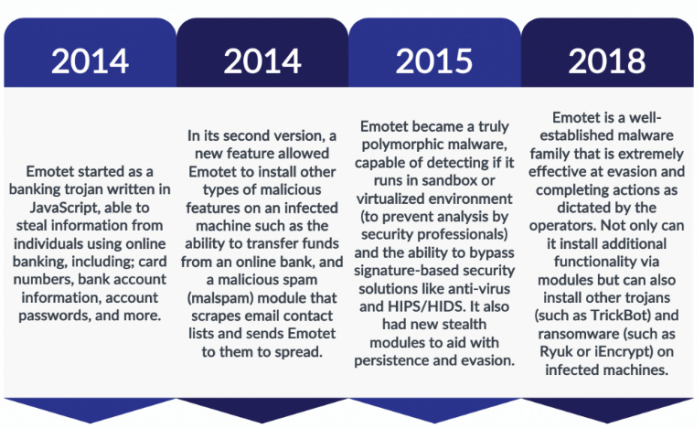
Global Campaign: Emotet

Emotet is one of the most widespread malware families that exist in the present day. Supposedly developed by a group tracked as "Mummy Spider" (TA542), it is an advanced modular and polymorphic trojan, which began its existence purely as a banking trojan, but today it operates more as a malware loader, where other malware operators can pay to add their malicious software such as trojans or ransomware, which will be downloaded to the compromised system when Emotet is run. This malware has become one of the most expensive and destructive pieces of malware, that affects not only nation-state organizations, which has previously cost up to $1 million per incident, but also any unfortunate system that downloads this malware and becomes infected.

EMOTET'S EVOLUTION

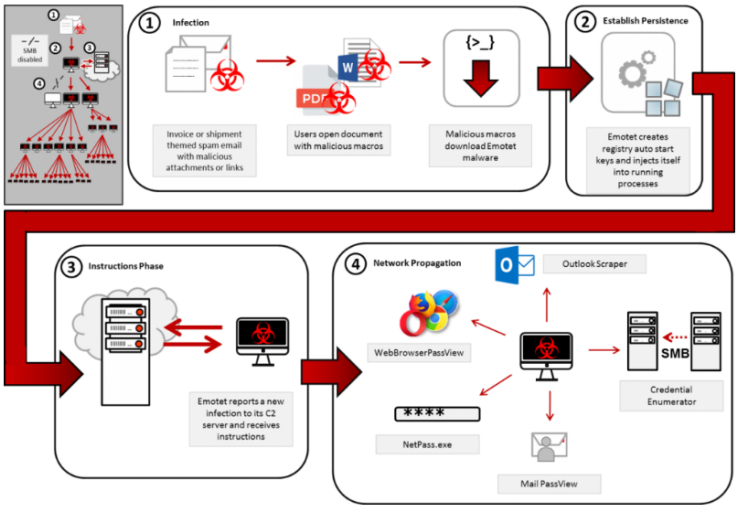
Below is a diagram we have created to show how Emotet has changed from 2014 to 2018, including new functionality and purpose that make Emotet what it is today.



INFECTION METHODS

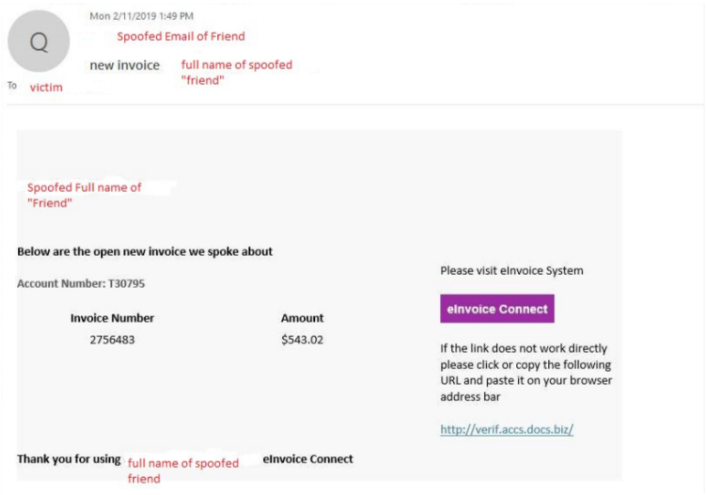
Emotet infections are typically a result of malicious spam campaigns, with hyperlinks to malicious or compromised

Emotet infections are typically a result of malicious spam campaigns, with hyperlinks to malicious or compromised domains or Microsoft Office documents that utilize malicious macros. Once the victim clicks on any of these elements, Emotet installation begins and, as soon as the device is infected, the malware starts trying to spread to other devices on the network and works to scrape Outlook email contacts to continue the malicious spam campaign.



Source: https://www.us-cert.gov/ncas/alerts/TA18-201A

Emotet campaigns typically use branded emails that impersonate receipts, shipping notifications or past-due invoices. The victim is convinced to interact with these malicious files or links using social engineering techniques including urgency, trust, and consequences.



Source: https://www.sentinelone.com/blog/inside-emotet-banking-trojan-malware-distributor/

Microsoft Office documents such as Word or Excel, once opened the file will display a warning banner at the top of the window, asking the user to "Enable Editing" within the document. This as an attempt to trick the user into executing the malicious macro script, which will immediately call out to a malicious or compromised domain to download Emotet.

Once the document is opened, a malicious macro is run that downloads the main Emotet module, this macro is highly obfuscated, making it very difficult to identify by traditional antivirus. This macro which is base64-encoded runs PowerShell, hidden in the document sequence and preventing its detection.

SANDBOX EVASION

One of the greatest features that Emotet has is its ability to identify whether it is running within a virtual machine or not. Once the file is executed, this malware performs a small check, where, creating a process with the same name as the executable file, it checks whether it is in a secure environment (where they can analyze its behavior) or not. For this, Emotet performs the following actions:

- **Checks the name of the system** (Virtual machine or sandboxes typically have names that don't follow standard naming conventions)
- **Checks the disk size** (Virtual machines or sandboxes typically only have a small amount of disk space allocated in an effort to reduce the resources they require)
- **Delays its launch, trying to avoid any antivirus actions**
- **Check the activity of the computer, reviewing the user's activity to verify if it is in a sandbox or not**

PERSISTENCE

Once the malware has verified that is working outside a sandbox, Emotet often proceeds to installs the Trickbot trojan in a directory that allows it to have administrator permissions every time it is run. Below is one of the many formats with which it can be located:

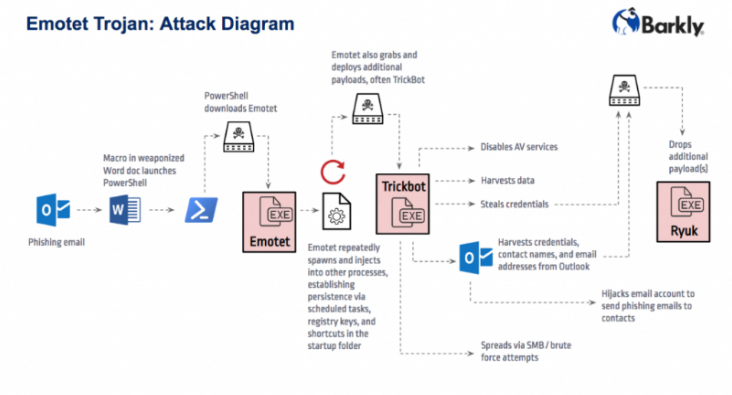
- *"C:\Users\admin\AppData\Local\msptermsizes\msptermsizes.exe*

Now, working under the name of "msptermsizes.exe", Emotet will proceed to create persistence in the system, through the registry key:

- **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run*msptermsizes***

ATTACK DIAGRAM

Once persistence is created and all the files and additional tools are installed, Emotet malware runs like the following diagram created by Barkly.



Emotet Attack Diagram. Source: Barkly

DEFENSIVE MEASURES

As Emotet is typically spread through malicious emails, having strong email security is important. This includes a spam filter, attachment scanning and sandboxing, marking external emails, and a strong security awareness training program for all employees that covers phishing and the risks associated with opening attachments or clicking links sent from unknown senders. As Emotet actors tend to use spear-phishing emails that appear legitimate, employees should be taught about this tactic so they can spot any warning signs, and teach them to report anything they're unsure of to the security team. We'd rather have a few more calls or emails than an Emotet infection.

Anti-virus and endpoint detection and response (EDR) solutions should be deployed on all employee devices to ensure they are protected, and appropriate action can be taken if an infection is identified.

Want to take a look at the war between security researchers and the groups behind Emotet? Follow @Cryptolaemus1 on Twitter to get Emotet related IOCs and threads about fighting this global malware.

Previous Topic
Mark Complete

Back to Lesson