All You Need to Know About Emotet in 2022

By The Hacker News

Published: 2022-11-26 · Archived: 2026-04-05 18:17:41 UTC

For 6 months, the infamous Emotet botnet has shown almost no activity, and now it's distributing malicious spam. Let's dive into details and discuss all you need to know about the notorious malware to combat it.

Why is everyone scared of Emotet?

Emotet is by far one of the most dangerous trojans ever created. The malware became a very destructive program as it grew in scale and sophistication. The victim can be anyone from corporate to private users exposed to spam email campaigns.

The botnet distributes through phishing containing malicious Excel or Word documents. When users open these documents and enable macros, the Emotet DLL downloads and then loads into memory.

It searches for email addresses and steals them for spam campaigns. Moreover, the botnet drops additional payloads, such as Cobalt Strike or other attacks that lead to ransomware.

The polymorphic nature of Emotet, along with the many modules it includes, makes the malware challenging to identify. The Emotet team constantly changes its tactics, techniques, and procedures to ensure that the existing detection rules cannot be applied. As part of its strategy to stay invisible in the infected system, the malicious software downloads extra payloads using multiple steps.

And the results of Emotet behavior are devastating for cybersecurity specialists: the malware is nearly impossible to remove. It spreads quickly, generates faulty indicators, and adapts according to attackers' needs.

How has Emotet upgraded over the years?

Emotet is an advanced and constantly changing modular botnet. The malware started its journey as a simple banking trojan in 2014. But since then, it has acquired a bunch of different features, modules, and campaigns:

- 2014. Money transfer, mail spam, DDoS, and address book stealing modules.
- 2015. Evasion functionality.
- 2016. Mail spam, RIG 4.0 exploit kit, delivery of other trojans.
- 2017. A spreader and address book stealer module.
- 2021. XLS malicious templates, uses MSHTA, dropped by Cobalt Strike.
- 2022. Some features remained the same, but this year also brought several updates.

This tendency proves that Emotet isn't going anywhere despite frequent "vacations" and even the official shutdown. The malware evolves fast and adapts to everything.

What features has a new Emotet 2022 version acquired?

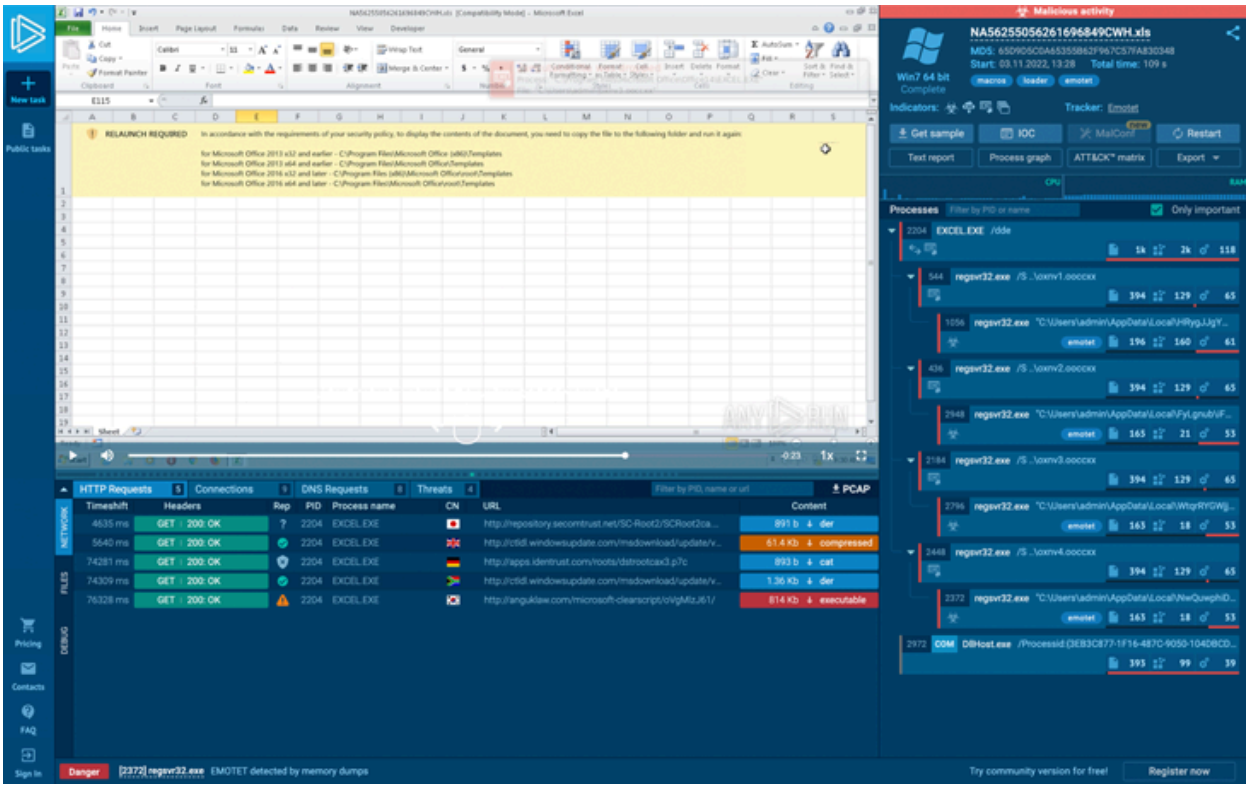
After almost half a year of a break, the Emotet botnet returned even stronger. Here is what you need to know about a new 2022 version:

- It drops IcedID, a modular banking trojan.
- The malware loads XMRig, a miner that steals wallet data.
- The trojan has binary changes.
- Emotet bypasses detection using a 64-bit code base.
- A new version uses new commands:

Invoke rundll32.exe with a random named DLL and the export PluginInit

Command values	Command definition
1	Update bot
2	Load module
3	Load executable
4	Load executable via regsvr32.exe
16343	Invoke rundll32.exe with a random named DLL and the export PluginInit

- Emotet's goal is to get credentials from Google Chrome and other browsers.
- It's also targeted to make use of the SMB protocol to collect company data
- Like six months ago, the botnet uses XLS malicious lures, but it adopted a new one this time:



The Emotet's Excel lure

How to detect Emotet?

The main Emotet challenge is to detect it in the system quickly and accurately. Besides that, a malware analyst should understand the botnet's behavior to prevent future attacks and avoid possible losses.

With its long story of development, Emotet stepped up in the anti-evasion strategy. Through the evolution of the process execution chain and malware activity inside the infected system changes, the malware has modified detection techniques drastically.

For example, in 2018, it was possible to detect this banker by looking at the name of the process – it was one of these:

> eventswrap, implrandom, turnedavatar, soundser, archivesymbol, wabmetagen, msrasteps, secmsi, crsdcard, narrowpurchase, smxsel, watchvsgd, mfidlisvc, searchatsd, lpiograd, noticesman, appxmware, sansidaho

Later, in the first quarter of 2020, Emotet started to create specific key into the registry - it writes into the key HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER value with the length 8 symbols (letters and characters).

Of course, Suricata rules always identify this malware, but detection systems often continue beyond the first wave because rules need to update.

Another way to detect this banker was its malicious documents - crooks use specific templates and lures, even with grammatical errors in them. One of the most reliable ways to detect Emotet is by the YARA rules.

To overcome malware's anti-evasion techniques and capture the botnet – use a malware sandbox as the most convenient tool for this goal. In ANY.RUN, you can not only detect, monitor, and analyze malicious objects but also get already extracted configurations from the sample.

There are some features that you use just for Emotet analysis:

- reveal C2 links of a malicious sample with the FakeNet
- use Suricata and YARA rulesets to successfully identify the botnet
- Get data about C2 servers, keys, and strings extracted from the sample's memory dump
- gather fresh malware's IOCs

The tool helps to perform successful investigations quickly and precisely, so malware analysts can save valuable time.

ANY.RUN sandbox has prepared incredible deals for **Black Friday 2022**! Now is the best time to boost your malware analysis and save some money! Check out special offers for their premium plans but for a limited time – from 22-29 November, 2022.

Emotet has not demonstrated full functionality and consistent follow-on payload delivery. Use modern tools like ANY.RUN online malware sandbox to improve your cybersecurity and detect this botnet effectively. Stay safe and good threat hunting!

Found this article interesting? This article is a contributed piece from one of our valued partners. Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.

Source: https://thehackernews.com/2022/11/all-you-need-to-know-about-emotet-in.html