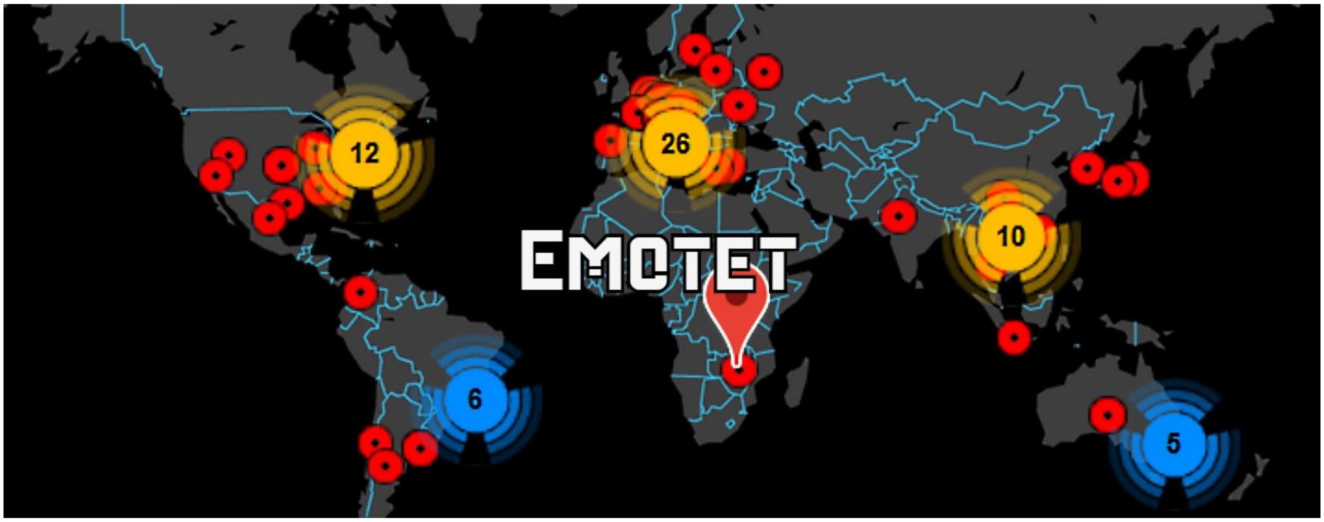
Emotet malware is back and rebuilding its botnet via TrickBot

bleepingcomputer.com/news/security/emotet-malware-is-back-and-rebuilding-its-botnet-via-trickbot/

Lawrence Abrams

By
Lawrence Abrams

- November 15, 2021
- 03:04 PM
- 0



The Emotet malware was considered the most widely spread malware in the past, using spam campaigns and malicious attachments to distribute the malware.

Emotet would then use infected devices to perform other spam campaigns and install other payloads, such as the QakBot (Qbot) and Trickbot malware. These payloads would then be used to provide initial access to threat actors to deploy ransomware, including Ryuk, Conti, ProLock, Egregor, and many others.

At the beginning of the year, an international law enforcement action coordinated by Europol and Eurojust took over the Emotet infrastructure and arrested two individuals.

German law enforcement used the infrastructure to deliver an Emotet module that uninstalled the malware from infected devices on April 25th, 2021.

Emotet returns after law enforcement operation

Today, Emotet research group Cryptolaemus, GData, and Advanced Intel have begun to see the TrickBot malware dropping a loader for Emotet on infected devices.

> This is our 3rd anniversary of Cryptolaemus1. Thanks for all the follows and sharing of intel these past 3 years! To celebrate, Ivan has released a new version of Emotet because he feels left out and wants to be part of the party. More details coming soon. As always watch URLHaus pic.twitter.com/Qwvel32ibB
>
> — Cryptolaemus (@Cryptolaemus1) November 15, 2021

While in the past Emotet installed TrickBot, the threat actors are now using a method that the Cryptolaemus group calls "Operation Reacharound," which rebuilds the botnet using TrickBot's existing infrastructure

Emotet expert and Cryptolaemus researcher Joseph Roosen told BleepingComputer that they had not seen any signs of the Emotet botnet performing spamming activity or found any malicious documents dropping the malware.

This lack of spamming activity is likely due to the rebuilding of the Emotet infrastructure from scratch and new reply-chain emails being stolen from victims in future spam campaigns.

Cryptolaemus has begun analyzing the new Emotet loader and told BleepingComputer that it includes new changes compared to the previous variants.

"So far we can definitely confirm that the command buffer has changed. There's now 7 commands instead of 3-4. Seems to be various execution options for downloaded binaries (since its not just dlls)," Cryptolaemus researchers told BleepingComputer.

Advanced Intel's Vitali Kremez has also analyzed the new Emotet dropper and warned that the rebirth of the malware botnet would likely lead to a surge in ransomware infections.

"It is an early sign of the possible impending Emotet malware activity fueling major ransomware operations globally given the shortage of the commodity loader ecosystem," Kremez told BleepingComputer in a conversation.
"It also tells us that the Emotet takedown did not prevent the adversaries from obtainging the malware builder and setting up the backend system bringing it back to life."

Samples of the Emotet loader dropped by TrickBot can be found at Urlhaus.

Kremez told BleepingComputer that the current Emotet loader DLL has a compilation timestamp of "6191769A (Sun Nov 14 20:50:34 2021)."

Defending against the new Emotet botnet

Malware tracking non-profit organization Abuse.ch has released a list of command and control servers utilized by the new Emotet botnet and strongly suggests network admins block the associated IP addresses.

> Fresh, active Emotet botnet C2 servers are now being pushed to Feodo Tracker
>
> https://t.co/TvIJyqHYVs
>
> We urge you to *BLOCK* these C2 servers and regularly update your block list to receive the maximum protection!
>
> https://t.co/if21bBHTpo pic.twitter.com/sdySouHxxb
>
> — abuse.ch (@abuse_ch) November 15, 2021

Unfortunately, the new Emotet infrastructure is growing rapidly, with over 246 infected devices already acting as command and control servers.

Network administrators are strongly advised to block all associated IP addresses to prevent their devices from being recruited into the newly reformed Emotet botnet.

Update 11/16/21: Updated to include source of Operation RA.

Related Articles:

Emotet botnet switches to 64-bit modules, increases activity

Microsoft detects massive surge in Linux XorDDoS malware activity

Microsoft: Sysrv botnet targets Windows, Linux servers with new exploits

New cryptomining malware builds an army of Windows, Linux bots

Historic Hotel Stay, Complementary Emotet Exposure included

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.