Forensics Analysis of the NSO Group's Pegasus Spyware

lifars.com/2022/01/forensics-analysis-of-the-nso-groups-pegasus-spyware/

January 12, 2022

NSO's Group Pegasus spyware was mentioned multiple times during 2021 in the media. It has been heavily analyzed by organizations such as Amnesty International [1] and the University of Toronto's Citizen Lab [2] [3] [4] [5].

The targets included journalists from Azerbaijan, France, Hungary, India, French human rights lawyers, French human rights activists, Rwandan activists, and Indian human rights activists. Citizen Lab also identified Bahraini activists, New York Times Journalist Ben Hubbard, and Palestinian human rights defenders as victims.

The Pegasus spyware has been distributed via one-click attacks (the target needs to click on a malicious link received via SMS messages, WhatsApp, etc.) and zero-click attacks (no interaction needed). Some of the recently used 0-day exploits developed by NSO Group include KISMET and FORCEDENTRY (also called Megalodon). It's important to mention that Apple patched all the vulnerabilities submitted regarding these attacks, and it's crucial to update your iOS devices regularly.

The FORCEDENTRY exploit has been analyzed by Google [6] and TrendMicro [7]. It has been attributed a CVE identifier of CVE-2021-30860 and represents a vulnerability in the CoreGraphics PDF parser. It is an integer overflow vulnerability which leads to out-of-bounds write. The crashing point inside the function JBIG2Stream::readTextRegionSeg is displayed below:

Source: TrendMicro

The Google Project Zero team performed a deep dive into the exploit and explained that the attackers could define a small computer architecture with registers and a 64-bit adder and comparator. It is computationally equivalent to JavaScript, and the team concluded that this is one of the most technically sophisticated exploits they've ever analyzed.

LIFARS team analyzed a suspected infection with Pegasus using the Mobile Verification Toolkit released by the Amnesty International Security Lab [8]. We've also used the NSO Group Pegasus IOCs (domains, iCloud accounts, files, process names) in our investigation [9].

We were able to identify six Pegasus processes that ran on the victim's iPhone. The infection occurred on February 1st, which coincided with when the NSO group deployed the FORCEDENTRY iMessage Zero-Click mentioned by the CitizenLab in their report [3].

Wifi In (MB)	Wifi Out (MB)	Wan In (MB)	Wan Out (MB)	Timestamp (UTC)	Process Name

1.6554	0.178541	0	0	2/1/2021 13:02:30	wifip2ppd
0.007	0.0019	0	0	2/1/2021 13:02:31	ABSCarryLog
29.8661	99.8687	1.2749	1.0464	2/1/2021 13:03:00	misbrigd
1.6548	0.1939	0	0	2/11/2021 23:31:38	cfprefssd
0.007	0.0019	0	0	2/11/2021 23:31:38	gssdp
75.6967	58.8612	7.6284	4.99	2/11/2021 23:32:04	libbmanaged

As shown in the table above, two processes performed data exfiltration. The libbmanaged process was running for over a week, based on a record from the DataUsage.sqlite database:

Wifi In (MB)	Wifi Out (MB)	Wan In (MB)	Wan Out (MB)	Timestamp (UTC)	Process Name
0	0	7.99	5.07	2/19/2021 1:16:18	libbmanaged

Before the malicious processes ran, we've identified the following process related to iMessage processing:

Wifi In (MB)	Wifi Out (MB)	Wan In (MB)	Wan Out (MB)	Timestamp (UTC)	Process Name
0	0	15.0895	0.4087	2/1/2021 12:52:55	IMTransferAgent

The file "/private/var/mobile/Library/Preferences/com.apple.identityservices.idstatuscache.plist" used by Amnesty International's Security Lab to extract the suspicious iMessage account lookups is missing in our case. The netusage.sqlite SQLite database is also missing, and we couldn't extract records from the Cache.db databases because we couldn't jailbreak the device.

The Pegasus spyware remains an active threat even if the NSO Group has been sanctioned by the United States. We recommend rebooting your iPhone daily in order to remove non-persistent malware.

References

[1] https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/
[2] https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/
[3] https://citizenlab.ca/2021/08/bahrain-hacks-activists-with-nso-group-zero-click-iphone-exploits/
[4] https://citizenlab.ca/2021/10/breaking-news-new-york-times-journalist-ben-hubbard-pegasus/
[5] https://citizenlab.ca/2021/11/palestinian-human-rights-defenders-hacked-nso-groups-pegasus-spyware/
[6] https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html
[7] https://www.trendmicro.com/en_us/research/21/i/analyzing-pegasus-spywares-zero-click-iphone-exploit-forcedentry.html
[8] https://github.com/mvt-project/mvt
[9] https://github.com/AmnestyTech/investigations/tree/master/2021-07-18_nso