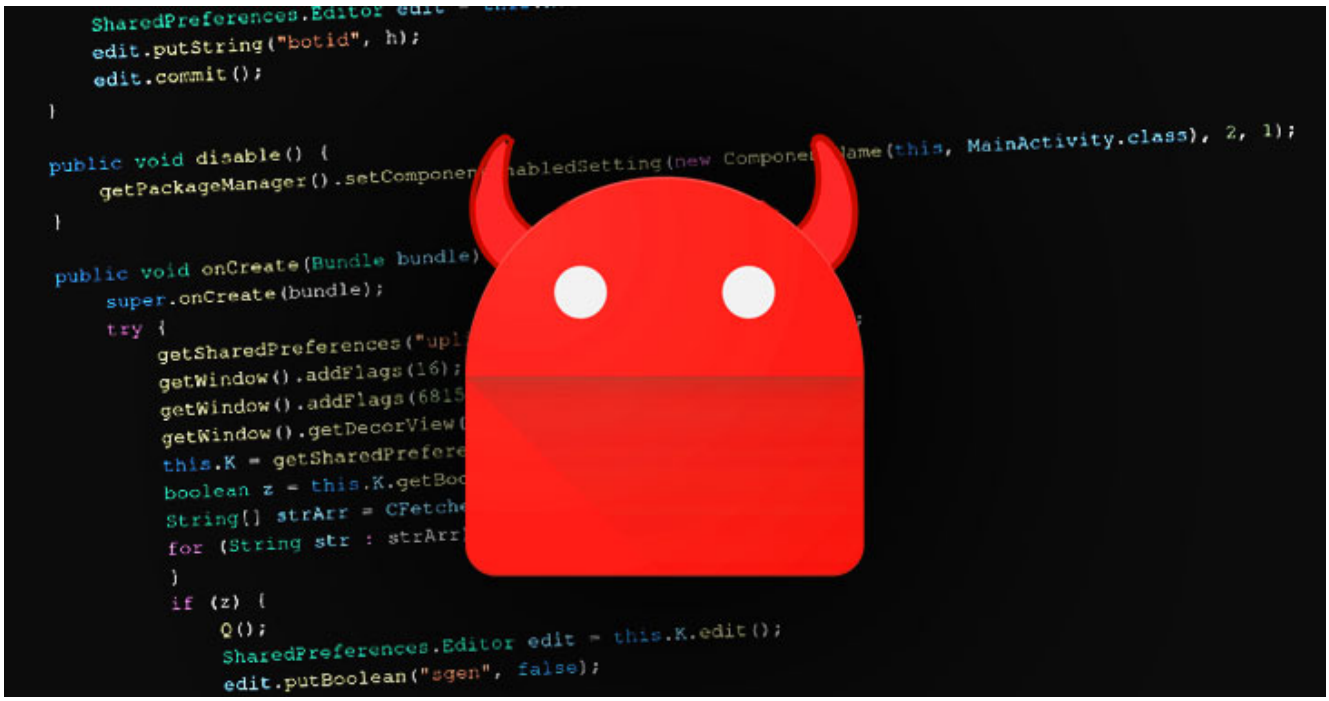
Cytrox's Predator Spyware Targeted Android Users with Zero-Day Exploits

thehackernews.com/2022/05/cytroxs-predator-spyware-target-android.html

May 20, 2022



Google's Threat Analysis Group (TAG) on Thursday pointed fingers at a North Macedonian spyware developer named Cytrox for developing exploits against five zero-day (aka 0-day) flaws, four in Chrome and one in Android, to target Android users.

"The 0-day exploits were used alongside n-day exploits as the developers took advantage of the time difference between when some critical bugs were patched but not flagged as security issues and when these patches were fully deployed across the Android ecosystem," TAG researchers Clement Lecigne and Christian Resell said.

Cytrox is alleged to have packaged the exploits and sold them to different government-backed actors located in Egypt, Armenia, Greece, Madagascar, Côte d'Ivoire, Serbia, Spain, and Indonesia, who, in turn, weaponized the bugs in at least three different campaigns.

The commercial surveillance company is the maker of Predator, an implant analogous to that of NSO Group's Pegasus, and is known to have developed tools that enables its clients to penetrate iOS and Android devices.

In December 2021, Meta Platforms (formerly Facebook) disclosed that it had acted to remove roughly 300 accounts on Facebook and Instagram that the company used as part of its compromise campaigns.

The list of the five exploited zero-day flaws in Chrome and Android is below -

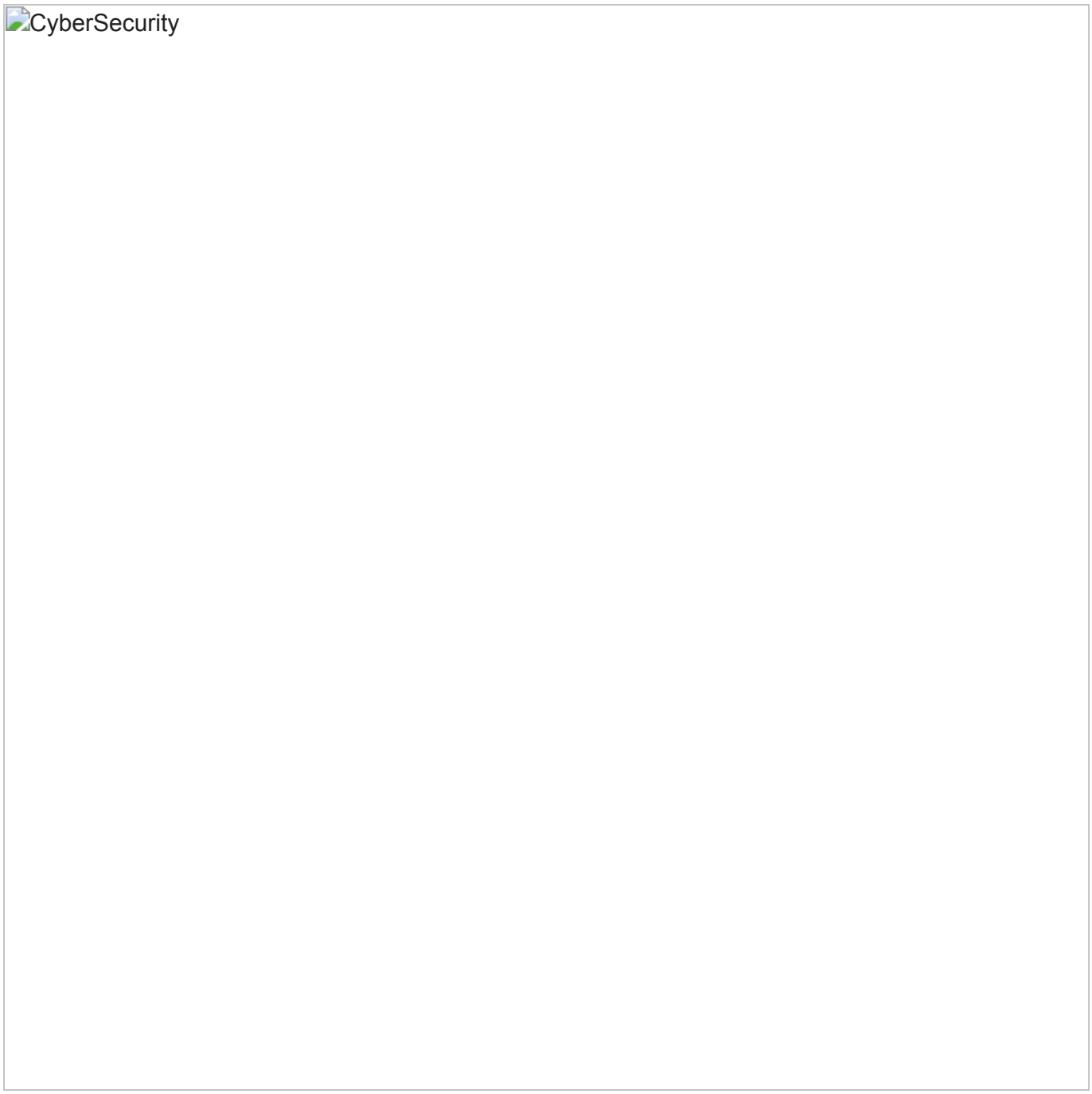
- **CVE-2021-37973** - Use-after-free in Portals API
- **CVE-2021-37976** - Information leak in core
- **CVE-2021-38000** - Insufficient validation of untrusted input in Intents (root cause analysis)
- **CVE-2021-38003** - Inappropriate implementation in V8, and
- **CVE-2021-1048** - Use-after-free in Android kernel (root cause analysis)

According to TAG, all the three campaigns in question commenced with a spear-phishing email that contained one-time links mimicking URL shortener services that, once clicked, redirected the targets to a rogue domain that dropped the exploits before taking the victim to an authentic site.

"The campaigns were limited — in each case, we assess the number of targets was in the tens of users," Lecigne and Resell noted. "If the link was not active, the user was redirected directly to a legitimate website."

The ultimate goal of the operation, the researchers assessed, was to distribute a malware dubbed Alien, which acts as a precursor for loading Predator onto infected Android devices.

The "simple" malware, which receives commands from Predator over an inter process communication (IPC) mechanism, is engineered to record audio, add CA certificates, and hide apps to evade detection.



The first of the three campaigns took place in August 2021. It used Google Chrome as a jumping off point on a Samsung Galaxy S21 device to force the browser to load another URL in the Samsung Internet browser without requiring user interaction by exploiting CVE-2021-38000.

Another intrusion, which occurred a month later and was delivered to an up-to-date Samsung Galaxy S10, involved an exploit chain using CVE-2021-37973 and CVE-2021-37976 to escape the Chrome sandbox (not to be confused with Privacy Sandbox), leveraging it to drop a second exploit to escalate privileges and deploy the backdoor.

The third campaign — a full Android 0-day exploit — was detected in October 2021 on an up-to-date Samsung phone running the then latest version of Chrome. It strung together two flaws, CVE-2021-38003 and CVE-2021-1048, to escape the sandbox and compromise the system by injecting malicious code into privileged processes.

Google TAG pointed out that while CVE-2021-1048 was fixed in the Linux kernel in September 2020, it wasn't backported to Android until last year as the fix was not marked as a security issue.

"Attackers are actively looking for and profiting from such slowly-fixed vulnerabilities," the researchers said.

"Tackling the harmful practices of the commercial surveillance industry will require a robust, comprehensive approach that includes cooperation among threat intelligence teams, network defenders, academic researchers and technology platforms."

SHARE □ □ □ □ ,)
SHARE □