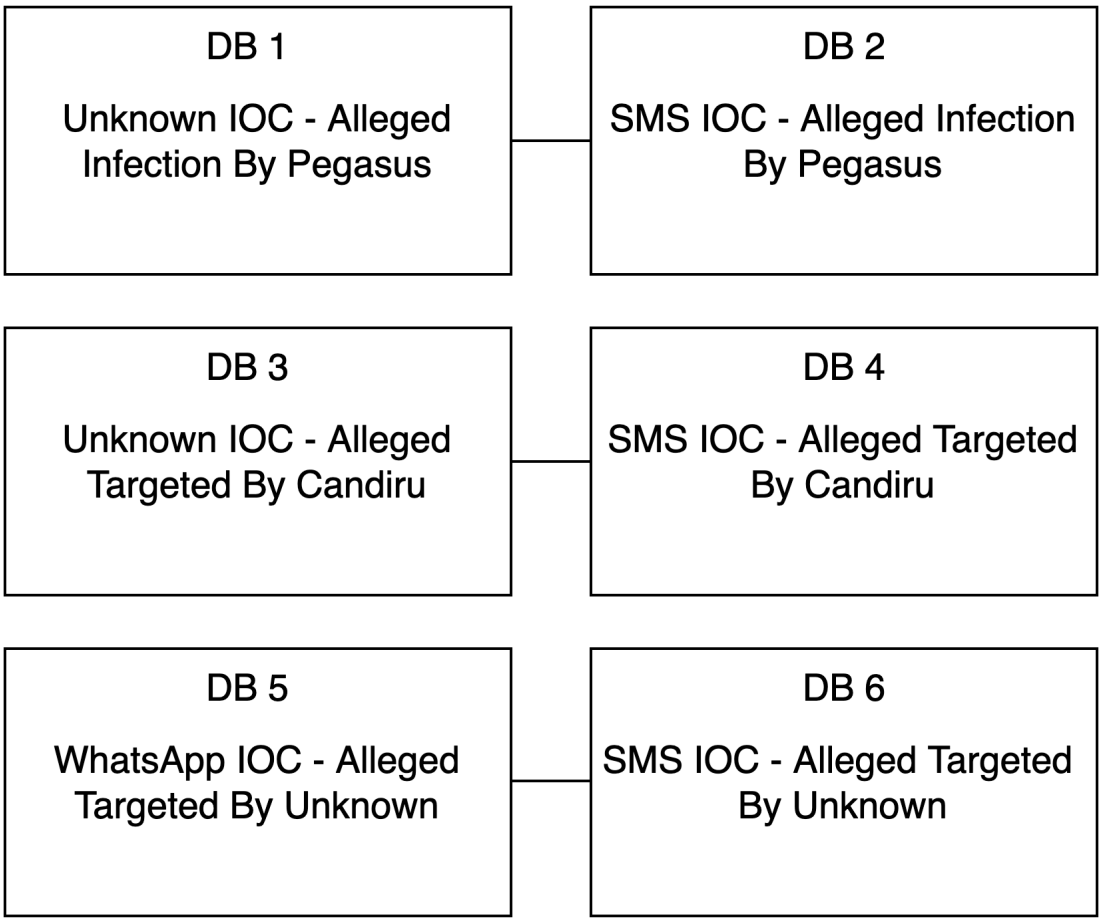
88.9% of research participants were able to successfully yield a false positive result of an infection. **11.1%** of participants did not have enough space on their iPhone to complete the controlled test. The inability to complete the test due to lack of memory on the iPhone raises a good point to note, and question. Did The Citizen Lab ever encounter this issue when conducting their forensics analysis? Statistically if 1 of 9 participants in my study encountered a memory issue this means that out of 65 confirmed targeted and infected Catalonians, there would be a minimum of 7 victims that experienced the same issues, and results would not be available.


Pegasus Spyware Detection Controlled Test Results
11.1%
88.9%
Sucessful False Positive Spyware Infections
Not Enough Free Space on iPhone

Analysis of The Alleged Victims

Citizen Lab presented a table of alleged victims of infection that can be found in Appendix A: Targets of the CatalanGate report. To say it is incoherent is an understatement. Appendix A is a mix of quantitative and qualitative data that is vague, littered with assumptions, missing attributes, empty cells, and nondeterministic values. This table is supposed to serve as truth and evidence that 65 Catalonians were targets, and or infected with spyware, but after extensive analysis of the data I have found no evidence of this claim.

In order to perform a deep analysis on the table provided by Citizen Lab, I organized Appendix A into 6 data blocks.



The data blocks are formed from the alleged **Indicator of Compromise (IOC)**, known or unknown, and the alleged **Infection/Target Status**, also known or unknown. I organized the alleged victims into their respective data block, and created tables that can be easily deciphered. Next, I created a graphical representation showing the percentage of people associated with the following attributes.

- ➔ Unknown infection date(s)
- ➔ Unable to determine specific infection date(s)
- ➔ Date Range of Alleged Infection > 12 months
- ➔ Date Range of Alleged Infection < 12 months
- ➔ Other Various Date Ranges of Alleged Infection

For example if 10/29 people in *DB1* have an Infection/Target Status as **Unable to determine specific infection date(s)**, the pie chart will represent this as 34.5%. Without having a proper understanding of the data presented, a false narrative about infections and targeting has been spreading around the world. Baseless assumptions, misdirection, deception, and illicit activity is largely in part how The Citizen Labs opporates. Not all data blocks will contain the same attributes, but each graphical representation contains a legend for interpretability.

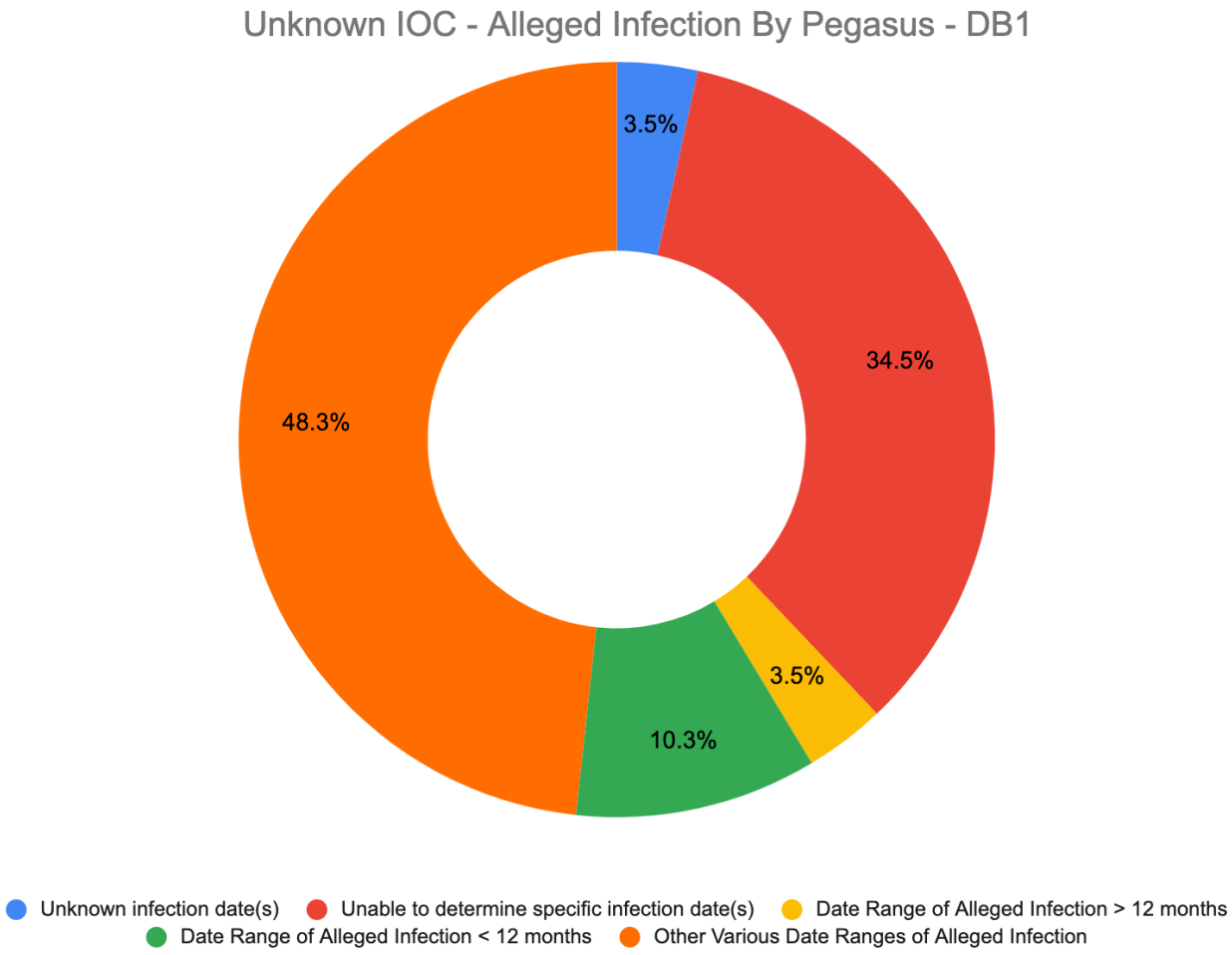
DB1

In DB1 **29 Catalonians** have been confirmed by The Citizen Lab to be infected by Pegasus spyware. The commonality between everyone in DB1 is that they do *not* have indicators of compromise. This means that they were not sent a text message or WhatsApp message, and how they became infected is unknown.

DB1 Data Analysis

10 out of 29 in DB1 have an infection date as: **Unable to determine specific infection date(s).** 1 out of 29 has a date that is **Unknown.** 1 out of 29 has a confirmed infection date range "sometime between[54]" 13 months. 3 out of 29 have a confirmed date range "sometime between" 11 months, 5 months, and 3 months. 14 out of 29 are said to be infected, "On or around," large lists of dates. According to the data provided, Pol Cruz is said to be infected on 16 different dates from August

[54]https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/



2019 to July 2020. All 16 dates of infection have an unknown method of infection.

DB1 Data Results

The claim that 29 Catalonians in DB1 were infected with Pegasus spyware fails. Over 51% of the data does not have dates of infection, and 100% of the subjects do not have IOCs attributed. Citizen Lab fails to present verifiable data, and fails to provide facts sufficient to support their claims.

Alleged Target	Date of Infection
Marc Solsona	Unknown infection date(s)
Albano Dante Fachin	Unable to determine specific infection date(s)
Anonymous 3	Unable to determine specific infection date(s)
Arnaldo Otegi	Unable to determine specific infection date(s)
Artur Mas	Unable to determine specific infection date(s)
David Madi	Unable to determine specific infection date(s)
Elena Jimenez	Unable to determine specific infection date(s)
Jaume Alonso Cuevillas	Unable to determine specific infection date(s)

Jaume Alonso Cuevillas	Unable to determine specific infection date(s)
Meritxell Serret	Unable to determine specific infection date(s)
Miriam Nogueras	Unable to determine specific infection date(s)
Anonymous 4	Sometime between 2018-10-04 – 2019-11-05
Dolors Mas	Sometime between 2018-09-27– 2019-08-28
Josep Rius	Sometime between 2019-07-23 – 2019-10-10
Antoni Comín	Sometime between 2019-08-16 – 2020-01-18
Anonymous 2	– On or around 2019-12-12
Diana Riba	– On or around 2019-10-28
Dr. Elies Campo	– On or around 2019-12-18
Joaquim Jubert	– On or around 2019-10-28
Maria Cinta Cid	– On or around 2019-12-17 – On or around 2019-12-19 – On or around 2019-12-23 – On or around 2019-12-28 – On or around 2019-12-30 – On or around 2020-01-03 – On or around 2020-01-05 – On or around 2020-01-09
Meritxell Bonet	– On or around 2019-06-04
Pol Cruz	– On or around 2020-07-07
Joan Matamala	– On or around 2019-08-07 – On or around 2019-11-18 – On or around 2019-11-20 – On or around 2019-11-26 – On or around 2020-02-18 – On or around 2020-03-02 – On or around 2020-04-11 – On or around 2020-04-14 – On or around 2020-05-06 – On or around 2020-05-25 – On or around 2020-06-05 – On or around 2020-06-17 – On or around 2020-06-23 – On or around 2020-07-02 – On or around 2020-07-09 – On or around 2020-07-13
Xavier Vendrell	– On or around 2019-11-04 – On or around 2020-04-14
Alba Bosch	– On or around 2020-05-14
Andreu Van den Eynde	– On or around 2020-05-14
Jon Iñarritu	– On or around 2020-12-02
Jordi Bosch	– On or around 2020-07-11
Albert Botran	– On or around 2020-01-12

DB2

In DB2 22 Catalonians were confirmed by The Citizen Lab to be infected by Pegasus spyware. The commonality between everyone in DB2 is that their indicator of compromise is an SMS text which means that they immediately became infected once they received a text message. The data provided specifically categorizes the infected individuals as being part of the SMS-Based attack, but the CatalanGate report also references a new zero-click attack alleged to be exploited via iMessage. Citizen Lab says that they *just* reported this zero-click vulnerability to Apple although their investigation started 3 years earlier. In a section of the CatalanGate titled "Discovering Homage," readers are provided a screenshot with a javascript code snippet, a partially redacted URL, and a bundle of dates with timestamps. The redacted URL is said to be a Pegasus exploit server. After researching for more information on the URL, I uncovered the following results.

theappanalytics.com

Although the URL in the screenshot is partially redacted, a subdomain is able to be read. **apiweb248.theappanalytics.com** is referenced by Amnesty International in their publication "Forensic Methodology Report: How to catch NSO Group's Pegasus." I cited this publication earlier in this white paper as it is known to be the report that "validates" Citizen Labs's forensics methodology. Citizen Lab states they, "*independently employed a similar methodology to Amnesty International in our analysis of potential Pegasus compromise (i.e., identifying process names proximate to communication with Pegasus servers) (Marczak et al., 2021).*"

Citizen Lab claims this never before seen exploit was "*used to hack Catalan targets' iPhones with Pegasus between 2017 and 2020 (Scott-Railton et al., 2022).*" Research data confirms that Amnesty International referenced this malicious domain, and webkit exploit in the 2021 Apple Inc. NSO Group Technologies Limited lawsuit. EXHIBIT 2 Case 5:21-cv-09078-NC, takes the Amnesty and Citizen Lab collusion to new heights stating,. "*Amnesty International thanks*

Citizen Lab for its peer-review of this research report. The Citizen Lab at the University of Toronto has independently peer-reviewed a draft of the forensic methodology outlined in this report. ***Bill Marczak*** *and others, Independent Peer Review of Amnesty International's Forensic Methods for Identifying Pegasus Spyware, Citizen Lab, 18 July 2021...these resolutions…apiweb248.theappanalytics.com…represent only a small subset of overall NSO Group Pegasus activity. (2021,* 5:21-cv-09078-NC)." In summary, Amnesty International acting as an independent validator and verifier of the CatalanGate report, allowed Citizen Lab to falsely claim that a previously unknown and newly discovered zero-click vulnerability had targeted Catalonians. For Citizen Lab to claim they had never seen this exploit before is false, as quoted in the Apple VS. NSO lawsuit Bill Marczak performed the peer review of Amnesty International's research that speaks directly to **apiweb248.theappanalytics.com**, and how it is associated with a zero-click exploit.

The only attribution that claims to show evidence that "*iMessage exploits were used to hack Catalan targets' iPhones with Pegasus between 2017 and 2020 (Scott-Railton et al., 2022),*" turns out to be false, and is nothing more than an intentionally concocted narrative framed by The Citizen Lab, and Amnesty International.

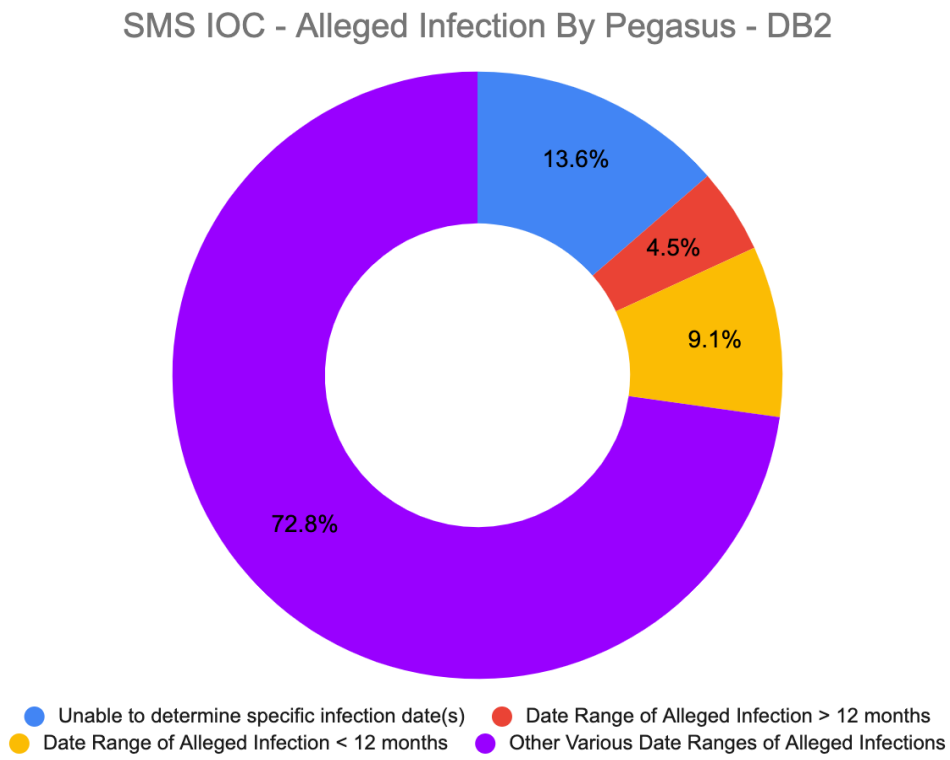
DB2 Data Analysis

3 of 22 have an infection date as: **Unable to determine specific infection date(s).** 1 of 22 have a date range of infection that is greater than 12 months. 2 of 22 have a date range that is less than 12 months, and 16 of 22 are said to be infected "On or around," large lists of dates. It should be noted that David Bonvehi, and Oriol Sagrera were analyzed as having an infection range of less than 12 months because of the mixture of data included.

DB2 Data Results

The claim that 22 Catalonians in DB2 were infected with Pegasus spyware fails. Over 27% have unknown dates of infection, Over 72% have dates without evidence for attribution. Citizen Lab fails to present verifiable data, and fails to provide facts sufficient to support their claims.

Alleged Target	Date of Infection
Josep Maria Jové	Unable to determine specific infection date(s)
Meritxell Budo	Unable to determine specific infection date(s)
Pere Aragonès	Unable to determine specific infection date(s)
Albert Batet	– On or around 2019-10-24 – On or around 2020-07-07
Anonymous 1	– On or around 2020-05-26
Carles Riera	– Sometime before 2019-06-11
David Bonvehi	Sometime between 2018-09-30 – 2019-01-30 – On or around 2019-02-15 – On or around 2019-04-05 – On or around 2019-04-09 – Sometime between 2020-02-08 – 2020-06-16
Elisenda Paluzie	– On or around 2019-10-29
Gonzalo Boye	– On or around 2020-10-30
Joaquim Torra	– On or around 2020-04-21 – On or around 2020-05-19 – On or around 2020-06-11 – On or around 2020-06-21 – On or around 2020-07-07 – On or around 2020-07-09 – On or around 2020-07-13 – On or around 2020-07-15
Jordi Baylina	– On or around 2019-10-29 – On or around 2019-11-15 – On or around 2019-11-26 – On or around 2019-11-26 – On or around 2019-12-11 – On or around 2019-12-23 – On or around 2020-06-19 – On or around 2020-07-11
Jordi Sanchez	– On or around 2017-05-26 – On or around 2017-09-11 – On or around 2017-09-15 – On or around 2017-10-13
Jordi Solé	– On or around 2020-06-11 – On or around 2020-06-27
Josep Costa	– On or around 2019-07-15 – On or around 2019-12-17 – On or around 2019-12-21 – On or around 2019-12-30
Josep Lluís Alay	– On or around 2020-07-13
Josep Ma Ganyet	– On or around 2019-10-23 – On or around 2020-01-08 – On or around 2020-03-02
Marcel Mauri	– On or around 2019-10-24 – On or around 2020-02-25 – On or around 2020-05-06
Marcela Topor	– On or around 2019-10-07 – On or around 2020-01-04
Marta Rovira	– On or around 2020-06-12 – On or around 2020-07-13
Oriol Sagrera	– On or around 2019-03-22 – On or around 2019-04-02 – Sometime between 2019-04-06 – 2019-10-06 – On or around 2020-07-08
Sergi Sabrià	– On or around 2020-04-11 – On or around 2020-05-05 – On or around 2020-05-10 – On or around 2020-05-13 – On or around 2020-07-13
Sònia Urpí	– On or around 2020-06-22



DB3

In DB3 3 Catalonians have been confirmed by The Citizen Lab to be targeted by Candiru spyware. The commonality between everyone in DB3 is that they do not have confirmed indicators of compromise, and they do not have dates associated with the alleged targeting. Citizen Lab decided to name a previously unnamed alleged target of Candiru in the CatalanGate report. Joan Matamala was "patient zero," in Citizen Labs's report titled "Hooking Candiru."

The mention of Joan Matamala in the CatalanGate report is completely irrelevant, and out of context. The claim that stat.email can be attributed to Candiru and the hacking of Matamala's PC is also unrelated to the CatalanGate report. The Hooking Candiru report attributes the Saudi government to the Candiru infection, and now Citizen Lab is wildly attributing the infection to the Spanish Government. Uzbekistan, Saudi Arabia, Singapore, and Qatar have been named as the alleged countries that have purchased Candiru (Marczak et al., 2021), there are no sources that can corroborate CL's claim that the Spanish government is a client using Candiru[55].

The narrative that Citizen Lab has engineered can easily be dismantled by

[55]https://www.forbes.com/sites/thomasbrewster/2019/10/03/meet-candiru-the-super-stealth-cyber-mercenaries-hacking-apple-and-microsoft-pcs-for-profit/?sh=54fd14025a39

reading the context of their claims. The only information about the individuals that are purportedly targets are names. Everything about DB3 is speculative, and in my professional experience I do not see evidence of anything more than a massive phishing campaign sent to people around the world.

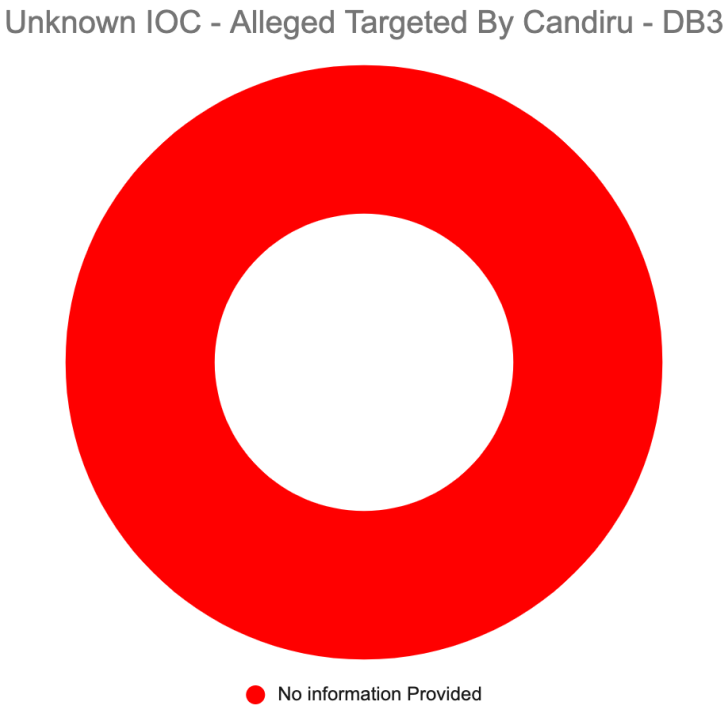
DB3 Data Analysis

3 of 3 confirmed targets of Candiru spyware do not have IOCs and dates of infection are not provided. Note: Joan Matamala is included in DB3 and DB1.

DB3 Data Results

100% of the alleged targeted victims by the Spanish government do not have data associated with the claim. The claim that Elies Campo, Joan Matamala, and Xavier Vives were targeted with Candiru spyware operated by the Spanish government fails. Citizen Lab fails to present verifiable data, and fails to provide facts sufficient to support their claims.

Alleged Target	Date of Targeting
Elies Campo	No Information Provided
Joan Matamala	No Information Provided
Xavier Vives	No Information Provided



DB4

In DB4 1 Catalonian have been confirmed by The Citizen Lab to be targeted by Candiru. The CatalanGate report suggests news105@tutanota.com "may be an email address used by the spyware operators," to target Pau Escrish. There is no definitive IOC assigned to the alleged targeting of Pau Escrish by the Spanish government. Citizen Lab then makes a claim that the Candiru phishing email sent to Pau Escrish looks like a Pegasus phishing text sent to Jordi Baylina. "The Mobile World Congress email containing a Candiru link is also noteworthy, as it echoes bait content in a Pegasus SMS sent to a separate target, Jordi Baylina (Scott-Railton et al., 2022)."

Why Citizen Lab is trying to make a completely unrelated correlation is unknown, but it seems clear that this is just more misdirection from them.

DB4 Data Analysis

1 of 1 confirmed targets of Candiru spyware do not have IOCs and dates of infection are not provided.

DB4 Data Results

100% of the alleged targeted victims by the Spanish government do not have data associated with the claim. The claim that Pau Escrish was targeted with Candiru spyware operated by the Spanish government fails. Citizen Lab fails to present verifiable data, and fails to provide facts sufficient to support their claims.

Alleged Target	Date of Targeting
Pau Escrich	No Information Provided

DB5

In DB5 5 Catalonians have been confirmed by The Citizen Lab to be targeted by unknown spyware via WhatsApp.

Unsurprisingly, pro-independence government officials Jordi Domingo, Anna Gabriel, and Roger Torrent whom The Citizen Lab had alerted in 2019, do not have dates associated with their alleged targeting, and because there are no dates listed in listed in the CatalanGate report, there is no spyware attributed either. The alleged dates of targeting via Pegasus spyware were confirmed by The Guardian via The Citizen Lab as being early 2019. “In addition to Torrent, researchers at Citizen Lab at the University of Toronto Munk School – who collaborated with WhatsApp after the alleged hacking attempts were discovered – alerted two other pro-independence individuals last year (2019) that they had been targeted (Kirchgaessner & Jones, 2020).” There are no indicators of compromise associated with the targeted victims, and no data to review. Moreover, the evidence I provided for the alleged IOCs, show that 8 of 9 domains that are claimed to have targeted Jordi Domingo, Anna Gabriel, Ernest Maragall, Sergi Miquel and Roger Torrent, were expired or did not exist at the time of the WhatsApp vulnerability. Only 1 of the 9 domains was active and there is no evidence to validate attribution.

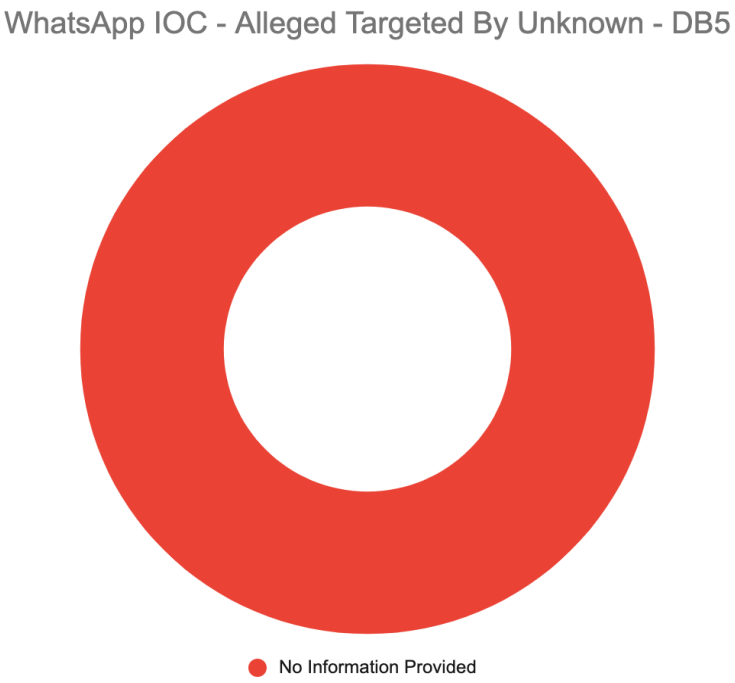
DB5 Data Analysis

5 of 5 confirmed targets of an unknown spyware via WhatsApp do not have IOCs and dates of infection are not provided.

DB5 Data Results

100% of the alleged targeted victims by the Spanish government do not have data associated with the claim. Citizen Lab fails to present verifiable data, and fails to provide facts sufficient to support their claims.

Alleged Target	Date of Targeting
Anna Gabriel	No Information Provided
Ernest Maragall	No Information Provided
Jordi Domingo	No Information Provided
Roger Torrent	No Information Provided
Sergi Miquel	No Information Provided



DB6

In DB6 7 Catalonians have been confirmed by The Citizen Lab to be targeted by unknown spyware via SMS. Roger Torrent is present in DB6 and DB5. Citizen Lab claims that Roger Torrent, and Laura Borràs as members of the Catalan legislation "*were extensively infected…either while in office or prior to taking office (Scott-Railton et al., 2022).*" There are no IOCs attributed to the infections, and there are no dates. There are only claims of targeting without any evidence to support the claims.

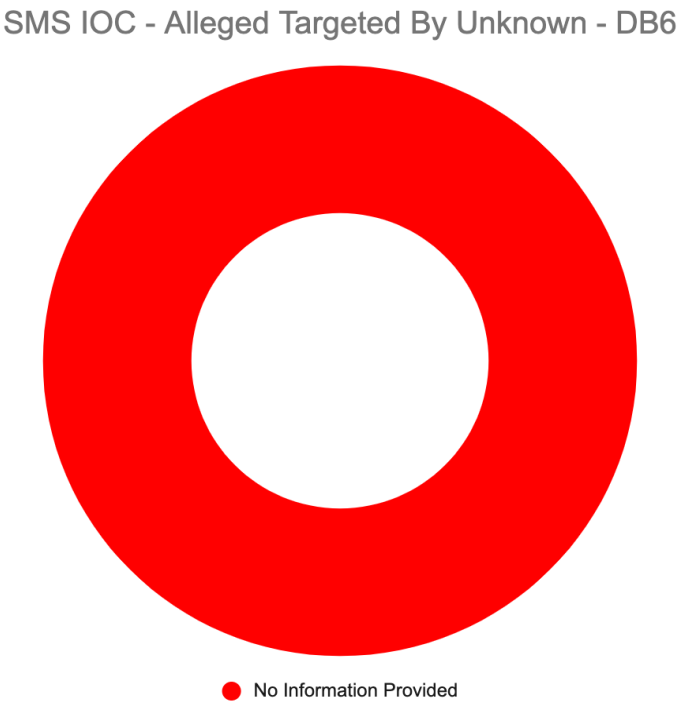
DB6 Data Analysis

7 of 7 confirmed targets of an unknown spyware via SMS do not have IOCs and dates of infection are not provided.

DB6 Data Results

100% of the alleged targeted victims by the Spanish government do not have data associated with the claim. Citizen Lab fails to present verifiable data, and fails to provide facts sufficient to support their claims.

Alleged Target	Date of Targeting
Arià Bayé	No Information Provided
David Fernández	No Information Provided
Elsa Artadi	No Information Provided
Ferran Bel	No Information Provided
Laura Borràs	No Information Provided
Marta Pascal	No Information Provided
Roger Torrent	No Information Provided



Complete Victim Data Results

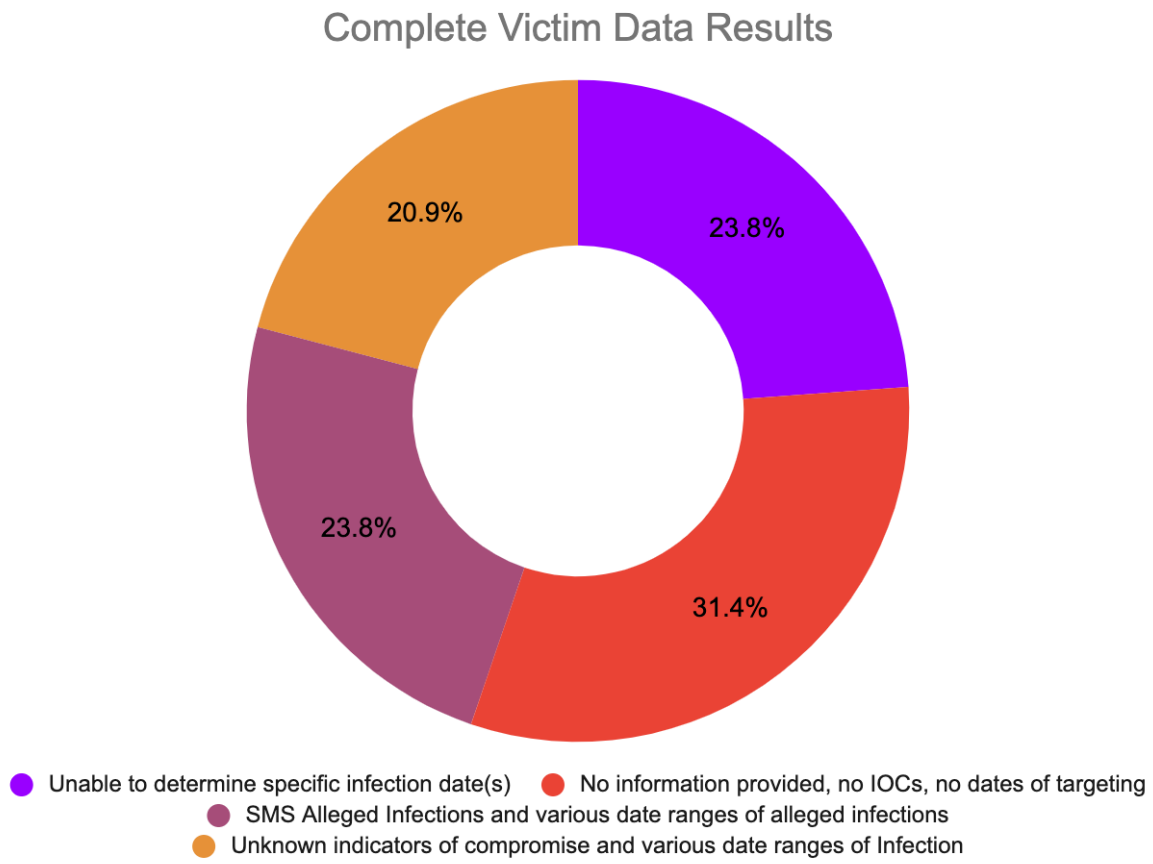
This analysis is based on 67 victims. Rogger Torrent and Joan Matamala are listed as being targeted by WhatsApp + SMS, and Pegasus + Candiru respectively. 16 of 67 victims (23.8%), Citizen Lab was unable to determine specific dates of infection. 21 of 67 victims (31.4%), Citizen Lab did not provide any indicators of compromise, nor did they provide any dates of targeting. 16 of 67 victims (23.8%) are alleged to be infected via SMS and had various date ranges of alleged infections. 14 of 67 victims (20.9%) had unknown indicators of compromise and various date ranges of alleged infection.

Alleged Target	Date of Targeting or Infection	Targeted or Infected
Arià Bayé	No Information Provided	Targeted
David Fernández	No Information Provided	Targeted
Elsa Artadi	No Information Provided	Targeted
Ferran Bel	No Information Provided	Targeted
Laura Borràs	No Information Provided	Targeted
Marta Pascal	No Information Provided	Targeted
Roger Torrent	No Information Provided	Targeted
Anna Gabriel	No Information Provided	Targeted
Ernest Maragall	No Information Provided	Targeted
Jordi Domingo	No Information Provided	Targeted
Roger Torrent	No Information Provided	Targeted
Sergi Miquel	No Information Provided	Targeted
Pau Escrich	No Information Provided	Targeted
Elies Campo	No Information Provided	Targeted
Joan Matamala	No Information Provided	Targeted
Xavier Vives	No Information Provided	Targeted
Josep Maria Jové	Unable to determine specific infection date(s)	Infected
Meritxell Budo	Unable to determine specific infection date(s)	Infected
Pere Aragonès	Unable to determine specific infection date(s)	Infected

Marc Solsona	Unknown infection date(s)	Infected
Albano Dante Fachin	Unable to determine specific infection date(s)	Infected
Anonymous 3	Unable to determine specific infection date(s)	Infected
Arnaldo Otegi	Unable to determine specific infection date(s)	Infected
Artur Mas	Unable to determine specific infection date(s)	Infected
David Madi	Unable to determine specific infection date(s)	Infected
Elena Jimenez	Unable to determine specific infection date(s)	Infected
Jaume Alonso Cuevillas	Unable to determine specific infection date(s)	Infected
Jaume Alonso Cuevillas	Unable to determine specific infection date(s)	Infected
Meritxell Serret	Unable to determine specific infection date(s)	Infected
Miriam Nogueras	Unable to determine specific infection date(s)	Infected
Anonymous 4	Sometime between 2018-10-04 – 2019-11-05	Infected
Dolors Mas	Sometime between 2018-09-27– 2019-08-28	Infected
Josep Rius	Sometime between 2019-07-23 – 2019-10-10	Infected
Antoni Comín	Sometime between 2019-08-16 – 2020-01-18	Infected
Carles Riera	Sometime before 2019-06-11	Infected
Oriol Sagrera	– Sometime between 2019-04-06 – 2019-10-06 – On or around 2019-03-22 – On or around 2019-04-02 – On or around 2020-07-08	Infected
David Bonvehi	Sometime between 2018-09-30 – 2019-01-30 Sometime between 2020-02-08 – 2020-06-16 – On or around 2019-02-15 – On or around 2019-04-05 – On or around 2019-04-09	Infected
Albert Batet	– On or around 2019-10-24 – On or around 2020-07-07	Infected
Anonymous 1	– On or around 2020-05-26	Infected
Elisenda Paluzie	– On or around 2019-10-29	Infected
Gonzalo Boye	– On or around 2020-10-30	Infected
Joaquim Torra	– On or around 2020-04-21 – On or around 2020-05-19 – On or around 2020-06-11 – On or around 2020-06-21 – On or around 2020-07-07 – On or around 2020-07-09 – On or around 2020-07-13	Infected

	– On or around 2020-07-15	
Jordi Baylina	– On or around 2019-10-29 – On or around 2019-11-15 – On or around 2019-11-26 – On or around 2019-11-26 – On or around 2019-12-11 – On or around 2019-12-23 – On or around 2020-06-19 – On or around 2020-07-11	Infected
Jordi Sanchez	– On or around 2017-05-26 – On or around 2017-09-11 – On or around 2017-09-15 – On or around 2017-10-13	Infected
Jordi Solé	– On or around 2020-06-11 – On or around 2020-06-27	Infected
Josep Costa	– On or around 2019-07-15 – On or around 2019-12-17 – On or around 2019-12-21 – On or around 2019-12-30	Infected
Josep Lluís Alay	– On or around 2020-07-13	Infected
Josep Ma Ganyet	– On or around 2019-10-23 – On or around 2020-01-08 – On or around 2020-03-02	Infected
Marcel Mauri	– On or around 2019-10-24 – On or around 2020-02-25 – On or around 2020-05-06	Infected
Marcela Topor	– On or around 2019-10-07 – On or around 2020-01-04	Infected
Marta Rovira	– On or around 2020-06-12 – On or around 2020-07-13	Infected
Sergi Sabrià	– On or around 2020-04-11 – On or around 2020-05-05 – On or around 2020-05-10 – On or around 2020-05-13 – On or around 2020-07-13	Infected
Sònia Urpí	– On or around 2020-06-22	Infected
Anonymous 2	– On or around 2019-12-12	Infected
Diana Riba	– On or around 2019-10-28	Infected
Dr. Elies Campo	– On or around 2019-12-18	Infected
Joaquim Jubert	– On or around 2019-10-28	Infected

Maria Cinta Cid	– On or around 2019-12-17 – On or around 2019-12-19 – On or around 2019-12-23 – On or around 2019-12-28 – On or around 2019-12-30 – On or around 2020-01-03 – On or around 2020-01-05 – On or around 2020-01-09	Infected
Meritxell Bonet	– On or around 2019-06-04	Infected
Pol Cruz	– On or around 2020-07-07	Infected
Joan Matamala	– On or around 2019-08-07 – On or around 2019-11-18 – On or around 2019-11-20 – On or around 2019-11-26 – On or around 2020-02-18 – On or around 2020-03-02 – On or around 2020-04-11 – On or around 2020-04-14 – On or around 2020-05-06 – On or around 2020-05-25 – On or around 2020-06-05 – On or around 2020-06-17 – On or around 2020-06-23 – On or around 2020-07-02 – On or around 2020-07-09 – On or around 2020-07-13	Infected
Xavier Vendrell	– On or around 2019-11-04 – On or around 2020-04-14	Infected
Alba Bosch	– On or around 2020-05-14	Infected
Andreu Van den Eynde	– On or around 2020-05-14	Infected
Jon Iñarritu	– On or around 2020-12-02	Infected
Jordi Bosch	– On or around 2020-07-11	Infected
Albert Botran	– On or around 2020-01-12	Infected



Sample Request

May, 2022, I sent a formal request to The Citizen Lab to obtain the samples taken from Ewa Wrzosek's mobile device. Citizen Lab had confirmed that Polish Prosecutor Ewa Wrzosek[56] had been infected with Pegasus Spyware, and with her full consent I submitted my request. As a computer scientist and mobile researcher, if I can see the samples taken from her mobile device, I can perform an in-depth analysis to determine if there is anything forensically that can be definitively linked to malicious servers. I have not received a response to my request from Citizen Lab.

[56] https://twitter.com/rondeibert/status/1473030751558017028

Conclusion

The CatalanGate report has been presented to the world as factual scientific discovery of a global threat. Just as medical reports demand proof of claim that can be verified by professionals, the same applies to spyware infection accusations. It is evident that the political stress of the CatalanGate publication has placed verification and validation of science to the side. Over 55% of the alleged target or infected Catalonians do not have dates of compromise associated with them. When reporting a crime the investigator will always ask, “when did this occur,” and if the response is, “I don’t know, I was told it happened,” how can the victim properly take action? I cannot express how disappointed I am in the information security community for allowing this to continue for more than a decade. People that have been told they are infected with spyware are living everyday believing that they have been violated when in fact this is not the case. It is time for the people to know the truth.

References

About Citizen Lab. (2022, May 9). *About the citizen lab*. The Citizen Lab. Retrieved June 30, 2022, from https://citizenlab.ca/about/

Amnesty Careers. (2022, June). *Amnesty International*. Amnesty International Careers. Retrieved July 1, 2022, from https://web.archive.org/web/20220615174336/https://careers.amnesty.org/vacancy/researcher-adviser-technology-and-human-rights---sabbatical-cover-3410/3438/description/

Amnesty International. (2021, July 18). *Forensic methodology report: How to catch nso group's pegasus*. Amnesty International. Retrieved July 1, 2022, from https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

AmnestyTech. (2022, April 18). *Update iocs · pull request #26 · AmnestyTech/investigations*. GitHub. Retrieved May 13, 2022, from https://github.com/AmnestyTech/investigations/pull/26

Awati, R. (2021, November 5). *What is cache poisoning and how does it work?* SearchSecurity. Retrieved June 29, 2022, from https://www.techtarget.com/searchsecurity/definition/cache-poisoning

Berkeley, I. C. I. S. (2014, August 21). *The blog of the International Computer Science Institute*. ICSI. Retrieved May 1, 2022, from https://www.icsi.berkeley.edu/icsi/blog/marczak-repressive-governments-use-of-cyber-attacks

Brewster, T. (2019, October 3). *Meet candiru - the mysterious mercenaries hacking Apple and Microsoft pcs for Profit*. Forbes. Retrieved July 4, 2022, from https://www.forbes.com/sites/thomasbrewster/2019/10/03/meet-candiru-the-super-stealth-cyber-mercenaries-hacking-apple-and-microsoft-pcs-for-profit/?sh=54fd14025a39

Center for International Governance Innovation. (2020). *Ronald J. Deibert*. Centre for International Governance Innovation. Retrieved June 29, 2022, from https://www.cigionline.org/people/ronald-j-deibert/

Citizen Lab. (2019, October 29). *NSO Group / Q cyber technologies: Over one hundred new abuse cases*. The Citizen Lab. Retrieved June 22, 2022, from https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/

Crowdstrike. (2022, March 31). *What are indicators of compromise? IOC explained: Crowdstrike*. crowdstrike.com. Retrieved May 13, 2022, from https://www.crowdstrike.com/cybersecurity-101/indicators-of-compromise/

CVE Details. (2016, August 25). *Vulnerability details : CVE-2016-4657*. CVE Details. Retrieved June 29, 2022, from https://www.cvedetails.com/cve/CVE-2016-4657/

Deibert, R. (2018, August 5). *The Citizen Lab Research and development at the intersection of digital media, global security, and human rights*. The Citizen Lab. Retrieved April 30, 2022, from https://citizenlab.ca/wp-content/uploads/2018/05/18033-Citizen-Lab-booklet-p-E.pdf

Deibert, R. (2022, May 14). Ronald Deibert - Response To European Parliament . Retrieved June 20, 2022, from https://deibert.citizenlab.ca/wp-content/uploads/2022/05/2022.05.13-L-Ferris-to-J-Canas.pdf

El Espanol. (2022, May 7). *El Currículum del Artífice del 'Catalangate', Bajo Sospecha*. Crónica Global. Retrieved June 20, 2022, from https://cronicaglobal.elespanol.com/politica/artifice-catalangate-elies-campo-curriculum_661667_102.html

Farrow, R. (2022, April 14). *How democracies spy on their citizens*. The New Yorker. Retrieved June 29, 2022, from https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens

Franceschi-Bicchierai, L., & Cox, J. (2020, July 14). *Source: Spain is customer of NSO Group*. VICE. Retrieved May 1, 2022, from https://www.vice.com/en/article/pkyzxz/spain-nso-group-pegasus-catalonia

GoDaddy Inc. (2020, April 6). *GoDaddy acquires Neustar's registry business*. GoDaddy Acquires Neustar's Registry Business. Retrieved July 3, 2022, from https://www.prnewswire.com/news-releases/godaddy-acquires-neustars-registry-business-301036134.html

González, M. (2020, July 15). *Los Servicios Secretos españoles tienen El Programa Que Espió a torrent*. El País. Retrieved May 1, 2022, from https://elpais.com/espana/2020-07-15/los-servicios-de-informacion-tienen-programas-como-el-que-espio-a-torrent.html

González, M. (2022, May 2). *Los Teléfonos de Sánchez y robles también han sido espiados por pegasus*. El País. Retrieved May 2, 2022, from https://elpais.com/espana/2022-05-02/el-gobierno-informa-que-los-telefonos-de-sanchez-y-robles-han-sido-infectados-con-el-programa-pegasus.html

Hostmines.com. (2021). *Terms of service*. Cheapest Web Hosting Provider with Free SSL for Lifetime. Retrieved June 22, 2022, from https://www.hostmines.com/tos/

hostplax.com. (2019, October 19). *Hostplax.com : Cheapest Domain and hosting: Free domain: Free SSL*. HostPlax.com | Cloud Shared Hosting, Linux shared hosting, $1 web hosting, Cloud VPS, Free SSL with Hosting, Cheapest Domain and Hosting. Retrieved

June 22, 2022, from
https://web.archive.org/web/20191001043847/https://www.hostplax.com/

Invar Technologies. (2019, August 10). *Hackers claim to auction data they stole from NSA-linked spies*. INVAR Technologies. Retrieved July 3, 2022, from
https://www.invar.nyc/2019/08/10/hackers-claim-auction-data-stole-nsa-linked-spies/

ISO.org. (2012). *Conformity assessment — Requirements for the operation of various types of bodies* . ISO. Retrieved May 13, 2022, from
https://www.iso.org/obp/ui/#iso:std:iso-iec:17020:ed-2:v1:en

Jones, S. (2022, April 18). *Catalan leaders targeted using NSO spyware, say cybersecurity experts*. The Guardian. Retrieved June 28, 2022, from
https://www.theguardian.com/world/2022/apr/18/catalan-leaders-targeted-using-nso-spyware-say-cybersecurity-experts

Kirchgaessner, S. (2020, July 28). *Whatsapp confirms Catalan politician's phone was target of 2019 attack*. The Guardian. Retrieved May 1, 2022, from
https://www.theguardian.com/technology/2020/jul/28/whatsapp-confirms-catalan-politicians-phone-was-target-of-2019-attack

Kirchgaessner, S., & Jones, S. (2020, July 13). *Phone of top Catalan politician 'targeted by government-grade spyware'*. The Guardian. Retrieved May 1, 2022, from
https://www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware

Marczak, B., Dalek, J., McKune, S., Senft, A., Scott-Railton, J., & Deibert, R. (2020, May 8). *Bad traffic: Sandvine's PacketLogic devices used to deploy government spyware in Turkey and redirect Egyptian users to affiliate ads?* The Citizen Lab. Retrieved June 21, 2022, from
https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/

Marczak, B., Scott-Railton, J., Anstis, S., & Deibert, R. (2021, July 19). *Independent peer review of Amnesty International's forensic methods for identifying pegasus spyware*. The Citizen Lab. Retrieved July 2, 2022, from
https://citizenlab.ca/2021/07/amnesty-peer-review/

Marczak, B., Scott-Railton, J., Berdan, K., Razzak, B. A., & Deibert, R. (2021, July 15). *Hooking candiru: Another mercenary spyware vendor comes into focus*. The Citizen Lab. Retrieved July 4, 2022, from
https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/

Marczak, B., Scott-Railton, J., McKune, S., Razzak, B. A., & Deibert, R. (2020, May 8). *Hide and seek: Tracking NSO group's pegasus spyware to operations in 45 countries*. The Citizen Lab. Retrieved June 21, 2022, from

https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

Megiddo, G. (2021, June 8). *Secretive Israeli cyber firm selling spy-tech to Saudi Arabia*. Haaretz.com. Retrieved July 3, 2022, from https://www.haaretz.com/israel-news/tech-news/2021-06-08/ty-article/.highlight/the-secret-israeli-cyber-firm-selling-spy-tech-to-saudia-arabia/0000017f-df07-d856-a37f-ffc724f80000

Mobile, L. G. (2022, January 31). *Vulnerability details : CVE-2022-23728*. CVE Details. Retrieved April 30, 2022, from https://www.cvedetails.com/cve/CVE-2022-23728/

Mobile, L. G. (2022, March 4). *CVE-2022-23729*. Open CVE. Retrieved April 30, 2022, from https://www.opencve.io/cve/CVE-2022-23729

Morelli, O. (2019, May 14). *WhatsApp users forced to update the app after a severe bug is patched*. Security and spyware news. Retrieved May 1, 2022, from https://www.2-spyware.com/whatsapp-users-forced-to-update-the-app-after-a-severe-bug-is-patched

Munk School of Global Affairs. (2022, February 28). *Fellow in residence - munk school of global affairs & public policy*. Munk School of Global Affairs and Public Policy. Retrieved June 30, 2022, from https://munkschool.utoronto.ca/opportunity/fellow-in-residence-munk-school-of-global-affairs-public-policy/

Network, V. (2017, September 28). *George Soros is funding the independence of Catalonia*. Voltaire Network. Retrieved June 28, 2022, from https://www.voltairenet.org/article198106.html

Neustar, Inc. . (2019, May 2). *About Us: Neustar*. home.neustar. Retrieved July 3, 2022, from https://www.home.neustar/about-us

NIST. (2022, May). Digital Investigation Techniques: A NIST Scientific Foundation Review. Retrieved June 30, 2022, from https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8354-draft.pdf

Olivas, J. J. (2022, May). Methodological and ethical Issues in citizen lab's spyware. Retrieved June 20, 2022, from https://www.researchgate.net/profile/Jose-Javier-Olivas-Osuna/publication/361140330_Methodological_and_ethical_issues_in_Citizen_Lab's_spyware_investigation_in_Catalonia/links/629f44ce6886635d5cc6fe64/Methodological-and-ethical-issues-in-Citizen-Labs-spyware-investigation-in-Catalonia.pdf

Person, & Christopher Bing, J. M. (2021, December 4). *U.S. state department phones hacked with Israeli company spyware - sources*. Reuters. Retrieved July 3, 2022, from https://www.reuters.com/technology/exclusive-us-state-department-phones-hacked-with-isr

aeli-company-spyware-sources-2021-12-03/#:~:text=NSO%20has%20long%20said%20it,directly%20involved%20in%20surveillance%20operations.

Piqué, A. M. (2018, January 23). *Catalonia at the International Film Festival on Human Rights*. In English. Retrieved June 30, 2022, from https://www.elnacional.cat/en/news/catalonia-international-film-festival-human-rights_232122_102.html

Reuters. (2020, July 14). *Catalan politician suspects was target of state phone tapping, spokesman says*. Reuters. Retrieved May 1, 2022, from https://www.reuters.com/article/spain-politics-spyware/catalan-politician-suspects-was-target-of-state-phone-tapping-spokesman-says-idUKL5N2EL1OC

SallésBarcelona, Q. (2016, August 17). *George Soros Financió a la Agencia de la Paradiplomacia catalana*. La Vanguardia. Retrieved June 30, 2022, from https://www.lavanguardia.com/politica/20160816/403969314802/george-soros-diplocat-financio.html

Scott, J. (2021, July 28). *Jonathandata1/pegasus_spyware: Decompiled pegasus_spyware*. GitHub. Retrieved April 30, 2022, from https://github.com/jonathandata1/pegasus_spyware

Scott-Railton, J., Campo, E., Marczak, B., Razzak, B. A., Anstis, S., Böcü, G., Solimano, S., & Deibert, R. (2022, April 18). *Catalangate: Extensive mercenary spyware operation against Catalans using pegasus and Candiru*. The Citizen Lab. Retrieved April 30, 2022, from https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/

Scott-Railton, J., Marczak, B., Herrero, P. N., Razzak, B. A., Al-Jizawi, N., Solimano, S., & Deibert, R. (2022, January 12). *Project Torogoz: Extensive hacking of Media & Civil Society in El Salvador with pegasus spyware*. The Citizen Lab. Retrieved July 1, 2022, from https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/

Snitow, A. (2014, March 4). *[liberationtech] New Citizen Lab Report*. Mailman mailing list tools. Retrieved June 24, 2022, from https://mailman.stanford.edu/pipermail/liberationtech/2014-March.txt

Toronto Star. (2009, June 12). *Filtering archives*. RONALD DEIBERT. Retrieved June 30, 2022, from https://deibert.citizenlab.ca/tag/filtering/

Turner, A. (2022, May 1). *How many people have smartphones worldwide (May 2022)*. BankMyCell. Retrieved April 30, 2022, from https://www.bankmycell.com/blog/how-many-phones-are-in-the-world#:~:text=How%20Many%20People%20Have%20Smartphones%20In%20The%20World%3F&text=According%20to%20Statista%2C%20the%20current,world's%20population%20owns%20a%20smartphone.

University of Toronto. (2019, July 1). *4. academic integrity*. 4. Academic Integrity | UTSC Calendar. Retrieved June 20, 2022, from https://utsc.calendar.utoronto.ca/4-academic-integrity

Vaas, L. (2022, February 2). *Quadream, 2nd Israeli spyware firm, weaponizes iPhone Bug*. Threatpost English Global threatpostcom. Retrieved June 29, 2022, from https://threatpost.com/quadream-israeli-spyware-weaponized-iphone-bug/178252/

Virus Bulletin. (2018, November 28). *Foreverdays: Tracking and mitigating threats targeting civil society orgs*. YouTube. Retrieved June 29, 2022, from https://www.youtube.com/watch?v=3x9wPyz6cOU

WhatsApp Complaint. (2019, October 10). *Read the whatsapp complaint against NSO Group*. The Washington Post. Retrieved June 29, 2022, from https://www.washingtonpost.com/context/read-the-whatsapp-complaint-against-nso-group/abc0fb24-8090-447f-8493-1e05b2fc1156/?itid=lk_inline_manual_5

WhatsApp. (2019, May 14). *CVE-2019-3568, WhatsApp*. CVE. Retrieved May 1, 2022, from https://www.opencve.io/cve/CVE-2019-3568

WhatsApp. (2019, May). *WhatsApp help center - protecting our users from a video calling Cyber Attack*. WhatsApp.com. Retrieved June 17, 2022, from https://faq.whatsapp.com/general/security-and-privacy/protecting-our-users-from-a-video-calling-cyber-attack/?lang=en

WhatsApp. (2019, October 30). *WhatsApp FAQ - protecting our users from a video calling Cyber Attack*. WhatsApp.com. Retrieved June 22, 2022, from https://web.archive.org/web/20191030231127/https://faq.whatsapp.com/help/video-calling-cyber-attack

Yavanoglu, U. (2018, March). *Citizenlab Deep Packet inspection scam - druraz.com*. Citizenlab Deep Packet inspection scam. Retrieved June 22, 2022, from http://www.druraz.com/blog1en.pdf