CoreBot banking trojan malware returns after two-year break

By Written by Danny Palmer, Senior WriterSenior Writer Nov. 3, 2017 at 7:18 a.m. PT

Archived: 2026-04-05 17:30:09 UTC

Video: Ransomware using trojan trick to expand threat

A form of banking trojan malware has suddenly reappeared after a two-year break and is targeting online banking customers.

Tech Pro Research

-
-
-
-
-
-

CoreBot trojan was mainly active in the summer of 2015, after suddenly switching its focus to target banks. After a relatively short campaign, the malware seemingly disappeared until making a sudden reappearance this week.

Spotted by researchers at Deep Instinct, a new version of CoreBot is being distributed in spam email campaigns with the intention of stealing information from customers of Canadian banking websites.

Customers of TD, Des-Jardins, RBC, Scotia Bank, Banque National are all targeted by those behind the campaign, with successful execution of the malware allowing the attackers to steal the credentials of infected users as they login into these sites.

The new CoreBot campaign claims to be an invoice and thanks the target for making a payment - a common tactic used in phishing campaigns which aims to panic the victim into thinking they've lost money.


corebot-lire.png

CoreBot email lure.

Image: Deep Instinct

The email contains a 'view invoice' link, which if clicked initiates the download of the malicious payload. This is different to previous CoreBot campaigns which distributed spam emails with malicious Word documents containing the payload.

This version of CoreBot also comes with with new evasion techniques in an attempt to avoid analysis of the malware code, indicating those behind it have spent time developing their malicious product to be stealthier.

Researchers also note that the command and control server domain has switched to a different IP address since the last known CoreBot campaign. Meanwhile, the IP addresses delivering the malware appear to be based in France and Canada.

Initial examination of the new CoreBot malware suggests it's related to other active banking malware campaigns, although researchers haven't yet stated which.

It's also uncertain who is behind this criminal campaign, but artefacts in the code could potentially point to a Chinese link, Deep Instinct told ZDNet.

Analysis of CoreBot is still ongoing, but bank customers are instructed to be cautious of any messages about an unexpected payment.


istock-468347435.jpg

Artefacts in the code could potentially point to a Chinese link.

Image: Getty Images/iStockphoto

Previous and related coverage

CoreBot malware evolves overnight into virulent banking Trojan

It didn't take long for hackers to take advantage of the malware's bolt-on structure and transform it into something dangerous.

TrickBot banking Trojan steps up attacks against UK targets

IBM X-Force researchers warn that this sophisticated malware family is fast becoming one of the most prevalent forms of data-stealing banking Trojans

Quick glossary: Malware[Tech Pro Research]

This list of 22 terms will help you grasp the vocabulary that describes malware and the technology that spawns it.

Read more on cybercrime

- Hacking group targets banks with stealthy trojan malware campaign
- Banking Trojan tests new attack techniques against high-profile targets
- Chinese trojan detected spreading through fake base stations [CNET]
- New Trojan malware campaign sends users to fake banking site that looks just like the real thing
- Nearly undetectable Microsoft Office exploit installs malware without an email attachment [TechRepublic]

Editorial standards
