Research > Targeted Threats

FORCEDENTRY

NSO Group iMessage Zero-Click Exploit Captured in the Wild

By Bill Marczak, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, and Ron Deibert

September 13, 2021

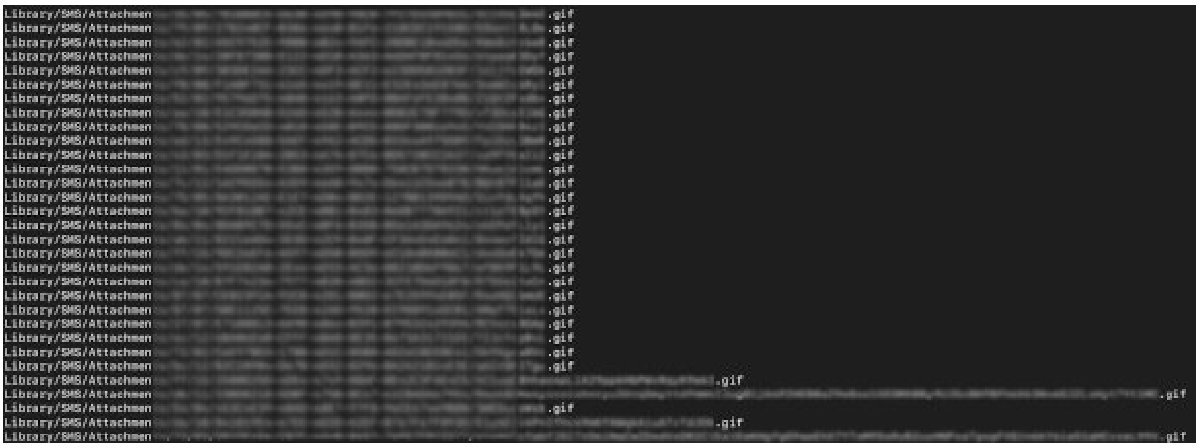
Summary

- While analyzing the phone of a Saudi activist infected with NSO Group's Pegasus spyware, we discovered a zero-day zero-click exploit against iMessage. The exploit, which we call ***FORCEDENTRY***, targets Apple's image rendering library, and was effective against Apple iOS, MacOS and WatchOS devices.
- We determined that the mercenary spyware company NSO Group used the vulnerability to remotely exploit and infect the latest Apple devices with the Pegasus spyware. We believe that ***FORCEDENTRY*** has been in use since at least February 2021.
- The Citizen Lab disclosed the vulnerability and code to Apple, which has assigned the ***FORCEDENTRY*** vulnerability CVE-2021-30860 and describes the vulnerability as "processing a maliciously crafted PDF may lead to arbitrary code execution."
- Today, September 13th, Apple is releasing an update that patches CVE-2021-30860. We urge readers to immediately update all Apple devices.

Devices affected by CVE-2021-30860 per Apple:
All iPhones with **iOS versions *prior to* 14.8**, All Mac computers with operating system versions ***prior to* OSX Big Sur 11.6**, **Security Update 2021-005 Catalina**, and all Apple Watches ***prior to* watchOS 7.6.2**.

Discovery

In March 2021, we examined the phone of a Saudi activist who has chosen to remain anonymous, and determined that they had been hacked with NSO Group's Pegasus spyware. During the course of the analysis we obtained an iTunes backup of the device.



```
Library/SMS/Attachmen[redacted].gif
Library/SMS/Attachmen[redacted].gif
Library/SMS/Attachmen[redacted].gif
Library/SMS/Attachmen[redacted].gif
Library/SMS/Attachmen[redacted].gif
Library/SMS/Attachmen[redacted].gif
Library/SMS/Attachmen[redacted].gif
Library/SMS/Attachmen[redacted].gif
Library/SMS/Attachmen[redacted].gif
Library/SMS/Attachmen[redacted].gif
Library/SMS/Attachmen[redacted].gif
Library/SMS/Attachmen[redacted].gif
Library/SMS/Attachmen[redacted].gif
Library/SMS/Attachmen[redacted].gif
Library/SMS/Attachmen[redacted].gif
Library/SMS/Attachmen[redacted].gif
Library/SMS/Attachmen[redacted].gif
Library/SMS/Attachmen[redacted].gif
Library/SMS/Attachmen[redacted].gif
Library/SMS/Attachmen[redacted].gif
Library/SMS/Attachmen[redacted].gif
Library/SMS/Attachmen[redacted].gif
Library/SMS/Attachmen[redacted].gif
Library/SMS/Attachmen[redacted].gif
Library/SMS/Attachmen[redacted].gif
Library/SMS/Attachmen[redacted].gif
Library/SMS/Attachmen[redacted].gif
Library/SMS/Attachmen[redacted].gif
Library/SMS/Attachmen[redacted].gif
Library/SMS/Attachmen[redacted].gif
Library/SMS/Attachmen[redacted].gif
```

Figure 1: The GIF files we found on the phone.

Recent re-analysis of the backup yielded several files with the “**.gif**” extension in **Library/SMS/Attachments** that we determined were sent to the phone immediately before it was hacked with NSO Group’s Pegasus spyware.

Payload

The files were:

- 27 copies of an identical file with the “.gif” extension. Despite the extension, the file was actually a 748-byte Adobe PSD file. Each copy of this file caused an IMTranscoderAgent crash on the device. These files each had random-looking ten-character filenames.
- Four different files with the “.gif” extension that were actually Adobe PDF files containing a JBIG2-encoded stream. Two of these files had 34-character names, and two had 97-character names.
- The output of the *pdfid* tool on these four “.gif” files was (NB: the stream had varying length):

```
PDF Comment '%PDF-1.3\n\n'

obj 1 0
 Type: /XRef
 Referencing:
 Contains stream

  << /Type /XRef /Size 9 /W [1 3 1] /Length ... /Filter [/FlateDecode /FlateDecode /JBIG2Decode]


trailer
  << /Size 2 >>
```

```
startxref 10


PDF Comment '%%EOF\n'
```

Discovery and Disclosure

Because the format of the files matched two types of crashes we had observed on another phone when it was hacked with Pegasus, we suspected that the ".gif" files might contain parts of what we are calling the ***FORCEDENTRY*** exploit chain.

Citizen Lab forwarded the artifacts to Apple on Tuesday, September 7. On Monday, September 13, Apple confirmed that the files included a zero-day exploit against iOS and MacOS. They designated the ***FORCEDENTRY*** exploit CVE-2021-30860, and describe it as "*processing a maliciously crafted PDF may lead to arbitrary code execution*."

The exploit works by exploiting an integer overflow vulnerability in Apple's image rendering library (CoreGraphics). We are publishing limited technical information about CVE-2021-30860 at this time.

Attribution to NSO Group

We observed multiple distinctive elements that allowed us to make a high-confidence attribution to NSO Group:

- The spyware installed by the ***FORCEDENTRY*** exploit exhibited a forensic artifact that we call ***CASCADEFAIL***, which is a bug whereby evidence is incompletely deleted from the phone's DataUsage.sqlite file. In ***CASCADEFAIL***, an entry from the file's ZPROCESS table is deleted, but not entries in the ZLIVEUSAGE table that refer to the deleted ZPROCESS entry. We have only ever seen this type of incomplete deletion associated with NSO Group's Pegasus spyware, and we believe that the bug is distinctive enough to point back to NSO. The specific CASCADEFAIL artifact can be detected by

```
SELECT "CASCADEFAIL" FROM ZLIVEUSAGE WHERE ZLIVEUSAGE.ZHASPROCESS NOT IN (SELECT Z_PK FROM ZPROC
```

- The spyware installed by the ***FORCEDENTRY*** exploit used multiple process names, including the name "setframed". That process name was used in an attack with NSO Group's Pegasus spyware on an Al Jazeera journalist in July 2020. Notably, we did not publish that detail at the time.

Previous NSO Zero-Click Exploits

FORCEDENTRY is the latest in a string of zero-click exploits linked to NSO Group. In 2019, WhatsApp fixed CVE-2019-3568, a zero-click vulnerability in WhatsApp calling that NSO Group used against more than 1400 phones in a two-week period during which it was observed, and in 2020, NSO Group employed the ***KISMET*** zero-click iMessage exploit.

To our knowledge, the ***KISMET*** vulnerability was never publicly identified, though we suspect that the underlying vulnerability (if it still exists) can no longer be exploited via iMessage due to Apple's introduction of the BlastDoor mitigation in iOS14. We suspect that NSO Group developed ***FORCEDENTRY***, which circumvents BlastDoor, in response to this mitigation.

Conclusion

Despite promising their customers the utmost secrecy and confidentiality, NSO Group's business model contains the seeds of their ongoing unmasking. Selling technology to governments that will use the technology recklessly in violation of international human rights law ultimately facilitates discovery of the spyware by investigatory watchdog organizations, as we and others have shown on multiple prior occasions, and as was the case again here.

In 2016, we titled our report on the discovery of an iOS and MacOS Apple zero-day the "Million Dollar Dissident." The title was chosen to reflect the huge sums that autocratic governments are willing to pay to hack their critics. Mercenary spyware companies devote substantial resources to identifying software vulnerabilities on widely used applications and then package those exploits to eager government clients, creating a highly lucrative but widely abused commercial surveillance marketplace.

Our latest discovery of yet another Apple zero day employed as part of NSO Group's arsenal further illustrates that companies like NSO Group are facilitating "despotism-as-a-service" for unaccountable government security agencies. Regulation of this growing, highly profitable, and harmful marketplace is desperately needed.

Our finding also highlights the paramount importance of securing popular messaging apps. Ubiquitous chat apps have become a major target for the most sophisticated threat actors, including nation state espionage operations and the mercenary spyware companies that service them. As presently engineered, many chat apps have become an irresistible soft target. Without intense engineering focus, we believe that they will continue to be heavily targeted, and successfully exploited.

Acknowledgements

We thank the targets of Pegasus spyware that have allowed us to analyze their devices, with a special thanks to the individual that worked with us on this case. It is thanks to them, and their bravery, that we were able to make this discovery.

Special thanks to all at Apple for quick and responsive action.

Thanks to our Citizen Lab colleagues for feedback and editing.

Thanks to TNG.

Share:

RESEARCH

Targeted Threats

Free Expression Online

Transparency and Accountability

App Privacy and Controls

Global Research Network

Tools & Resources

All Publications

NEWS

In the Media

Events

Opportunities

Newsletter Archives

ABOUT

About the Citizen Lab

People

Media Resources

Teaching

Donate

CONNECT

NEWSLETTER

Your email address Sign up

Privacy Policy

Unless otherwise noted this site and its contents are licensed under a Creative Commons Attribution 2.5 Canada license.

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

UNIVERSITY OF
TORONTO