reuters.com

Exclusive: Massive spying on users of Google's Chrome shows new security weakness

Joseph Menn

5–6 minutes

SAN FRANCISCO (Reuters) - A newly discovered spyware effort attacked users through 32 million downloads of extensions to Google's market-leading Chrome web browser, researchers at Awake Security told Reuters, highlighting the tech industry's failure to protect browsers as they are used more for email, payroll and other sensitive functions.

Alphabet Inc's

Google said it removed more than 70 of the malicious add-ons from its official Chrome Web Store after being alerted by the researchers last month.
“When we are alerted of extensions in the Web Store that violate our policies, we take action and use those incidents as training material to improve our automated and manual analyses,” Google spokesman Scott Westover told Reuters.

Most of the free extensions purported to warn users about questionable websites or convert files from one format to another. Instead, they siphoned off browsing history and data that provided credentials for access to internal business tools.

Based on the number of downloads, it was the most far-reaching malicious Chrome store campaign to date, according to Awake co-founder and chief scientist Gary Golomb.

Google declined to discuss how the latest spyware compared with prior campaigns, the breadth of the damage, or why it did not detect and remove the bad extensions on its own despite past promises to supervise offerings more closely.

It is unclear who was behind the effort to distribute the malware. Awake said the developers supplied fake contact information when they submitted the extensions to Google.

“Anything that gets you into somebody’s browser or email or other sensitive areas would be a target for national espionage as well as organized crime,” said former National Security Agency engineer Ben Johnson, who founded security companies Carbon Black and Obsidian Security.

The extensions were designed to avoid detection by antivirus companies or security software that evaluates the reputations of web domains, Golomb said.

If someone used the browser to surf the web on a home computer, it would connect to a series of websites and transmit information, the researchers found. Anyone using a corporate network, which would include security services, would not transmit the sensitive information or even reach the malicious versions of the websites.

“This shows how attackers can use extremely simple methods to hide, in this case, thousands of malicious domains,” Golomb said.

After this story's publication, Awake released its research, including the list of domains and extensions. here

All of the domains in question, more than 15,000 linked to each other in total, were purchased from a small registrar in Israel, Galcomm, known formally as CommuniGal Communication Ltd.

Awake said Galcomm should have known what was happening.

In an email exchange, Galcomm owner Moshe Fogel told Reuters that his company had done nothing wrong.

“Galcomm is not involved, and not in complicity with any malicious activity whatsoever,” Fogel wrote. “You can say exactly the opposite, we cooperate with law enforcement and security bodies to prevent as much as we can.”

Fogel said there was no record of the inquiries Golomb said he made in April and again in May to the company’s email address for reporting abusive behavior, and he asked for a list of suspect domains.

After publication, Fogel said the majority of those domain names were inactive and that he would continue to investigate the others.

The Internet Corp for Assigned Names and Numbers, which oversees registrars, said it had received few complaints about Galcomm over the years, and none about malware.

While deceptive extensions have been a problem for years, they are getting worse. They initially spewed unwanted advertisements, and now are more likely to install additional malicious programs or track where users are and what they are doing for government or commercial spies.

Malicious developers have been using Google’s Chrome Store as a conduit for a long time. After one in 10 submissions was deemed malicious, Google said in 2018 here it would improve security, in part by increasing human review.

But in February, independent researcher Jamila Kaya and Cisco Systems’ Duo Security uncovered here a similar Chrome campaign that stole data from about 1.7 million users. Google joined the investigation and found 500 fraudulent extensions.

“We do regular sweeps to find extensions using similar techniques, code and behaviors,” Google's Westover said, in identical language to what Google gave out after Duo's report.

Reporting by Joseph Menn; Editing by Greg Mitchell, Leslie Adler and Jonathan Oatis

Our Standards: The Thomson Reuters Trust Principles., opens new tab