IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 22, Issue 4, Ser. II (Jul. – Aug. 2020), PP 31-41
www.iosrjournals.org

Emotet Malware – A Banking Credentials Stealer

Sivaraju Kuraku[1], Dinesh Kalla[2]
[1]*Department of Computer Information Sciences/ University of the Cumberlands, United States of America*
[2]*Department of Computer Science/Colorado Technical University, United States of America*

Abstract: *Internet users use the web every day for Browsing, Email, Banking, Social Media, and Web File & Video downloads. This research paper aims to help world internet users how not to get victimized to Emotet Malware - A Banking Credentials Stealer. Emotet is a very advanced modular trojan malware that primarily targets financial systems and internet users to steal financial and personal information by sending phishing emails to the people in question and self-spreading. Emotet also drops and downloads other banking trojans such as Trickbot, Ursnif, and IceDiD to exploit systems further and encrypts the large chunk of victim sensitive data with Ryuk ransomware payloads to benefit cyber attackers. United States Computer Emergency Readiness Team (US-CERT) issues an alert already concerning malicious Emotet campaign attackers. US-CERT also concluded that Emotet malware is the most destructive and costly malware affecting federal, state, local, tribal governments, private businesses, non-profit organizations, and individuals. A research conducted by top cybersecurity company CrowdStrike revealed that dealing with Emotet infections costs $1 million per incident to remediate. In general, Emotet spreads through emails when a user opens phishing attachments and clicking on phishing links such as malicious URL links, fake PDFs, and macro-enabled Microsoft Word documents. Therefore, this paper aims to address a complete understanding of Emotet malware and will present robust Security Situational Awareness (SSA) to all internet users aboutEmotet Malware. This paper will use a survey questionnaire as a qualitative research methodology instrument to collect data and know-how internet users are familiar with Emotet malware. The survey results are shocked to see how internet users lack situational awareness about Emotet. In conclusion, the paper provides precautions, mitigation actions, and recommendations to prevent user computers from Emotet infections with Security Situational Awareness (SSA).*
Keywords*: Emotet; Geodo; Mummy Spider; Banking Trojan; Phishing; Credentials Theft; Malware Payloads; Trickbot; Ursnif; IceDiD; Security Situational Awareness(SSA); C2C; Spam; Ryuk ransomware; Worm.*

Date of Submission: 26-07-2020 Date of Acceptance: 10-08-2020

I. Introduction

Emotet malware was discovered in June 2014, and it has recently evolved into an international threat distributor acting as **Malware-as-a-Service** by distributing and dropping other banking Trojans such as Trickbot, Ursnif, Ryuk payload, and IceDiD.

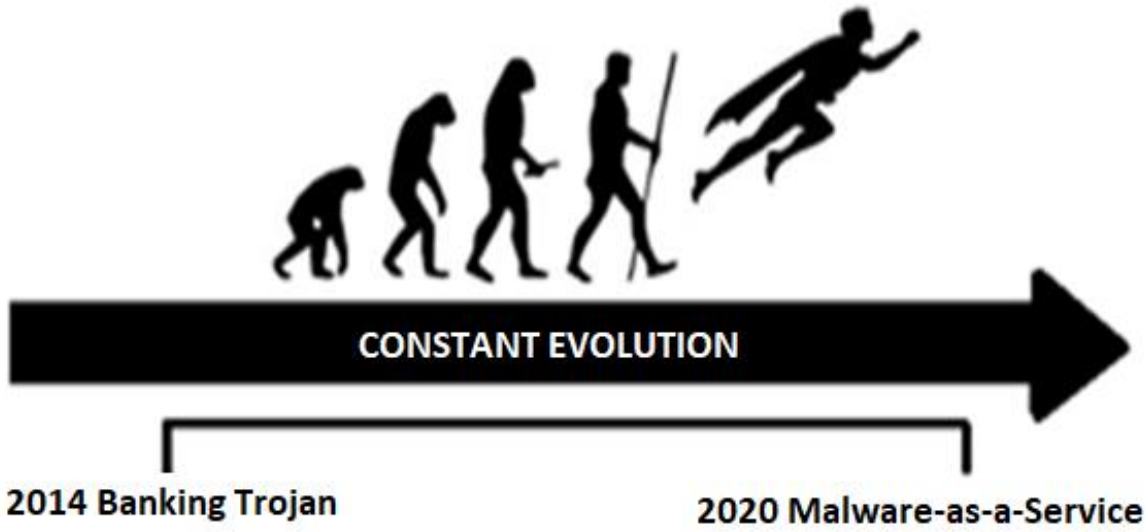


Fig.no 1: Evolution of Emotet Malware

Emotet is also known as Geodo, and the top cybersecurity firm CrowdStrike categorized this malware actor as MUMMY SPIDER. The malware is recognized as an evolved binary due to different iterations over the years as it continuously changes its payloads all the time. Emotet malware poses a threat to many computers and networks because it duplicates itself into standard permanent locations on the windows system in charge of handling files.

The main goals of this malware are gaining access to the infected device, collecting much different information on the victim from the device, and downloading payload modules from the C2 made in a way that it takes the most advantage of the profile of the machine and steal credentials. Due to its persistence capabilities such as random services creation, auto-start registry values, and loaded DLLs, it is difficult for the Malware Analysts to remove this malware altogether. It is, therefore, a severe malware that is capable of delivering other malware payloads for criminals contracting with the operators of the malware so that they can drop the malware for them.

Traditionally the payloads have mostly been other banking Trojans, with Trickbot and ransomware the most prevalent. This research will offer a better understanding of the malware by analyzing its operational capabilities and infection variant methods. G Data company researchers study revealed that more than 33,000 variations of the Emotet malware in the first of the 2019 year alone. Some of the variants of Emotet are discussed as follows.

Emotet Variant 1 has different modular structure capabilities, which include an installation module, a banking module, and a spam bot module. All these modules combined to conduct organized DDOS attacks to steal address books from MS Outlook and money from the Emotet infected victims bank account directly [1].

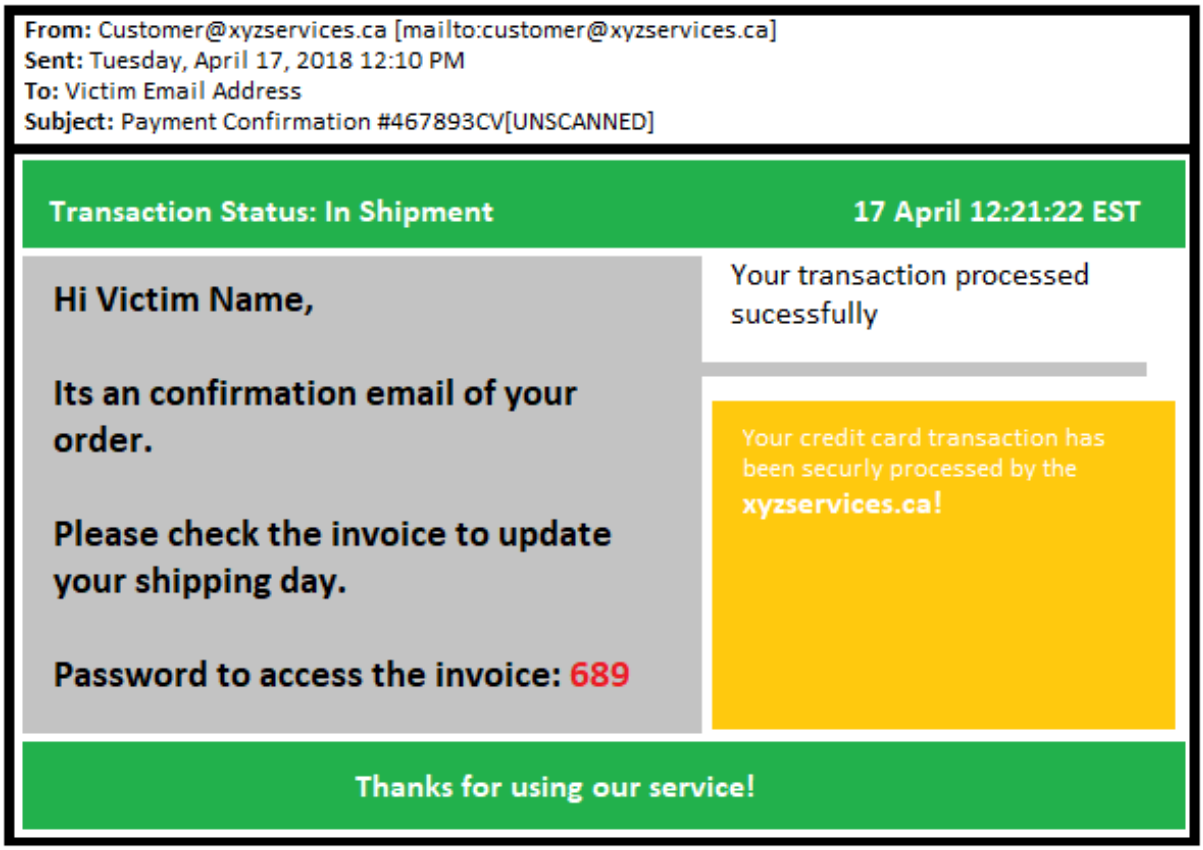


Fig. no 2: Example of Emotet Variant 1 Spam Email

Emotet Variant 2 uses a generic module to establish a code injection technique with three stages, such as opening a process, writing a process in memory, and creating a remote thread. This variant target \AppData\ folder and saves itself with a random binary name of eight characters such as abcxyzkl.exe with persistence capabilities in the below registry path and once it establishes persistence in the registry and it deletes itself from \AppData\ folder.

- Registry Path: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

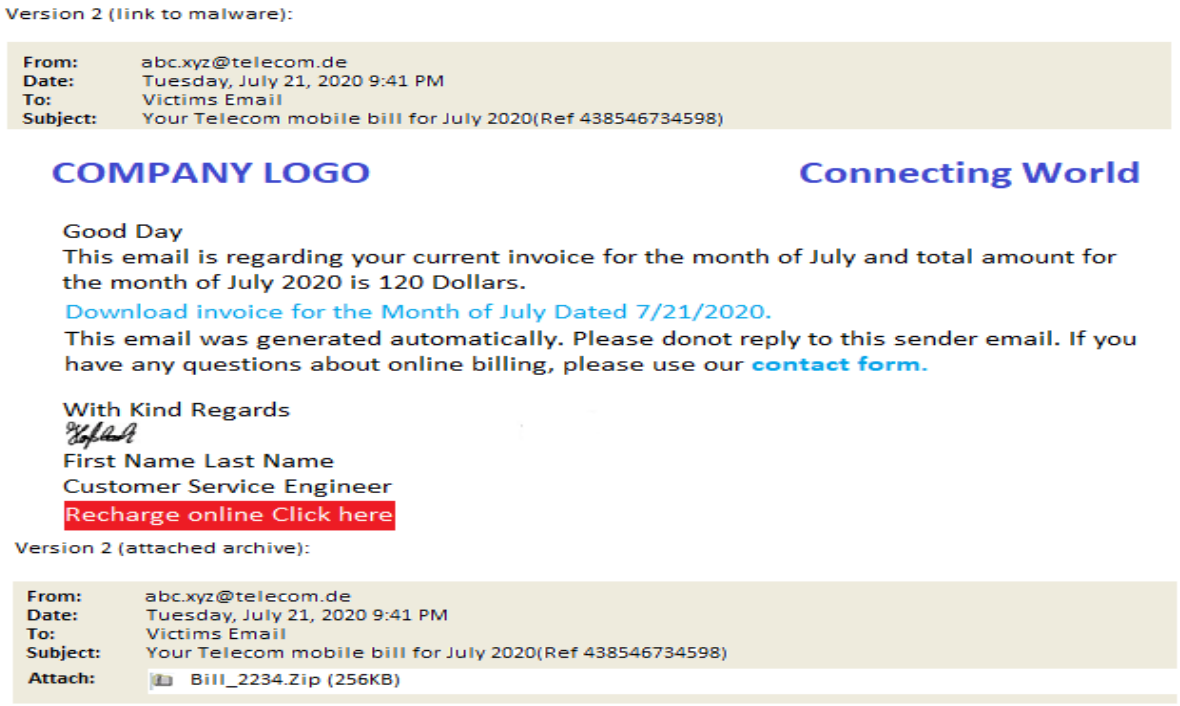


Fig.no 3: Example of Emotet Variant 2 Spam Email

Emotet Variant 3 only uses two stages, such as opening a process and writing a process in memory to launch itself. In writing a process in the memory stage, the address space of explorer.exe will be altered with the injected code of Emotet [2]. This variant targets folder: \Appdata\Microsoft\ and saves itself with a random binary name such as abcdxyz1234.exe in the below-mentioned file path and also adds persistence capabilities in the registry path as follows. Once it establishes persistence in the registry and it deletes itself from the \AppData\Microsoft folder.

- File Path: C:\Documents and Settings\Administrator\Application Data\Microsoft\abcdxyz1234.exe.
- Registry Path :HKU\Software\Microsoft\Windows\CurrentVersion\Run

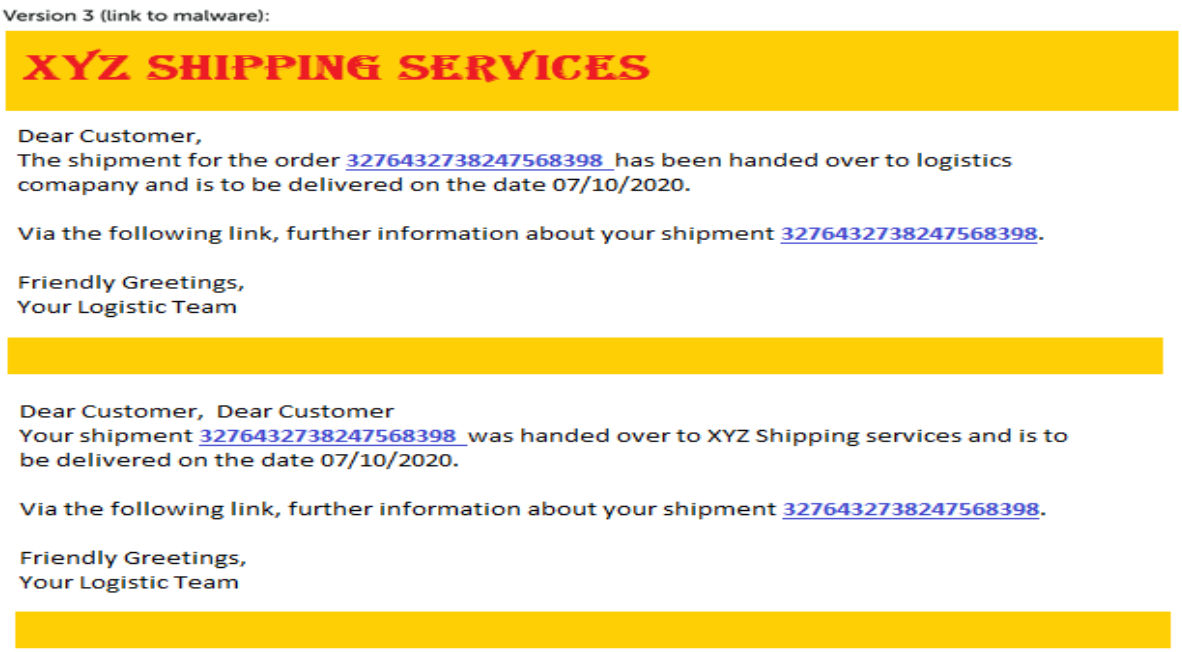


Fig.no 4: Example of Emotet Variant 3 Spam Email

II. Emotet Operation

Emotet malware infects devices through emails because most organizations and individuals rely on emails for communication and business matters. Once Emotet gets initial access via email attachments or links, it will infect the system with malicious payloads and take control of the user system. Then, it will spread over the network like a worm with no human interaction. Figure 5 demonstrates how Emotet operates step by step, as shown below.

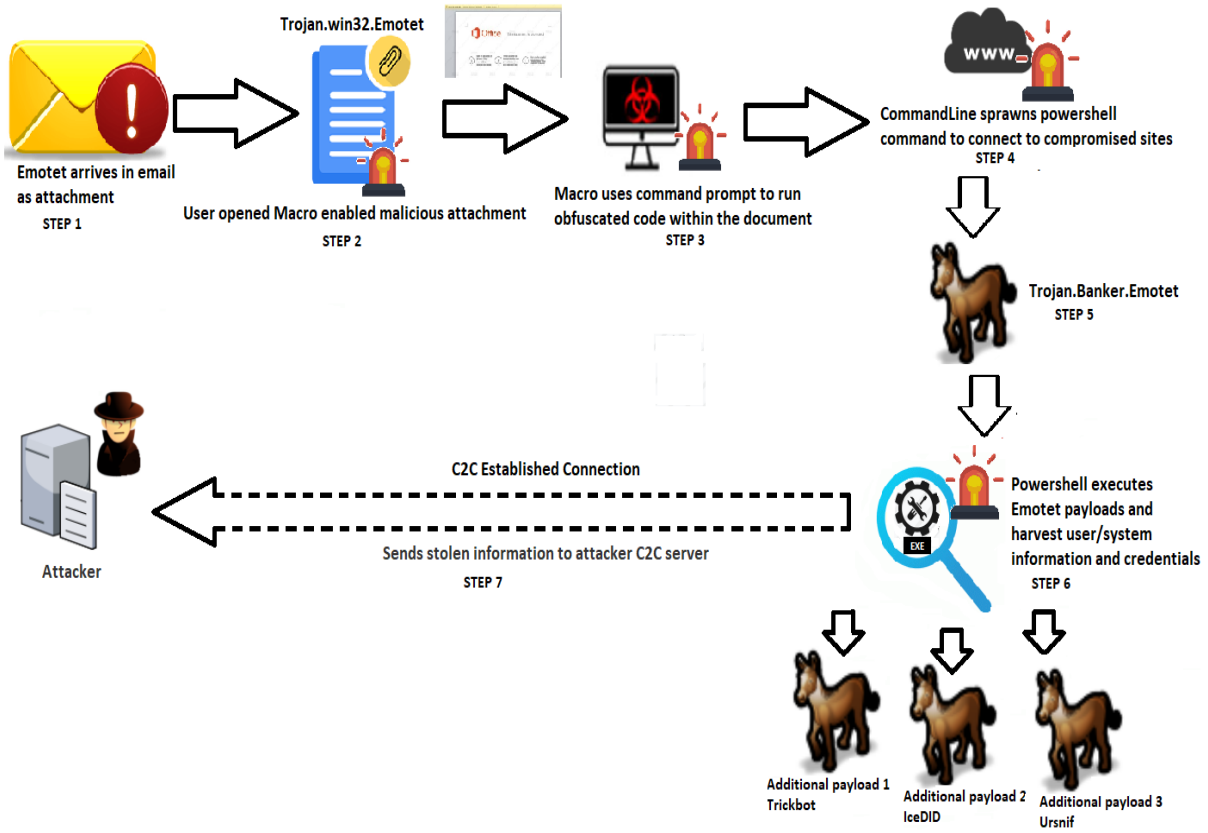


Fig. no 5: Emotet Malware Operation

Step 1: User receives an Emotet in email as a Microsoft Word attachment

Step 2: User opens Microsoft word document by accepting the license agreement which enables Emotet macros as shown in figure 6

Step 3: Macros use Command Prompt (cmd.exe) in the background of the system to run the obfuscated code within the document

Step 4: Command Prompt will also run PowerShell to connect to malicious Emotet sites.

Step 5: Malicious Emotet sites drop Emotet payloads onto the victim computer.

Step 6: Emotet also drops other Trojan modules such as Trickbot, IceDiD, and Ursnif onto the victim machine to steal user financial and personal information

Step 7: Emotet sends the stolen information to the attacker via C2C established connection

The distribution of Emotet malware occurs basically through phishing emails containing links to malicious PDFs, files, or Word attachments. Not only that, Emotet, in its latest form, can hijack existing email threads and insert a malicious link or file without changing the content of the email threads. Clicking on the malicious link installs a self-executable copy of Emotet malware on the systems, paving the way for more sophisticated attacks like targeted Ryuk and Maze ransomware attacks. Moreover, Emotet can evade antivirus tools and signature-based detection pattern capabilities and keeps its presence and moves across the network after removal with its persistence capabilities such as random services, Auto-start registry key values, and loaded DLLs (Dynamic Link Library).

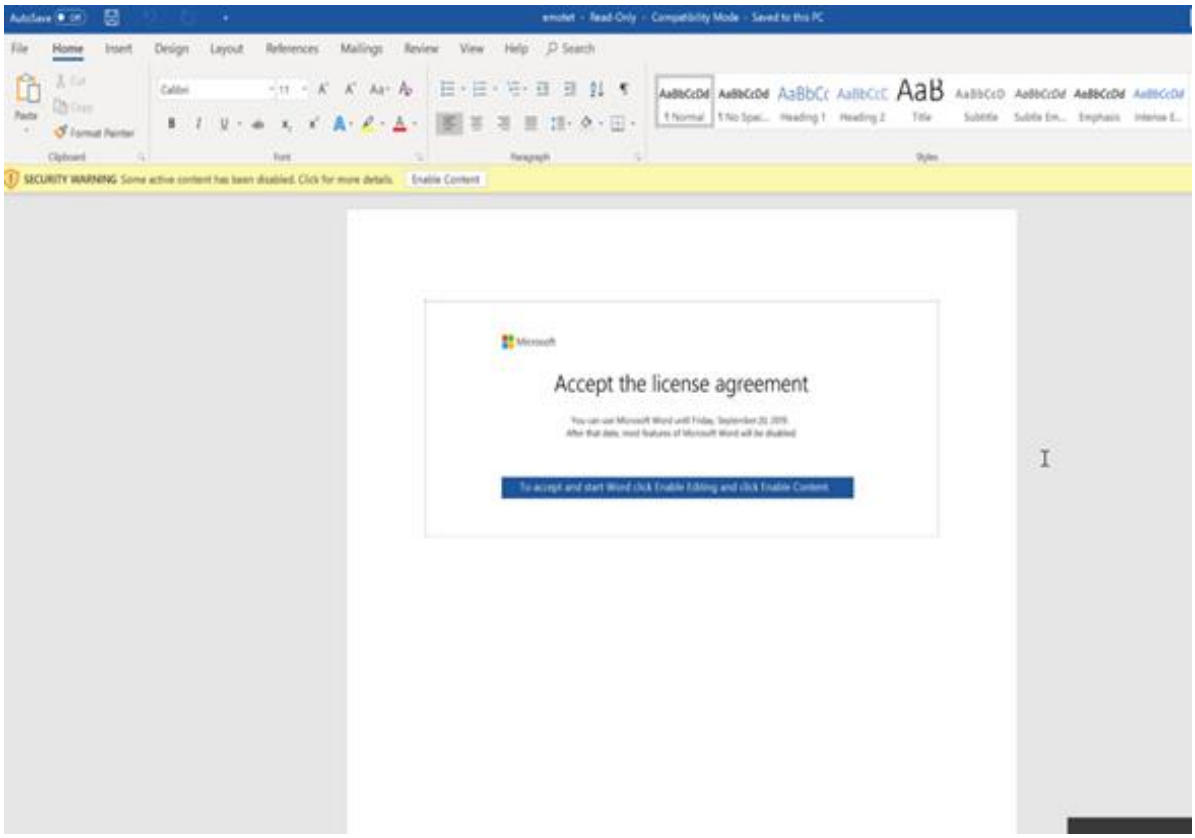


Fig. no 6: Word Document with Embedded Emotet Macros

III. Literature Review

Emotet malware is a common malware spread through spam emails, and it has been existence for many years [3]. It gets to a device through malicious scripts, links, or macro-enabled document files. The emails linked to the malware may look fancy with branded logos and designs to make them look like legitimate emails. The malware, therefore, tries to lure its users into clicking the malicious links using attracting language like "your invoice" or "payment details." Malware has undergone various iterations [4]. The first version was malicious JavaScript files, and it has evolved to incorporate the use of macro-enabled documents to drop the virus. The malware is hard to detect hence making it hard for organizations and individuals to analyze it. It is additionally polymorphic in that it can transform itself every time it gets downloaded on the machine, and its polymorphic capabilities also make AVs fail in detecting them efficiently and proactively. Not only that, but this malware employs the use of C & C servers to acquire updates and operates the same way the operating system updates itself on a laptop and does not contain any signals. This malware helps the hackers install various versions of the malware such as banking Trojans. Malware could also dump stolen data, such as sensitive information such as passwords, usernames, and email addresses [4].

The malware is widely known for its behavior of going through contact lists, particularly email addresses and sending itself to the top contacts. The emails do not look like spams become they come from legitimate sources, and recipients have a high likelihood of downloading the files because they come from trusted sources. When a user connects a device to a network, the malware spreads through the most popular passwords, and it spreads to other connected systems through the brute-force attacks. If a user uses the password as "password," the chances of the malware finding its way to the financial servers are high. The malware spreads through Eternal blue vulnerabilities (MS17-010) that linked to WannaCryattacks [4]. The attacks take advantage of weaknesses in windows security and other systems to allow the installation of the malware with or without less human interaction. The typical targets of the malware are government entities, individuals, and companies in Europe and the United States. Malware also targets financial data and bank logins [5]. The first step in protecting advice from the malware is learning how the malware works and providing situational awareness to users, not to open malicious links and macro enables documents. The organization ought to ensure that it is relevant with the latest patches from Microsoft Windows. Pekta & Acarman team argue that avoiding suspicious emails can also help to protect the device from infecting with the malware [6]. However, previous literature did not provide any Security Situation Awareness (SSA) for the users on Emotet malware. This paper

will get into the bottom of this user awareness issue and give the users solid Security Situational Awareness on Emotet malware.

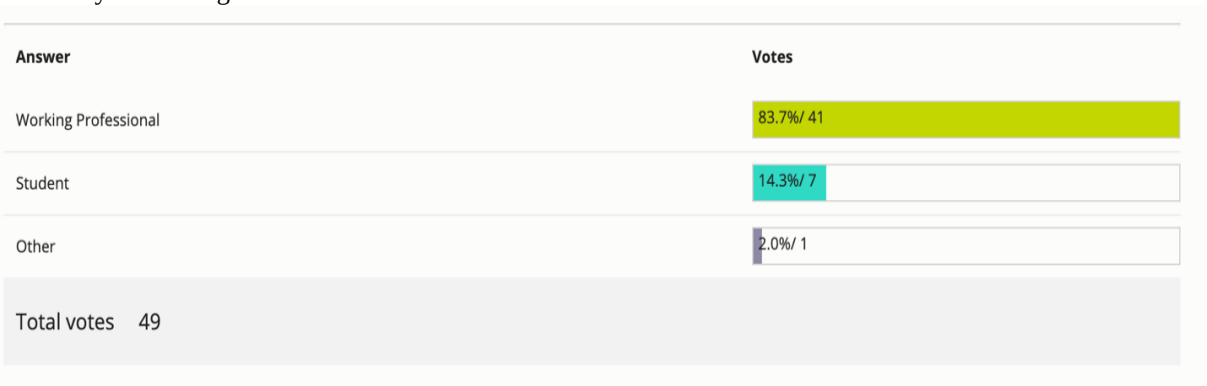
IV. Method

The research used a survey questionnaire instrument method for data collection. In the survey questionnaire method, the survey question format was sent to IT working professionals and the student groups for responses using Opinion Stage - Online interactive content service platform. The survey questionnaire format was well designed with five closed-ended questions. However, the numbers of questions were also limited to respondent comfort and easiness. More than 45 responses were collected and analyzed. The data collection will be examined and explained clearly in the "Results' section. Based on responses and previous literature, this research study will design and develop Security Situational Awareness (SSA) to prevent Emotet infections.

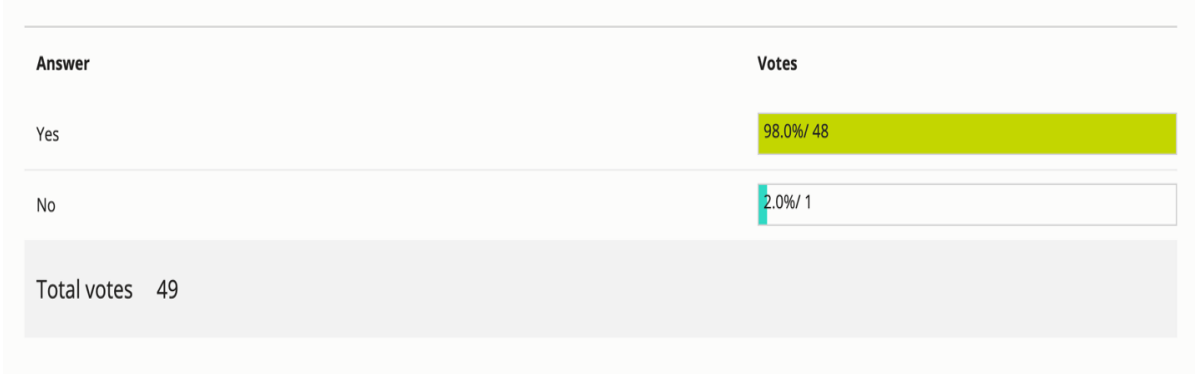
V. Results

Opinion Stage - Online interactive content service is used to conduct a survey questionnaire. The survey questionnaire was posted in groups of Students and IT working people. The following five questions were asked. The responses of the respondents helped to understand how users are familiar with Emotet Malware.

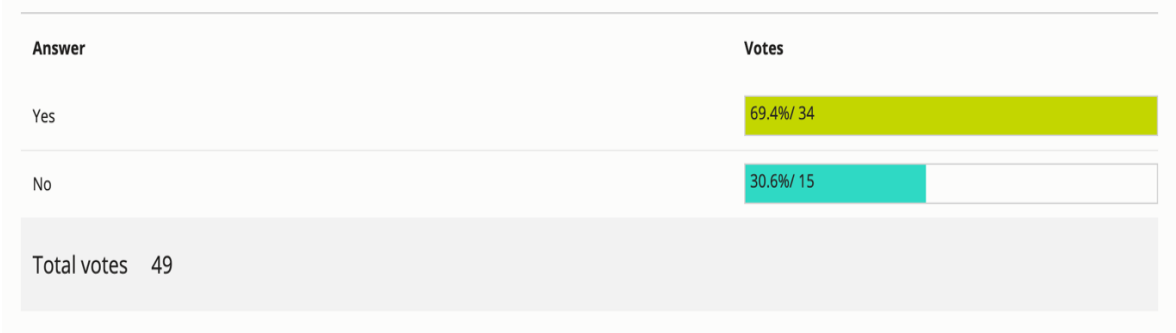
1. Are you working Professional or Student?



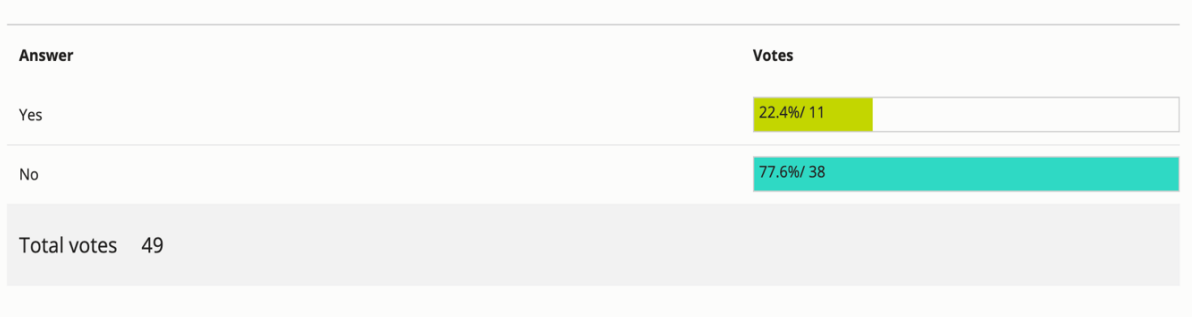
2. Do you use a computer frequently?



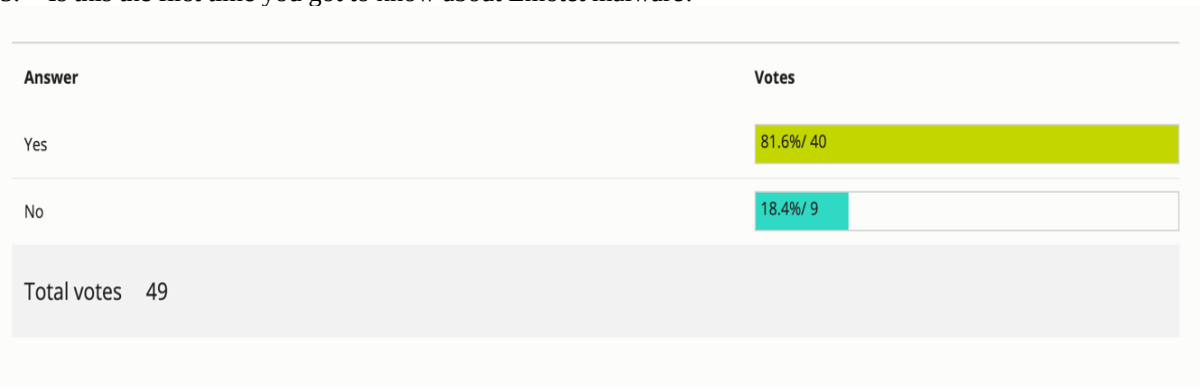
3. Do you have Antivirus software installed on your Personal Computer?



4. Have you heard about Emotet malware in the news recently?



5. Is this the first time you got to know about Emotet malware?



From all the above responses, it revealed that very few people know about the Emotet malware even though they use everyday computers. In questions 4 &5, more than 75% of respondents said that they have not heard about the Emotet malware. This response rate clearly shows that user situational security awareness about Emotet is very less. Therefore, Security Situational Awareness (SSA) about Emotet malware, its operation, and countermeasures are much needed for individuals and organizations.

VI. Security Situational Awareness (SSA)

The first line of defense against Emotet is to provide users with solid Security Situational Awareness (SSA) on Emotet malware. SSA helps users not to click on Spear Phishing links and not to opening Spear Phishing Attachments. Let's say if the user paranoid that he/she is infected with Emotet phish, the following Indicators of Compromise (IOCs) and Security Situational Awareness steps on the victim computer will help users to act immediately to prevent spreading it to other computers over the network.

Look for Emotet random Services that are created from remote hosts to spread over the network. Use the following instructions to see if Emotet created random services on the user computer.

- Using GUI:
  - Type services.msc on windows search, which will take to windows services.

    OR
  - Task Manager > Services
- Using PowerShell:
  - gwmi win32_service |select name, pathname | fl

    OR
  - Get-WmiObject win32_service | select Name, DisplayName, State, PathName | Format-List
- Using Command Line:
  - sc query | more

    OR
  - reg query HKLM\system\controlset001\services

Look for random binaries if Emotet dropped in AppData folders:

- C:\Users\<UserName>\AppData\Roaming\123456.exe
- C:\Users\<UserName>\AppData\Local\abcd.exe
- C:\Users\<UserName>\AppData\Local\Temp\xyz.exe
- C:\Users\<UserName>\AppData\Local\MicroSoft\Windows\abcdxyz.exe

Look for random binaries if Emotet dropped in System Root directories:

- C:\123456.exe
- C:\windows\abcd.exe
- C:\windows\system32\123456.exe
- C:\windows\sysWow54\xyz.exe

Look for Emotet persistence capabilities in Registry Keys:

- Using GUI
  - Registry Editor app
- Using Command Line
  - reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run
  - reg query HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
  - reg query HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
  - reg queryHKLM\Software\wow6432node\Microsoft\windows\currentversion\RunOnce
  - reg query HKEY_USERS\<User SID> \Software\Microsoft\windows\CurrentVersion\Run
  - reg query HKU\<User SID> \Software\Microsoft\windows\CurrentVersion\Run

Look for Emotet persistence capabilities in Schedule Tasks:

- Using GUI
  - Task Scheduler app
- Using Command Line
  - ls C:\Windows\System32\Tasks
  - ls C:\Windows\Syswow64\Tasks
  - schtasks | more

IOCs, as mentioned above, will determine that the user is infected with Emotet after clicking on Spear-Phishing link or opening Spear-Phishing attachment. Once Emotet infection is established, it is required to contain the victim machine first from VLAN or network infrastructure to prevent its worming capabilities from spreading to other computers in the network. If multiple computers in the network are infected with Emotet malware, following Security Situational Awareness (SSA) steps, mitigation and remediation actions are recommended:

- Identify Emotet infection on the machine with IOC's, Shutdown and Isolate the system from the network
- Identify persistence capabilities of the infection especially in Services, ScheduledTasks, Registry entries to prevent reinfections
- Block SMB communications between infected systems in a network to mitigate Emotet worming capabilities. Group Policy Setting and configuration host-based Intrusion Prevention Systems (HIPS) can block SMB communications
- Look out IOCs and artifacts for dropped TrojansTrickbot, Ursnif, and IceDiD
- Avoid logging into the infected system using Local and Domain administrator accounts

- Move the infected system to separate VLAN to remove all artifacts while remediating the system
- Reimage the system
- Reset Local and domain credentials on the system
- Change credentials for any applications passwords which were stored and used on the system
- Make sure to review the Mail inbox and remove Emotet Phish emails
- Make sure to apply and change email filter and block rules accordingly
- Make sure to block Emotet payload domains at the firewall level
- Make sure to have Antivirus software and host-based Intrusion Prevention Systems (HIPS) on the system

The paper also recommends that solid Security Situational Awareness (SSA) is essential and required for individuals and organizations to know how to block Emotet by taking necessary countermeasures in the first place.

- First and most, organizations should provide Security Situational Awareness (SSA) training on Social Engineering and phishing attacks
- Organizations must urge employees not to click or open phishing links and phishing attachments. The employees must be made to know that they should not share personal information, passwords, and usernames, especially from a request coming from an unsolicited source. Also, they must be trained on how to avoid posting confidential data online and should not open an email deemed suspicious or click links related to such emails
- Organizations should make use of GPO configuration on Windows firewall rules to block inbound SMB communications between client systems.
- If organizations are using Host-based Intrusion Prevention Systems(HIPS), make sure to control of client-to-client SMB communication
- Individuals should use latest and reliable antivirus tools and conduct automatic periodic scans accordingly
- Organizations and individuals should patch the systems immediately whenever patches are available
- Organizations should have firewall and email policies to block to detect and prevent malicious IP addresses, suspicious emails, phishing attachments, and other malicious IOCs
- Organizations should have a policy where employees or individuals in the organization must inform the IT security department or Incident Response team if they are accidentally open or click on a phishing email.
- Organizations should have an external email policy where emails should be marked using a RED banner to ascertain that they are from an external source hence enabling users to take note of spoofed emails
- Organizations should have the least privilege policy where it mandates and minimizes the employee's level of access needed to finish a given task. Designated administrators should be used to limit the number of workers who can access administrative credentials
- Organizations should have the domain-based message authentication reporting, and conformance (DMARC) should be established to enhance validation and reduce spam emails. The system uses digital signatures and domain name system (DNS) to take note of email spoofing[7]
- Individuals should adopt and setup Multi-factor authentication for systems and applications
- Individuals should adopt IP Geo-facing and set up transaction alerts for bank accounts and prevent stealing funds from their bank accounts.
- The best approach to prevent Emotet infection or any malware infection is to secure all machines in the organization with up-to-date patches and with less PowerShell usage.

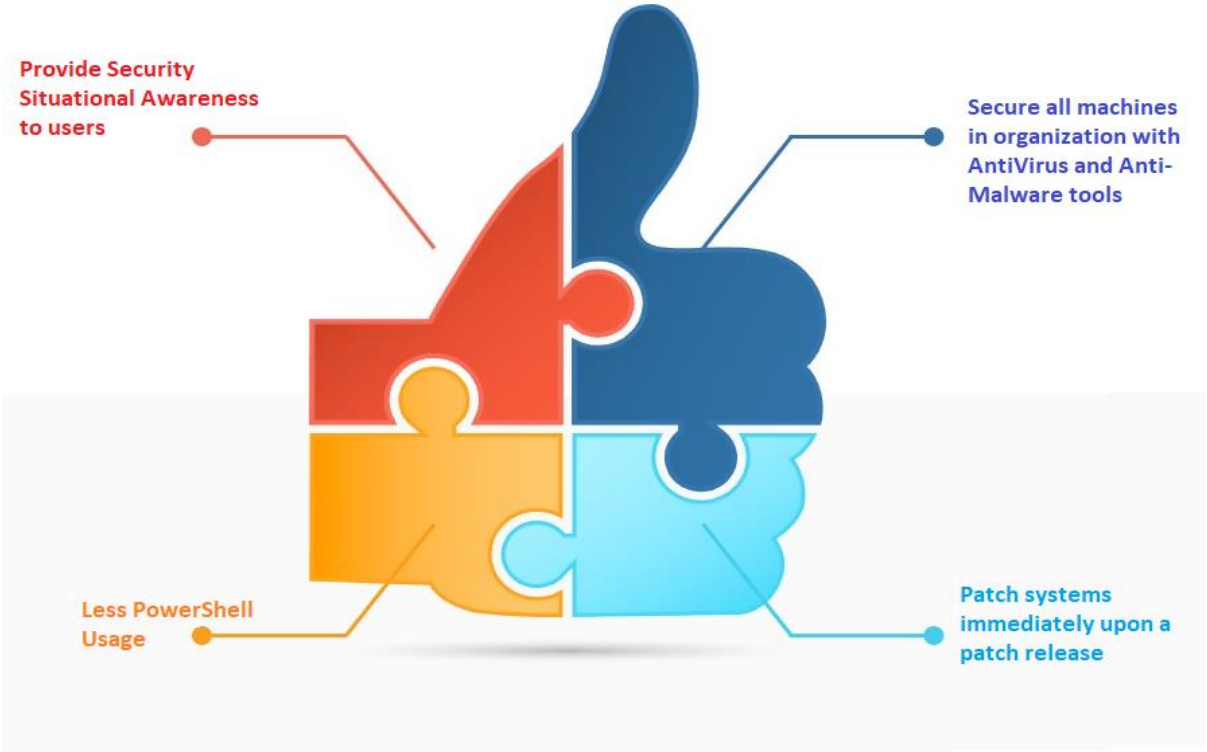


Fig. no 7: Best approaches to prevent Emotet Malware or any other malware infection

VII. Discussion

The Emotet malware uses social engineering tricks such as Spear phishing links and Spear phishing attachments to infect devices. The infection chain begins with a phishing email that can be sent from a legitimate email address but can be compromised given the fact that the malware's spamming module provides it with access to remote email service providers and spam emails from accounts that are infected. After a user clicks on the malicious link or downloads the attachment, he or she downloads an Emotet dropper unknowingly. A dropper is a document file with a malicious macro. When a dropper successfully runs, the downloading of Emotet executable occurs to establish a C2C connection to steal the data with exfiltration. Based on the analysis of the data, it is evident that users are not familiar with the Emotet Malware. It is an ongoing discussion of how efficiently organizations will put effort into detecting Emotet Malware due to its different variants and how well individuals can be trained on security situational awareness to preventEmotet Malware infections at first. Will internet users stop not clicking on phishing links and documents out of curiosity even though they went through proper cybersecurity training? The answer is NO because this is always a crucial topic and discussion of Emotet infection or any other malware infection. Not only that, but it also critical to employ the use of host-based intrusion prevention systems and group policy settings to restrict the server message protocol communications that occur in systems of a given network. The SMB enhances inter-process communication, and it enables services and applications of network-connected computers to communicate with each other. In other words, SMB is the protocol used by computers to establish communication between networks. If Emotet manages to gain access to the SMB, then the entire domains that include clients and servers become infected. Hence, further research is also needed to determine various approaches that can be used to reduce the risk posed by Emotet malware and how to protect devices from them.

VIII. Conclusion

Emotet malware is one of the malware families affecting many individuals and businesses because they are hard to detect with its different variants. Emotet malware has developed over the years, and every iteration presents new challenges for individuals and incident respondents trying to eliminate the malware. Emotet malware infects computers after victims clicking on links and opening attachments in emails. The individuals or users that are profoundly affected by Emotet malware are Western Europe and the United States. What organizations and individuals can do for now is avoid suspicious opening emails because this Emotet malware gets to devices through the emails. Hence, the only one precaution and countermeasure towards Emotet malware is to train users and employees on not to click on phishing links and not to open phishing documents. This paper well addressed the importance of Security Situational Awareness (SSA) on Emotet and provided precautions,

mitigations, and recommendations for individuals and organizations to prevent Emotet infections. This paper also stated that monitoring SMB communications for Emotet infections between client systems in the network is very critical and should be restricted via group policy settings or in the configuration of Host-based Intrusion Prevention Systems (HIPS). In a nutshell, this paper addressed a lack of necessary awareness on a banking trojan malware Emotet. It provided Situational Security Awareness (SSA) to computer users on how not to fall victim to Emotet.

References

[1]. Niu, W., Li, T., Zhang, X., Hu, T., Jiang, T., & Wu, H. (2019). Using XGBoost to Discover Infected Hosts Based on HTTP Traffic. *Security and Communication Networks, 2019*.

[2]. Ceschin, F., Botacin, M., Gomes, H. M., Oliveira, L. S., &Grégio, A. (2019, November). Shallow security: On the creation of adversarial variants to evade machine learning-based malware detectors. In Proceedings of the 3rd Reversing and Offensive-oriented Trends Symposium (pp. 1-9).

[3]. Bhardwaj, A., & Goundar, S. (2019). A framework for effective threat hunting. Network Security, 2019(6), 15-19. doi:10.1016/s13534858(19)30074-1.

[4]. Azab, A., Layton, R., Alazab, M., & Oliver, J. (2014). Mining malware to detect variants. 2014 Fifth Cybercrime and Trustworthy Computing Conference. doi:10.1109/ctc.2014.11.

[5]. Threat Advisory. (2019). The evolution of Emotet: From banking Trojan to threat distributor. https://www.symantec.com/blogs/threat-intelligence/evolution-emotet-trojan-distributor.

[6]. Pektaş, A., & Acarman, T. (2018). Malware classification based on API calls and behavior analysis. IET Information Security, 12(2), 107-117. doi:10.1049/iet-ifs.2017.0430.

[7]. Soomro, T. R., & Hussain, M. (2019). Social Media-Related Cybercrimes and Techniques for Their Prevention. Applied Computer Systems, *24*(1), 9-17.

[8]. Alert (TA18-201A) Emotet Malware. (July 20, 2018). Retrieved from https://www.us-cert.gov/ncas/alerts/TA18-201A**.**

[9]. Emotet: Nastier Than WannaCry and Harder to Stop. (Feb 2010). A Sophos Whitepaper Retrieved from https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/2019/Sophos_LC_Q219_emotet-nastier-than-wannacry-wp.PDF.

[10]. Littlefield (May 31, 2019). Three's a crowd: New Trickbot, Emotet & Ryuk Ransomware. Mediumhttps://littlefield.co/threes-a-crowd-new-trickbot-emotet-ryuk-ransomware-16d1e25f72f4.

[11]. Alexey Shulmin (Apr 9, 2015). The Banking Trojan Emotet: Detailed Analysis. Secure list. https://securelist.com/the-banking-trojan-Emotet-detailed-analysis/69560.

[12]. Cybereason Nocturnus (Apr 2, 2019). Triple Threat: Emotet Deploys Trickbot to Steal Data & Spread RYUK. Cybereason. https://www.cybereason.com/blog/triple-threat-emotet-deploys-trickbot-to-steal-data-spread-ryuk-ransomware.

[13]. ESET Research (Nov 9, 2018). Emotet Launches Major new Spam Campaign. Welivesecurity. https://www.welivesecurity.com/2018/11/09/emotet-launches-major-new-spam-campaign/

[14]. ASEC Report. Emotet Returns to Prey on Banking Information (2017).

Sivaraju Kuraku, et. al. "Emotet Malware – A Banking Credentials Stealer." *IOSR Journal of Computer Engineering (IOSR-JCE)*, 22(4), 2020, pp. 31-41.