Emotet Trojan Malware
Health Sector Cybersecurity Coordination Center (HC3)
HC3@HHS.GOV
Date: 12/06/2018

Executive Summary

Emotet is currently one of the more prolific, destructive, and costly malware programs cybercriminals use to target organizations across all sectors. Organizations hit with Emotet can face up to $1 million in recovery costs up to recover from network-wide infections, full network compromises, data breaches, account takeovers (ATO), and cyberespionage activities.[iii,iii,iv] While first identified in 2014, the Emotet developers continue to adapt the program to provide cybercriminals with additional malicious capabilities. At this point Emotet has modules for capturing passwords, sending malicious spam (MALSPAM), and stealing user credentials, as well as modules to fetch and install other malicious payloads, such as ransomware.[v] The frequent modifications also help the malware avoid detection by many antivirus programs.[vi] Emotet is frequently spread through e-mail campaigns, and the US Healthcare and Public Health (HPH) sector faces significant risk from, and is sometimes specifically targeted by, these campaigns.

Recommended strategies for mitigating the risk from the Emotet malware include conducting user awareness training around spam emails and suspicious documents, implementing the principle of least privilege to limit the chance of an attacker gaining administrative access, ensuring the use of strong and unique passwords across the organization's environment, and disabling/restricting macros from running within Microsoft Office documents. Organizations are encouraged to follow the recommendations included at the end of this paper, as well as the Department of Homeland Security (DHS) best practices recommendations.

Emotet's Tactics, Techniques, and Procedures (TTPs)

Emotet infection campaigns are all relatively similar: they typically begin with the cybercriminals distributing phishing and MALSPAM with either malicious attachments or links to malicious Microsoft Word documents that will, upon clicking the link or enabling macros, initiate the infection chain.[vii] Both the spoofed sender email addresses and the malicious document file names aim to build trust with the potential victims – social engineering – by employing lures such as invoices, PayPal receipts, shipping notifications, and holiday-themed messages.[viii]

Typically, the cybercriminals behind Emotet campaigns will send as many phishing or malicious spam emails as they can to increase the chances and rate of infection. This tactic would support the theft of as many credentials as possible, leading to malicious follow-on activity such as the sale of the fraudulently obtained information, account takeovers (ATO), and highly-targeted spearphising operations. In other, less common campaigns, the cybercriminals were observed deliberately targeting organizations with Emotet as the initial infection before deploying a secondary payload which was, in these cases, ransomware.[ix]

The malware spreads rapidly through the use of victim-tailored MALSPAM campaigns (emails containing malicious attachments or links). Once a user clicks on a link or attachment in the email, Emotet gets installed into the user's system and further downloads its component files, including a configuration and .DLL (dynamic link library, which is a module that contains functions and data that can be used by another module) file.[x]

Once Emotet has been downloaded, it will create registry auto start keys and begin injecting itself into running processes. The malware will then report the new infection to its Command and Control (C2) server and begin receiving instructions. Finally, Emotet will begin network propagation activities, executing module capabilities, and ultimately fetch and deliver additional malware payloads, such as banking Trojans, cryptomining malware, and ransomware.

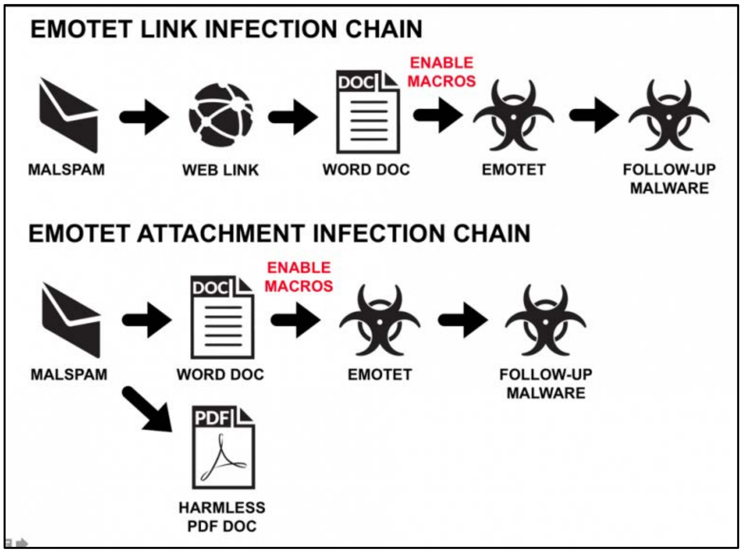

Figure 1: Unit42 - Emotet infection chain

Emotet Capabilities

Emotet is considered an advanced, modular, and polymorphic, meaning it has the ability to change itself dynamically so as to remain undetected by anti-virus solutions.[xi] The configuration file contains information about the systems targeted by the malware, whereas the .DLL file is responsible for intercepting and logging outgoing network traffic.[xii] Being virtual machine-aware, Emotet can generate false indicators if run in a virtual environment. Once downloaded, Emotet establishes persistence and attempts to propagate the local networks through five distinct incorporated spreader modules:

- Netpass.exe: recovers all network passwords stored on a system for the current logged-on user.
- Outlook Scraper: takes names and email addresses from the victim's Outlook accounts and uses that information to send out additional phishing emails from the compromised accounts.
- WebBrowserPassView: password recovery tool that captures passwords stored by web browsers passes them to the credential enumerator module.
- Mail PassView: small password recovery tool that reveals the passwords and other account details for email clients.
- Credential enumerator: self-extracting RAR file that contains two components: a bypass component and a service component.

In November 2018, Emotet introduced a new module that harvests entire email contents stretching back 180 days and greatly increases the risk of losing sensitive information and means that victims of this Emotet attack would be required to initiate data breach notification protocols.[xiii] With the harvesting of entire email messages, the cybercriminals can initiate specially-crafted spear-phishing campaigns, cyberespionage activities, and potentially extortion.

Proliferation and Evolution

When first observed in the wild (ITW) in 2014, Emotet was primarily used to target banking customers in Germany. Since that time, Emotet has evolved into a more modular malware, with separate modules for different capabilities. Although Emotet was most seen largely infecting users of the EMEA region (i.e., Europe, the Middle East and Africa), research in the first half of 2018 suggests its focus is mainly on targets in the U.S.[xiv] As of 2017, Emotet had grown in sophistication and the developers apparently began to offer the malware as an "end-to-end" service for delivery of threats. It delivers the threats, obfuscates them to reduce the chances of detection, and provides a spreader module that allows the threats to self-propagate. Most notably, Emotet has been used to spread the IcedID banking Trojan, Trickbot ransomware, and Ryuk Ransomware.

Emotet continues evolve, utilized by malicious actors in a variety of new campaign tactics and strategies, and the developers continue to add new functionality to the malware. For instance, Emotet originally had no email exfiltration capability in its arsenal and could only take contact information from email sources. Recently, however, researchers have discovered campaigns in which Emotet is harvesting entire emails.[xv] In addition to the evolution of functions involving Emotet itself, Emotet has also been observed being used in conjunction with other malware, most notably ransomware and other Trojans. For instance, recent activities indicate that once Emotet is downloaded and can reach back to its C2 server, it can receive instructions to fetch and install malware such as Ryuk or Trickbot.[xvi] The effectiveness of Emotet as financial exploitation capability will most likely lead to its continued usage and evolution in future malware campaigns.

Mitigation Strategies

US-CERT, in conjunction with NCCIC and MS-ISAC, has recommended a variety of general best practices to limit the effect of Emotet and similar MALSPAM. Organizations should prioritize preventing infections in the first place by training employees on social engineering and phishing. Organizations should also emphasize multiple, overlapping, and mutually supportive defensive systems to guard against single point failures in any specific technology or protection method. This includes deployment of endpoint, email, and web gateway protection technologies as well as firewalls and vulnerability assessment solutions (Emotet is polymorphic and can evade traditional antivirus software). Additional recommendations for mitigate the Emotet malware threat include:

- Conduct user awareness training around spam emails and suspicious documents

- Implement the principle of least privilege to limit the chance of an attacker gaining administrative access (the malware requires local administrative access on the remote system to copy and execute from the $admin SMB share)
- Ensure the use of strong and unique passwords across the corporate environment
- Disable macros from running within Microsoft Office documents
- Software Restriction Policies (SRP) should be deployed to allow only known applications to run and prevent the execution of files from temporary directories
- Ensure that Anti-Virus software conducts scans in regular and frequent intervals
- Segregate networks and business functions
- Perform out-of-band network management on critical devices
- Block or restrict access to SMB file shares
- Implement account lockout policies for mitigating attempts to brute force access to other accounts and machines on the network in the case of an infection

Conclusion

Emotet continues to be a significant cyber threat for organizations, especially those within the Healthcare and Public Health (HPH) sector. Its ability to deploy ransomware payloads and steal Protected Health Information (PHI) has made it valuable to malicious actors looking for financial gain. Healthcare organizations should practice due diligence in understanding Emotet as a threat and stay aware of the best mitigation strategies issued by organizations such as US-CERT and DHS. The best strategy against threats such as Emotet continues to be user awareness and training.

[i] "Alert (TA18-201A) Emotet Malware," US-CERT, 20 Jul 2018, accessed 29 Oct 2018; https://www.us-cert.gov/ncas/alerts/TA18-201A.

[ii] Barry Cruver, "Emotet Attack Costs City of Allentown, PA $1 Million," Barkly, Mar 2018, accessed 4 Dec 2018; https://blog.barkly.com/allentown-pa-emotet-malware-attack-2018

[iii] "Alert (TA18-201A) Emotet Malware," US-CERT, 20 Jul 2018, accessed 29 Oct 2018; https://www.us-cert.gov/ncas/alerts/TA18-201A.

[iv] Barry Cruver, "Emotet Attack Costs City of Allentown, PA $1 Million," Barkly, Mar 2018, accessed 4 Dec 2018; https://blog.barkly.com/allentown-pa-emotet-malware-attack-2018

[v] "Trojan.Emotet," MalwareBytes, accessed 3 Dec 2018; https://blog.malwarebytes.com/detections/trojan-emotet/

[vi] "New Immense Attack of Emotet Trojan Targeted Thousands of Users," Comodo, 17 Aug 2018, accessed 4 Dec 2018; https://blog.comodo.com/comodo-news/new-immense-attack-emotet-trojan-targeted-thousands-users/

[vii] Brad Duncan, "Malware Team Up: MALSPAM Pushing Emotet + Trickbot," Unit 42, 18 Jul 2018, accessed 4 Dec 2018; https://researchcenter.paloaltonetworks.com/2018/07/unit42-malware-team-MALSPAM-pushing-emotet-trickbot/

[viii] David Bisson, "The Top 10 Banking Trojans in 2018: What You Need to Know," Barkly, Oct 2018, accessed 4 Dec 2018; https://blog.barkly.com/top-10-banking-trojans-2018

[ix] Jonathan Crowe, "Alert: Emotet is Back with Major Spam Campaign, Email Exfiltration Module," Nov 2018, accessed 4 Dec 2018; https://blog.barkly.com/emotet-email-exfiltration-module-november-2018

[x] "Dynamic-Link Libraries," Microsoft, 30 May 2018, accessed 4 Dec 2018; https://docs.microsoft.com/en-us/windows/desktop/dlls/dynamic-link-libraries

[xi] Joe CISO, "Emotet — The Polymorph Strikes Back," Medium, 12 Apr 2018, accessed 4 Dec 2018; https://medium.com/@JoeCISO/emotet-the-polymorph-strikes-back-1e25d80abfd9

[xii] Swati Khandelwal, "New Banking Malware with Network Sniffer Spreading Rapidly Worldwide," The Hacker News, 27 June 2014, accessed 31 Oct 2018; https://thehackernews.com/2014/06/new-banking-malware-with-network.html.

[xiii] Jonathan Crowe, "Alert: Emotet is Back with Major Spam Campaign, Email Exfiltration Module," Nov 2018, accessed 4 Dec 2018; https://blog.barkly.com/emotet-email-exfiltration-module-november-2018

[xiv] Symantec Attack Investigation Team, "The Evolution of Emotet: From Banking Trojan to Threat Distributor," Symantec. 18 July 2018, accessed 29 Oct 2018; https://www.symantec.com/blogs/threat-intelligence/evolution-emotet-trojan-distributor.

[xv] Kryptos Logic, "Emotet Awakens With New Campaign of Mass Email Exfiltration," Kryptos Research. 31 Oct 2018, accessed 1 Nov 2018; https://blog.kryptoslogic.com/malware/2018/10/31/emotet-email-theft.html.

[xvi] Jonathan Crowe, "The Ransomware Attack on a North Carolina Water Utility May Not Have Been What It Seemed," Barkly, 15 Oct 2018, accessed 29 Oct 2018; https://blog.barkly.com/north-carolina-water-utility-ransomware-emotet.