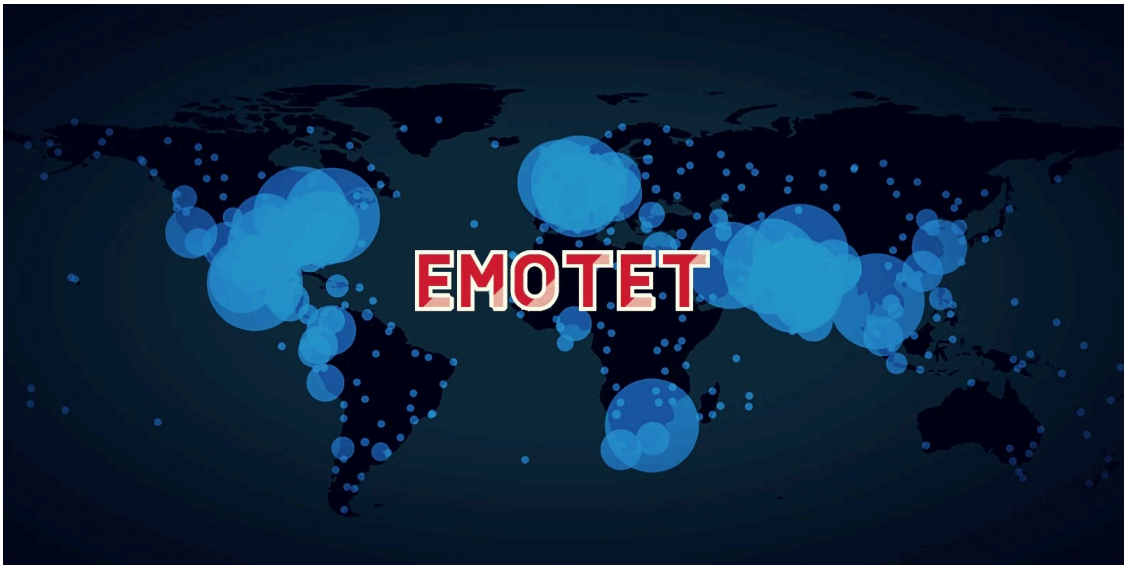
Emotet malware now steals credit cards from Google Chrome users

By Sergiu Gatlan

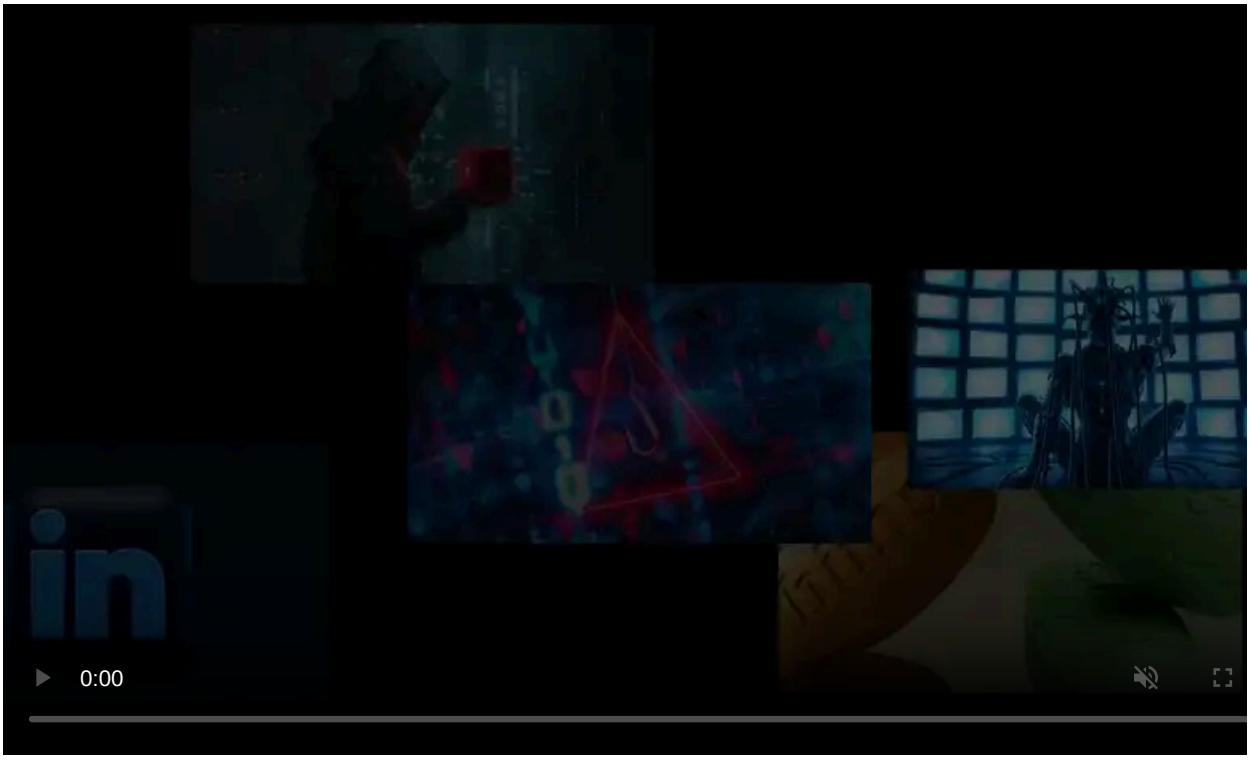
Published: 2022-06-08 · Archived: 2026-04-05 17:26:29 UTC

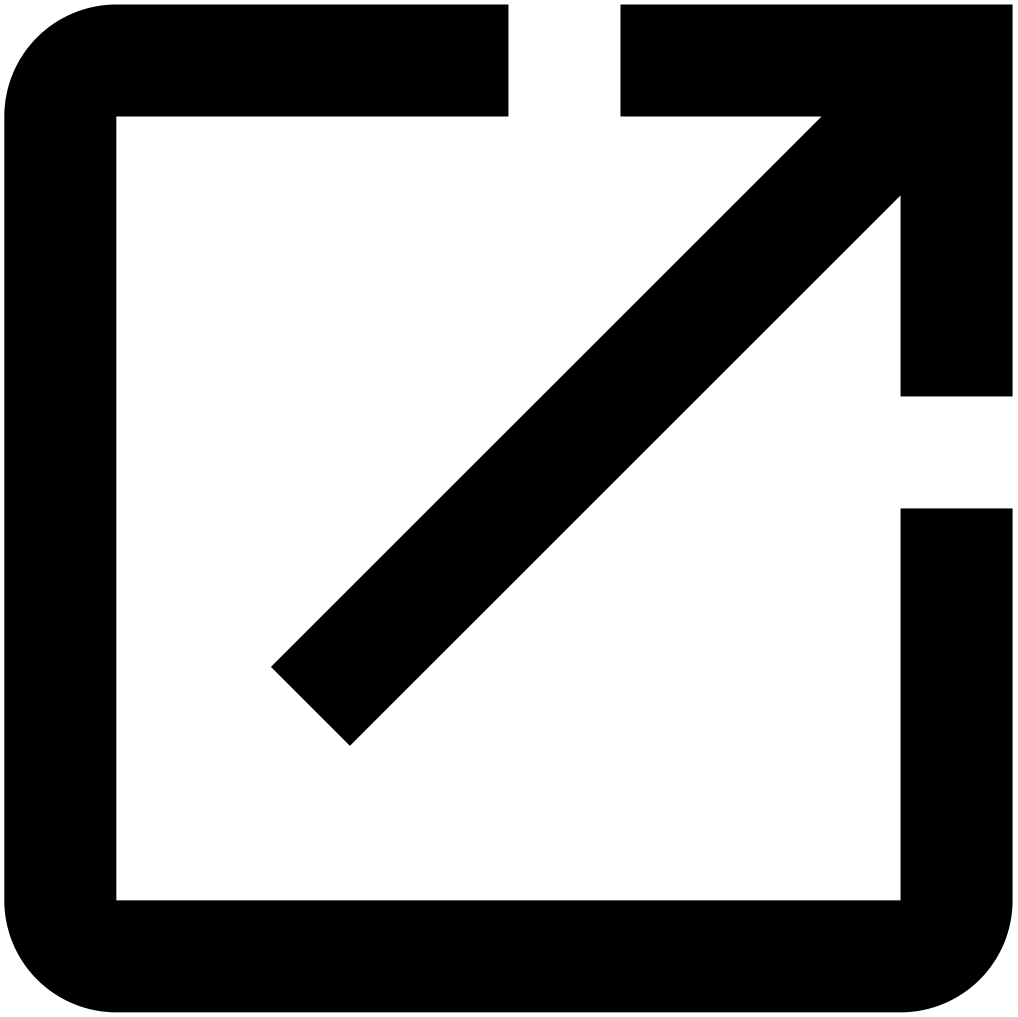


The Emotet botnet is now attempting to infect potential victims with a credit card stealer module designed to harvest credit card information stored in Google Chrome user profiles.

After stealing the credit card info (i.e., name, expiration month and year, card numbers), the malware will send it to command-and-control (C2) servers different than the ones the Emotet card stealer module uses.

"On June 6th, Proofpoint observed a new Emotet module being dropped by the E4 botnet," the Proofpoint Threat Insights team said.


0:00



"To our surprise it was a credit card stealer that was solely targeting the Chrome browser. Once card details were collected they were exfiltrated to different C2 servers than the module loader."

This behavior change comes after increasing activity during April and a switch to 64-bit modules, as the Cryptolaemus security research group spotted.

One week later, Emotet started using Windows shortcut files (.LNK) to execute PowerShell commands to infect victims' devices, moving away from Microsoft Office macros now disabled by default starting with early April 2022.

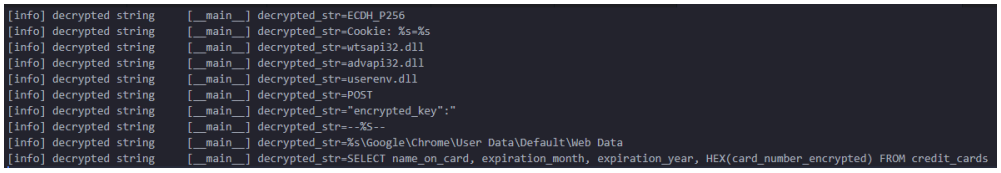


Image: Proofpoint

Emotet's revival

The Emotet malware was developed and deployed in attacks as a banking trojan in 2014. It has evolved into a botnet the TA542 threat group (aka Mummy Spider) uses to deliver second-stage payloads.

It also allows its operators to steal user data, perform reconnaissance on breached networks, and move laterally to vulnerable devices.

Emotet is known for dropping Qbot and Trickbot malware trojan payloads on victims' compromised computers, which are used to deploy additional malware, including Cobalt Strike beacons and ransomware such as Ryuk and Conti.

At the beginning of 2021, Emotet's infrastructure was taken down in an international law enforcement action that also led to the arrest of two individuals.

German law enforcement used Emotet's own infrastructure against the botnet, delivering a module that uninstalled the malware from infected devices on April 25th, 2021.

The botnet came back in November 2021 using TrickBot's already existing infrastructure when Emotet research group Cryptolaemus, computer security firm GData, and cybersecurity firm Advanced Intel all detected the TrickBot malware being used to push an Emotet loader.

As ESET revealed on Tuesday, Emotet has seen a massive increase in activity since the start of the year, "with its activity growing more than 100-fold vs T3 2021."
