# Emotet Is Back and Is Deadlier Than Ever! A Rundown of the Emotet Malware

infosecurity-magazine.com/blogs/a-rundown-of-the-emotet-malware/

March 21, 2022

**Vinugayathri Chinnasamy Content Writer**

Emotet is a type of malware and a cybercrime operation that is believed to have originated in Ukraine. The Emotet malware was first detected in 2014. After that, it was considered extremely dangerous and one of the most harmful threats of the decade because of how it evolved. What started as a malware strain grew into an entire cybercrime organization, selling system access acquired through the malware to other cybercrime gangs like the Ryuk gang and ransomware operations.

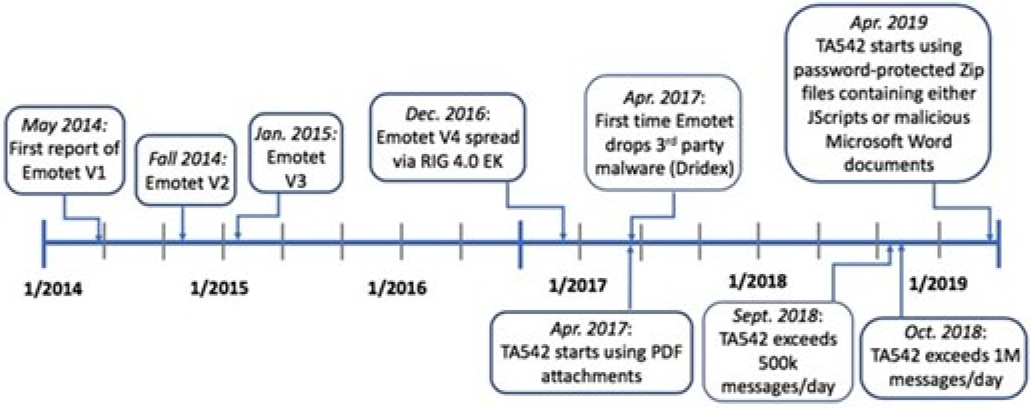
May 2014: First report of Emotet V1
Fall 2014: Emotet V2
Jan. 2015: Emotet V3
Dec. 2016: Emotet V4 spread via RIG 4.0 EK
Apr. 2017: First time Emotet drops 3rd party malware (Dridex)
Apr. 2019 TA542 starts using password-protected Zip files containing either JScripts or malicious Microsoft Word documents
1/2014
1/2015
1/2016
1/2017
1/2018
1/2019
Apr. 2017: TA542 starts using PDF attachments
Sept. 2018: TA542 exceeds 500k messages/day
Oct. 2018: TA542 exceeds 1M messages/day

Image source:

Proofpoint

Through a collaborative effort between authorities in the Netherlands, Germany, the US, the UK, France, Lithuania, Canada and Ukraine, with international activity coordinated by Europol and Eurojust, cyber law enforcement units disrupted Emotet operations, took control of its botnet infrastructure and made arrests in Ukraine in January 2021.

In November 2021, however, new potential cases of Emotet cropped up. *Luca Ebach*, a security researcher at G Data, posted a blog on November 15 2021, in which he stated, “We observed on several of our Trickbot trackers that the bot tried to download a DLL to the system. According to internal processing, these DLLs have been identified as Emotet.”

On December 08 2021, Intel 471 stated*,* “Last month, Intel 471 observed the emergence of Emotet, a notorious strain of malware that had been dormant for most of 2021 after law enforcement agencies forced it offline.”

Cybersecurity experts and researchers from multiple cybersecurity companies have warned that Emotet has indeed returned. In addition, they are experiencing an increase in Trickbot infections**,** a trojan malware that infects Microsoft Windows and other operating systems and extensively spreads using Emotet infected systems. New Emotet samples were also discovered in November 2021, which had a similar code to the malware taken down in January.

## How Did Emotet Operate?

In early 2014, when Emotet was first detected, it was a trojan malware targeted at banks and financial institutions with the purpose of hijacking hosts and stealing banking credentials.

Over time, the malware strain evolved and was reconfigured to work as a ‘loader,’ a malware strain that hijacks a system and gives the hijackers access to download additional payloads onto the host. These payloads can be any executable code, like ransomware code. The first strains of the virus were spread through email attachments.

Emails disguised as invoices, shipping details, COVID-19 information, etc., with infected Word files were sent to victims, and these emails appeared to come from known senders. The Emotet group used this guise to lure unsuspecting victims into downloading and opening these Word files.

Once opened, the Word file would prompt users to enable macros. Once enabled, the malicious code inserted in the Word file would execute through the macros and install the Emotet malware on the victim’s computer.

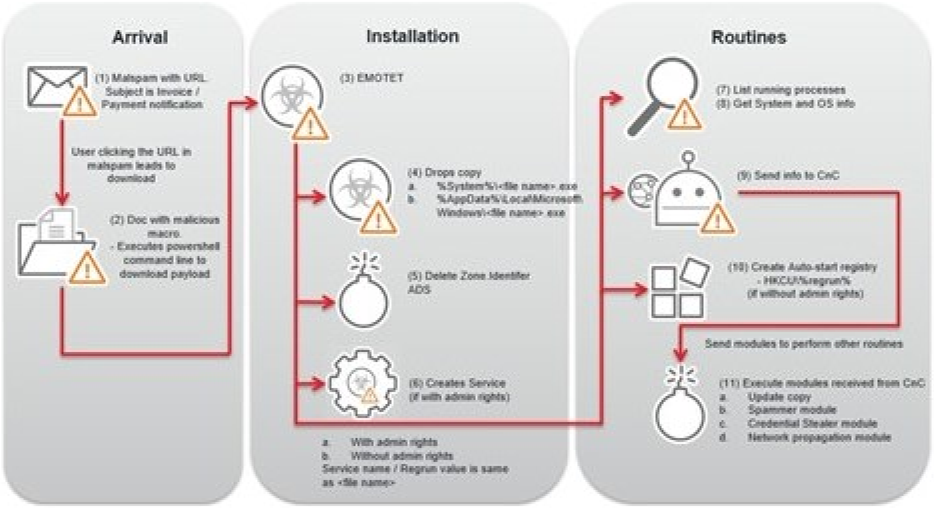
Arrival
(1) Malspam with URL
Subject is Invoice / Payment notification
User clicking the URL in malspam leads to download
(2) Doc with malicious macro.
- Executes powershell command line to download payload
Installation
(3) EMOTET
(4) Drops copy
a. %System%\<file name>.exe
b. %AppData%\Local\Microsoft\Windows\<file name>.exe
(5) Delete Zone.Identifier ADS
(6) Creates Service (if with admin rights)
a. With admin rights
b. Without admin rights
Service name / Regrun value is same as <file name>
Routines
(7) List running processes
(8) Get System and OS info
(9) Send info to CnC
(10) Create Auto-start registry
- HKCU\%regrun%
(if without admin rights)
Send modules to perform other routines
(11) Execute modules received from CnC
a. Update copy
b. Spammer module
c. Credential Stealer module
d. Network propagation module

Image source:

Trend Micro

The Emotet operation then evolved into two streams of cybercrime:

1. One was the delivery of malicious code to victims’ computers. The Emotet group would inject either their own malware or malicious code from other cybercrime gangs (like ransomware code) onto computers infected with Emotet.
2. The second was selling the access to infected systems to other cybercrime units, similar to an Infrastructure-as-a-service (IaaS) model.

This later became known as malware-as-a-service (MaaS) and cybercrime-as-a-service (CaaS) in the cybersecurity community. It was discovered that the Emotet network was used to rent access to infected computers to the Ryuk gang for ransomware operations.

This made Emotet particularly dangerous. Potentially, any cybercrime agency could run their operations by ‘renting’ infected servers from Emotet or hiring the Emotet group to run their malicious code.

The Emotet group created a botnet of infected computers by systematically infecting systems across the globe. The malware later evolved and would automatically use the contacts on an infected computer to send automated phishing emails, increasing the botnet’s size.

## Events Leading to Emotet’s Destruction

Emotet was known to have run three separate botnets as of September 2019, Epoch 1, Epoch 2 and Epoch 3.

Emotet operations were detected globally in July 2020. The main malware being injected was TrickBot and Qbot, both of which were used primarily to steal banking account credentials and automate the spread of Emotet. Additionally, researchers had uncovered that the malicious files being spread would install malware that would run a PowerShell script to pull payloads from other malicious websites and infected systems.

Later in November 2020, Emotet operations extended to using parked domains to distribute payloads to infected systems.

In January 2021, Europol and Eurojust teamed up with other cybercrime authorities worldwide and launched a massive attack against the Emotet group. By then, the Emotet botnet was hundreds of servers wide and spread across the globe.

Through the joint efforts of international cybercrime units, law enforcement was able to gain control of Emotet's infrastructure and dismantle it from the inside. To cripple the group completely, a new approach was implemented. Infected machines were redirected to a law enforcement-controlled infrastructure to prevent any remote control by hackers.

## Protecting Against Emotet

- Microsoft Windows computers are particularly vulnerable. Systems running Windows should be up-to-date with the latest patches for Windows.
- The Emotet malware is still being circulated via email. Do not download or click any suspicious file or link. Malicious emails appear to come from contacts, so beware of emails that seem legitimate as well.
- Use cybersecurity software to protect local files and browsing activity.
- Use heuristic detection with the help of Indusface WAS or manual pen-testing

## Final Words

The return of Emotet is especially problematic for businesses because of its tie to ransomware. However, businesses can protect their servers from being infected with proper precautions. Educate employees and users within the organization network about best practices for emails to stay safe.