



## Catalangate Vectors: An Analysis of WhatsApp's Impact on Citizen Privacy & Amnesty International's MVT-Tool

Gregorio Martín Quetglas<sup>1</sup>, Jonathan Boyd Scott<sup>2</sup>

<sup>1</sup>Professor of Computer Science, Valencia University, Valencia Spain.

<sup>2</sup>Executive Director, Milad Group LLC.

**Abstract** – The Catalangate espionage argues the existence of infections by using vectors of a very different nature. Vector A (WhatsApp Pegasus Notification) dates back to May 2019 when META released a patch to the CVE-2019-3568 exploit. Media publications such as EL PAÍS and The Guardian claimed that WhatsApp confirmed the President of the Catalan Parliament, and four other politicians had been infected by NSO Group's Pegasus software via the WhatsApp messaging network. A court case filed in Barcelona in 2022 regarding the hacking allegations was dismissed due to the inability to identify the offenders and the lack of a response from WhatsApp's headquarters in Ireland. Citizen Lab's Catalangate report only references the alleged hacking of the President of Catalan Parliament and does so without specifying the date of infection. Catalangate's Vectors B (Pegasus SMS's) and C (Forensically Confirmed Pegasus Infections) are based on the use of MVT-Tool managed by Amnesty International. The MVT-Tool is a compilation of indicators that is used to identify devices that have been alleged to be compromised by Pegasus software developed by NSO Group. These indicators have been gathered through research conducted by Amnesty International's Security Lab and other partners. The Pegasus Project, which is a collaboration led by Forbidden Stories and includes a global network of investigative journalists, also provided technical information. It should be noted that the tool used may have some deficiencies in forensic analysis, which may lead to the production of false positives. The Catalangate report presents 65 cases of infections or targeting's that are alleged to be caused by the Pegasus software and or other. Four of these cases, known as Candiru, are not related to the alleged Pegasus attacks. The remaining cases are divided into three vectors, Vector A, Vector B and Vector C, which are believed to be related to Pegasus. This white paper will focus on analyzing the accuracy of the accusations related to Vector A, which does not utilize Amnesty International's MVT-Tool methodology, and the inaccuracies in the conclusions drawn from Vector B and Vector C that make use of Amnesty International's MVT-Tool methodology.

**Keywords:** Catalangate, digital espionage, mobile forensics, mobile malware, NSO Group, Pegasus Spyware, MVT-Tool.

### 1. VECTOR A

On May 13th, 2019, the Financial Times reported a critical flaw in WhatsApp (Srivastava, 2019 [1]), later identified as CVE-2019-3568 (Mitre, 2019 [2]), posing a grave threat to 1.5 billion users on Android, iOS, and Windows Phone. Suspicions pointed towards NSO Group's Pegasus software, known for targeting phone numbers. WhatsApp shared a list of potentially affected numbers, including Roger Torrent's, President of the Catalan Parliament, with The Citizen Lab. This incident, among others, ignited what would later be dubbed Catalangate. The Catalangate report claims that Jordi Domingo, Anna Gabriel, Ernest Maragall, Sergi Miquel, and Roger Torrent were under surveillance through WhatsApp, allegedly by the Spanish



government (Scott-Railton et al., 2022 [3]). However, the evidence provided is limited to a table labeled "2019 WhatsApp Pegasus Notification 2019," which simply lists each alleged victim's name alongside a "true" designation, without specifying when these infections occurred. It's worth mentioning that the Catalangate report refers to an article in The Guardian (Kirchgaessner, 2020 [4]), where WhatsApp's Director of Public Policy, Niamh Sweeney, explains, "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." Furthermore, the report neglects to disclose the identity of the informant or shed light on the method of communication used to notify the individuals affected. Despite reports from sources like The Guardian and EL PAÍS, which cite disclosures from John Scott-Railton of The Citizen Lab (Kirchgaessner & Joens, 2020 [5]) indicating infections occurring between 2019 and 2021, the Catalangate report heavily relies on self-referential citations from media outlets to bolster its claims and outline the timeline of alleged infections. This overreliance on unsubstantiated references from external sources undermines the credibility of the report's findings. Despite the lack of concrete evidence supporting the claims of surveillance, various media platforms (Marks & Schaffer, 2022 [6]) have disseminated information sourced from The Citizen Lab as though it were irrefutable truth. One of the primary media sources referenced in the Catalangate report is The Guardian. However, The Guardian's participation in The Pegasus Project (Forbidden Stories, 2021 [7]), a collaborative effort involving various media organizations and Amnesty International Technologists, raises concerns regarding the impartiality and independence of the information being disseminated. Notably, Amnesty International's Tech team, which is cited as the source of the Catalangate's purported independent validation (Scott-Railton et al., 2022 Independent Validation [8]), is not as detached from bias as it may seem. As an example, Amnesty International and The Citizen Lab often receive financial support from shared donors such as The Ford Foundation (Ford Foundation, 2021 [9]) and MacArthur Foundation (MacArthur Foundation, 2020 [10]). To ensure genuine independence in the review process, it's imperative that both parties are devoid of any potential conflicts of interest (Makarem et al., 2023 [11]).

**Table -1:** WhatsApp infection data found in the Catalangate report published by The Citizen Lab

<b>Catalangate Vectors: An Analysis of WhatsApp's Impact on Citizen Privacy &amp; Amnesty International's MVT-Tool</b>					
Name	Organization(s)	2019 WhatsApp Pegasus Notification	Pegassus SMSes	Forensically Confirmed Pegasus Infection	Targeted / Infected with Candiru
Anna Gabriel	Member of the Parliament of Catalonia,	Yes			



	Esquerra Republicana de Catalunya.				
Ernest Maragall	Member of the Parliament of Catalonia,  Esquerra Republicana de Catalunya.	Yes			
Jordi Domingo	Member, Assemblea Nacional Catalana	Yes			
Roger Torrent	Minister of Business and Labour of Catalonia,  Former President of the Parliament of Catalonia,  Esquerra Republicana de Catalunya	Yes	1		
Sergi Miquel	General Manager Council for the Republic of Catalonia	Yes			

## 2. VECTOR B

When Amnesty International agreed to act as an independent peer reviewer for the Catalangate findings in March–April 2022 (Deibert & Cañas, 2022 [12]), they faced a critical forensics challenge. By the time Amnesty validated the findings, all domains associated with the WhatsApp infections for Vector A victims had either expired or were parked. Nevertheless, Amnesty confirmed The Citizen Lab's findings. Upon the release of the Catalangate report on April 18, 2022, all Vector A domains were listed as actively malicious. Consequently, over 10 Anti-Virus vendors and IOC aggregators quickly added these domains to their lists as malicious URLs without any validation. After being contacted, several organizations acknowledged their mistake and removed the domains. For instance, Heimdal Security (Figure 1) determined all domains to be false positives. Additionally, after conducting a thorough analysis, Seclookup (Figure 2) whitelisted all reported Catalangate domains. Depending solely on domains as indicators of compromise (IOCs) can



result in numerous false positives and may not provide a comprehensive understanding of an attack. It is recommended to complement IOCs with tactics, techniques, and procedures (TTPs) for a more thorough understanding. Atomic IOCs, which cannot be further subdivided, should be combined with TTPs to offer a detailed perspective of the attack, thereby improving the accuracy of identifying and mitigating malicious activity. The National Institute of Standards and Technology (NIST) publication 800-115 (2016) provides guidelines for sharing cyber threat information, defining TTPs as descriptions of attacker behavior, including the use of specific malware variants (Johnson et al., 2016 [13]).

**Dragos Dirmon (Heimdal Security)**

Oct 17, 2022, 14:11 GMT+3

Hello Jonathan, Thank you for contacting Heimdal Security Support. We have checked the websites submitted by you and it looks like a false positive case. We decided to remove them from our blacklist and they should be available for you in 48 hours or less.

Kind Regards,

Dragos Dirmon Heimdal Security A/S & Heimdal Security SRL <http://www.heimdalsecurity.com/>

Oct 16, 2022, 10:26 GMT+3

The following is a list of IOCs that need to be reevaluated

[statsupplier.com](http://statsupplier.com)

[redirstats.com](http://redirstats.com)

[adsmetrics.co](http://adsmetrics.co)

[statsads.co](http://statsads.co)

[nnews.co](http://nnews.co)

[123tramites.com](http://123tramites.com)

Respectfully,

Jonathan Scott

**Fig -1:** Heimdal Security Whitelists all Catalangate domains, calling them false positives



Jonathan Scott ·  
to Seclookup ▾

The following is a list of IOCs that need to be reevaluated

[infoquiz.net](http://infoquiz.net)

[statsupplier.com](http://statsupplier.com)

[redirstats.com](http://redirstats.com)

[adsmetrics.co](http://adsmetrics.co)

[statsads.co](http://statsads.co)

[nnews.co](http://nnews.co)

Respectfully,  
Jonathan Scott



Seclookup Support  
to me ▾

Hi Jonathan Scott,

After careful examination and analysis, we have **whitelisted** all the reported domains below in the email. It might take 24 to 48 hours to whitelist to be effective on Virustotal.

**Please note:** This whitelisting is not permanent, and domain may reappear in malicious category if compromised or used for malicious purposes.

Please reopen this ticket in case of any issues.

<https://seclookup.freshdesk.com/helpdesk/tickets/1031>

Regards,  
Seclookup Engineering Team

**Fig -2:** Seclookup whitelists all Catalangate domains and finds them to not be malicious



## 2.1 Vector B IOC Experiment

After examining interviews with Amnesty security researcher Etienne Maynier (Villarreal, 2022 [14]) and The Citizen Lab Director Ron Deibert (Quino Petit, 2022 [15]), it became clear that both organizations relied solely on iCloud backups provided by alleged victims for their analysis of the Catalangate incident, without inspecting the physical mobile devices. Director Deibert explained that having the physical device might not be useful in their methodology. Both Amnesty and The Citizen Lab concluded that all seven domains listed in the Catalangate incident were malicious. Amnesty used their MVT-Tool (Mobile Verification Toolkit) (Amnesty International, 2021 [16]) to verify their findings, and Maynier confirmed that both organizations employed the same methodologies and data for their forensic examinations. A study was conducted to explore the potential implications of relying exclusively on iCloud backups without physical examination, additional context, or a controlled environment for forensic analysis by Amnesty and The Citizen Lab.

## 2.2 Vector B IOC Experiment – Scenario 1 & Setup

The iPhone is not connected to a network, Wi-Fi, or lighting to ethernet adapter.

open safari, and for each line item below open a new tab, after entering the address press go on you iPhone keyboard

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.

## 2.3 Vector B IOC Experiment – Scenario 1 Results

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"
```

Fig -3: All 7 Domains listed as malicious without the phone ever being connected to the internet

### 2.4 Vector B IOC Experiment – Scenario 2 & Setup

The iPhone is connected to a network, Wi-Fi, or lighting to ethernet adapter

open safari, and for each line item below open a new tab, after entering the address press go on you iPhone keyboard

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-tool to decrypt

### 2.5 Vector B IOC Experiment – Scenario 2 Results

The MVT-Tool identified only 6 addresses as positive for Pegasus infection. However, the domain statsads.co which redirects to 11165151.addotnet.com was not recognized as a malicious indicator of compromise (IOC) due to this redirection.

```
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"
```

Fig -4: Only 6 Domains listed as malicious when connected to the internet

### 2.6 Vector B IOC Experiment – Conclusion

The MVT-Tool primarily relies on string matching to detect a Pegasus infection. It does not incorporate logical reasoning or TTPs, which are essential for precise identification. This approach can result in false positives because the tool may trigger even if a malicious domain is manually entered into the browser, regardless of whether the device is infected. Additionally, the MVT-Tool's functionality is influenced by the device's internet connectivity status, further complicating the determination of true infection versus manual domain entry and increasing the risk of false positives. To ensure accurate identification of infections, it's imperative to consider logical reasoning, TTPs (Anand et al., 2022 [17]), and other factors alongside string matching.

### 3. VECTOR C

Vector C aggregates various findings from files extracted from iOS phone backups, including DataUsage.sqlite, Manifest.db, OS Analytics AD Daily, and private files like those containing WhatsApp activity. While analyzing iCloud backups, both Amnesty International and The Citizen Lab detected unfamiliar data within DataUsage.sqlite and Manifest.db, deeming these indicators of Pegasus spyware. However, relying solely on iCloud backups for forensic analysis has limitations, as highlighted by leading mobile forensics firm Elcomsoft. According to Elcomsoft's article, "The Worst Mistakes in iOS Forensics (Katalov, 2020 [18])," relying solely on iCloud backups excludes a significant amount of data, and if iTunes sync is not disabled before connecting the device to a computer, the device's content may alter.

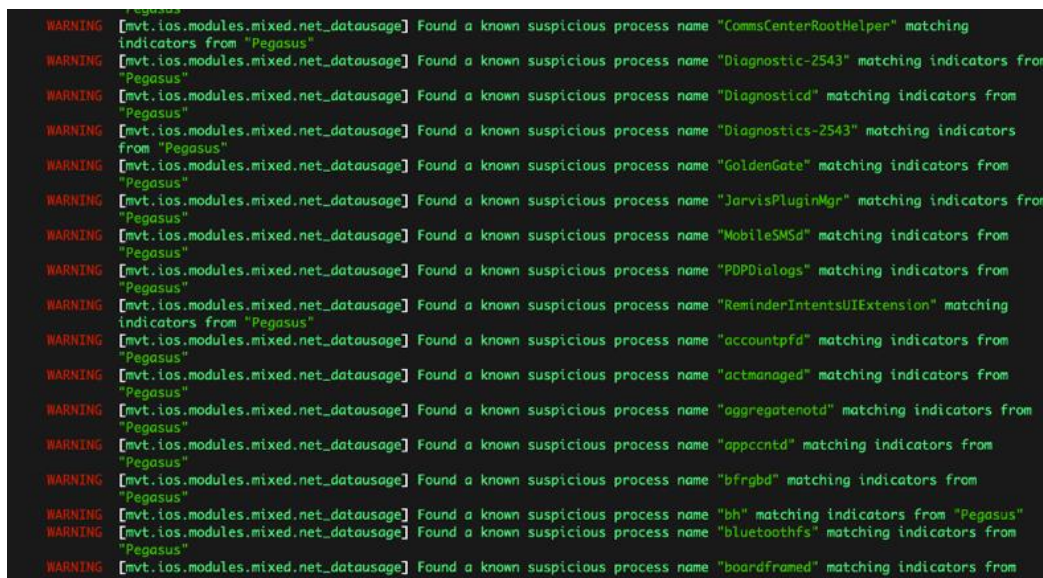
#### 3.1 Vector C IOC Experiment – Setup

1. Download the CSV I used to inject here [https://github.com/jonathandata1/Pegasus-CatalanGate-False-Positives/blob/main/IOC\\_CSV/ZPROCESS\\_2.csv](https://github.com/jonathandata1/Pegasus-CatalanGate-False-Positives/blob/main/IOC_CSV/ZPROCESS_2.csv)

2. 0d609c54856a9bb2d56729dfd1d68f2958a88426b = DataUsage.sqlite
3. Make an encrypted backup
4. decrypt with mvt tool
5. cd into the decrypted backup folder
6. run the following from the command line: `sqlite3 0d609c54856a9bb2d56729dfd1d68f2958a88426b ".import --csv ZPROCESS_2.csv ZPROCESS"`

### 3.2 Vector C IOC Experiment – Results

It was shown that false positives can arise for all processes listed in the Amnesty Investigations. To illustrate, a record, `com.apple.CrashReporter.plist`, not originally part of the process list, was added as an example. When added into the SQLite database, this rogue record appears at the end. The MVT-Tool, however, fails to recognize `com.apple.CrashReporter.plist` as a sign of compromise for processes. Instead, it marks all 80 processes as malicious. This underscores the limitations of the methodology and the risk of false positives.



```
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 "Pegasus"
```

**Fig -5:** All 80 alleged malicious processes could be forged into the iPhone due to database manipulation, resulting in a Positive match for Pegasus.

### 3.3 Vector C IOC Experiment – Conclusion

It's crucial to physically access the device and verify the integrity of suspected databases and files containing Indicators of Compromise (IOCs) using cryptographic hashing methods during forensic analysis. These steps are key to ensuring the authenticity and integrity of iCloud backup data, whether provided by an alleged victim or obtained by a third-party forensic team. Without these measures, there's a risk of data alteration or manipulation, which could lead to inaccurate and potentially false results. Cryptographic hashing techniques like SHA-256, SHA-512, or MD5 can help maintain data integrity and prevent tampering (Rasjid et al., 2017 [19]). Moreover, physically examining the device allows for gathering additional data, such as hardware information, which further confirms the authenticity of data and improves analysis accuracy.





#### 4. CONCLUSIONS

The recent revelations in the Catalangate case highlight a concerning vulnerability: iPhone backups can be manipulated to appear as being Pegasus infected. This risk is exacerbated by the absence of oversight from mobile forensics professionals and the heavy reliance on iCloud backups for data analysis. Additionally, the methodology employed by the MVT-Tool lacks critical safeguards like cryptographic hashing, which undermines its credibility in forensic investigations. Furthermore, the failure to quarantine potentially compromised devices as criminal evidence further undermines confidence in the investigative process. These procedural shortcomings and deviations from digital forensics standards render the obtained data inadmissible in court and raise doubts about the validity of the analysis. It's crucial to adhere to established digital forensics protocols, including access to physical devices, data hashing, and proper quarantine measures, to ensure the reliability of investigation results. The Catalangate case serves as a reminder of the importance of upholding data integrity in forensic investigations and highlights the need for a thorough review of methodologies and protocols to maintain credibility. Given the ease of forgery demonstrated in the Catalangate case, it's necessary to conduct a retrospective review of past research and investigations by Amnesty International and The Citizen Lab. This review should involve an assessment of methodologies, protocols, and tools used, alongside a comparison to established digital forensics standards. Implementing a robust review process within a coalition, involving independent analysis and validation by qualified experts, can enhance data integrity and credibility. Exploring alternative methods, such as advanced machine learning, and global collaboration among experts can further improve the effectiveness of mobile forensics investigations and better protect individuals and organizations from threats.

#### REFERENCES

- [1] Srivastava, M. (2019, May 13). WhatsApp voice calls used to inject Israeli spyware on phones. Financial Times. <https://www.ft.com/content/4da1117e-756c-11e9-be7d-6d846537acab>
- [2] Mitre. (2019). A buffer overflow vulnerability in WhatsApp VOIP stack allowed remote code execution via specially crafted series of RTCP packets sent to a target phone number. The issue affects WhatsApp for Android prior to v2.19.134, WhatsApp Business for Android prior to v2.19.44, WhatsApp for iOS prior to v2.19.51, WhatsApp Business for iOS prior to v2.19.51, WhatsApp for Windows Phone prior to v2.18.348, and WhatsApp for Tizen prior to v2.18.15. CVE-2019-3568. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-3568>
- [3] 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. <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/> M. Young, *The Technical Writer's Handbook*. Mill Valley, CA: University Science, 1989.
- [4] Kirchgaessner, S. (2020, July 28). Whatsapp confirms Catalan politician's phone was target of 2019 attack. The Guardian. <https://www.theguardian.com/technology/2020/jul/28/whatsapp-confirms-catalan-politicians-phone-was-target-of-2019-attack> K. Elissa, "Title of paper if known," unpublished.
- [5] Kirchgaessner, S., & Joens, S. (2020, July 13). Phone of top Catalan politician "targeted by government-grade spyware." The Guardian. <https://www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware>
- [6] Marks, J., & Schaffer, A. (2022, April 28). Catalan VP calls spyware scandal a test for Spanish democracy . THE CYBERSECURITY 202. <https://www.washingtonpost.com/politics/2022/04/28/catalan-vp-calls-spyware-scandal-test-spanish-democracy/>
- [7] Forbidden Stories. (2021, July 18). About the pegasus project. <https://forbiddenstories.org/about-the-pegasus-project/>
- [8] Scott-Railton, J., Campo, E., Marczak, B., Razzak, B. A., Anstis, S., Böcü, G., Solimano, S., & Deibert, R. (2022a, April 18). Catalangate: Extensive mercenary spyware operation against Catalans using pegasus and



- Candiru. The Citizen Lab. <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/#independent-validation>
- [9] 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. Twitter. <https://x.com/FordFoundation/status/1463568098489946120>
- [10] MacArthur Foundation. (2020). Return of private foundation 990-PF. [https://www.macfound.org/media/files/macarthur-foundation-2020-form-990-pf-\(final\).pdf](https://www.macfound.org/media/files/macarthur-foundation-2020-form-990-pf-(final).pdf)
- [11] Makarem, A., Mroué, R., Makarem, H., Diab, L., Hassan, B., Khabsa, J., & Akl, E. A. (2023). Conflict of interest in the Peer Review Process: A Survey of Peer Review Reports. PLOS ONE, 18(6). <https://doi.org/10.1371/journal.pone.0286908>
- [12] Deibert, R., & Cañas, J. (2022, May 13). Re: Letter to the University of Toronto - Citizen Lab report "CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru." <https://deibert.citizenlab.ca/wp-content/uploads/2022/05/2022.05.13-L-Ferris-to-J-Canas.pdf> - Pg. 6
- [13] Johnson, C. S., Badger, M. L., Waltermire, D. A., Snyder, J., & Skorupka, C. (2016). Guide to cyber threat information sharing. NIST Special Publication 800-150 - Guide to Cyber Threat Information Sharing. <https://doi.org/10.6028/nist.sp.800-150>
- [14] Villarreal, A. (2022, May 3). "Nunca Hemos visto un ataque con pegasus que no estuviera asociado a un gobierno." [elconfidencial.com. https://www.elconfidencial.com/tecnologia/2022-05-03/pegasus-spyware-catalangate-etienne-maynier\\_3417134/](https://www.elconfidencial.com/tecnologia/2022-05-03/pegasus-spyware-catalangate-etienne-maynier_3417134/)
- [15] Quino Petit, M. G. (2022, May 15). Ronald Deibert, Fundador de Citizen Lab: "los gobiernos usan pegasus porque tienen apetito de espiar." El País. <https://elpais.com/espana/2022-05-15/ronald-deibert-fundador-de-citizen-lab-los-gobiernos-usan-pegasus-porque-tienen-apetito-de-espiar.html>
- [16] Amnesty International. (2021). Mobile Verification Toolkit. Mobile verification toolkit. <https://docs.mvt.re/en/latest/>
- [17] Anand, A., Singhal, M., Guduru, S., & Chandavarkar, B. R. (2022). A survey on threat intelligence techniques for constructing, detecting, and reacting to advanced intrusion campaigns. Springer Proceedings in Mathematics & Statistics, 341–355. [https://doi.org/10.1007/978-3-031-16178-0\\_23](https://doi.org/10.1007/978-3-031-16178-0_23)
- [18] Katalov, V. (2020, January 30). The worst mistakes in los Forensics. ElcomSoft blog. <https://blog.elcomsoft.com/2020/01/the-worst-mistakes-in-ios-forensics/>
- [19] Rasjid, Z. E., Soewito, B., Witjaksono, G., & Abdurachman, E. (2017). A review of collisions in cryptographic hash function used in digital forensic tools. Procedia Computer Science, 116, 381–392. <https://doi.org/10.1016/j.procs.2017.10.072>