Cyber-espionage group uses Chrome extension to infect victims

By Catalin Cimpanu

Published: 2018-12-05 · Archived: 2026-04-05 23:20:00 UTC

In what appears to be a first on the cyber-espionage scene, a nation-state-backed hacking group has used a Google Chrome extension to infect victims and steal passwords and cookies from their browsers.

This is the first time an APT (Advanced Persistent Threat --an industry term for nation-state hacking groups) has been seen (ab)using a Chrome extension, albeit it's not the first time one has used a browser extension, as the Russian-linked Turla APT previously used a Firefox add-on in 2015 [1, 2].

According to a report that's going to be published later today by the ASERT team at Netscout reveals the details of a spear-phishing campaign that's been pushing a malicious Chrome extension since at least May 2018.

Hackers used spear-phishing emails to lure victims on websites copied from legitimate academic organizations. These phishing sites, now down, showed a benign PDF document but prevented users from viewing it, redirecting victims to the official Chrome Web Store page to install a (now removed) Chrome extension named Auto Font Manager.


kimsuky-apt.jpg
Image: Mr. J0hn D0ugh

Netscout researchers say the extension had the ability to steal both cookies and site passwords, but they've also seen email forwarding on some compromised accounts.

Speaking to ZDNet, Netscout researchers said the spear-phishing campaigns using this Chrome extension targeted the academic sector but did not want to give out the names of the victims just yet.

"We've identified three universities based in the United States and one non-profit institution based in Asia [that] we're certain to have been targeted," researchers told us.

"A large number of the victims, across multiple universities, had expertise in biomedical engineering, possibly suggesting a motivation for the attackers' targeting," researchers added separately, in their report.

But while looking into this recent attacks, researchers also discovered that the same infrastructure that hosted these phishing sites had also been previously used in another hacking campaign that relied on breaking into universities' networks via Remote Desktop Connections (RDP) connections.

Netscout told ZDNet that "the two separate threads of activity have shared infrastructure and overlapping victims, but it's unclear which came first."

Investigators also added that the people behind this recent campaign, which Netscout named Stolen Pencil, have been very sloppy when it came to hiding their tracks. Researchers said they found evidence suggesting that the

group may be based in North Korea.

"Poor OPSEC led to users finding open web browsers in Korean, English-to-Korean translators open, and keyboards switched to Korean language settings," researchers said.

But while Netscout researchers didn't want to link this campaign to a specific North Korean APT (Advanced Persistent Threat --an industry term for nation-state hacking groups), multiple industry sources to whom ZDNet showed the Chrome extension file hashes yesterday pointed us to a cyber-espionage group known as Kimsuky (also known as Velvet Chollima).

A 2013 Kaspersky Lab report presented evidence linking the group to North Korea's regime. The same report also detailed Kimsuky's propensity for going after academic targets, the same ones targeted with this most recent campaign.

As for what the hackers were after, Netscout researchers told ZDNet that they've "seen no evidence of data theft, but like any intrusion, we can't entirely discount the possibility. None of the tools or commands were specifically geared towards stealing information - they were focused on credential theft and maintaining access."

Universities have always been an attractive target for nation-state hackers, especially those looking for proprietary information or unreleased research. While both Chinese and Russia state hackers have been known to go after the academic sector on a regular basis, Iranian hackers have been the most active of the bunch.

Earlier this year in March, the US indicted 10 Iranians for hacks against 320 universities in 22 countries, 144 of which were in the US. Some of the research papers the hackers stole were eventually published online on pay-for-access portals operated by some of the indicted hackers, who, apparently, found a way to generate side profits from their day-to-day state-sponsored hacking campaigns. The indictments didn't stop Iranian hackers from their attacks, though.

More security coverage:

- **Czech Republic blames Russia for multiple government network hacks**
- **Ukrainian police arrest hacker who infected over 2,000 users with DarkComet RAT**
- **New industrial espionage campaign leverages AutoCAD-based malware**
- **The CoAP protocol is the next big thing for DDoS attacks**
- **Atlanta ransomware attack hit 'mission critical' systems** **CNET**
- **FBI dismantles gigantic ad fraud scheme operating across over one million IPs**
- **Hackers are opening SMB ports on routers so they can infect PCs with NSA malware**
- **Banking trojans, not ransomware, are the biggest threat now** **TechRepublic**
