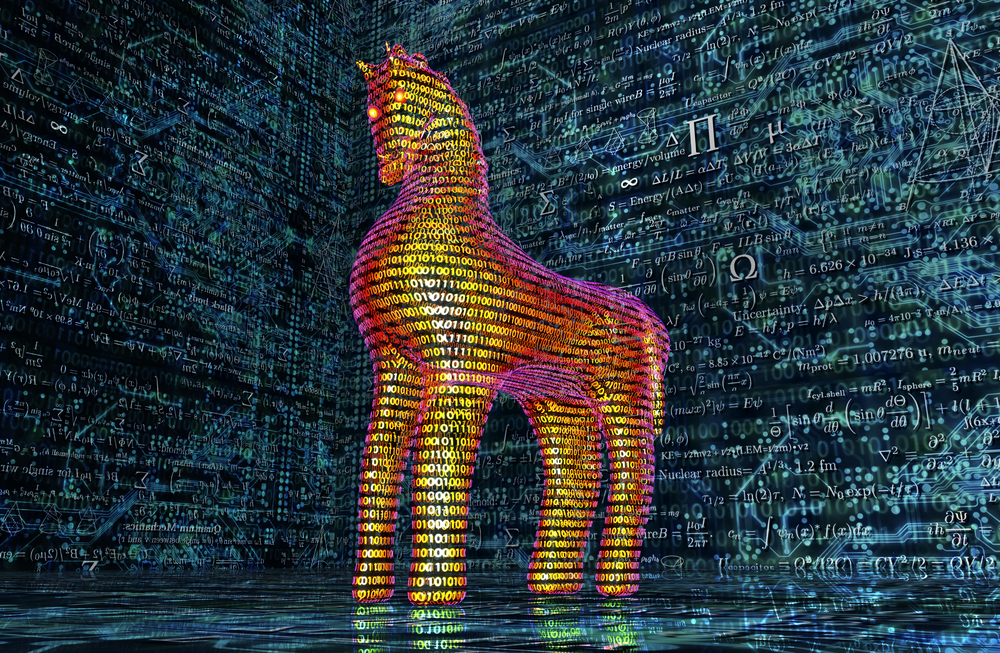
**EMOTET**

The Polymorphic Modular Banking Trojan



**Emotet Malware Project**

**August 27, 2019**

**Prepared By**

**Taylor Boyles, Zach Butler, Byron Turner, Jorian Loftin, Joshua Dickinson, and Abraham Moncar**

**Emotet - The Polymorphic Modular Banking Trojan**

The banking malware or at least that is what Emotet started out as anyway. First developed in 2014, Emotet is considered to be one of the most costly and destructive malware to date. On average, it can be as costly as up to one million dollars per case to rectify an Emotet infection. So, the question is, how does it work? How does it get there? And who can be impacted? Let’s start off with a high-level overview of these questions then we will take a deep dive it to the technical analysis, containment, and awareness.

How does it work? Well, that's the interesting part. It changes how it works, on its own. As you may noticed in the title, Emotet is considered polymorphic. This means that it changes based on the goal it is trying to accomplish. While it's true it was considered to be a banking trojan, it has become so much more. When it was first developed, Emotet would gain access to a system, sniff network traffic, and take banking credentials from specific countries in Europe. Now, it is considered a downloader or dropper of other malware. This means, that Emotet will gain access to a system and distribute a second payload, potentially another malware, ransomware, or even a worm. Do not worry; we will go more in detail during our technical analysis.

Now, how does it get there? Well, that part is quite simple. Emotet gains access from someone you know, well, at least you believe it to be someone you know. This is part of what makes Emotet terrifying. Emotet will get into your system/network disguised as a pdf or word document from someone you now. This, or it will come as a past due bill, a zip file, or even something as simple as an “I love you letter”. Now, we have to ask ourselves; but how does it come from someone I know? Once it gains access to your system Emotet will attempt to self-propagate. This means that it will attempt to spread on its own through a few different methods. It will actually use something called Outlook Scraper to view your personal outlook contacts list. At this point, it will attempt to spread itself through the method we spoke of before, but this time, it would seem as though it came from you. That is part of what Emotet as dangerous as it is, it seems as though it is safe to open.

So, who can be impacted? Well that is even simpler than the last one. Everyone, you, me, governments, you name it. All it takes is one person who isn't familiar with proper cyber techniques such as how to open email attachments safely. So, I guess an even better question is, how can one prevent from getting Emotet? Well, let’s dig a little deeper with the technical analysis before we can talk about prevention. Here is a static and dynamic analysis of Emotet:

**Technical Expose**

**Synopsis of executable**

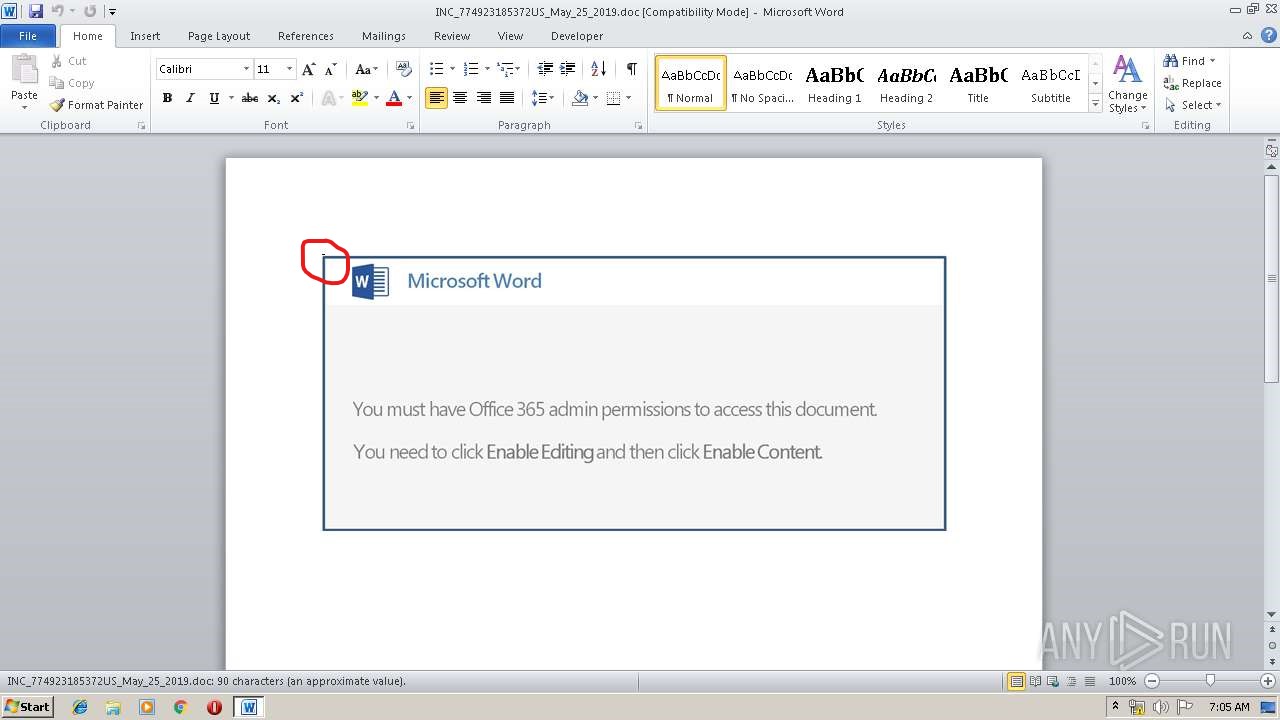
This section contains a summary of the uploaded executable: INC\_774923185372US\_May\_25\_2019.doc

The file type was a .doc file, it was 123.88 KB (126848 bytes), and the compilation date of the .exe was 2019-05-24 19:43:00. The analysis date was 2019-08-19 23:34:23, the first submission date was 2019-05-24 21:18:34, and the last submission date was 2019-06-08 01:36:33. Most anti-malware programs seem to see this as a trojan/trojan downloader or some kind of trojan vba agent

**Initial Behavior**

The table below shows some of the activity after the file is executed:

|  |  |
| --- | --- |
| **Activity Type** | **Count** |
| HTTP Requests | 13 |
| DNS Requests | 5 |
| Connections | 13 |
| File Changes | 1,956 read events/522 write events |



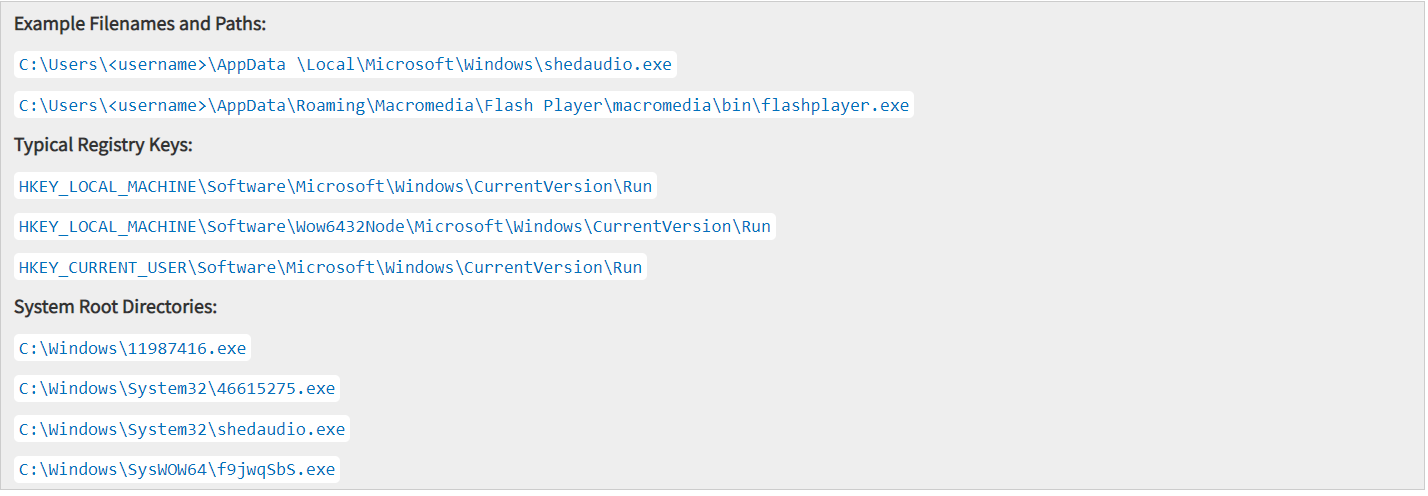
In the photo above in the top left corner of the document is a tiny text box (where I have circled in red), so small it almost looks like a dead pixel on your screen. This edit box is where the changes for each malware infection are made. If you were to expand it, you would find the command line instructions that later get run in the command line. The Macro grabs the contents of the edit box and then calls cmd.exe, passing the content of the edit box as a parameter (in this case it is a PowerShell script). After the PowerShell command is executed, it tries to find at least one of 5 servers called command and control servers after it finds the C&C server this is when it downloads the Emotet malware.

In most cases, Emotet is proliferated into a network via emails that spoof known contacts. These emails usually look as though they are a past due bill, a billing invoice and an attachment that looks as if it is from someone you know. Once this attachment is opened, it will ask the user to enable macros in order to show all content. Once opened and the macros enabled, the contaminated file will execute a PowerShell script that will contact the C&C servers for the actual malware Emotet. Once in the system, Emotet will look for any saved browser passwords and usernames, then report them back to the server and await further commands. These commands will range from dropping additional ransomware, trojans and other various malware. One of the most interesting and suspicious behaviors we observed is that Emotet will make multiple HTTP requests to known malicious servers, which inject code into the process. This adds additional executables to the hkey registry keeping antivirus and users unaware of how to easily isolate it.

Once the initial process is completed Emotet will do a few different things one of those being. One of Emotet’s main “features” which is that it has sand box detection. If Emotet detects it is in a sandbox environment it will lay dormant, it has quite a few different methods of detecting or evading a sandbox environment. One of those being that it checks for recently completed user tasks such as recently opened documents, mouse movement, and user mouse clicks. Another way it detects sandbox environments is that is comes as an XML files with a .doc extension this is because most sandbox environments require a true file type

Once Emotet is downloaded, it will try and spread itself through the network by making use of two different built in tools. The first of these tools being outlook scraper, which scrapes names and email, addresses from your contact list. The second tool being Credential enumerator, this tool has two different components one of these components being a bypass component, the second being a service component. The bypass component is used for the enumeration of network resources and either finds writeable share drives using SMB or tries to brute-force attack user accounts including admin, once it finds a system. The service component writes Emotet into services on the system, which writes Emotet onto the disk. Emotet’s access to SMB can result in the infection of an entire domain (server and clients). Emotet use three tools to steal credentials, these tools are Netpass.exe, WebBrowserPassView, and Mail.PassView.

The photo below shows some of the common file paths the Emotet malware likes to move itself, note that the file names may vary, although it tries to mock legitimate applications:



Once the virus is analyzed, it is time to work on a containment strategy.

**Containment Strategy**

**Scope**

Emotet is an advanced, polymorphic modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans. Everyone is a target for Emotet. To date, Emotet has hit individuals, companies, and government entities across the United States and Europe. The primary attack surface is the use of spam email to spread malware to steal stealing banking logins, financial data, and Bitcoin wallets. Once infected, it can be found installed on:

* Browsers
* Windows Services
* Autorun Registry Entries

**Severity**

Emotet is very difficult to detect and remove. Emotet has several methods for maintaining persistence, including auto-start registry keys and services, and it uses modular Dynamic Link Libraries (DLLs). Emotet has the ability to be VM-aware, avoid spam filters, and/or uninstall security programs. Emotet also uses five known spreader modules to steal credentials:

* NetPass.exe
* WebBrowserPassView
* MailPassView
* Outlook Scraper
* Credential Enumerator

Since Emotet is polymorphic and modular, it can evade typical signature-based detection.

This makes Emotet difficult to remove. Due to the lateral movement via EternalBlue. This particular exploit requires system admins follow a strict policy of isolating infected endpoints from the network, patching, disabling Administrative Shares, and finally removing the Trojan before reconnecting to the network. Otherwise, the cleaned endpoints will continue to become re-infected repeatedly by infected peers. The most serious consequences that an organization can experience as a result of an Emotet attack include:

* Theft of personally identifiable information (PII)
* Leaking of financial and confidential information
* Theft of login credentials, making other accounts vulnerable
* Disruption to regular business operations
  + Long remediation periods for network administrators
  + Loss of productivity of employees whose endpoints have to be isolated from the network
  + Financial losses incurred to restore systems and files
* Potential negative impact to the company’s reputation

Emotet is a very advanced threat, there is no single-layer of security that can stop it. You need multiple layers of detection techniques in place to make it as difficult as possible for them to infect and spread. If infected, a patching timeline of several days to a couple of weeks is recommended.

**Solution**

There is a call to manage office networks and proactively monitor them to ensure they do not become victimized by the Emotet Trojan. In this regard, ensure ALL machines are up to date with their Windows updates. This includes the recent Microsoft SMB update. The threat normally uses newly released exploits by its constant updates. Below are some strategies for preventing future attacks:

* Investigate where payloads are being launched from with incident path visualization and deny access to them.
* Clear any registry modifications and scheduled tasks. Otherwise, they'll continue to spawn additional payloads and the infection will just keep coming back.
* The need to change the DOMAIN and LOCAL passwords for each user on ALL machines. It will need to be a STRONG password, which is alphanumeric and contains at least one capital letter.
* Review the log files and the Outlook mailbox rules associated with the infected user account to ensure further compromises have not occurred. It is possible that the Outlook account will now have rules to auto-forward all emails to an external email address, which could result in a data breach.
* In a network environment, isolate any suspected node immediately. Once isolated, proceed to patch and clean the infected system.
  + Emotet spreads across most networks; a clean computer can be re-infected when plugged back into an infected network.
  + Clean every computer on your network one-by-one.
* Verify ALL users listed in the AD and on each LOCAL machine are legitimate.
* 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.
  + Always keep these security solutions up-to-date with the latest protection capabilities.
* Require everyone in your organization to have long, complex passwords that are changed frequently. Encourage users to avoid reusing the same passwords on multiple websites, and sharing passwords with others should be forbidden.
* Use Group Policy Object to set a Windows Firewall rule to restrict inbound SMB communication between client systems. If using an alternative host-based intrusion prevention system (HIPS), consider implementing custom modifications for the control of client-to-client SMB communication. At a minimum, create a Group Policy Object that restricts inbound SMB connections to clients originating from clients.
* Consider blocking file attachments that are commonly associated with malware, such as .dll and .exe, and attachments that cannot be scanned by antivirus software, such as .zip files.
* Because Emotet scrapes additional credentials, consider password resets for other applications that may have had stored credentials on the compromised machine(s).
* Mark **external** emails with a banner denoting it is from an external source. This will assist users in detecting spoofed emails.
* System administrators can disable Office macros and harden endpoint security. Since social engineering plays a big part in the majority of these campaigns, training the staff on recognizing malicious emails is also a big step towards protecting an organization.
* Infected machines should NOT be used as per Microsoft and the industry's standards.
  + Allowing the user to use the machine spreads the threat to other nodes.
  + Do not log in to infected systems using domain or shared local administrator accounts.
  + Create a policy that prevent malicious Word docs from downloading the initial payload to begin with.
  + Use End task solutions to end suspected software running on the background. Also, carefully examine any suspected files since the virus does modifications to existing files.

**Awareness Training**

**Identification**

It is important to make those within a company fully aware of Emotet. The first thing to do if a system is infected is to take it off the network to be inspected. To look for to check for Emotet if potentially infected, one can look for Microsoft Word spawned command line, a command line contained obfuscated environmental variables, a PowerShell command leveraged the Invoke-Item cmdlet, a PowerShell command contained a URL, or a PowerShell downloaded a file. One can also check the network for downloads from unknown IP addresses. In most cases, one cannot check for Emotet within a virtual machine or sandbox. If infected, be sure to notify your containment analysis team, system admins, and higher officials of the infected company, as well as potentially warn employees.

**Quarantine and Response**

Due to the virus’s large amount of damage, it is vital that precautions are taken to ensure Emotet is kept out of a company’s network. Emotet’s main form of spreading is using phishing emails. Phishing emails are emails that are made to look like ordinary everyday emails or safe emails that contain a link that if clicked, will download the trojan virus. It is important to provide training to tell employees to be careful on clicking links from emails. Any unknown links or downloadable file can be harmful to begin with.

Steps to help prevent an Emotet infection are use Group Policy to set a Windows Firewall rule to restrict inbound SMB communication between client systems. Use antivirus programs on clients and servers, with automatic updates of signatures and software. Apply appropriate patches and updates immediately after appropriate testing. Implement filters at the email gateway to filter out emails with known malspam indicators, such as known malicious subject lines, and block suspicious IP addresses at the firewall. Also, if you do not have a policy regarding suspicious emails, consider creating one.

**Escalation**

Specify that all suspicious emails should be reported to the security and/or IT departments. Provide social engineering and phishing training to employees. Adhere to the principle of least privilege, ensuring that users have the minimum level of access required to accomplish their duties. Limit administrative credentials to designated administrators. Implement Domain-Based Message Authentication, Reporting & Conformance (DMARC), and a validation system that minimizes spam emails by detecting email spoofing using Domain Name System (DNS) records and digital signatures.

In conclusion, this breakdown covers the Overview, Technical Expose, Containment Strategy, and Awareness Training for the Emotet virus.

**Sources**

* https://www.cisecurity.org/blog/top-10-malware-january-2019/
* https://www.malwarebytes.com/emotet/
* https://www.us-cert.gov/ncas/alerts/TA18-201A
* https://blog.malwarebytes.com/cybercrime/2019/03/emotet-revisited-this-pervasive-persistent-threat-is-still-a-danger-to-businesses/
* https://blog.malwarebytes.com/detections/trojan-emotet/
* https://www.cisecurity.org/white-papers/ms-isac-security-primer-emotet/
* https://www.pandasecurity.com/mediacenter/malware/solution-emotet-corporate-security/