Exonerating Morocco EXONERATING MOROCCO DISPROVING THE SPYWARE

Technical Report · February 2023

DOI: 10.13140/RG.2.2.30357.81126

Jonathan Scott

33 PUBLICATIONS **1** CITATION

Exonerating Morocco

Disproving The Spyware

2023

Jonathan Boyd Scott

EXONERATING MOROCCO
DISPROVING THE SPYWARE

Jonathan Boyd Scott

02/18/2023

Abstract

This report delves into the scientific methodologies, data, and events surrounding many cases of alleged digital espionage perpetrated by the Moroccan government. There have been forensic investigations conducted by Amnesty International and The Citizen Lab, but concerns have been raised regarding their reputations in the information security and scientific communities. Their research has often not been independently verified or reproduced by anyone outside of their trusted network, and their disregard for international forensics policies and procedures is alarming. Despite these shortcomings, they have formed partnerships with several global media outlets, including the coalition of journalists from Forbidden Stories who are part of “The Pegasus Project”. It is important to approach these partnerships with increased scrutiny and validation to ensure the accuracy and impartiality of any investigations conducted.

Recent events reveal that the investigations conducted by these organizations significantly lack rigor. Specifically, it has come to light that the mobile forensics results used to support the allegations of Pegasus spyware on Omar Radi, Claude Mangin, and others phones have been tampered, and forged, by way of several false positive results that were not disclosed by the researchers.

From a scientific posture, it is paramount to highlight the importance of transparent and rigorous investigation methods in cases involving spyware technology. False positives in forensic analysis lead to erroneous conclusions, which can have significant implications for the individuals involved and the broader political landscape. It is also important to note that accusations of government surveillance carry significant weight and can have a profound impact on international relations, which further underscores the need for thorough and impartial investigations.

The lack of transparency regarding the false positive results raises concerns about the intentionality of the investigation and calls into question the credibility of the conclusions drawn by Amnesty International and The Citizen Lab. This highlights the need for increased scrutiny and independent validation of investigations involving sensitive political issues.

Background

Accusations of the Moroccan government engaging in unlawful surveillance against members of civil society first surfaced over a decade ago[1] and it began with a group of public policy researchers from the University of Toronto known as The Citizen Lab. They made their initial accusations in 2012 and subsequently released a three-part series of reports labeling Morocco as a repressive regime[2]. Other human rights advocacy groups and NGOs such as Human Rights Watch, Amnesty International, Privacy International, Electronic Frontier Foundation, and Forbidden Stories have joined in with similar or exact allegations of unlawful surveillance against civil society members perpetuated by The Kingdom of Morocco.

Despite significant false positive results in forensics reports, the allegations against Morocco have continued to mount over time. The situation has reached a critical point, with the European Parliament ignoring scientific evidence that exonerates Morocco of any wrongdoing and instead passing a JOINT MOTION FOR A RESOLUTION[3] on the matter, strongly condemning Morocco's unlawful surveillance.

Citizen Case Zero

In 2012, The Citizen Lab wrote a report titled, **Backdoors are Forever Hacking Team and the Targeting of Dissent?[4]**, and definitively stated the Moroccan government used Hacking Team's RCS surveillance technology to target the journalism project Mamfakinch. The alleged attack happened when someone sent a phishing message to the group that contained a link to download a Microsoft Word document claiming to have breaking news. The message was submitted via a WordPress contact form on the Mamfakinch website and the IP address of the message sent was associated to a block owned by Maroc Telecom. Former Citizen Lab senior researcher Morgan Marquis-Boire used that IP address range to attribute the phishing message to the Moroccan government and but provides no evidence to support this attribution.

The report cites an article written by Slate to bolster their claims of the Moroccan government espionage. Past the pejorative language calling Morocco draconian, the

[1] The date of this report is Friday, February 17th, 2023
[2] https://citizenlab.ca/2014/06/backdoor-hacking-teams-tradecraft-android-implant/#Introduction [§2]
[3] https://www.europarl.europa.eu/doceo/document/RC-9-2023-0057_EN.html
[4] https://citizenlab.ca/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent/

author, journalist Ryan Gallagher states, "*While it's not possible to say for sure whether Moroccan authorities are using RCS, it's certainly being deployed by countries in that region of the world*[5]."

According to The Citizen Lab's report, they claimed to have acquired a leaked PDF document detailing Hacking Team's ability, but this assertion was completely fabricated. Hacking Team had already disclosed the capabilities of their Remote Control System (RCS) software. Video demos of their desktop and mobile software was on their website since 2009, and a graphic on their homepage containing a download link for the PDF brochure of RCS that Citizen Lab calls "leaked" can be seen as far back September 26th, 2011[6]. The Hacking Team was diligent in updating their PDFs and the so called "leaked" document was available until mid 2013 for anyone to view and download. This case would go on to be referenced for over a decade, and laid the foundation for future accusations against Morocco.

Uncovering Citizen Case Zero

For Citizen Lab, the irrefutable evidence confirming the Moroccan government had attacked Mamfakinch was a single IP address. Criminal courts around the world have unequivocally dismissed cases that were brought forth with nothing more than an IP address as evidence of a crime. This is especially true in cases involving computer hacking or digital espionage, where the use of IP addresses as the sole evidence has been found to be unreliable and insufficient to establish guilt beyond a reasonable doubt. Arstechnica, a long-time supporter of The Citizen Lab and Amnesty International, released an article in 2011 titled, **Court confirms: IP address aren't people**[7]. The article summarized the UK court's judgement on a case that stated simply citing an Internet Protocol (IP) address is not sufficient evidence to convict someone of a crime. Arstechnica journalist Mathew Lasar, writes "*Just because some lawyer cites an Internet Protocol (IP) address where illegal file sharing may have taken place, that doesn't mean that the subscriber living there necessarily did the dirty deed. Or is responsible for others who may have done it.*"

Tracing an IP address to identify technical information is a common practice that is widely accepted and can inform the development of a malicious payload based on

[5] https://slate.com/technology/2012/08/moroccan-website-mamfakinch-targeted-by-government-grade-spyware-from-hacking-team.html
[6] https://web.archive.org/web/20110926182858/http://hackingteam.it/
[7] https://arstechnica.com/tech-policy/2011/02/court-confirms-ip-addresses-arent-people-and-p2p-lawyers-know-it/

the reconnaissance conducted. Relying solely on an IP address to identify a person or entity is not a dependable method, as academic sources have demonstrated the limitations and inaccuracies of IP geolocation, as well as the high risk of false positives. For instance, in 2014, D. Brian Nichols and Casey Canfield published a paper in the Journal of Digital Forensics, Security and Law titled "False Positives in IP Geolocation: Estimating Error Rates," while Amirali Sanatinia, Tristan Gurtler, and Nicholas Hopper published a paper in IEEE Security & Privacy in 2017 titled "On the Reliability of IP Geolocation."

Hacking Team Files

In 2015, a large collection of internal documents and emails from Hacking Team, an Italian company that specialized in the sale of surveillance software to government and law enforcement agencies, was leaked to the public. The source of the leak remains unknown, but the release of the files provided insight into Hacking Team's business practices The release of the documents caused significant controversy and led to calls for greater regulation of the surveillance industry. Many critics argued that the activities of Hacking Team and other similar companies represented a serious threat to privacy and human rights, and that these companies needed to be held accountable for their actions. In response to the leak, Hacking Team said that the they had always operated within the law, but ultimately the leak led to a significant loss of business, and the company shut down in 2016.

The leaked files gave us a rare view of the internal interactions surrounding the allegations that Morocco hacked Mamfakinch. The events leading up to the Citizen Lab report and the internal communications after the report start to reveal the truth.

Table 1 Timeline of events first accusing Morocco of digital espionage

Date	Event
October, 2011	Ryan Gallagher contacts Hacking Team and asks for a statement about the kind of work they do.
October, 2011	Hacking Team grants Ryan an interview.
August, 2012	Ryan Gallagher reports the hacking of Mamfakinch.
August, 2012	Hacking Team becomes aware of Gallagher's report, and states the following[8]. *In October of last year I had granted an interview by mail (mail is perhaps the most safe to release interviews: everything is already written, it cannot be manipulated) to this Ryan. I basically told him that we make a tool to fight various crime types and that we only sell it to governments. Nothing more than what's in the brochure.* *Now this Ryan has decided to make a living doing the activist journalist and in fact on Twitter he devotes a lot of space to Julian Assange. The article doesn't worry us. I ask everyone to NEVER give any interviews to anyone and also to avoid talking to reporters even just tell them "No comment".*
October, 2012	The Citizen Lab releases the Mamfakinch hacking report and also embedded in that report are detailed of an alleged hack on Ahmed Mansoor.
October, 2012	Ryan Gallagher writes another article[9] about the alleged Moroccan government hacking, and also the alleged the Ahmed Mansoor hacking by the UAE. This article echoes The Citizen Lab by saying the malware found in the Mamfakinch hack is within the same class as the Ahmed Mansoor hack.
October, 2012	Hacking Team speak internally about the 2nd article written by Ryan Gallagher say they say[10]: *I think he's referring to the fact that the sample was an exploit that downloaded the second stage from our old demo server...* *the doubt that comes to me from this is the "it was also linked" which I cannot understand if they mean that citizen also found this or if this too has come to him…*

According to the email communications that have been made public, Citizen Lab researcher Morgan Marquis-Boire stumbled upon an outdated demo server that was once used by Hacking Team to demonstrate its software capabilities. Four sectors of the Canadian RCMP also requested demonstrations from Hacking Team[11]. Additionally, the software was configured during a demo and trial period in a way that would prevent it from being used in the field[12], limiting it solely to internal use, which means it would not be possible for anyone from the Moroccan government to have even attempted to attack Mamfakinch. The Citizen Lab report lacks any endpoint communications that were captured and analyzed between the alleged Mamfakinch infected machine and the C2 (Command and Control) server, yet this is never questioned by information security researchers.

[8] https://wikileaks.org/hackingteam/emails/emailid/449677

[9] https://slate.com/technology/2012/10/ahmed-mansoor-uae-activst-allegedly-tricked-by-phoney-wikileaks-into-downloading-hacking-team-spyware.html

[10] https://wikileaks.org/hackingteam/emails/emailid/449796

[11] https://wikileaks.org/hackingteam/emails/emailid/600803

[12] https://wikileaks.org/hackingteam/emails/emailid/567378

Table 2 List of publications by The Citizen Lab accusing Morocco of espionage

Publication Title	Year	Surveillance Firm Used	Software Name
Backdoors are Forever Hacking Team and the Targeting of Dissent?	October 10, 2012	Hacking Team	RCS
Open letter to Hacking Team	August 8, 2014	Hacking Team	RCS
Mapping Hacking Team's "Untraceable" Spyware	February 17, 2014	Hacking Team	RCS
Hacking Team's Government Surveillance Malware	June 24, 2014	Hacking Team	RCS
The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender			
Hacking Team's US Nexus	February 28, 2014	Hacking Team	RCS
Hacking Team's US Nexus: Appendix A	February 28, 2014	Hacking Team	RCS
US-based Servers Part of Hacking Team's Surveillance Infrastructure	February 28, 2014	Hacking Team	RCS
Mapping Hacking Team's Covert Surveillance Networks	February 17, 2014	Hacking Team	RCS
Canadian Cyberbullying Legislation Threatens to Further Legitimize Malware Sales	June 5th, 2014	Hacking Team & Gamma Group	RCS & FinFisher
Schrodinger's Cat Video and the Death of Clear-Text	August 15, 2014	Hacking Team	RCS
Pay No Attention to the Server Behind the Proxy Mapping FinFisher's Continuing Proliferation	October 15, 2015	Gamma	FinFisher

On October 15th, 2015, Citizen Lab accused Morocco of deploying Gamma Group's FinFisher surveillance tools[13], despite being aware of Wikileaks' disclosures and acknowledging that there was no evidence linking Morocco to Gamma Group and their FinFisher technology. In their report, Citizen Lab claimed to have found evidence that the Moroccan government had deployed FinFisher, but stated that they were unable to provide all the data to corroborate their claims due to possible ongoing criminal investigations that involved the usage of FinFisher. It should be noted that FinFisher was originally designed to be used for lawful interception purposes, which indicates that Citizen Lab was not primarily seeking to identify any unlawful activities when analyzing the use of these surveillance tools. Rather, their focus was on locating the presence of such tools and then making attributions to a government.

Citizen Lab claims to have discovered a FinFisher server in a range of an IP addresses registered to a Moroccan user named "Conseil Superieur De La Defense Nationale" as evidence of Moroccan government deployment of Gamma Group's tools is again primarily based on an IP address. While Citizen Lab believes the

[13] https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

agency to be the same as CSDN[14], they acknowledged limited open-source information about the agency and adding more to their assumptive claims. Furthermore, Citizen Lab cited their 2012 article about Morocco's alleged hacking of Mamfakinch to support this new allegation, which is merely a circular self-citation that is not supported by any factual evidence. Although Citizen Lab asserts that their reporting is crucial in holding governments accountable, they have failed to provide any evidence that is reproducible or verifiable beyond assumptions.

Following researcher Morgan Marquis-Boire's removal from the Citizen Lab advisory board on account of alleged sexual assault during a Citizen Lab event[15], several individuals whom he had enlisted to work at the Citizen Lab persisted in actively seeking out targets of spyware. Notably, Claudio Guarnieri opted to leave Citizen Lab and accept the position of head of security research at Amnesty International's security lab[16].

The Budapest Convention

In 2021, the Pegasus Project[17], was launched by a French non-profit organization called Forbidden Stories. This project is a collaboration between journalists, media outlets, and Amnesty International's Security Lab, aimed at identifying individuals from civil society who have been targeted by Pegasus, a surveillance tool developed by the Israeli company NSO Group. To detect Pegasus infections, Claudio Guarnieri and his team at Amnesty Tech created a forensics methodology[18] and a software program called MVT-Tool. However, the details of the software's logic and reasoning have not been publicly disclosed and yet widely accepted by the information security community.

Furthermore, I would like to emphasize that fundamental and essential components have been missing from every forensics investigation undertaken by The Citizen Lab and Amnesty International. This reality is highly concerning, as the integrity of every alleged case of espionage has been rendering completely unreliable and invalid. Immediate and thorough attention must be given to these core missing components as their absence undermines the criminal justice system of Morocco and every country accused of digital espionage.

[14] Government body responsible for advising the Moroccan King on defense and national security matters

[15] https://arstechnica.com/tech-policy/2017/11/report-infosec-researcher-accused-of-numerous-instances-of-sexual-assault/

[16] https://www.speakers.co.uk/speakers/claudio-guarnieri/

[17] https://forbiddenstories.org/about-the-pegasus-project/

[18] https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

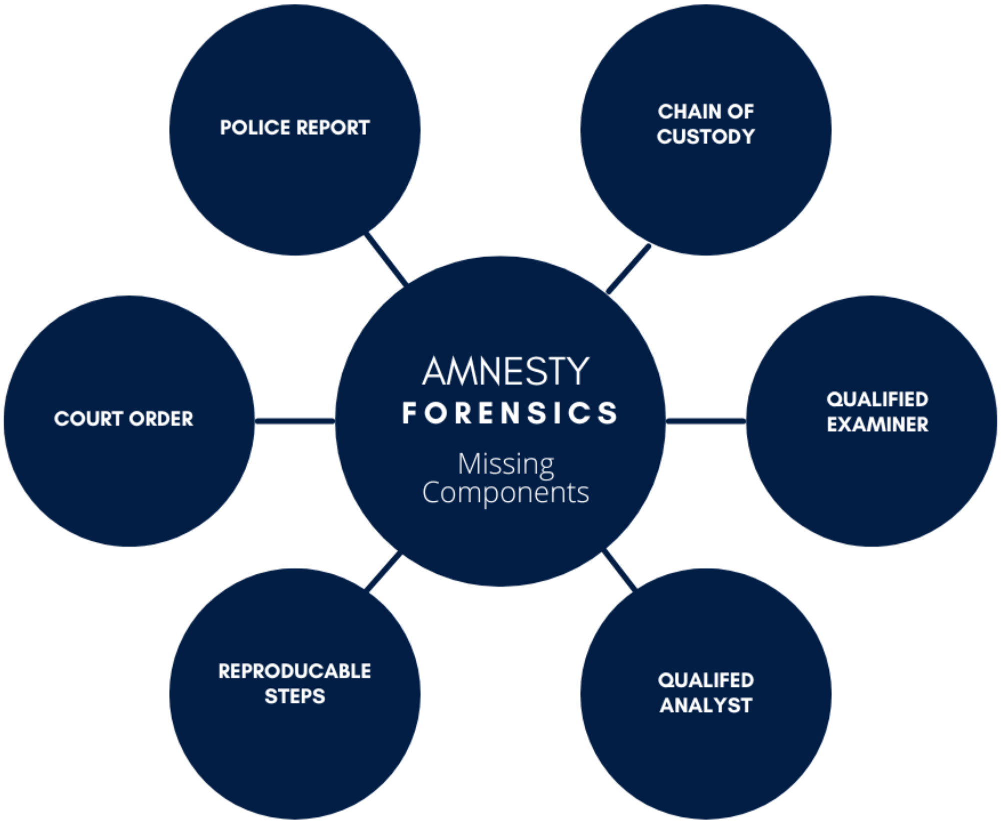


Figure 1 Amnesty Forensics Missing Components

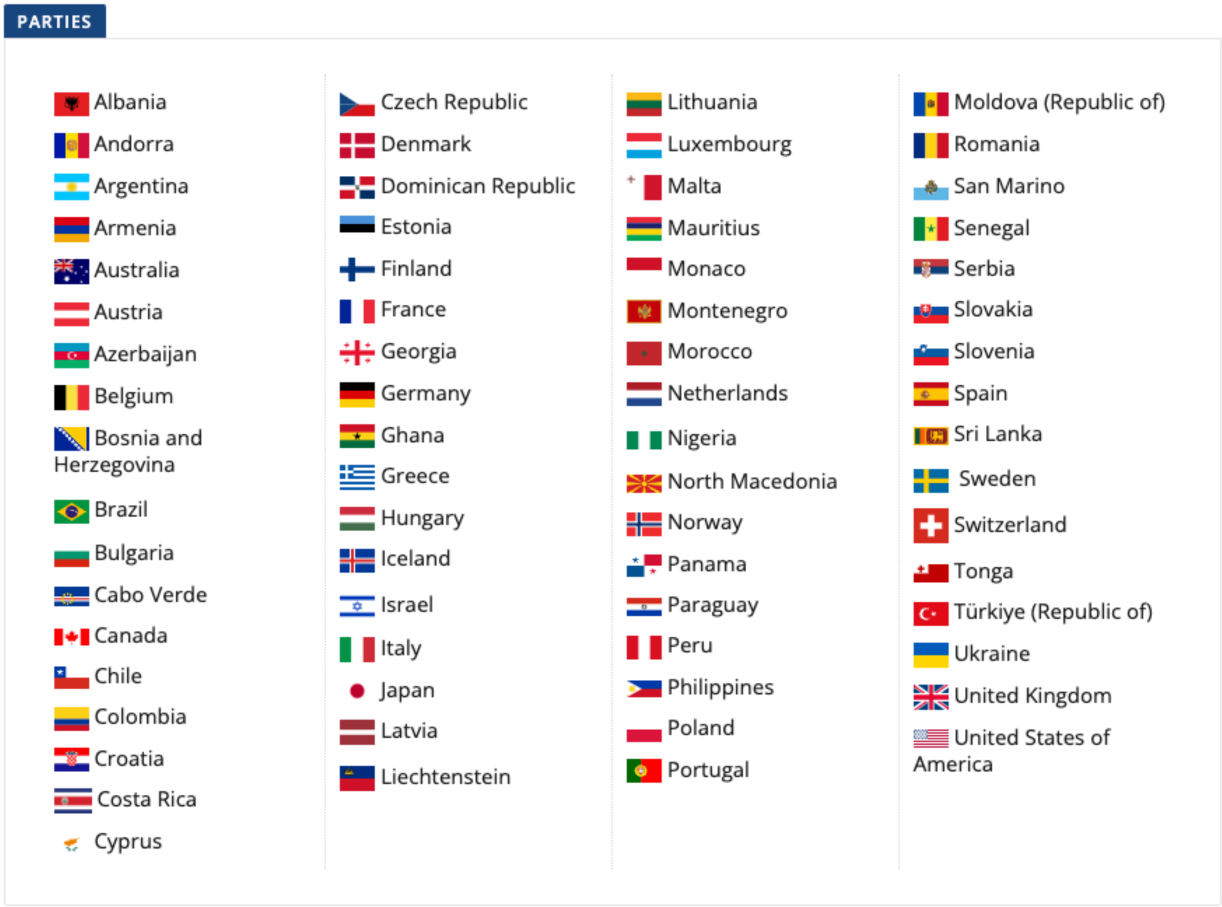
Amnesty International, The Citizen Lab, and Forbidden Stories are exerting undue pressure on Morocco to contravene its commitment to the Budapest Convention on Cybercrime, which it acceded to in 2018[19]. Morocco has repeatedly demanded that Amnesty provide substantiated evidence of its allegations related to Pegasus, yet these demands have gone unmet[20]. The Budapest Convention (ETS No. 185[21]) lays down globally accepted procedures that are designed to facilitate the collection of digital evidence in the course of criminal investigations[22].

Furthermore, the Budapest Convention agrees that "*The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer*

[19] https://www.coe.int/en/web/cybercrime/t-cy-news/-/asset_publisher/GxUcENEFhivB/content/morocco-joins-the-budapest-convention-on-cybercrime-an-becomes-it-s-60th-member-?inheritRedirect=false
[20] https://www.moroccoworldnews.com/2022/03/347777/morocco-demands-amnesty-international-for-proof-over-pegasus-allegations
[21] https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185
[22] https://rm.coe.int/1680081561 [pg 12. Chapter III Section 1 Article 23]

systems and data, or for the collection of evidence in electronic form of a criminal offence[23]." The EU Parliament disregarded its obligation to honor the legally binding treaty ratified by its member states and proceeded to penalize Morocco[24] based on unsubstantiated claims of digital espionage concerning Omar Radi, brought forth by Amnesty International, The Citizen Lab, and Forbidden Stories. This glaring oversight cannot be overlooked, especially considering the fact that 65 nations have pledged to uphold this treaty, which is being treated with disdain and disrespect by non-governmental organizations and special interest groups.

Table 3 All countries that have signed Treaty No. 185 The Budapest Convention on Cybercrime



PARTIES

Albania
Andorra
Argentina
Armenia
Australia
Austria
Azerbaijan
Belgium
Bosnia and Herzegovina
Brazil
Bulgaria
Cabo Verde
Canada
Chile
Colombia
Croatia
Costa Rica
Cyprus

Czech Republic
Denmark
Dominican Republic
Estonia
Finland
France
Georgia
Germany
Ghana
Greece
Hungary
Iceland
Israel
Italy
Japan
Latvia
Liechtenstein

Lithuania
Luxembourg
Malta
Mauritius
Monaco
Montenegro
Morocco
Netherlands
Nigeria
North Macedonia
Norway
Panama
Paraguay
Peru
Philippines
Poland
Portugal

Moldova (Republic of)
Romania
San Marino
Senegal
Serbia
Slovakia
Slovenia
Spain
Sri Lanka
Sweden
Switzerland
Tonga
Türkiye (Republic of)
Ukraine
United Kingdom
United States of America

[23] https://rm.coe.int/1680081561 [pg 13. Chapter III Section 1 Article 25]

[24] https://www.europarl.europa.eu/doceo/document/RC-9-2023-0057_EN.html

The Reports

Referring to Amnesty International and The Citizen Lab's unverified documents as forensic evidence or forensic reports not only weakens the integrity of forensic science but also damages the credibility of computer science as a field of study. In the case of Omar Radi, a convicted rapist presently serving a prison sentence for his offense, Amnesty and The Citizen Lab have resorted to a defense strategy known as SaaD (Spyware as a Defense) to have him released from prison. I first introduced SaaD in response to the case of Carine Kanimba, an American who alleged being spied on by the Rwandan government. Kanimba also included her father, Paul Rusesabagina - a convicted terrorist and the character depicted in the movie Hotel Rwanda - as a victim of Pegasus. Supported by Amnesty and The Citizen Lab SaaD was deployed to secure Paul Rusesabagina's release from prison in Kigali, but Rwanda is aware of this strategy and President Paul Kagame suggested, "*Only an invasion of his country could force him to release Paul Rusesabagina*[25]."

The terminology used by Amnesty, such as forensics analysis, forensics traces, and forensics reports, cannot be accurately labeled as such since they lack the necessary components previously mentioned. Additionally, often there is no mobile device used for conducting forensic analysis. Instead, both Amnesty and the Citizen Lab solely rely on iCloud backups of an iPhone to conduct their analysis. When asked by an El PAIS reporter why they don't possess the physical devices to perform the forensics, the Director of The Citizen Lab responded, "*We don't need it. Receiving the mobile might not be that useful for us*[26]." Citizen Lab acknowledges that they do not require the device to carry out a mobile forensics examination and rely solely on an iCloud backup. Furthermore, in 2021, Citizen Lab '*independently*' validated Amnesty's forensics methodology. However, the only information provided to Citizen Lab by Amnesty to authenticate their forensics was an iCloud backup. "*Forbidden Stories and Amnesty International requested that the Citizen Lab undertake an independent peer review of a sample of their forensic evidence and their general forensic methodology. We were provided with iTunes backups of several devices and a separate methodology brief. No additional context or information about the*

[25] https://www.nytimes.com/2022/12/14/us/politics/rwanda-president-kagame-rusesabagina.html

[26] https://elpais.com/espana/2022-05-15/ronald-deibert-fundador-de-citizen-lab-los-gobiernos-usan-pegasus-porque-tienen-apetito-de-espiar.html

devices or the investigation was provided to us[27]." Citizen Lab continues by calling Amnesty's methodologies "*sound*."

To complete the circular independent validation loop, The Citizen Lab says, "*We shared a selection of Pegasus cases with Amnesty International's Tech Lab, which independently validated our forensic methodology*[28]." In addition to their questionable validation methods, the conflict of interest resulting from the funding these organizations receive from the same institutions they are tasked with investigating raises serious concerns about the integrity of their findings. This includes financial support from institutions such as the Ford Foundation and the MacArthur Foundation, which have both funded The Citizen Lab and Amnesty International in their efforts to uncover Pegasus victims. This conflict-of-interest calls into question the impartiality of their investigations and undermines the credibility of their research.

November 24, 2021 The Ford Foundation tweeted, "*Important step to defend civic space against surveillance, and welcomed recognition of the work of grantees @citizenlab & @AmnestyTech whose research uncovered the organized and deliberate use of spyware targeting global activists and journalists*[29]." We can also see financials from the MacArthur Foundation funding The Citizen Lab, $500,000 USD, and Amnesty International $120,000 USD[30].

Further adding to the conflict of interest is The University of Toronto's funding[31] and collaboration[32] with US blacklisted Chinese AI spyware firm iFLYTEK, and The Citizen Lab's funding[33], multiple[34] collaborations[35], and endorsement of American spyware firm Palantir. Palantir was named as the #4 evil spyware firm[36] by Slate.com, the same media outlet that accused Morocco of espionage.

Although several critical concerns such as conflicts of interest, the reliance on

[27] https://citizenlab.ca/2021/07/amnesty-peer-review/

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

[29] https://twitter.com/FordFoundation/status/1463568098489946120

[30] https://www.macfound.org/media/files/macarthur-foundation-2020-form-990-pf-(final).pdf

[31] https://web.archive.org/web/20211028035847/https://www.urap.ca/all-canadian-universities-must-critically-reassess-their-collaborations-with-china/

[32] https://aclanthology.org/W18-3707.pdf

[33] The Information Warfare Monitor is a public-private venture between two Canadian institutions: the Citizen Lab at the Munk School of Global Affairs, University of Toronto and the SecDev Group, an operational think tank based in a Ottawa (Canada). The Information Warfare Monitor is an advanced research activity tracking the emergence of cyberspace as a strategic domain. We are an independent research effort. Our mission is to build and broaden the evidence base available to scholars, policy makers, and others. We aim to educate and inform. The research of the Citizen Lab and the Information Warfare Monitor is supported by the Canada Centre for Global Security Studies (University of Toronto), a generous grant from the John D. and Catherine T. MacArthur Foundation, in-kind and staff contributions from the SecDev Group, and a generous donation of software from **Palantir Technologies Inc**. https://citizenlab.ca/2010/11/koobface-inside-a-crimeware-network/

[34] https://twitter.com/citizenlab/status/3888203174?s=20

[35] https://twitter.com/citizenlab/status/3888711632?s=20

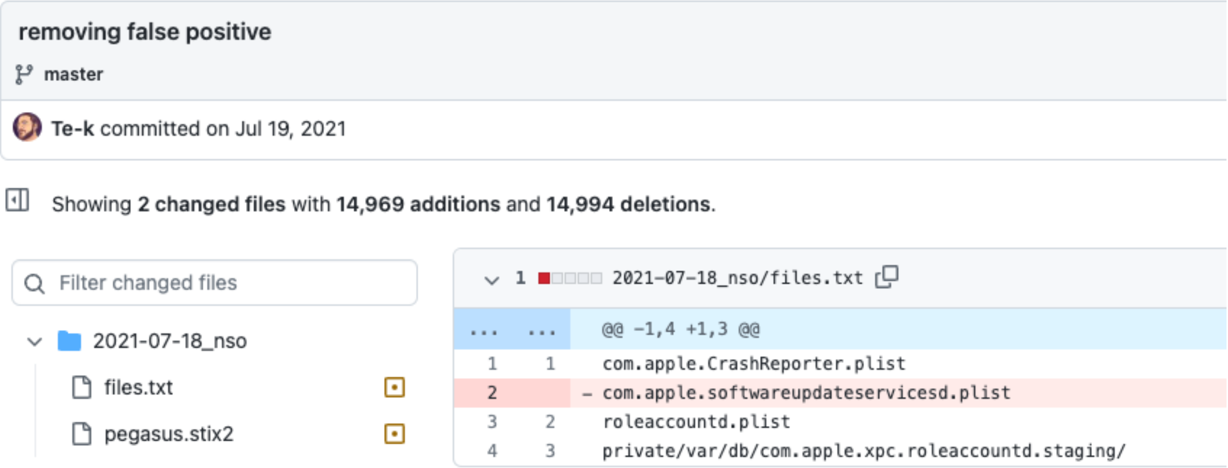
[36] https://slate.com/technology/2020/01/evil-list-tech-companies-dangerous-amazon-facebook-google-palantir.html

an IP address as a conclusive indicator of compromise, and insufficient execution of forensic analyses have been brought to attention, the most detrimental factor to Morocco is Amnesty's acknowledgement of presenting false data regarding Pegasus.

Stopping a Coup d'état

In the interest of maintaining the highest standards of accuracy and reliability, I submitted a comprehensive and detailed GitHub issue[37] challenging the forensics methodology employed by the MVT-Tool. My findings have revealed significant flaws that have the potential to facilitate forgery and false identification. Furthermore, I identified several known false positives that have gravely compromised the credibility and reliability of the reports and methodologies jointly confirmed by Amnesty and Citizen Lab regarding alleged victims of Pegasus.

One particularly concerning aspect of the Forensics Methodology Report is a single line that reads: "***Amnesty International verified that no legitimate binaries of the same names were distributed in recent versions of iOS***[38]." July 19th, 2021 Amnesty International recognized that an indicator of compromise that they alleged to be Pegasus was not Pegasus, but just a normal iOS process inside of the iPhone. Amnesty quietly removed the process **[com.apple.softwareupdateservicesd.plist]** from their Pegasus indicator list[39].



removing false positive

master

Te-k committed on Jul 19, 2021

Showing **2 changed files** with **14,969 additions** and **14,994 deletions**.

1 2021-07-18_nso/files.txt

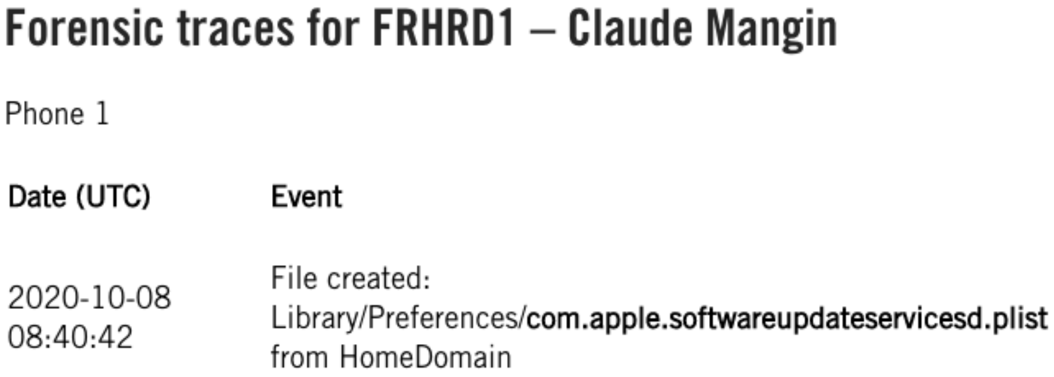
```
@@ -1,4 +1,3 @@
  com.apple.CrashReporter.plist
- com.apple.softwareupdateservicesd.plist
  roleaccountd.plist
  private/var/db/com.apple.xpc.roleaccountd.staging/
```

Figure 2 Amnesty acknowledges a false positive and quietly removes it from their list of Pegasus indicators

[37] https://github.com/mvt-project/mvt/issues/321
[38] https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/
[39] https://github.com/AmnestyTech/investigations/commit/1c694217c3efb4e40f34822b6ef99a7b5bd8a064

This issue is particularly significant, as it impacted the investigations into the alleged cases of Pegasus infection for both Omar Radi and Claude Mangin. The now-discredited indicator of compromise, [com.apple.softwareupdateservicesd.plist], was central to the investigation of both cases. In a formal mobile forensics trace, it is critical that the events are reproducible and serve as the basis for the methodology employed.

The methodology presented by Amnesty and The Citizen Lab has been deemed impractical to follow as the initial event in Claude Mangin's trace has been invalidated, rendering the entire trace and its outcome invalid. A similar issue has occurred with Omar Radi's events due to the acknowledged false positive result. The problem with their forensic traces is rooted in the iCloud backup methodology, which does not contain memory that can be scanned or rebuilt. A physical data extraction of the mobile device, live network monitoring, chipset extraction and analysis, among other controlled lab environment procedures, would produce a more comprehensive, accurate, and precise result that can be replicated by any forensic and computer scientist globally. The 2017 IEEE International Conference on Big Data Proceedings features a qualified and peer-reviewed forensic analysis that explores the Wi-Fi communication traces present on mobile devices. This analysis provides valuable insights into what these traces are expected to look like when conducting a forensic analysis on a mobile device[40].



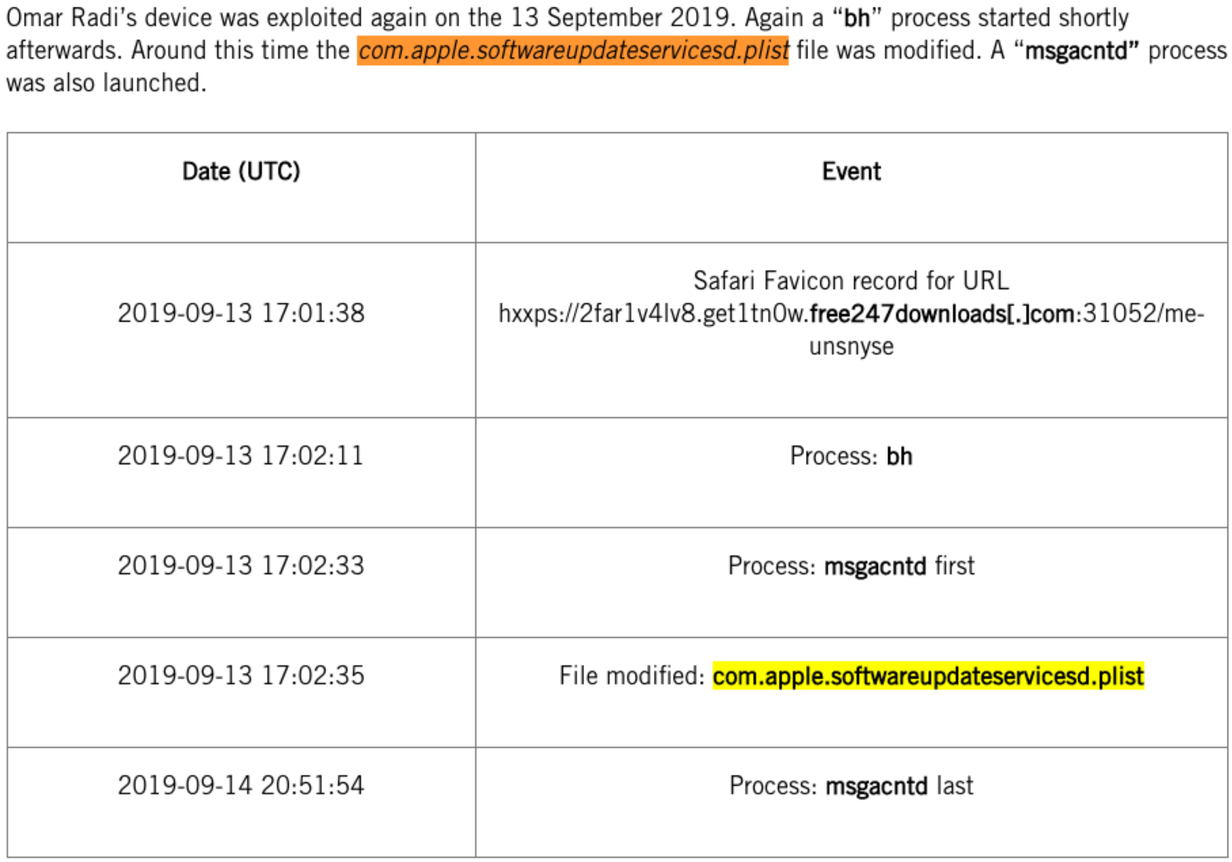
Forensic traces for FRHRD1 – Claude Mangin

Phone 1

Date (UTC)	Event
2020-10-08 08:40:42	File created: Library/Preferences/**com.apple.softwareupdateservicesd.plist** from HomeDomain

Figure 3 Claude Mangin’s 1st step in her phone trace is a discredited indicator of compromise

[40] https://researchonline.gcu.ac.uk/ws/portalfiles/portal/25640096/PID5133269.pdf



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

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

Figure 4 Omar Radi's forensics traces showing the false positive result

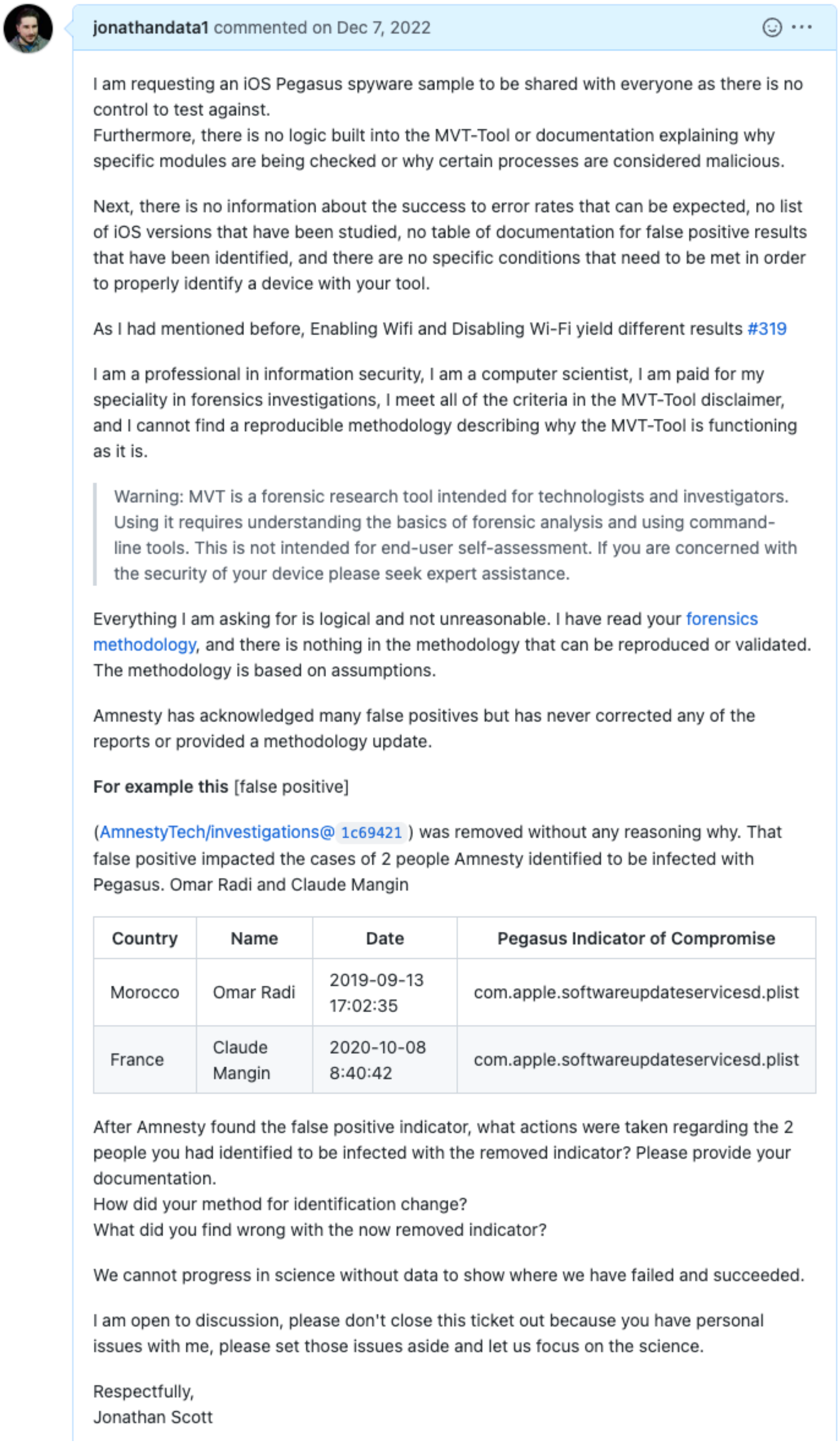
Raising Issues

have raised 4 Github issues with Amnesty International, 3 issues of which I demonstrate how easily false positive results can be derived, and forged. All 3 issues were closed as "not planned." Not planned means that the project maintainers have considered the issue and decided not to address it. This could be because the issue is not considered a priority, it does not fit within the project's scope or vision, or it is not technically feasible or desirable to implement[41].

[41] https://github.blog/changelog/2022-03-10-the-new-github-issues-march-10th-update/#:~:text=When%20closing%20an%20issue%2C%20you,reason%3A%22not%20planned%22%20.

GitHub Issue 321[42]

iOS Pegasus spyware sample request - MVT methods lack a control



jonathandata1 commented on Dec 7, 2022

I am requesting an iOS Pegasus spyware sample to be shared with everyone as there is no control to test against.
Furthermore, there is no logic built into the MVT-Tool or documentation explaining why specific modules are being checked or why certain processes are considered malicious.

Next, there is no information about the success to error rates that can be expected, no list of iOS versions that have been studied, no table of documentation for false positive results that have been identified, and there are no specific conditions that need to be met in order to properly identify a device with your tool.

As I had mentioned before, Enabling Wifi and Disabling Wi-Fi yield different results #319

I am a professional in information security, I am a computer scientist, I am paid for my speciality in forensics investigations, I meet all of the criteria in the MVT-Tool disclaimer, and I cannot find a reproducible methodology describing why the MVT-Tool is functioning as it is.

> Warning: MVT is a forensic research tool intended for technologists and investigators. Using it requires understanding the basics of forensic analysis and using command-line tools. This is not intended for end-user self-assessment. If you are concerned with the security of your device please seek expert assistance.

Everything I am asking for is logical and not unreasonable. I have read your forensics methodology, and there is nothing in the methodology that can be reproduced or validated. The methodology is based on assumptions.

Amnesty has acknowledged many false positives but has never corrected any of the reports or provided a methodology update.

For example this [false positive]

(AmnestyTech/investigations@ `1c69421`) was removed without any reasoning why. That false positive impacted the cases of 2 people Amnesty identified to be infected with Pegasus. Omar Radi and Claude Mangin

Country	Name	Date	Pegasus Indicator of Compromise
Morocco	Omar Radi	2019-09-13 17:02:35	com.apple.softwareupdateservicesd.plist
France	Claude Mangin	2020-10-08 8:40:42	com.apple.softwareupdateservicesd.plist

After Amnesty found the false positive indicator, what actions were taken regarding the 2 people you had identified to be infected with the removed indicator? Please provide your documentation.
How did your method for identification change?
What did you find wrong with the now removed indicator?

We cannot progress in science without data to show where we have failed and succeeded.

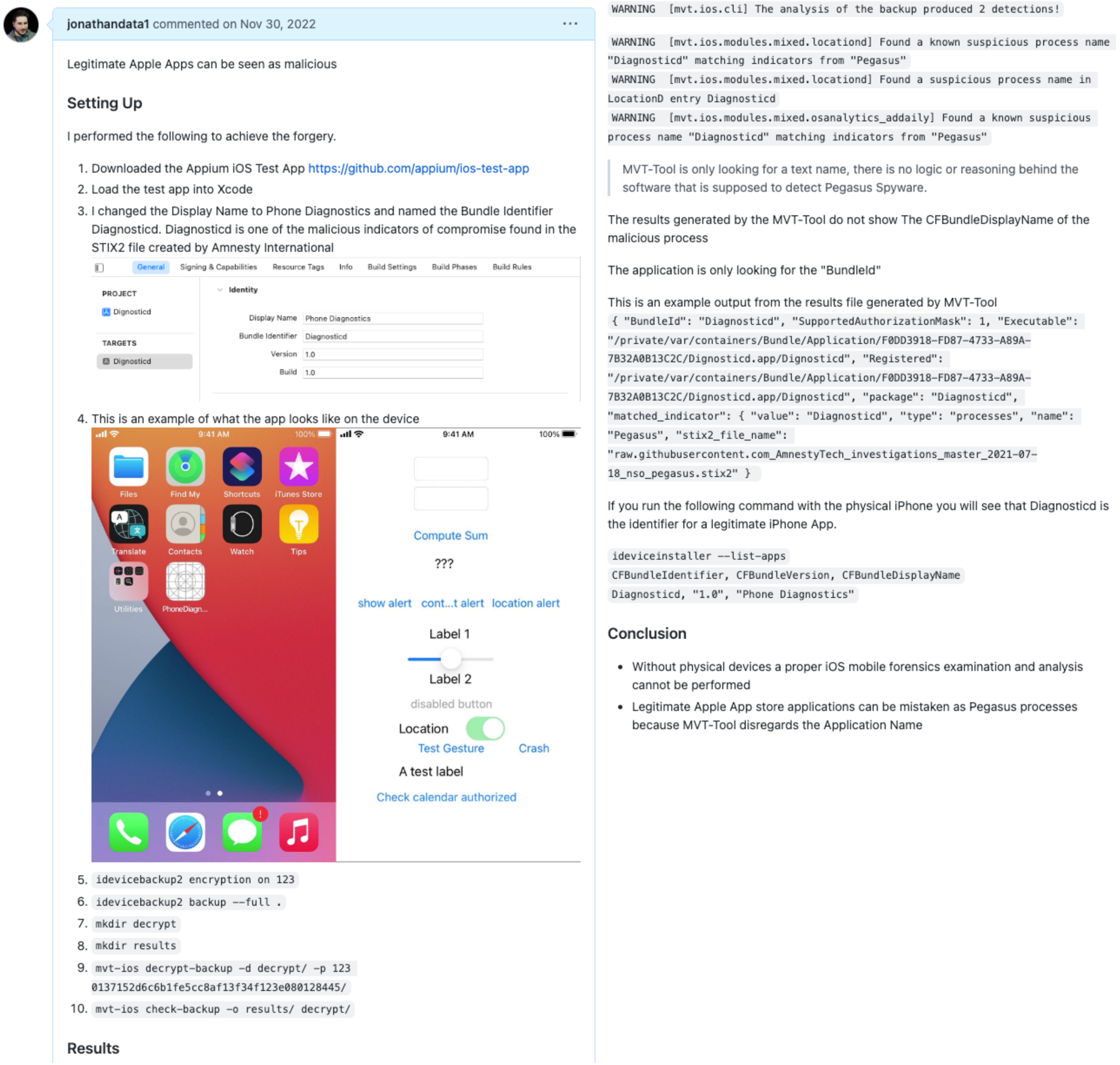
I am open to discussion, please don't close this ticket out because you have personal issues with me, please set those issues aside and let us focus on the science.

Respectfully,
Jonathan Scott

[42] https://github.com/mvt-project/mvt/issues/321

Github Issue 320[43]

Legitimate Apple Apps can be seen as malicious with MVT



jonathandata1 commented on Nov 30, 2022

Legitimate Apple Apps can be seen as malicious

Setting Up

I performed the following to achieve the forgery.

1. Downloaded the Appium iOS Test App https://github.com/appium/ios-test-app
2. Load the test app into Xcode
3. I changed the Display Name to Phone Diagnostics and named the Bundle Identifier Diagnosticd. Diagnosticd is one of the malicious indicators of compromise found in the STIX2 file created by Amnesty International

Display Name: Phone Diagnostics
Bundle Identifier: Diagnosticd
Version: 1.0
Build: 1.0

4. This is an example of what the app looks like on the device

5. `idevicebackup2 encryption on 123`
6. `idevicebackup2 backup --full .`
7. `mkdir decrypt`
8. `mkdir results`
9. `mvt-ios decrypt-backup -d decrypt/ -p 123 0137152d6c6b1fe5cc8af13f34f123e080128445/`
10. `mvt-ios check-backup -o results/ decrypt/`

Results

```
WARNING  [mvt.ios.cli] The analysis of the backup produced 2 detections!

WARNING  [mvt.ios.modules.mixed.locationd] Found a known suspicious process name
"Diagnosticd" matching indicators from "Pegasus"
WARNING  [mvt.ios.modules.mixed.locationd] Found a suspicious process name in
LocationD entry Diagnosticd
WARNING  [mvt.ios.modules.mixed.osanalytics_addaily] Found a known suspicious
process name "Diagnosticd" matching indicators from "Pegasus"
```

> MVT-Tool is only looking for a text name, there is no logic or reasoning behind the software that is supposed to detect Pegasus Spyware.

The results generated by the MVT-Tool do not show The CFBundleDisplayName of the malicious process

The application is only looking for the "BundleId"

This is an example output from the results file generated by MVT-Tool

```
{ "BundleId": "Diagnosticd", "SupportedAuthorizationMask": 1, "Executable":
"/private/var/containers/Bundle/Application/F0DD3918-FD87-4733-A89A-
7B32A0B13C2C/Dignosticd.app/Dignosticd", "Registered":
"/private/var/containers/Bundle/Application/F0DD3918-FD87-4733-A89A-
7B32A0B13C2C/Dignosticd.app/Dignosticd", "package": "Diagnosticd",
"matched_indicator": { "value": "Diagnosticd", "type": "processes", "name":
"Pegasus", "stix2_file_name":
"raw.githubusercontent.com_AmnestyTech_investigations_master_2021-07-
18_nso_pegasus.stix2" }
```

If you run the following command with the physical iPhone you will see that Diagnosticd is the identifier for a legitimate iPhone App.

```
ideviceinstaller --list-apps
CFBundleIdentifier, CFBundleVersion, CFBundleDisplayName
Diagnosticd, "1.0", "Phone Diagnostics"
```

Conclusion

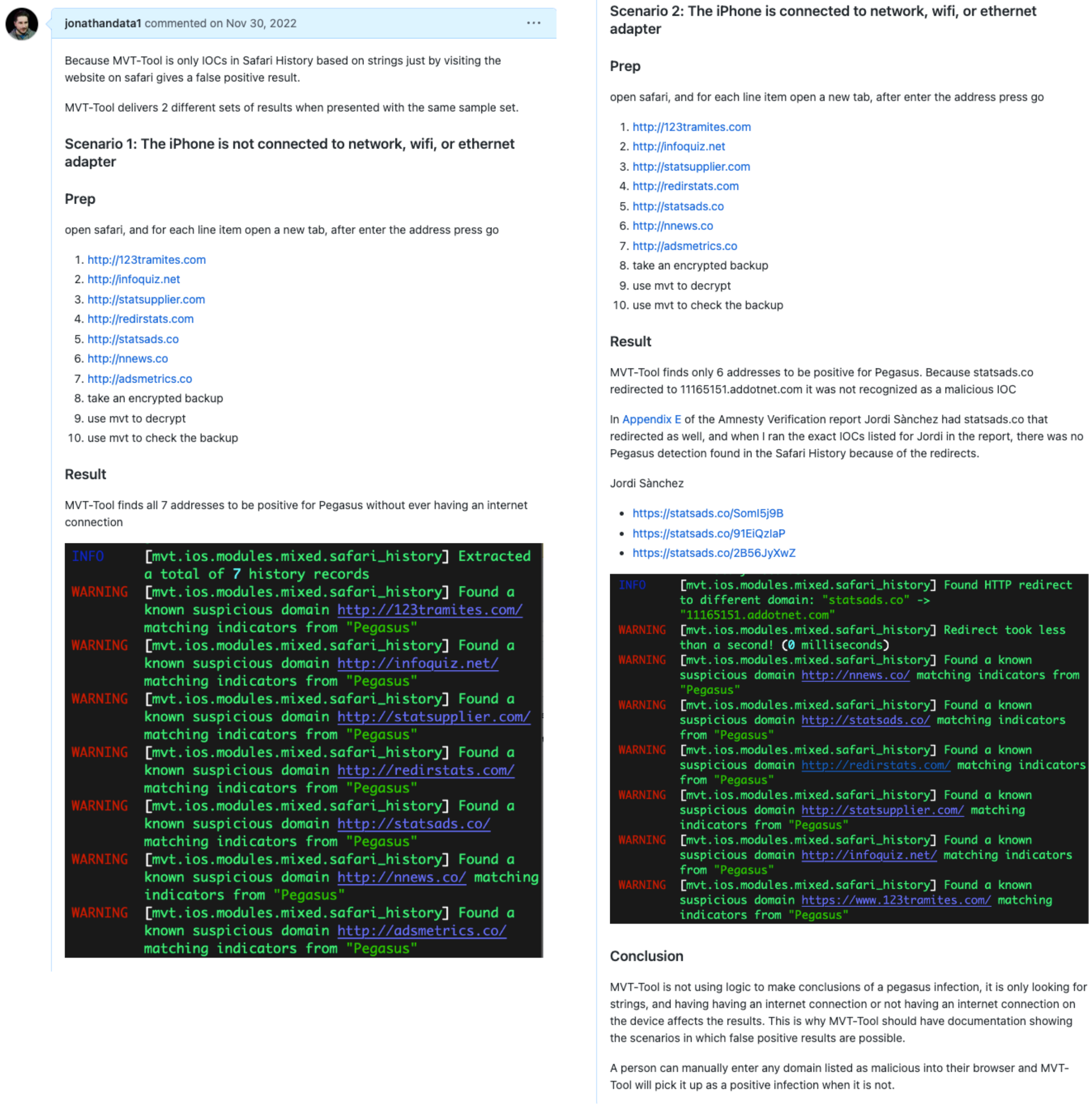
- Without physical devices a proper iOS mobile forensics examination and analysis cannot be performed
- Legitimate Apple App store applications can be mistaken as Pegasus processes because MVT-Tool disregards the Application Name

Figure 5 MVT-Tool Issue Legitimate Apple Apps can be seen as malicious with MVT

[43] https://github.com/mvt-project/mvt/issues/320

Github Issue 319[44]

Domain False Positive Results When Wi-Fi On or Off



jonathandata1 commented on Nov 30, 2022

Because MVT-Tool is only IOCs in Safari History based on strings just by visiting the website on safari gives a false positive result.

MVT-Tool delivers 2 different sets of results when presented with the same sample set.

Scenario 1: The iPhone is not connected to network, wifi, or ethernet adapter

Prep

open safari, and for each line item open a new tab, after enter the address press go

1. http://123tramites.com
2. http://infoquiz.net
3. http://statsupplier.com
4. http://redirstats.com
5. http://statsads.co
6. http://nnews.co
7. http://adsmetrics.co
8. take an encrypted backup
9. use mvt to decrypt
10. use mvt to check the backup

Result

MVT-Tool finds all 7 addresses to be positive for Pegasus without ever having an internet connection

```
INFO      [mvt.ios.modules.mixed.safari_history] Extracted
          a total of 7 history records
WARNING   [mvt.ios.modules.mixed.safari_history] Found a
          known suspicious domain http://123tramites.com/
          matching indicators from "Pegasus"
WARNING   [mvt.ios.modules.mixed.safari_history] Found a
          known suspicious domain http://infoquiz.net/
          matching indicators from "Pegasus"
WARNING   [mvt.ios.modules.mixed.safari_history] Found a
          known suspicious domain http://statsupplier.com/
          matching indicators from "Pegasus"
WARNING   [mvt.ios.modules.mixed.safari_history] Found a
          known suspicious domain http://redirstats.com/
          matching indicators from "Pegasus"
WARNING   [mvt.ios.modules.mixed.safari_history] Found a
          known suspicious domain http://statsads.co/
          matching indicators from "Pegasus"
WARNING   [mvt.ios.modules.mixed.safari_history] Found a
          known suspicious domain http://nnews.co/ matching
          indicators from "Pegasus"
WARNING   [mvt.ios.modules.mixed.safari_history] Found a
          known suspicious domain http://adsmetrics.co/
          matching indicators from "Pegasus"
```

Scenario 2: The iPhone is connected to network, wifi, or ethernet adapter

Prep

open safari, and for each line item open a new tab, after enter the address press go

1. http://123tramites.com
2. http://infoquiz.net
3. http://statsupplier.com
4. http://redirstats.com
5. http://statsads.co
6. http://nnews.co
7. http://adsmetrics.co
8. take an encrypted backup
9. use mvt to decrypt
10. use mvt to check the backup

Result

MVT-Tool finds only 6 addresses to be positive for Pegasus. Because statsads.co redirected to 11165151.addotnet.com it was not recognized as a malicious IOC

In Appendix E of the Amnesty Verification report Jordi Sànchez had statsads.co that redirected as well, and when I ran the exact IOCs listed for Jordi in the report, there was no Pegasus detection found in the Safari History because of the redirects.

Jordi Sànchez

- https://statsads.co/SomI5j9B
- https://statsads.co/91EiQzlaP
- https://statsads.co/2B56JyXwZ

```
INFO      [mvt.ios.modules.mixed.safari_history] Found HTTP redirect
          to different domain: "statsads.co" ->
          "11165151.addotnet.com"
WARNING   [mvt.ios.modules.mixed.safari_history] Redirect took less
          than a second! (0 milliseconds)
WARNING   [mvt.ios.modules.mixed.safari_history] Found a known
          suspicious domain http://nnews.co/ matching indicators from
          "Pegasus"
WARNING   [mvt.ios.modules.mixed.safari_history] Found a known
          suspicious domain http://statsads.co/ matching indicators
          from "Pegasus"
WARNING   [mvt.ios.modules.mixed.safari_history] Found a known
          suspicious domain http://redirstats.com/ matching indicators
          from "Pegasus"
WARNING   [mvt.ios.modules.mixed.safari_history] Found a known
          suspicious domain http://statsupplier.com/ matching
          indicators from "Pegasus"
WARNING   [mvt.ios.modules.mixed.safari_history] Found a known
          suspicious domain http://infoquiz.net/ matching indicators
          from "Pegasus"
WARNING   [mvt.ios.modules.mixed.safari_history] Found a known
          suspicious domain https://www.123tramites.com/ matching
          indicators from "Pegasus"
```

Conclusion

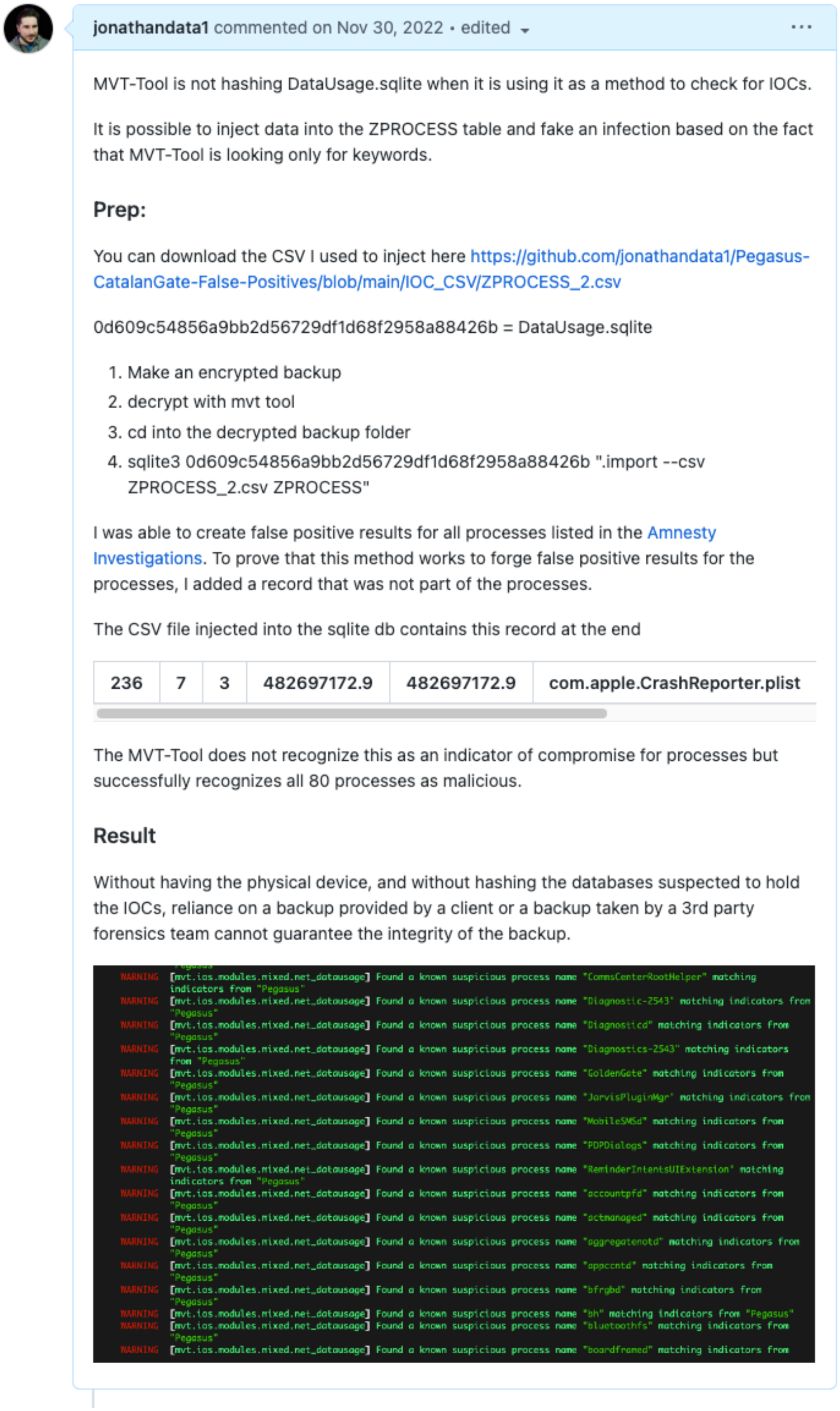
MVT-Tool is not using logic to make conclusions of a pegasus infection, it is only looking for strings, and having having an internet connection or not having an internet connection on the device affects the results. This is why MVT-Tool should have documentation showing the scenarios in which false positive results are possible.

A person can manually enter any domain listed as malicious into their browser and MVT-Tool will pick it up as a positive infection when it is not.

Github Issue 318[45]

[44] https://github.com/mvt-project/mvt/issues/319
[45] https://github.com/mvt-project/mvt/issues/318

SQL Data Injection – Leads to False Positive Results



jonathandata1 commented on Nov 30, 2022 • edited

MVT-Tool is not hashing DataUsage.sqlite when it is using it as a method to check for IOCs.

It is possible to inject data into the ZPROCESS table and fake an infection based on the fact that MVT-Tool is looking only for keywords.

Prep:

You can download the CSV I used to inject here https://github.com/jonathandata1/Pegasus-CatalanGate-False-Positives/blob/main/IOC_CSV/ZPROCESS_2.csv

0d609c54856a9bb2d56729df1d68f2958a88426b = DataUsage.sqlite

1. Make an encrypted backup
2. decrypt with mvt tool
3. cd into the decrypted backup folder
4. sqlite3 0d609c54856a9bb2d56729df1d68f2958a88426b ".import --csv ZPROCESS_2.csv ZPROCESS"

I was able to create false positive results for all processes listed in the Amnesty Investigations. To prove that this method works to forge false positive results for the processes, I added a record that was not part of the processes.

The CSV file injected into the sqlite db contains this record at the end

236	**7**	**3**	**482697172.9**	**482697172.9**	**com.apple.CrashReporter.plist**

The MVT-Tool does not recognize this as an indicator of compromise for processes but successfully recognizes all 80 processes as malicious.

Result

Without having the physical device, and without hashing the databases suspected to hold the IOCs, reliance on a backup provided by a client or a backup taken by a 3rd party forensics team cannot guarantee the integrity of the backup.

```
    WARNING  [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "CommsCenterRootHelper" matching
             indicators from "Pegasus"
    WARNING  [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "Diagnostic-2543" matching indicators from
             "Pegasus"
    WARNING  [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "Diagnosticd" matching indicators from
             "Pegasus"
    WARNING  [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "Diagnostics-2543" matching indicators
             from "Pegasus"
    WARNING  [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "GoldenGate" matching indicators from
             "Pegasus"
    WARNING  [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "JarvisPluginMgr" matching indicators from
             "Pegasus"
    WARNING  [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "MobileSMSd" matching indicators from
             "Pegasus"
    WARNING  [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "PDPDialogs" matching indicators from
             "Pegasus"
    WARNING  [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "ReminderIntentsUIExtension" matching
             indicators from "Pegasus"
    WARNING  [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "accountpfd" matching indicators from
             "Pegasus"
    WARNING  [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "actmanaged" matching indicators from
             "Pegasus"
    WARNING  [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "aggregatenotd" matching indicators from
             "Pegasus"
    WARNING  [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "appccntd" matching indicators from
             "Pegasus"
    WARNING  [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "bfrgbd" matching indicators from
             "Pegasus"
    WARNING  [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "bh" matching indicators from "Pegasus"
    WARNING  [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "bluetoothfs" matching indicators from
             "Pegasus"
    WARNING  [mvt.ios.modules.mixed.net_datausage] Found a known suspicious process name "boardframed" matching indicators from
```

Conclusion

The disregard for legal systems designed to prosecute illicit actions has allowed certain organizations to become their own global judicial system, exempt from the rules of criminal procedure and not required to provide verifiable evidence for their claims. Such departure from the foundations of our collective justice systems poses a grave threat to science and geo-politics. To combat the spread of fear, uncertainty, and doubt, a collaborative effort is required between scientists, geo-political analysts, and legal professionals to equip government organizations with the necessary tools and expertise to respond effectively to false accusations and sensationalism.

The allegations against the Moroccan government engaging in unlawful surveillance against civil society members are of utmost concern and demand immediate attention because the evidentiary basis for the allegations lacks scientific verifiability and reproducibility. Despite the admission of falsification by the accusers, a significant number of individuals, including information security professionals, politicians, and members of the public, continue to propagate the allegations of illicit spyware use by Morocco.

The accusations of committing a crime against humanity by the Moroccan government have the potential to jeopardize international relations with other countries and have significant consequences for the Kingdom. The allegations of malicious software installed on the mobile devices of political opponents have been shown to be nothing more than normal iPhone processes that exist in every device. The perpetuation of such false claims by NGOs, non-profits, and other special interest groups undermines computer and forensics science as a whole.

References

Amnesty Tech. (2021, July 18). *Forensic methodology report: How to catch nso group's pegasus*. Amnesty International. Retrieved February 17, 2023, from https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

AmnestyTech. (2021, July 19). *Removing false positive · AmnestyTech/investigations@1c69421*. GitHub. Retrieved February 17, 2023, from https://github.com/AmnestyTech/investigations/commit/1c694217c3efb4e40f34822b6ef99a7b5bd8a064

Amundsen, A., & Ovens, K. (2017). Forensics analysis of Wi-Fi communication traces in mobile devices ... Retrieved February 18, 2023, from https://researchonline.gcu.ac.uk/ws/portalfiles/portal/25640096/PID5133269.pdf

Council of Europe. (2001). *Convention on cybercrime*. Council of Europe Treaty Office. Retrieved February 18, 2023, from https://rm.coe.int/1680081561

Council of Europe. (2018, August 30). *Morocco joins the Budapest Convention on Cybercrime and its protocol on xenophobia and racism - cybercrime - publi.coe.int*. Cybercrime. Retrieved February 17, 2023, from https://www.coe.int/en/web/cybercrime/t-cy-news/-/asset_publisher/GxUcENEFhivB/content/morocco-joins-the-budapest-convention-on-cybercrime-an-becomes-it-s-60th-member-?inheritRedirect=false

Crowley, M. (2022, December 14). *Rwanda's president says the United States can't 'bully' him into releasing a political opponent.* The New York Times. Retrieved February 17, 2023, from https://www.nytimes.com/2022/12/14/us/politics/rwanda-president-kagame-rusesabagina.html

CSA. (n.d.). *Claudio Guarnieri*. CSA Celebrity Speakers. Retrieved February 17, 2023, from https://www.speakers.co.uk/speakers/claudio-guarnieri/

European Council. (2004, January 7). *Budapest Convention* . ETS No. 185. Retrieved February 17, 2023, from https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

Farivar , C. (2017, November 19). *Infosec star accused of sexual assault booted from professional affiliations*. Ars Technica. Retrieved February 13, 2023, from https://arstechnica.com/tech-policy/2017/11/report-infosec-researcher-accused-of-numerous-instances-of-sexual-assault/

Forbidden Stories. (2021). *About the pegasus project*. Forbidden Stories. Retrieved February 17, 2023, from https://forbiddenstories.org/about-the-pegasus-project/

Foundation, F. (2021, November 24). *Important step to defend civic space against surveillance, and welcomed recognition of the work of grantees @citizenlab & @amnestytech whose research uncovered the organized and deliberate use of spyware targeting global activists and journalists. https://t.co/nmljyjqdcd*. Twitter. Retrieved February 17, 2023, from https://twitter.com/FordFoundation/status/1463568098489946120

Gallagher, R. (2012, August 20). *How government-grade spy tech used a fake scandal to Dupe Journalists*. Slate Magazine. Retrieved February 12, 2023, from https://slate.com/technology/2012/08/moroccan-website-mamfakinch-targeted-by-government-grade-spyware-from-hacking-team.html

Gallagher, R. (2012, October 10). *Phony wikileaks tricks activist into downloading government-grade spyware*. Slate Magazine. Retrieved February 17, 2023, from https://slate.com/technology/2012/10/ahmed-mansoor-uae-activst-allegedly-tricked-by-phoney-wikileaks-into-downloading-hacking-team-spyware.html

GitHub. (2022, March 11). *The new github issues - March 10th update: Github changelog*. The GitHub Blog. Retrieved February 18, 2023, from https://github.blog/changelog/2022-03-10-the-new-github-issues-march-10th-update/#:~:text=When%20closing%20an%20issue%2C%20you,reason%3A%22not%20planned%22%20.

Hacking Team. (2011, July 24). Hacking Team Emails. Retrieved February 17, 2023, from https://wikileaks.org/hackingteam/emails/emailid/600803

Hacking Team. (2012, August 21). Hacking Team Emails. Retrieved February 17, 2023, from https://wikileaks.org/hackingteam/emails/emailid/449677

Hacking Team. (2012, May 4). Hacking Team Emails. Retrieved February 17, 2023, from https://wikileaks.org/hackingteam/emails/emailid/571259

Hacking Team. (2012, October 10). *Hacking Team Emails*. WikiLeaks. Retrieved February 17, 2023, from https://wikileaks.org/hackingteam/emails/emailid/449796

Hajjaji, D. (2019, July 1). *Moroccan independent journalists describe climate of pervasive surveillance, harassment*. Committee to Protect Journalists. Retrieved February 12, 2023, from https://cpj.org/2019/07/moroccan-independent-journalists-describe-climate/

Jonathan Scott. (2022, November 30). *Domain history - false positive results · issue #319 · MVT-Project/MVT*. GitHub. Retrieved February 18, 2023, from https://github.com/mvt-project/mvt/issues/319

Jonathan Scott. (2022, November 30). *Legitimate apple apps can be seen as malicious - false positive results · issue #320 · MVT-Project/MVT*. GitHub. Retrieved February 18, 2023, from https://github.com/mvt-project/mvt/issues/320

Jonathan Scott. (2022, November 30). *SQL injection - leads to false positive results - · issue #318 · MVT-Project/MVT*. GitHub. Retrieved February 18, 2023, from https://github.com/mvt-project/mvt/issues/318

Lab, C. (2009, September 10). *Http://bit.ly/226Wws Palantir brainstorming session at psiphon office*. Twitter. Retrieved February 17, 2023, from https://twitter.com/citizenlab/status/3888711632?s=20

Lab, C. (2009, September 10). *Palantir visit to the PSIPHON and Citizen Lab offices today for brainstorming session on cyber investigations*. Twitter. Retrieved February 17, 2023, from https://twitter.com/citizenlab/status/3888203174?s=20

Lab, C. (2017, July 8). *Koobface: Inside a crimeware network*. The Citizen Lab. Retrieved February 17, 2023, from https://citizenlab.ca/2010/11/koobface-inside-a-crimeware-network/

MacArthur Foundation. (2020). *MacArthur Foundation - MacArthur Foundation*. MacArthur Foundation Form 990. Retrieved February 18, 2023, from https://www.macfound.org/media/files/macarthur-foundation-2020-form-990-pf-(final).pdf

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 February 17, 2023, from https://citizenlab.ca/2021/07/amnesty-peer-review/

Marquis-Boire, M. (2012, October 10). *Backdoors are forever: Hacking team and the targeting of dissent*. The Citizen Lab. Retrieved February 13, 2023, from https://citizenlab.ca/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent/

MCCUAIG-JOHNSTON, M. A. R. G. A. R. E. T. (2021, June 18). *All Canadian universities must critically reassess their collaborations with China*. URAPca. Retrieved February 17, 2023, from https://web.archive.org/web/20211028035847/https://www.urap.ca/all-canadian-universities-must-critically-reassess-their-collaborations-with-china/

Quino Petit, M. G. (2022, May 15). *Ronald Deibert, Fundador de Citizen Lab: "los gobiernos usan pegasus porque tienen apetito de espiar"*. El País. Retrieved February 17, 2023, from https://elpais.com/espana/2022-05-15/ronald-deibert-fundador-de-citizen-lab-los-gobiernos-usan-pegasus-porque-tienen-apetito-de-espiar.html

Rahhou, J. (2022, March 19). *Morocco demands Amnesty International for proof over pegasus allegations*. https://www.moroccoworldnews.com/. Retrieved February 17, 2023, from https://www.moroccoworldnews.com/2022/03/347777/morocco-demands-amnesty-international-for-proof-over-pegasus-allegations

Scott-Railton, J., Campo, E., Marczak, B., Razzak, B. A., Anstis, S., Böcü, G., Solimano, S., & Deibert, R. (2022, December 23). *Catalangate: Extensive mercenary spyware operation* *against Catalans using pegasus and Candiru*. The Citizen Lab. Retrieved February 17, 2023, from https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/

Scott-Railton, J., Senft, A., Poetranto, I., & McKune, S. (2015, October 15). *Mapping Finfisher's continuing proliferation*. The Citizen Lab. Retrieved February 17, 2023, from https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

slate. (2020, January 15). *Which tech company is really the most evil?* Slate Magazine. Retrieved February 17, 2023, from https://slate.com/technology/2020/01/evil-list-tech-companies-dangerous-amazon-facebook-google-palantir.html

Various. (2018). *Chinese grammatical error diagnosis using statistical ... - ACL anthology*. Chinese Grammatical Error Diagnosis using Statistical and Prior Knowledge driven Features with Probabilistic Ensemble Enhancement. Retrieved February 18, 2023, from https://aclanthology.org/W18-3707.pdf