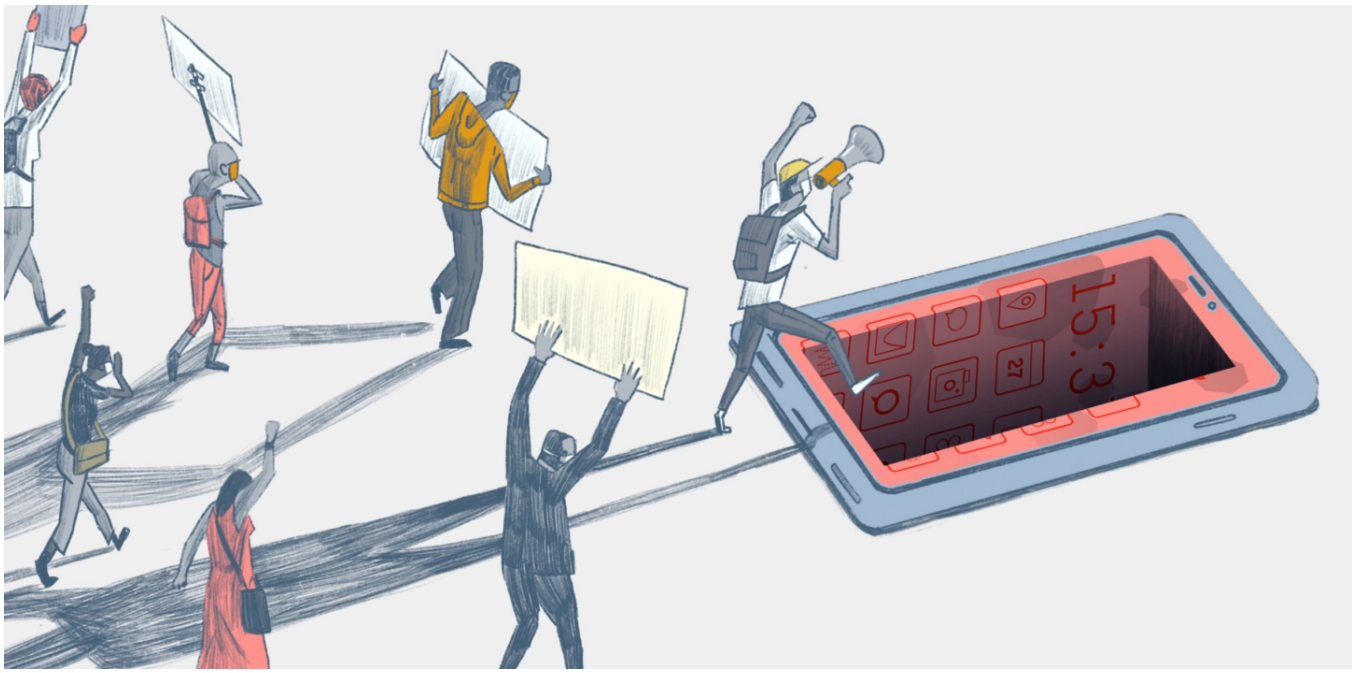
Forensic Methodology Report: How to catch NSO Group's Pegasus

amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

July 18, 2021



July 18, 2021
A copy of this report is available for download here.

Introduction

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

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

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

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

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

The Pegasus attacks detailed in this report and accompanying appendices are from 2014 up to as recently as July 2021. These also include so-called "zero-click" attacks which do not require any interaction from the target. Zero-click attacks have been observed since May 2018 and continue until now. Most recently, a successful "zero-click" attack has been observed exploiting multiple zero-days to attack a fully patched iPhone 12 running iOS 14.6 in July 2021.

Sections 1 to 8 of this report outline the forensic traces left on mobile devices following a Pegasus infection. This evidence has been collected from the phones of HRDs and journalists in multiple countries.

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

domains.

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

1. Discovering Pegasus network injection attacks

Amnesty International's technical investigation into NSO Group's Pegasus intensified following our discovery of the targeting of an Amnesty International staffer and a Saudi activist, Yahya Assiri, in 2018. Amnesty International's Security Lab began refining its forensics methodology through the discovery of attacks against HRDs in Morocco in 2019, which were further corroborated by attacks we discovered against a Moroccan journalist in 2020. In this first section we detail the process which led to the discovery of these compromises.

Numerous public reports had identified NSO Group's customers using SMS messages with Pegasus exploit domains over the years. As a result, similar messages emerged from our analysis of the phone of Moroccan activist Maati Monjib, who was one of the activists targeted as documented in Amnesty International's 2019 report.

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

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

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

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

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

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

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

Date (UTC)	URL
2019-02-11 14:45:53	https://d9z3sz93x5ueidq3.get1tn0w.free247downloads[.]com:30897/rdEN5YP
2019-09-13 17:01:38	https://2far1v4lv8.get1tn0w.free247downloads[.]com:31052/meunsnyse#0113565702571172968348457040223389731330224333972
2019-09-13 17:01:56	https://2far1v4lv8.get1tn0w.free247downloads[.]com:31052/meunsnyse#0680995616146262785199253586387891615724278336453
2020-01-17 11:06:32	https://gnyjv1xltx.info8fvhgl3.urlpush[.]net:30875/zrnv5revj#0741964198279879192740015486227389198355567483259 46%2324

2020-01-27 11:06:24	https://gnyjv1xltx.info8fvhgl3.urlpush[.]net:30875/zrnv5revj#0741964198279879192740015486227389198355567483259 46

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

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

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

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

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

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

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

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

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

2. Pegasus' BridgeHead and other malicious processes appear

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.1 Additional suspicious processes following BridgeHead

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

Less than a minute later a “**roleaboutd**” process first appears.

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

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

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

Based on the timing and context of exploitation, Amnesty International believes the **roleaboutd** and **msgacntd** processes are a later stage of the Pegasus spyware which was loaded after a successful exploitation and privilege escalation with the **BridgeHead payload**.

Similarly, the forensic analysis of Maati Monjib's phone revealed the execution of more suspicious processes in addition to **bh**. A process named **pcsd** and one named **fmld** appeared in 2018:

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

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

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

3. Pegasus processes following potential Apple Photos exploitation

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

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

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

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

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

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

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

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

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

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

4. An iMessage zero-click 0day used widely in 2019

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

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

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

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

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

2019-08-16 12:49:21	Process: **aggregatenotd**

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

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

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

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

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

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

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

5. Apple Music leveraged to deliver Pegasus in 2020

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

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

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

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

2020-07-06 05:22:21	Lookup of **f\x00\** by iMessage (com.apple.madrid)
2020-07-10 14:12:09	Pegasus request by Apple Music app: **https://x1znqjo0x8b8j.php78mp9v.opposedarrangement[.]net:37271/afAVt89Wq/stadium/pop2.html?key=501_4&n=7**
2020-07-10 14:12:21	Process: **roleaccountd**
2020-07-10 14:12:53	Process: **stagingd**
2020-07-13 05:05:17	Pegasus request by Apple Music app: **https://4n3d9ca2st.** **php78mp9v.opposedarrangement[.]net:37891/w58Xp5Z/stadium/pop2.html?key=501_4&n=7**

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

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

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

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

6. Megalodon: iMessage zero-click 0-days return in 2021

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

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

Date (UTC)	Event
2021-02-08 10:42:40	Lookup of **** by iMessage (com.apple.madrid)

2021-02-08 11:27:10	com.apple.coretelephony performs an HTTP request to **https://d38j2563clgblt.cloudfront[.]net/fV2GsPXgW//stadium/megalodon?m=iPhone9,1&v=18C66**
2021-02-08 11:27:21	Process: **gatekeeperd**
2021-02-08 11:27:22	gatekeeperd performs an HTTP request to **https://d38j2563clgblt.cloudfront.net/fV2GsPXgW//stadium/wizard/01-00000000**
2021-02-08 11:27:23	Process: **gatekeeperd**

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

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

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

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

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

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

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

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

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

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

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

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

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

Date (UTC)	Event
2021-05-17 13:39:16	Lookup for iCloud account **benjiburns8[@]gmail.com** (iMessage)
2021-05-17 13:40:12	File: /private/var/mobile/Library/SMS/Attachments/dc/12/DEAE6789-0AC4-41A9-A91C-5A9086E406A5/.eBDOuIN1wq.gif-2hN9
2021-05-17 13:40:21	File: /private/var/mobile/Library/SMS/Attachments/41/01/D146B32E-CA53-41C5-BF61-55E0FA6F5FF3/.TJi3flbHYN.gif-bMJq
…	…
2021-05-17 13:44:19	File: /private/var/mobile/Library/SMS/Attachments/42/02/45F922B7-E819-4B88-B79A-0FEE289701EE/.v74ViRNkCG.gif-V678

Amnesty International found no evidence that the 17 May attack was successful. Later attacks on the 18 June and 23 June were successful and led to Pegasus payloads being deployed on the device.

Initially, many iMessage (com.apple.madrid) push notifications were received, and attachment chunks were written to disk. The following table show a sample of the 48 attachment files found on the filesystem.

Date (UTC)	Event
2021-06-23 20:45:00	8 push notifications for topic com.apple.madrid (iMessage)
2021-06-23 20:46:00	46 push notifications for topic com.apple.madrid (iMessage)
2021-06-23 20:46:19	File: /private/var/tmp/com.apple.messages/F803EEC3-AB3A-4DC2-A5F1-9E39D7A509BB/.cs/ChunkStoreDatabase

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

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

Date (UTC)	Event
2021-06-23 20:48:56	Process with PID 1192 and name ReportCrash
2021-06-23 20:48:56	Process with PID 1190 and name IMTransferAgent
2021-06-23 20:48:56	Process with PID 1153 and name SCHelper
2021-06-23 20:48:56	Process with PID 1151 and name CategoriesService
2021-06-23 20:48:56	Process with PID 1147 and name MessagesBlastDoorService
2021-06-23 20:48:56	Process with PID 1145 and name NotificationService

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

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

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

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

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

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

7. Incomplete attempts to hide evidence of compromise

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

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

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

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

Date (UTC)	Event
2021-01-31 23:59:02	Process: **libtouchregd** (PID 7354)
2021-02-21 23:10:09	Process: **mptbd** (PID 5663)

2021-02-21 23:10:09	Process: **launchrexd** (PID 4634)
2021-03-21 06:06:45	Process: **roleaboutd** (PID 12645)
2021-03-28 00:36:43	Process: **otpgrefd** (PID 2786)
2021-04-06 21:29:56	Process: **locserviced** (PID 5492)
2021-04-23 01:48:56	Process: **eventfssd** (PID 4276)
2021-04-23 23:01:44	Process: **aggregatenotd** (PID 1900)
2021-04-28 16:08:40	Process: **xpccfd** (PID 1218)
2021-06-14 00:17:12	Process: **faskeepd** (PID 4427)
2021-06-14 00:17:12	Process: **lobbrogd** (PID 4426)
2021-06-14 00:17:12	Process: **neagentd** (PID 4423)
2021-06-14 00:17:12	Process: **com.apple.rapports.events** (PID 4421)
2021-06-18 08:13:35	Process: **faskeepd** (PID 4427)
2021-06-18 15:31:12	Process: **launchrexd** (PID 1169)
2021-06-18 15:31:12	Process: **frtipd** (PID 1168)
2021-06-18 15:31:12	Process: **ReminderIntentsUIExtension** (PID 1165)
2021-06-23 14:31:39	Process: **launchrexd** (PID 1169)
2021-06-23 20:59:35	Process: **otpgrefd** (PID 1301)
2021-06-23 20:59:35	Process: **launchafd** (PID 1300)
2021-06-23 20:59:35	Process: **vm_stats** (PID 1294)
2021-06-24 12:24:29	Process: **otpgrefd** (PID 1301)

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

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

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

8. Pegasus processes disguised as iOS system services

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

Several of these process names spoof legitimate iOS binaries:

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

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

9. Unravelling the Pegasus attack infrastructure over the years

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

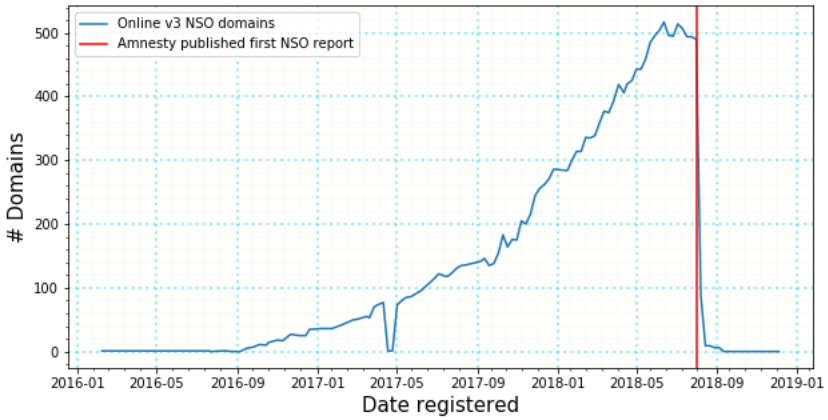
In August 2018, Amnesty International published a report "*Amnesty International Among Targets of NSO-powered Campaign*" which described the targeting of an Amnesty International staff member and a Saudi human rights defender. In this report, Amnesty International presented an excerpt of more than 600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

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

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

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

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



Amnesty International

9.1 Further attempts by NSO Group to hide their infrastructure

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

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

Amnesty International confirmed this domain was tied to NSO Group by observing distinctive Pegasus artefacts created on the device shortly after the infection URL was opened. With this new domain in hand, we were able to begin mapping the Pegasus **Version 4 (V4)** infrastructure.

NSO Group re-factored their infrastructure to introduce additional layers, which complicated discovery. Nevertheless, we could now observe at least 4 servers used in each infection chain.

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

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

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

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

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

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

   We assume that each infection webserver is part of the new generation **"Pegasus Anonymizing Transmission Network"**. Connections to the infection server are likely proxied back to the customer's Pegasus infrastructure.
4. **Command and Control server**: In previous generations of the PATN, NSO Group used separate domains for the initial infection and later communication with the spyware. The iPwn report from Citizen Lab provided evidence that Pegasus is again using separate domains for command and control. To avoid network-based discovery, the Pegasus spyware made direct connections the Pegasus C&C servers without first performing a DNS lookup or sending the domain name in the TLS SNI field.

9.2 Identifying other NSO attack domains

Amnesty International began by analysing the configuration of the infection domains and DNS servers used in the attacks against Moroccan journalists and human rights defenders.

Based on our knowledge of the domains used in Morocco we developed a fingerprint which identified 201 Pegasus Installation domains which had infrastructure active at the time of the initial scan. This set of 201 domains included both **urlpush[.]net** and **free247downloads[.]com**.

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

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

9.3 What can be learned from NSO Group's infrastructure

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

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

The V4 DNS server infrastructure began going offline in early 2021 following the Citizen Lab iPwn report which disclosed multiple Pegasus V4 domains.

Amnesty International suspects the shutting down of the V4 infrastructure coincided with NSO Group's shift to using cloud services such as Amazon CloudFront to deliver the earlier stages of their attacks. The use of cloud services protects NSO Group from some Internet scanning techniques.

9.4 Attack infrastructure hosted primarily in Europe and North America

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

Country	Servers per country
Germany	212
United Kingdom	79

Switzerland	36
France	35
United States	28
Finland	9
Netherlands	5
Canada	4
Ukraine	4
Singapore	3
India	3
Austria	3
Japan	1
Bulgaria	1
Lithuania	1
Bahrain	1

The following table shows the number of DNS servers hosted with each hosting provider. Most identified servers are assigned to the US-owned hosting companies Digital Ocean, Linode and Amazon Web Services (AWS).

Many hosting providers offer server hosting in multiple physical locations. Based on these two tables it appears that NSO Group is primarily using the European datacentres run by American hosting companies to run much of the attack infrastructure for its customers.

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

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

Domain name	DNS server IP	Network
drp32k77.todoinfonet.com	104.223.76.216	ASN-QUADRANET-GLOBAL
imgi64kf5so6k.transferlights.com	165.227.52.184	DIGITALOCEAN-ASN
pc43v65k.alignmentdisabled.net	167.172.215.114	DIGITALOCEAN-ASN
img54fsd3267h.prioritytrail.net	157.245.228.71	DIGITALOCEAN-ASN

jsfk3d43.netvisualizer.com	104.248.126.210	DIGITALOCEAN-ASN
cdn42js666.manydnsnow.com	138.197.223.170	DIGITALOCEAN-ASN
css1833iv.handcraftedformat.com	134.209.172.164	DIGITALOCEAN-ASN
js43fsf7v.opera-van.com	159.203.87.42	DIGITALOCEAN-ASN
pypip36z19.myfundsdns.com	167.99.105.68	DIGITALOCEAN-ASN
css912jy6.reception-desk.net	68.183.105.242	DIGITALOCEAN-ASN
imgi64kf5so6k.transferlights.com	206.189.214.74	DIGITALOCEAN-ASN
js85mail.preferenceviews.com	142.93.80.134	DIGITALOCEAN-ASN
css3218i.quota-reader.net	165.227.17.53	DIGITALOCEAN-ASN
mongo87a.sweet-water.org	142.93.113.166	DIGITALOCEAN-ASN
react12x2.towebsite.net	3.13.132.96	AMAZON-02
jsb8dmc5z4.gettingurl.com	13.59.79.240	AMAZON-02
react12x2.towebsite.net	3.16.75.157	AMAZON-02
cssgahs5j.redirigir.net	18.217.13.50	AMAZON-02
jsm3zsn5kewlmk9q.dns-analytics.com	18.225.12.72	AMAZON-02
imgcss35d.domain-routing.com	13.58.85.100	AMAZON-02
jsb8dmc5z4.gettingurl.com	18.191.63.125	AMAZON-02
js9dj1xzc8d.beanbounce.net	199.247.15.15	CHOOPA
jsid76api.buildyourdata.com	108.61.158.97	CHOOPA
cdn19be2.reloadinput.com	95.179.177.18	CHOOPA
srva9awf.syncingprocess.com	66.175.211.107	Linode
jsfk3d43.netvisualizer.com	172.105.148.64	Linode
imgdsg4f35.permalinking.com	23.239.16.143	Linode
srva9awf.syncingprocess.com	45.79.190.38	Linode

9.5 Infection domain resolutions observed in Passive DNS database

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

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

A subdomain will only be recorded in passive DNS records if the subdomain was successfully resolved and the resolution transited a network which was running a passive DNS probe.

This probe data is collected based on agreements between network operators and passive DNS data providers. Many networks will not be covered by such data collection agreements. For example, no passive DNS resolutions were recorded for either Pegasus infection domains used in Morocco.

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

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

nodesj44s.unusualneighbor.com	38
jsonapi2.linksnew.info	30
img9fo658tlsuh.securisurf.com	19
pc25f01dw.loading-url.net	12
dbm4kl5d3faqlk6.healthyguess.com	8
img359axw1z.reload-url.net	5
css2307.cssgraphics.net	5
info2638dg43.newip-info.com	3
img87xp8m.catbrushcable.com	2
img108jkn42.av-scanner.com	2
mongom5sxk8fr6.extractsight.com	2
img776cg3.webprotector.co	1
tv54d2ml1.topadblocker.net	1
drp2j4sdi.safecrusade.com	1
api1r3f4.redirectweburl.com	1
pc41g20bm.redirectconnection.net	1
jsj8sd9nf.randomlane.net	1
php78mp9v.opposedarrangement.net	1

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

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

10. Mobile devices, security and auditability

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

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

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

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

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

11. With our Methodology, we release our tools and indicators

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

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

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

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

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

Among others, some of the features MVT has include:

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

Acknowledgements

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

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

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

Appendix A: Peer review of Methodology Report by Citizen Lab

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

Appendix B: Suspicious iCloud Account Lookups

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

iCloud Account	Target
emmaholm575[@]gmail.com	• AZJRN1 – Khadija Ismayilova
filip.bl82[@]gmail.com	• AZJRN1 – Khadija Ismayilova
kleinleon1987[@]gmail.com	• AZJRN1 – Khadija Ismayilova

bergers.o79[@]gmail.com	• Omar Radi • FRHRL1 – Joseph Breham • FRHRL2 • FRJRN1 – Lenaig Bredoux • FRJRN2 • FRPOI1 • FRPOI2 – François de Rugy
naomiwerff772[@]gmail.com	• Omar Radi • FRHRL1 – Joseph Breham • FRPOI1
bogaardlisa803[@]gmail.com	• FRHRL1 – Joseph Breham • FRJRN1 – Lenaig Bredoux • FRJRN2
linakeller2203[@]gmail.com	• FRHRD1 – Claude Mangin • FRPOI3 – Philippe Bouyssou • FRPOI4 • FRPOI5 – Oubi Buchraya Bachir • MOJRN1 – Hicham Mansouri
jessicadavies1345[@]outlook.com	• HUJRN1 – András Szabó • HUJRN2 – Szabolcs Panyi
emmadavies8266[@]gmail.com	• HUJRN1 – András Szabó • HUJRN2 – Szabolcs Panyi
k.williams.enny74[@]gmail.com	• HUPOI1 • HUPOI2 – Adrien Beauduin • HUPOI3
taylorjade0303[@]gmail.com	• INHRD1 – SAR Geelani • INJRN6 – Smita Sharma • INPOI1 – Prashant Kishor
lee.85.holland[@]gmail.com	• INHRD1 – SAR Geelani • INJRN6 – Smita Sharma • INPOI1 – Prashant Kishor
bekkerfredi[@]gmail.com	• INHRD1 – SAR Geelani • INPOI2
herbruud2[@]gmail.com	• INJRN1 – Mangalam Kesavan Venu • INJRN2 – Sushant Singh • INPOI1 – Prashant Kishor
vincent.dahl76[@]gmail.com	• KASH01 – Hatice Cengiz • KASH02 – Rodney Dixon
oskarschalcher[@]outlook.com	• KASH03 – Wadah Khanfar
benjiburns8[@]gmail.com	• RWHRD1 – Carine Kanimba

Appendix C: Detailed Traces per Target

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

C.1 Forensic Traces Overview for Maati Monjib

Date (UTC)	Event
2017-11-02 12:29:33	Pegasus SMS with link to hxxps://tinyurl[.]com/y73qr7mb redirecting to hxxps://**revolution-news[.]co**/ikXFZ34ca
2017-11-02 16:42:34	Pegasus SMS with link to hxxps://**stopsms[.]biz**/vi78ELI
2017-11-02 16:44:00	Pegasus SMS with link to hxxps://**stopsms[.]biz**/vi78ELI from +212766090491

2017-11-02 16:45:10	Pegasus SMS with link to Hxxps://**stopsms[.]biz**/bi78ELI from +212766090491
2017-11-02 16:57:00	Pegasus SMS with link to Hxxps://**stopsms[.]biz**/bi78ELI from +212766090491
2017-11-02 17:13:45	Pegasus SMS with link to Hxxps://**stopsms[.]biz**/bi78ELI from +212766090491
2017-11-02 17:21:57	Pegasus SMS with link to Hxxps://**stopsms[.]biz**/bi78ELI from +212766090491
2017-11-02 17:30:49	Pegasus SMS with link to Hxxps://**stopsms[.]biz**/bi78ELI from +212766090491
2017-11-02 17:40:46	Pegasus SMS with link to Hxxps://**stopsms[.]biz**/bi78ELI from +212766090491
2017-11-15 17:05:17	Pegasus SMS with link to hxxps://**videosdownload[.]co**/nBBJBIP
2017-11-20 18:22:03	Pegasus SMS with link to hxxps://**infospress[.]com**/LqoHgMCEE
2017-11-24 13:43:17	Pegasus SMS with link to hxxps://tinyurl[.]com/y9hbdqm5 redirecting to hxxps://**hmizat[.]co**/JaCTkfEp
2017-11-24 17:26:09	Pegasus SMS with link to hxxps://**stopsms[.]biz**/2Kj2ik6
2017-11-27 15:56:10	Pegasus SMS with link to hxxps://**stopsms[.]biz**/yTnWt1Ct
2017-11-27 17:32:37	Pegasus SMS with link to hxxps://**hmizat[.]co**/ronEKDVaf
2017-12-07 18:21:57	Pegasus SMS with link to hxxp://tinyurl[.]com/y7wdcd8z redirecting to hxxps://**infospress[.]com**/Ln3HYK4C
2018-01-08 12:58:14	Pegasus SMS with link to hxxp://tinyurl[.]com/y87hnl3o redirecting to hxxps://**infospress[.]com**/asjmXqiS
2018-02-09 21:12:49	Process: **pcsd**
2018-03-16 08:24:20	Process: **pcsd**
2018-04-28 22:25:12	Process: **bh**
2018-05-04 21:30:45	Process: **pcsd**
2018-05-21 21:46:06	Process: **fmld**

2018-05-22 17:36:51	Process: **bh**
2018-06-04 11:05:43	Process: **fmld**
2019-03-27 21:45:10	Process: **bh**
2019-04-14 23:02:41	Safari favicon from URL hxxps://c7r8x8f6zecd8j.get1tn0w.**free247downloads[.]com**:30352/Ld3xuuW5
2019-06-27 20:13:10	Safari favicon from URL hxxps://3hdxu4446c49s.get1tn0w.**free247downloads[.]com**:30497/pczrccr#05204587120282683733730818475002323863084688
2019-07-22 15:42:32	Safari visit to hxxps://bun54l2b67.get1tn0w.**free247downloads[.]com**:30495/szev4hz
2019-07 22 15:42:32	Safari visit to hxxps://bun54l2b67.get1tn0w.**free247downloads[.]com**:30495/szev4hz#048634787343287485982474853012724998054718494423
2019-07-22 15:43:06	Safari favicon from URL hxxps://bun54l2b67.get1tn0w.**free247downloads[.]com**:30495/szev4hz#048634787343287485982474853012724998054718494423
n/a	WebKit IndexedDB file for URL hxxps://c7r8x8f6zecd8j.get1tn0w.**free247downloads[.]com**
n/a	WebKit IndexedDB file for URL hxxps://bun54l2b67.get1tn0w.**free247downloads[.]com**
n/a	WebKit IndexedDB file for URL hxxps://keewrq9z.get1tn0w.**free247downloads[.]com**
n/a	WebKit IndexedDB file for URL hxxps://3hdxu4446c49s.get1tn0w.**free247downloads[.]com**

C.2 Forensic Traces Overview for Omar Radi

Date (UTC)	Event
2019-02-11 14:45:45	Webkit IndexedDB file for URL hxxps://d9z3sz93x5ueidq3.get1tn0w.**free247downloads[.]com**
2019-02-11 13:45:53	Safari favicon from URL hxxps://d9z3sz93x5ueidq3.get1tn0w.**free247downloads[.]com**:30897/rdEN5YP
2019-02-11 13:45:56	Process: **bh**
2019-02-11 13:46:16	Process: **roleaboutd**
2019-02-11 13:46:23	Process: **roleaboutd**
2019-02-11 16:05:24	Process: **roleaboutd**
2019-08-16 17:41:06	iMessage lookup for account **bergers.o79[@]gmail.com**
2019-09-13 15:01:38	Safari favicon for URL hxxps://2far1v4lv8.get1tn0w.**free247downloads[.]com**:31052/meunsnyse#0113565702571172968348457040223389731330224333

2019-09-13 15:01:56	Safari favicon for URL hxxps://2far1v4lv8.get1tn0w.**free247downloads[.]com**:31052/meunsnyse#06809956161462627851992535863878916157242783364
2019-09-13 15:02:11	Process: **bh**
2019-09-13 15:02:20	Process: **msgacntd**
2019-09-13 15:02:33	Process: **msgacntd**
2019-09-14 15:02:57	Process: **msgacntd**
2019-09-14 18:51:54	Process: **msgacntd**
2019-10-29 12:21:18	iMessage lookup for account **naomiwerff772[@]gmail.com**
2020-01-27 10:06:24	Safari favicon for URL hxxps://gnyjv1xltx.info8fvhgl3.**urlpush[.]net**:30875/zrnv5revj#07419641982798791927400154862273891983555674832594 6
2020-01-27 10:06:26	Safari visit to hxxps://gnyjv1xltx.info8fvhgl3.**urlpush[.]net**:30875/zrnv5revj#07419641982798791927400154862273891983555674832594 6#2
2020-01-27 10:06:26	Safari visit to hxxps://gnyjv1xltx.info8fvhgl3.**urlpush[.]net**:30875/zrnv5revj#07419641982798791927400154862273891983555674832594 6#24
2020-01-27 10:06:32	Safari favicon for URL hxxps://gnyjv1xltx.info8fvhgl3.**urlpush[.]net**:30875/zrnv5revj#07419641982798791927400154862273891983555674832594 6%2324

Appendix D: Pegasus Forensic Traces per Target

Appendix D can be found here.

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

[2] Email to Amnesty International, May 2021

[3] Email to Amnesty International, July 2021.