Rebirth of Emotet: New Features of the Botnet and How to Detect it

By The Hacker News

Published: 2022-02-28 · Archived: 2026-04-05 13:24:10 UTC

One of the most dangerous and infamous threats is back again. In January 2021, global officials took down the botnet. Law enforcement sent a destructive update to the Emotet's executables. And it looked like the end of the trojan's story.

But the malware never ceased to surprise.

November 2021, it was reported that TrickBot no longer works alone and delivers Emotet. And ANY.RUN with colleagues in the industry were among the first to notice the emergence of Emotet's malicious documents.

First Emotet malicious documents

And this February, we can see a very active wave with crooks running numerous attacks, hitting the top in the rankings. If you are interested in this topic or researching malware, you can make use of the special help of ANY.RUN, the interactive sandbox for the detection and analysis of cyber threats.

Let's look at the new version's changes that this disruptive malware brought this time.

Emotet history

Emotet is a sophisticated, constantly changing modular botnet. In 2014 the malware was just a trivial banking trojan. Since that it has acquired 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.

Polymorphic nature and numerous modules allow Emotet to avoid detection. The team behind the malware constantly changes its tactics, techniques, and procedures to make the existing detection rules useless. It downloads extra payloads using numerous steps to stay in the infected system. Its behavior makes malware nearly impossible to get rid of. It spreads fast, creates faulty indicators, and adapts to attackers' needs.

And on November 14, 2021, Emotet was reborn with a new version.

Why was Emotet reborn?

Throughout Emotet's history, it got several breaks. But after the global police operations in January 2021, we were ready that it would be gone for good. Joint enforcement arrested several gang members, took over servers, and destroyed backups.

Nevertheless, the botnet got back even more robust. It's skillful at evasion techniques and uses several ways to compromise networks making it as dangerous as it used to be.

It was tracked that Trickbot tried to download a dynamic link library (DLL) to the system. And the DLLs turned out to be Emotet, and later, researchers confirmed the fact.

In 2021 after the comeback, Emotet led the top 3 of uploads in ANY.RUN sandbox. Even after such a long break, it still got popular. All statistics on Emotet trends are available in Malware Trends Tracker, and the numbers are based on the public submissions.

Top malware uploads for the last week

No wonder now when its operations are back on rails, ANY. RUN's database gets almost **3 thousand** malicious samples per week. And it's getting clear that you need to get ready for this kind of attack anytime.

What new features has Emotet acquired?

The trojan is already a serious threat to any company. Knowing all malware updates can help avoid such a threat and be cautious. Let's investigate what features a new version brings and how it differs from the previous ones.

Templates

The Emotet campaigns begin with a malspam email that contains Malicious Office Documents (weaponized Microsoft Office documents) or hyperlinks attached to the phishing email, which is widely distributed and lures victims into opening malicious attachments. The weaponized Microsoft Office document has a VBA code and AutoOpen macro for its execution. The Emotet group lures its victims to enable the macros, and this is the only user interaction required to initiate the attack. This user interaction allows bypassing sandboxes tests and verifications.

Emotet distributes using malicious email campaigns that usually consist of Office Documents. And the malware gets very creative with templates of its maldocs. The botnet constantly changes them: it imitates programs'

updates, messages, files. And the content embeds the obfuscated VBA macro and makes different execution chains. The authors behind the malware trick users into enabling macros to start the attack.

And a new version also has a twist. In summer 2020, Emotet used a doc with Office 365 message. The image remains unchanged, but it switched to the XLS format. Also, in this new version, the first time was used in hexadecimal and octal formats to represent the IP address from which the second stage was downloaded. A later technique was changed again, and crooks don't use the HEX encoded IP to download the payload.

Emotet templates in February

New techniques

Emotet keeps raising the bar as a polymorphic creature by attaining new techniques. The latest malware version has come up with some minor changes in the tactics: it leverages MSHTA again. In general, Macro 4.0 leverages Excel to run either CMD, Wscript, or Powershell, which starts another process such as MSHTA or one mentioned above that downloads the main payload and runs it by rundll32.

The botnet is keen on masking malicious strings and content like URLs, IPs, commands, or even shellcodes. But sometimes, you can grab the list of URLs and IPs from the file's script. You can definitely find it by yourself in ANY. RUN's Static Discovering – just give it a try!

URLs list from the Emotet's fake PNG file

Companions

We know that Emotet usually drops other malware to worsen the infection. In November, it was identified that the botnet delivered the Trickbot banking trojan on the compromised hosts.

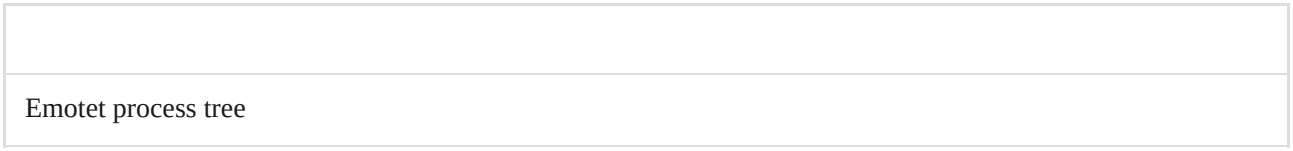
Currently, we can notice that Emotet works with Cobalt Strike. It is a C2 framework used by penetration testers and criminals as well. Having Cobalt Strike in the scenario means that the time between the initial infection and a ransomware attack shortens significantly.

A list of Cobalt Strike IOCs from Emotet infection

Process tree

The chain of execution also got some modifications. In most cases, we can notice a CMD child process, a PowerShell, and Rundll32, and various samples prove that authors prefer to mix processes, constantly changing

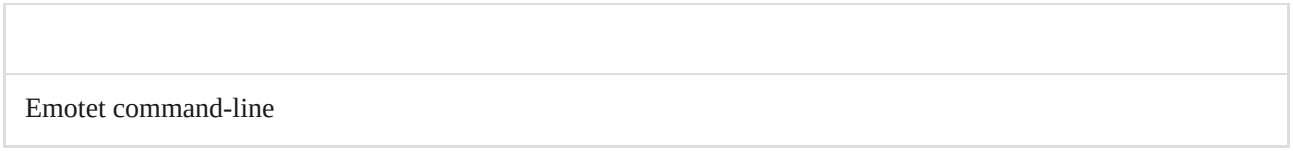
their order. The main goal behind it is to avoid detection by rulesets that identify a threat by child processes of an application.



Emotet process tree

Command-line

Emotet switched from EXE files to DLL a long time ago, so the main payload ran under the Rundll32. Abundant use of Powershell and CMD remains unchanged:



Emotet command-line

How to detect and protect against Emotet?

If you need a fast and convenient way to get complete information on the Emotet sample – use modern tools. ANY.RUN interactive sandbox allows monitoring processes in real-time and receiving all necessary data immediately.

Suricata rulesets successfully identify different malicious programs, including Emotet. Moreover, with the Fake net feature to reveal C2 links of a malicious sample. This functionality also helps gather malware's IOCs.

Emotet samples come and go, and it's hard to keep up with them. So, we advise you to check out fresh samples that are updated daily in our public submissions.

Emotet proves to be a beast among the most dangerous cyber threats in the wild. The malware improves its functionality and works on evading detection. That is why it is essential to rely on effective tools like ANY.RUN.

Enjoy malware 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.
