Security Newsletter

19 Jul 2021

Subscribe to this newsletter

iOS zero-day let SolarWinds hackers compromise fully updated iPhones

The Russian state hackers who orchestrated the SolarWinds supply chain attack last year exploited an iOS zero-day as part of a separate malicious email campaign aimed at stealing Web authentication credentials from Western European governments, according to Google and Microsoft.

In a post Google published on Wednesday, researchers Maddie Stone and Clement Lecigne said a “likely Russian government-backed actor” exploited the then-unknown vulnerability by sending messages to government officials over LinkedIn.

Attacks targeting CVE-2021-1879, as the zero-day is tracked, redirected users to domains that installed malicious payloads on fully updated iPhones. The attacks coincided with a campaign by the same hackers who delivered malware to Windows users, the researchers said.

Read More on Ars Techinca

Even More Google's blog

Ransomware Giant REvil's Sites Disappear

Just days after President Biden demanded that Russian President Putin shut down ransomware groups, the servers of one of the biggest groups mysteriously went dark.

All of REvil's Dark Web sites slipped offline as of early Tuesday morning, and it's not clear whether it's due to the ransomware gang getting busted or whether the threat actors did it on purpose.

One possibility: It could be that the U.S. shut down the servers. Then again, perhaps it was the Russian government. The timing would make sense, given the White House's saber-rattling at Russia over the ransomware plague. The silenced servers come just a few days after President Biden called President Vladimir V. Putin of Russia and demanded that he shut down ransomware groups attacking American targets.

Read More on Threatpost

More #News

- US govt offers $10 million reward for tips on nation-state hackers
- Critical Cloudflare CDN flaw allowed compromise of 12% of all sites
- Microsoft: Israeli firm used Windows zero-days to deploy spyware
- Google Chrome will add HTTPS-First Mode to keep your data safe
- Google: Russian SVR hackers targeted LinkedIn users with Safari zero-day
- Chinese cyberspies' wide-scale APT campaign hits Asian govt entities

- REvil ransomware gang's web sites mysteriously shut down
- CISA orders federal agencies to patch Windows PrintNightmare bug
- Interpol urges police to unite against 'potential ransomware pandemic'
- Hackers got past Windows Hello by tricking a webcam
- Facebook catches Iranian spies catfishing US military targets
- Instagram Launches 'Security Checkup' to Help Users Recover Hacked Accounts

#Breach Log

- Ransomware hits law firm counseling Fortune 500, Global 500 companies
- Ecuador's state-run CNT telco hit by RansomEXX ransomware
- Cyberattack on Moldova's Court of Accounts destroyed public audits
- Fashion retailer Guess discloses data breach after ransomware attack
- Hackers Move to Extort Gaming Giant EA

#Patch Time!

- New Windows print spooler zero day exploitable via remote print servers
- HelloKitty ransomware is targeting vulnerable SonicWall devices
- D-Link issues hotfix for hard-coded password router vulnerabilities
- Google patches 8th Chrome zero-day exploited in the wild this year
- WooCommerce fixes vulnerability exposing 5 million sites to data theft
- Software maker removes "backdoor" giving root access to radio devices
- Adobe updates fix 28 vulnerabilities in 6 programs
- Microsoft July 2021 Patch Tuesday fixes 9 zero-days, 117 flaws
- SolarWinds patches critical Serv-U vulnerability exploited in the wild

#Tech and #Tools

- How the Kaseya VSA Zero Day Exploit Worked
- Practical MFA Bypass Techniques
- Forensic Methodology Report: How to catch NSO Group's Pegasus
- Security Analysis of Telegram
- Remote code execution in cdnjs of Cloudflare

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred Group is one of the world's leading online gambling operators with business across Europe, US and Australia, offering 30 million customers across 9 brands a great form of entertainment in a safe, fair and sustainable environment. The company, which employs about 1,600 people, is listed on Nasdaq Stockholm Large Cap and is a member of the European Gaming and Betting Association (EGBA) and founding member of IBIA (Sports Betting Integrity Association). Kindred Group is audited and certified by eCOGRA for compliance with the 2014 EU Recommendation on Consumer Protection and Responsible Gambling (2014/478/EU). Read more on www.kindredgroup.com.

You can access the previous newsletters at https://news.infosecgur.us