These hackers are using Android surveillance malware to target opponents of the Syrian government

By Written by Danny Palmer, Senior WriterSenior Writer Dec. 10, 2018 at 3:15 a.m. PT

Archived: 2026-04-05 20:00:15 UTC

Hackers working on behalf of the Syrian government are targeting political opponents with surveillance malware being distributed in trojanised versions of messaging applications including WhatsApp and Telegram.

Security

-
-
-
-

The Syrian Electronic Army group of hackers works in support of Syrian President Bashar Al-Assad and targets groups and individuals opposed to his regime. The group also has a history of hacking into and defacing websites -- including that of the US army -- and social media accounts, the most high profile of which saw the Twitter account of the Associated Press compromised.

Such is the notoriety of the SEA that the US charged three Syrian nationals with being members of the group in 2016, with two added to the FBI's Most Wanted List.

In recent years, the group has seemingly kept a low profile, but the SEA hasn't ceased activity: it's altered tactics and is now delivering custom Android malware to opponents of the Assad regime for the purposes of surveillance.

Dubbed SilverHawk by researchers at security firm Lookout, they detailed their findings at the Black Hat Europe conference in London. The malware is thought to have been in operation since mid-2016 and is capable of secretly recording audio, taking photos, downloading files, monitoring contacts, tracking location and more.

"You can imagine the implications for political dissidents who might be in sensitive meetings and the enemy would love to know what they're talking about -- if their phone's infected, they can just remotely start recording audio," said Kristin Del Rosso, security intelligence engineer at Lookout.

SEE: Cyberwar predictions for 2019: The stakes have been raised

The Google Android malware isn't widely spread, suggesting that the SEA is using it sparingly in highly targeted campaigns. The main method of delivering SilverHawk is by tricking victims into downloading malicious versions of messaging apps from watering hole sites or social engineering via phishing emails.

"Typically you'll see this deployed inside trojanised secure messaging applications, secure connectivity applications and that was the case here," said Michael Flossman, head of threat intelligence at Lookout. "The

threat actors behind this really favour trojanising updates to WhatsApp, Telegram as well as a system package update."

To help remain undetected, the malicious app doesn't place an icon on the home screen. SilverHawk has also been built to avoid the rapid battery drain which can be a telltale sign that a malicious app has been installed. The creators of the malware have built in a survival counter that gives it two attempts to connect back to its command and control servers.

"What happens is every time there's a connection to the command and control servers that's successful, it resets to two, then every time a connection isn't made or the C2 server is down it drops down by one," Del Rosso explained.

"When the device is rebooted, however, the counter is back to 2, allowing the surveillance-ware to attempt to continue its spying abilities," she added. It also prevents repeated attempts at connection from draining the battery and arousing suspicion that something is wrong.

Analysis by Lookout suggests that SilverHawk has been successful in carrying out its tasks and remaining stealthy as the malware has rarely needed to be reworked to avoid detection by security solutions, and when changes have been made, they're relatively minor.

https://www.zdnet.com/article/what-is-malware-everything-you-need-to-know-about-viruses-trojans-and-malicious-software/

SEE: Can Russian hackers be stopped? Here's why it might take 20 years (TechRepublic cover story) | download the PDF version

While SilverHawk only targets Google Android on mobile devices, the Syrian Electronic Army is also known to target dissidents using Windows malware, with delivery typically via phishing emails containing attachments related to military operations in the region. Common forms of malware used in these campaigns include NjRAT, H-Worm Plus and DarkComet.

In instances of both the Android and Windows campaigns the use of open directories and poor operational security by the attackers has enabled Lookout to attribute the attacks to the SEA.

"There is no indication that they are using this tooling or the associated infrastructure that we've identified in targeted attacks against western interests at this time," Flossman told ZDNet.

However, he has advice for anyone who might be asked to install a version of a messaging service which asks for total control of the phone in exchange for installing the app.

"You should probably not fall for what they're saying when they ask for administrator access as that'll give them compromising control over your device," he said.

READ MORE ON CYBER CRIME

- **Hackers are using this Android malware to spy on Israeli soldiers**
- **How a Facebook page sent one Syrian dissenter to prison CNET**

- **Cyber security: Hackers step out of the shadows with bigger, bolder attacks**
- **The future of cyberwar: Weaponised ransomware, IoT attacks and a new arms race** **TechRepublic**
- **Too little, too late? Should we be faster to point the finger of blame at cyber attackers?**
