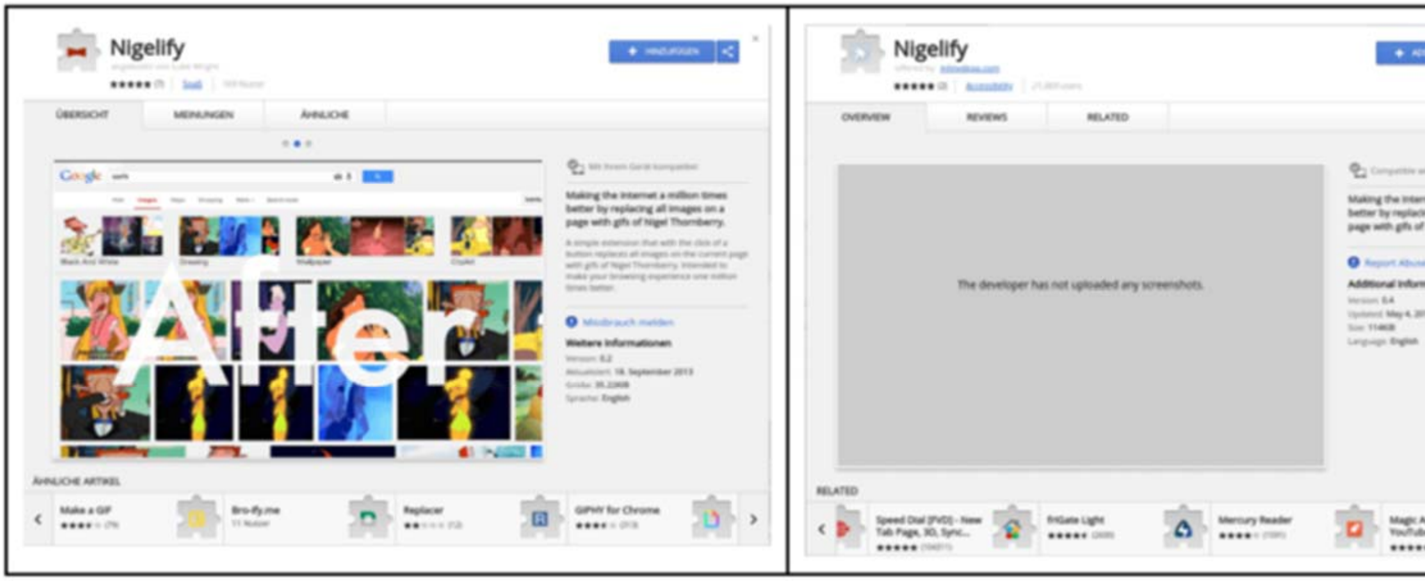
Malicious Chrome extensions infect 100,000-plus users, again

Over two months, seven extensions stole credentials and installed currency miners.

DAN GOODIN - 5/10/2018, 3:30 PM



Enlarge / **On the left, a legitimate Chrome extension. On the right, one of seven recently discovered malicious Chrome extensions impersonating it.**

Radware

Criminals infected more than 100,000 computers with browser extensions that stole login credentials, surreptitiously mined cryptocurrencies, and engaged in click fraud. The malicious extensions were hosted in Google's official Chrome Web Store.

The scam was active since at least March with seven malicious extensions known so far, researchers with security firm Radware reported Thursday. Google's security team removed five of the extensions on its own and removed two more after Radware reported them. In all, the malicious add-ons infected more than 100,000 users, at least one of which was inside a "well-protected network" of an unnamed global manufacturing firm, Radware said.

Secure browser, weak link

FURTHER READING

After phishing attacks, Chrome extensions push adware to millions

Over the past eight months, malicious Chrome extensions have proved to be an Achilles' heel for the Internet's most widely used and arguably most secure browser. Last August, lax rules for securing extension-developer accounts led to the compromise of two extensions installed on millions of computers. In two separate incidents in January, researchers found at least five malicious extensions installed more than 500,000 times. Two weeks ago, Trend Micro documented the return of FacexWorm, a malicious extension that was first spotted seven months earlier.

FURTHER READING

Google Chrome extensions with 500,000 downloads found to be malicious

Google manages to proactively detect and remove many malicious extensions, as evidenced by Radware's finding that five of the seven extensions it discovered were no longer available in the Chrome Web Store. But the regular success attackers enjoy all but guarantees the rash of bad extensions will continue.

"As this malware spreads, the group will continue to try to identify new ways to utilize the stolen assets," Radware researchers Adi Raff and Yuval Shapira wrote on Thursday, referring to the criminals behind the latest batch of extensions. "Such groups continuously create new malware and mutations to bypass security controls."

A Google spokeswoman said company employees removed the extensions from the Chrome Web Store and the infected users' browsers within hours of receiving the report.

The extensions were being pushed in links sent over Facebook that led people to a fake YouTube page that asked for an extension to be installed. Once installed, the extensions executed JavaScript that made the computers part of a botnet. The botnet stole Facebook and Instagram credentials and collected details from a victim's Facebook account. The botnet then used that pilfered information to send links to friends of the infected person. Those links pushed the same malicious extensions. If any of those friends followed the link, the whole infection process started all over again.

The botnet also installed cryptocurrency miners that mined the monero, bytecoin, and electroneum digital coins. Over the past six days, the attackers appeared to generate about $1,000 in digital coin, mostly in monero. To prevent users from removing the malicious extensions, the attackers automatically closed the extensions tab each time it was opened and blacklisted a variety of security tools provided by Facebook and Google.

The seven extensions masqueraded as legitimate extensions. Their names were:

- Nigelify
- PwnerLike
- Alt-j
- Fix-case
- Divinity 2 Original Sin: Wiki Skill Popup
- Keeprivate
- iHabno

Thursday's Radware blogpost includes extension IDs for each one.

The extensions came to the attention of Radware researchers through machine-learning algorithms that analyzed communication logs of the protected network that was infected. The Radware researchers said they believe the group behind the extensions has never been detected before. Given the regular success in getting malicious extensions hosted in the Chrome Web Store, it wouldn't be surprising if the group strikes again.

DAN GOODIN Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications. **EMAIL** dan.goodin@arstechnica.com // **TWITTER** @dangoodin001