Emotet is Back

By Maria Jose Erquiaga,

Published: 2022-03-28 · Archived: 2026-04-05 17:18:41 UTC

The text below is a joint work of Maria Jose Erquiaga, Onur Erdogan and Adela Jezkova from Cisco Cognitive team

---

Emotet (also known as Geodo and Heodo) is a banking trojan, but it is also a modular malware that can be used to download other malware as Trickbot and IcedID [8, 9, 13]. Emotet was observed for the first time in 2014 [9]. In January 2021, in a combined effort by Interpol and Eurojust, Emotet was taken down [12]. However, Emotet rose again in November 2021, and it has shown more activity since 2022) [6, 7].

Even though Emotet was born as a banking trojan, it evolved in time and became highly modular threat. This evolution granted adversaries a tool for different purposes. Emotet can be used as an initial payload and remain inactive for extended periods of time until the adversaries decide to leverage it [10]. This feature of Emotet gives the adversaries the flexibility to carry out a multi-stage infection process. This means that Emotet can act as banking trojan, but also has been observed to drop additional malware in the infected systems [1]. Emotet has the capability to gathering information of the infected systems and the adversaries can evaluate the value of the asset [14, 15] Some analysis shows that Emotet can drop CobaltStrike, which then drops ransomware [11]. For example, one of the ransomware dropped by Emotet is Ryuk [9].

In the past few months, Emotet malware has been observed in the wild, and its detection growth considerably [1]. Even though this Emotet re-appearance happened at (almost) the same time as Log4J vulnerability was discovered, there is not enough evidence that these two things are related. However, CobaltStrike, which is known to be related to Emotet, was using Log4J vulnerability [4].

The reappearance of Emotet motivated our deeper research and effort to update the detection ability for Global Threat Alerts customers. As a result of it, the customers of Cisco Secure Network Analytics and Secure Endpoint using GTA get better coverage of the threat now.

We summarize in this blog Emotet threat, it’s lifecycle and typical detectable patterns. In the second part of the blog we show how to use GTA to detect the Emotet.

Summary of Emotet characteristics

- Modular banking trojan
- Downloader/Dropper
- Polymorphic – can evade signature-based detection
- Virtual machine aware

Emotet behavior

The attack flow is detailed in Figure 1. According to the analysis presented by Brad Duncan [2], the attack vector seems to be phishing, via an email with an attached file (1). The file contained in the phishing email, is an Office document (2). When the victims open the office document files and enable macros (3) the Emotet DLL is downloaded in the victim's device (4). After downloaded, this DLL file is executed (5) and it generates the connection with Emotet Command and control (6) [5, 7].

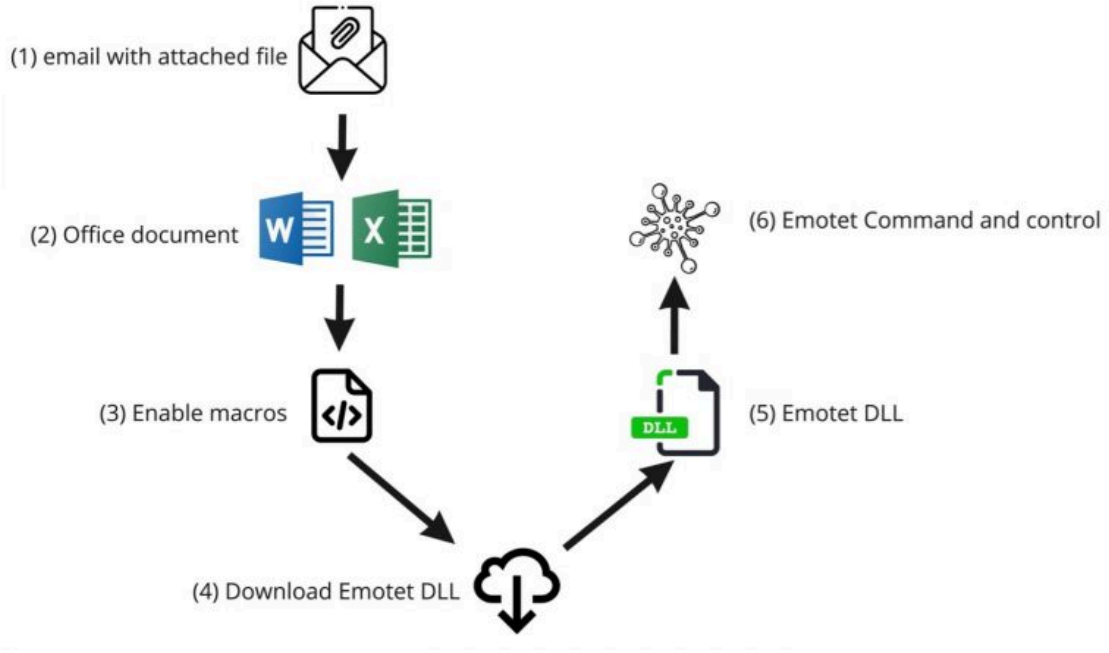

Figure 1. Emotet attack flow

Attached files and PowerShell execution

Once the victim opens and executes the infected files and enables the macros (mainly with docx or xml extensions), a command is executed to obtain and execute a HTML application. The pattern of the URL observed for this step is the following:

hxxp://{IP address}/[yy]/[y].{html|png}

Where "yy" are usually two alphabetical characters.

For example, one of the of the URLs founded in the wild:

hxxp://91.240.118[.]172/hh/hello.png

Then, it downloads PowerShell payload then it leads to downloading Emotet binary, which is a dll file from any of the given URLs contained in the URL described above. The format, in this case can vary, some of the URL's patterns look like this:

http://ttisecurity[.]com/cgi/7RFeiqkgymCs/

Where the regex is:
.*/(gci/){0,1}[a-z0-9_]{3,20}$

Another pattern related to Emotet was

.*/(wp-admin/){0,1}[a-z0-9_]{3,20}$

During the download of the Emotet payload, user agent pattern was, Mozilla/5.0 (Windows NT; Windows NT %; en-US) WindowsPowerShell/5.1.%

DLL execution and Emotet C2

Once the DLL files is in the infected system, it downloads a PE file and then establishes a communication with its Command and Control, using HTTP or HTTPS protocols, on ports 80, 8080 and 443 [2]. Even though some researchers claim there is no relationship between Log4J vulnerability and Emotet, there are some common behaviours, as the use of the same IPs for C2. For example, those IP addresses are both related to Emotet and Log4j:

- 250.21[.]2 and 116.124.128[.]206 founded in [4]
- 94.252[.]3
- 31.163[.]17
- 178.186[.]134
- 79.205[.]117

Detecting Emotet with Global Threat Alerts

GTA (Global Threat Alerts) detects Emotet as a High-risk threat. The threat description includes the MITRE software code and the techniques used by Emotet.

Figure 2. Detail of Emotet description in GTA

The threat detail (see Figure 3) contains also extra information regarding the files that could have been modified, deleted, or created by a particular threat. This information is enriched with the analysis of Emotet samples in Cisco Threat Grid [16]. The patterns of the files that could have been modified by Emotet, the probability of the malware behaviour, and the severity level for each one of the events are provided. This extra information helps network administrators and security teams to mitigate the threat not only in the network, but also in the devices.

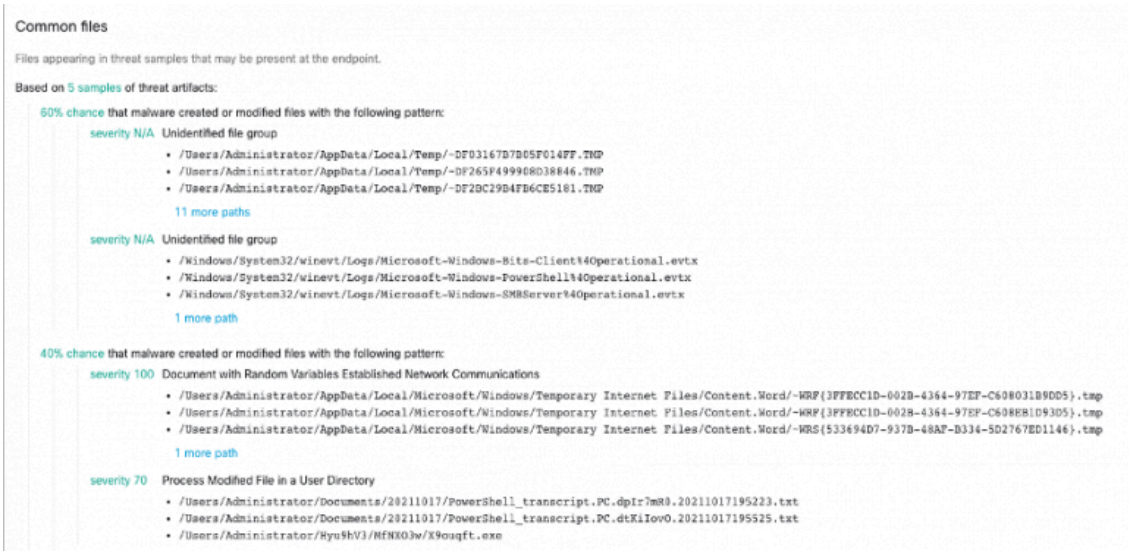

Figure 3. Information regarding the behaviour of Emotet in endpoints, based on samples from Emotet. Includes probability of the event occurrence and severity level.

Figures 4, 5, and 6, show different asset details from Emotet Alerts. It is possible to observe there the traffic from the infected device to malicious IPs, hosts, and domains that are known to be related to Emotet. In the first case, the asset established communication with the hostnames 201.213.32[.]59, 45.55.82[.]2 and 89.32.150[.]160 (Figure 4). In the second example, the asset communicated with the hostnames robertmchilespe[.]com and vbaint[.]com (Figure 5). In the third example, the detection found communication to the domain 104.131.148[.]38 (Figure 6).

Figure 4. Communication from the asset to hostnames 201.213.32[.]59, 45.55.82[.]2 and 89.32.150[.]160 related to Emotet

Figure 5. Communication from the asset to hostnames robertmchilespe[.]com and vbaint[.]com, related to Emotet

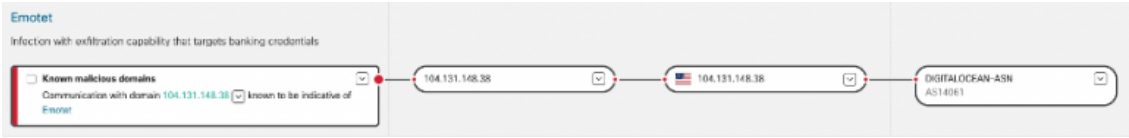

Figure 6. Communication from the asset to the domain 104.131.148[.]38, related to Emotet

To verify if Emotet was detected in your environment, click Emotet Threat detail.

Emotet mitigation

To prevent Emotet, we suggest the following measures:

- Block emails with any attachment files that are suspicious
- Scan suspicious files before opening them
- Isolate the infected devices from the rest of the network to avoid spreading
- Restrict the use of PowerShell and remote tools if possible
- Reset all the user's passwords in the infected devices
- Consider use 2FA (such as Cisco DUO)

Conclusions

We conducted research to find not only new IOCs (IPs, domains and samples) but also URL patters related to this new Emotet wave to keep our customers up to date on the latest threats evolutions. The processed IOCs are also seeds to machine learning GTA algorithms which help to further enrich the detections. GTA users of Secure Endpoint and Secure Network Analytics can detect Emotet in their systems, execute mitigation actions and stay safe from the evolution of this threat.

References

1. Back from the dead: Emotet re-emerges, begins rebuilding to wrap up 2021. Talos report, November 2021.
2. Emotet Return. Published: 2021-11-16. Brad Duncan
3. How to Respond to Apache Log4j using Cisco Secure Analytics. Robert Harris
4. Emotet epoch 5 IOCs list, Brad Duncan. 2022
5. New Emotet Infection Method. By Saqib Khanzada, Tyler Halfpop, Micah Yates and Brad Duncan. February 15, 2022
6. Cybersecurity Threat Spotlight: Emotet, RedLine Stealer, and Magnat Backdoor. By Artsiom Holub. February 3, 2022
7. Emotet description. Malpedia. Fraunhofer Institut. Germany
8. Emotet description, Wikipedia
9. Back from vacation: Analyzing Emotet's activity in 2020. November 2020. Cisco Talos. https://blog.talosintelligence.com/2020/11/emotet-2020.htmlhttps://blog.talosintelligence.com/2020/11/emotet-2020.htmlhttps://blog.talosintelligence.com/2020/11/emotet-2020.html
10. Detecting Emotet Malware with Cognitive Intelligence
11. Corporate Loader "Emotet": History of "X" Project Return for Ransomware. *By Yelisey Boguslavskiy & Vitali Kremez. December 2021*
12. World's most dangerous malware EMOTET disrupted through global action. January 2021. Europol
13. Emotet Software description. MITRE
14. The Commoditization of Multistage Malware Attacks. Chris Gerritz. DarkReading, July 2019.

15. Emotet growing slowly but steadily since November resurgence. Bill Toulas. Bleeping computer. March 2022
16. Cisco Secure Malware Analytics (Threat Grid)

We’d love to hear what you think. Ask a Question, Comment Below, and Stay Connected with Cisco Secure on social!

Cisco Secure Social Channels

Instagram
Facebook
Twitter
LinkedIn
