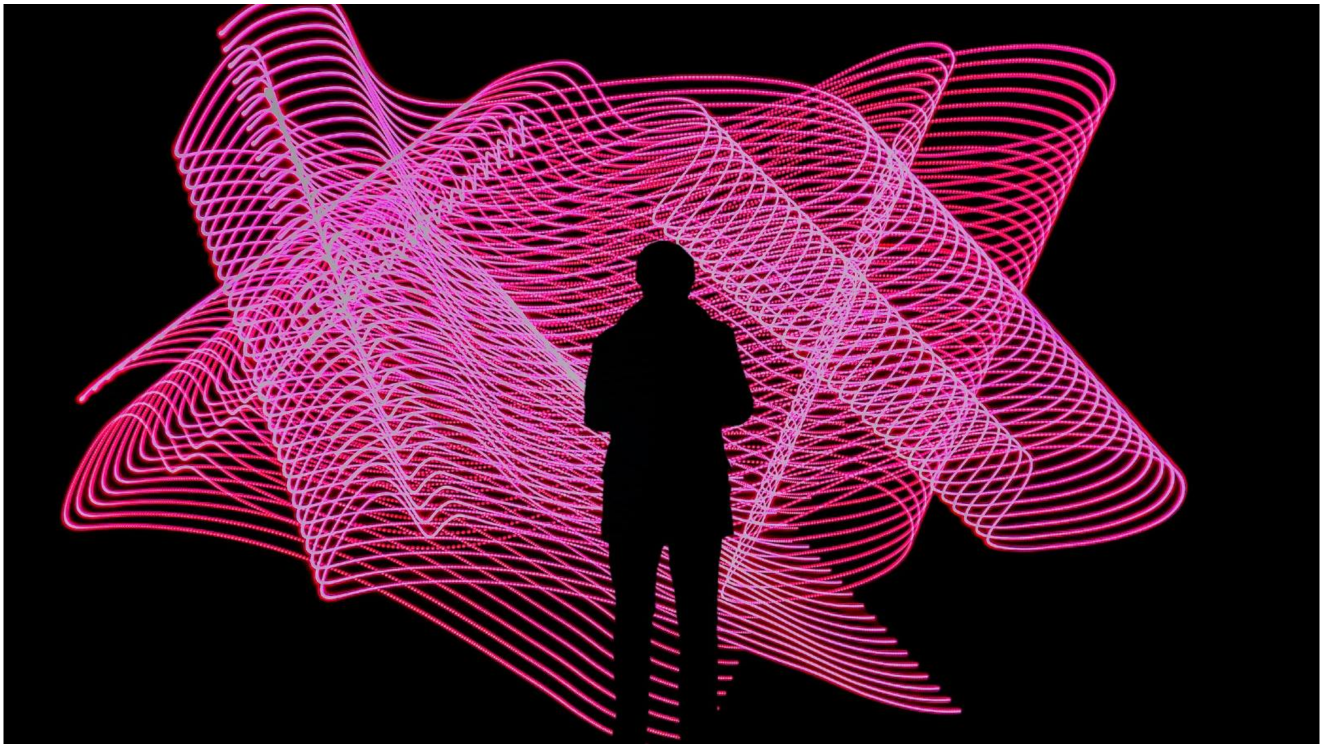
Google: Predator spyware infected Android devices using zero-days

bleepingcomputer.com/news/security/google-predator-spyware-infected-android-devices-using-zero-days/

Sergiu Gatlan

By
Sergiu Gatlan

- May 22, 2022
- 10:00 AM
- 0



Google's Threat Analysis Group (TAG) says that state-backed threat actors used five zero-day vulnerabilities to install Predator spyware developed by commercial surveillance developer Cytrox.

In these attacks, part of three campaigns that started between August and October 2021, the attackers used zero-day exploits targeting Chrome and the Android OS to install Predator spyware implants on fully up-to-date Android devices.

"We assess with high confidence that these exploits were packaged by a single commercial surveillance company, Cytrox, and sold to different government-backed actors who used them in at least the three campaigns discussed below," said Google TAG members Clement Lecigne and Christian Resell.

The government-backed malicious actors who purchased and used these exploits to infect Android targets with spyware are from Egypt, Armenia, Greece, Madagascar, Côte d'Ivoire, Serbia, Spain, and Indonesia, according to Google's analysis.

These findings align with a report on Cytrox mercenary spyware published by CitizenLab in December 2021, when its researchers discovered the malicious tool on the phone of exiled Egyptian politician Ayman Nour.

Nour's phone was also infected with NSO Group's Pegasus spyware, with the two tools being operated by two different government clients per CitizenLab's assessment.

Zero-days exploited in three campaigns targeting Android users

The five previously unknown 0-day security vulnerabilities used in these campaigns include:

- CVE-2021-37973, CVE-2021-37976, CVE-2021-38000, CVE-2021-38003 in Chrome
- CVE-2021-1048 in Android

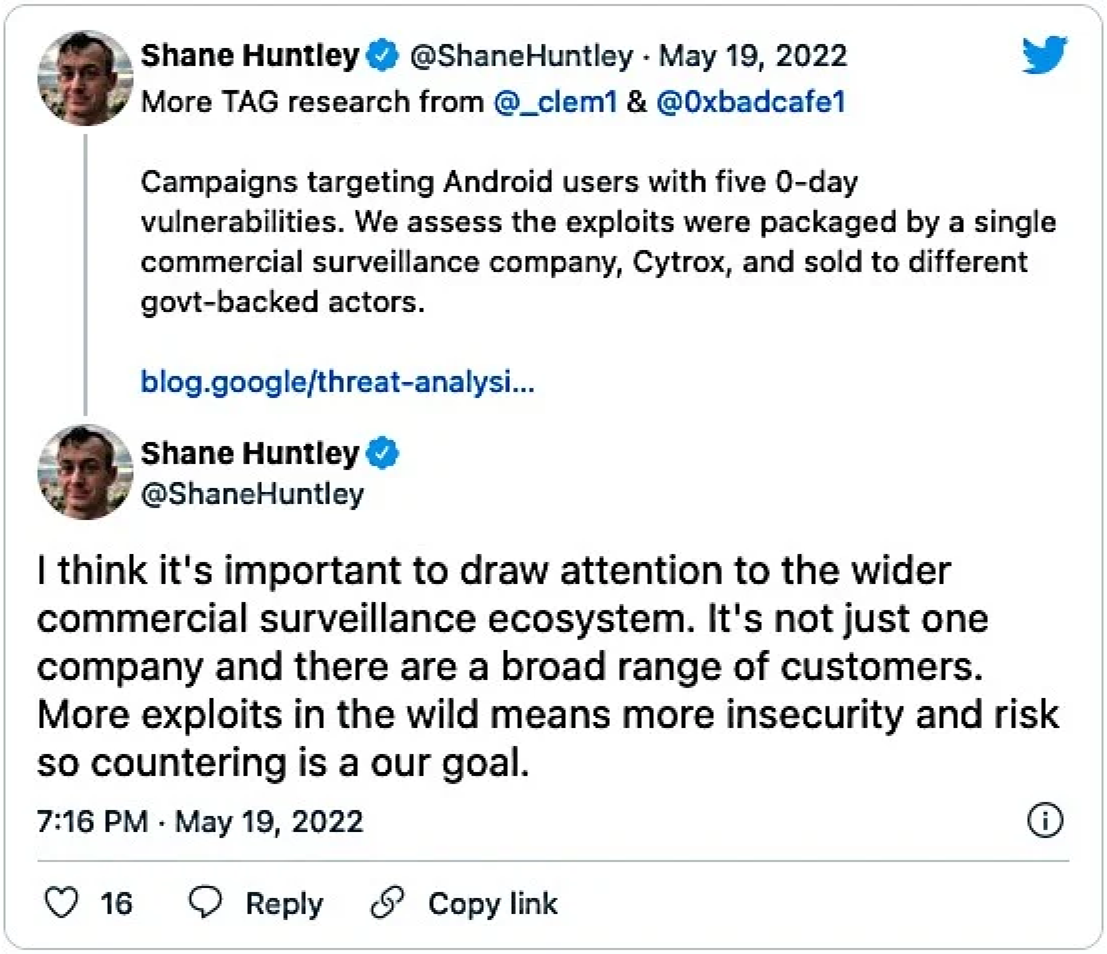
The threat actors deployed exploits targeting these zero-days in three separate campaigns:

- Campaign #1 - redirecting to SBrowser from Chrome (CVE-2021-38000)
- Campaign #2 - Chrome sandbox escape (CVE-2021-37973, CVE-2021-37976)
- Campaign #3 - Full Android 0-day exploit chain (CVE-2021-38003, CVE-2021-1048)

"All three campaigns delivered one-time links mimicking URL shortener services to the targeted Android users via email. The campaigns were limited — in each case, we assess the number of targets was in the tens of users," the Google TAG analysts added.

"Once clicked, the link redirected the target to an attacker-owned domain that delivered the exploits before redirecting the browser to a legitimate website. If the link was not active, the user was redirected directly to a legitimate website."

This attack technique was also used against journalists and other Google users who were alerted that they were the target of government-backed attacks.



Shane Huntley @ShaneHuntley · May 19, 2022
More TAG research from @_clem1 & @0xbadcafe1

Campaigns targeting Android users with five 0-day vulnerabilities. We assess the exploits were packaged by a single commercial surveillance company, Cytrox, and sold to different govt-backed actors.

blog.google/threat-analysi...

Shane Huntley
@ShaneHuntley

I think it's important to draw attention to the wider commercial surveillance ecosystem. It's not just one company and there are a broad range of customers. More exploits in the wild means more insecurity and risk so countering is a our goal.

7:16 PM · May 19, 2022

Spyware implant dropped using Android banking trojan

In these campaigns, the attackers first installed the Android Alien banking trojan with RAT functionality used to load the Predator Android implant, allowing recording audio, adding CA certificates, and hiding apps.

This report is a follow-up to a July 2021 analysis of four other 0-day flaws discovered in 2021 in Chrome, Internet Explorer, and WebKit (Safari).

As Google TAG researchers revealed, Russian-backed government hackers linked to the Russian Foreign Intelligence Service (SVR) exploited the Safari zero-day to target iOS devices belonging to government officials from western European countries.

"TAG is actively tracking more than 30 vendors with varying levels of sophistication and public exposure selling exploits or surveillance capabilities to government-backed actors," Google TAG added on Thursday.

Related Articles:

Mozilla fixes Firefox, Thunderbird zero-days exploited at Pwn2Own

Google: Chinese state hackers keep targeting Russian govt agencies

Google gives 50% bonus to Android 13 Beta bug bounty hunters

Google Play Store now forces apps to disclose what data is collected

Google Chrome emergency update fixes zero-day used in attacks