Assignment:

Research and Exploit- Part B:

The *"Emotet"* Trojan Horse

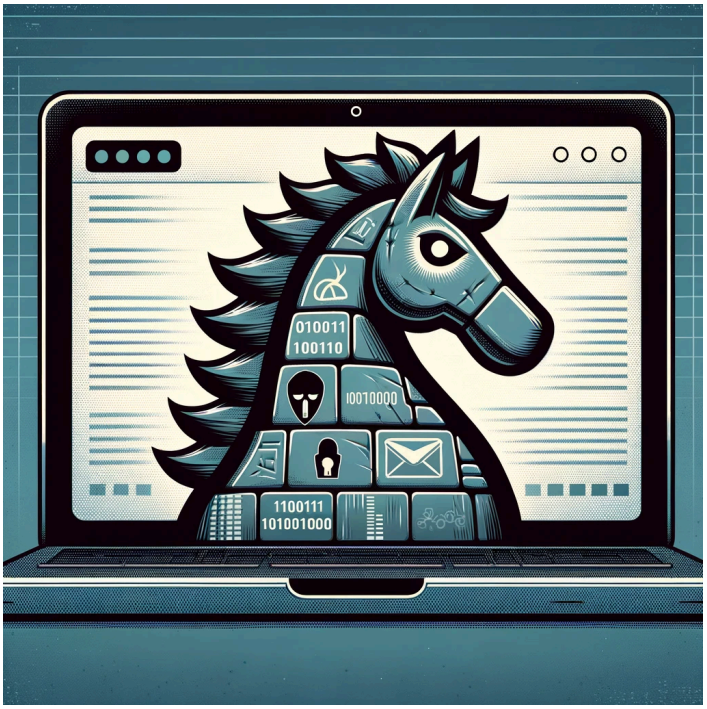

Image Generated by Dalle-E 2 from chat GPT

Prepared for

Kokub Sultan

Prepared by Group 6

Valentine Jingwa, Jean-Pierre Nde-Forgwang

Security System, Cohort E

School of Advance Digital Technology

SAIT

20 January 2024

Index

Emotet

- ## *What is Emotet:*

  Emotet is a virus which started as a banking Trojan design to steal financial data, however it has evolved into a sophisticated and layered malware delivery service. It now uses malspan ("designate malware that is delivered via email messages" [1])as a dynamic means of transportation [2].

- ## *What type of Virus is Emotet?*

  Trojan Horse: "[F]ile, program, or piece of code that [masquerades and] appears to be legitimate and safe, but is actually malware [3]."

- ## *Where does Emotet Originate from?'*

  In terms of Emotet, "Ukraine" [4] is believed to be its origin. However, it is impossible to know the exact origin of complex and elaborate malwhare, as is the case due to its sophisticated and secretive creation.

- ## *Where and when was Emotet Detected?*

  Emotet was first identified in "2014 [2]", the first iteration was aimed at targeting bank account details. Origin believed to be "Ukraine [4]"

- ## *How does Emotet Work?*

  Emotet, being a Trojen; as the name suggest, it disguises itself as legitimate and authentic, however embedded within it (*file, data, link, code*) is malware. Beginning by reaching victims email via phishing *("[p]hishing is a type of online scam that targets consumers by sending them an e-mail that appears to be from a well-known source* [5]"), tricking the user into opening the attachment or link. At this point the malicious malware is downloaded and installed, infecting the users computer or device. Emotet uses varicose techniques to evade antivirus and malware detection software, it then accesses the contact list existing within infected device. This allows Emotet to share the same "phishing email [5]" to users contact list; spreading. Once Emotet is installed, it

becomes a gateway for other malware and ransomware, downloading it into the infected device. This opens the floodgates to data theft and fraud [6],[7].

- *Who is often its main target?*

In terms of Emotet and its target, nobody is safe; No person, bank, government, or institution is immune to an Emotet attack. A speculation for an Emotet attack would be a means to steal data and secure monetary gains.

- *What damages did Emotet cause?*

Emotet is not a solved virus, due to its complexity and sophisticated nature, and its ability to update itself and evolve to its environment, making it prevalent today. The damage caused is dependant on the severity of the attack, its speculated to cost about one million per incident [8]. In terms of damage, an Emotet attack could compromise sensitive and classified data, as well as cause financial refraction to those affected. There could also be escalated cause and effect of which cannot be measured.

- AllenTown Pensylvania, February 2018

In February 2018, the city of Allentown, Pennsylvania, suffered a severe Emotet infection that significantly disrupted municipal operations and services. Financial operations, including transactions and payments, were severely disrupted.
The city's police department was also affected, although emergency services remained operational.The recovery was lengthy and expensive, with initial estimates for remediation and recovery efforts reaching up to $1 million.[11]

- *What are the legal or ethical problems associated with Emotet?*

Emotet presents significant legal and ethical challenges. Legally, it involves criminal activities like unauthorized access to computer systems, data theft, and financial fraud, which are offenses under various national and international cybercrime laws. Ethically, Emotet raises concerns about privacy invasion and the unethical use of technology for malicious purposes [8].

-

- *How can Emotet be Mitigated or Stopped? [9]*

  In terms of stopping Emotet, it seems impossible with our current technology, mitigation is possible:
  - "Invest in a reliable anti-malware solution" [9]
  - "Use common sense when downloading programs and opening files" [9]
  - "Be careful with file sharing" [9]

  Emotet is a complicated and sophisticated piece of malware, the best defence is knowledge and awareness of its existence.

- *Who was or was responsible for the propagation of Emotet? What was their motivation behind it and what legal consequences do or did they face?*

  The specific individuals behind Emotet's propagation are not definitively known due to the anonymous nature of cybercrimes. However, cybercrime organizations, often motivated by financial gain, are typically responsible for such sophisticated malware. Legally, perpetrators face severe consequences, including international law enforcement collaboration leading to arrests, charges of cybercrime, fraud, and even terrorism in some cases [8],[10].

- *What security practices could have been placed to have prevented the access of the trojan horse into their system and consequently the loss of privacy to their data and spread of the trojan's influence to their systems?*

  The Allentown incident is a stark reminder of the potential impact of Emotet and similar malware. It underscores the importance of maintaining robust cybersecurity defenses, including up-to-date antivirus software, regular patch management, employee training on phishing awareness, and effective backup and disaster recovery plans.

Reference:

[1] "Malspam," Malwarebytes, [Online]. Available: *https://www.malwarebytes.com/blog/threats/malspam.* [Accessed: Jan. 20, 2024].

[2] "Emotet," Malwarebytes, [Online]. Available: *https://www.malwarebytes.com/emotet.* [Accessed: Jan. 19, 2024].

[3] "What is a Trojan Horse?," Avast, [Online]. Available: *https://www.avast.com/c-trojan.* [Accessed: Jan. 19, 2024].

[4] "Emotet," Wikipedia, [Online]. Available: *https://en.wikipedia.org/wiki/Emotet.* [Accessed: Jan. 19, 2024].

[5] "Phishing Scams," Federal Trade Commission, [Online]. Available: *https://www.ftc.gov/news-events/topics/identity-theft/phishing-scams.* [Accessed: Jan. 19, 2024].

[6] "Emotet Malware Analysis," YouTube, [Online]. Available: *https://www.youtube.com/watch?v=oYQrIgx0wV4.* [Accessed: Jan. 19, 2024].

[7] "A Deep Dive Look at Emotet Malware," Microstrat, [Online]. Available: *https://www.microstrat.com/resources/insights-events/blog/a-deep-dive-look-at-emotet-malware/#How_does_it_work.* [Accessed: Jan. 19, 2024].

[8] "Emotet Malware Disrupted," FBI, [Online]. Available: *https://www.fbi.gov/news/stories/emotet-malware-disrupted-020121#:~:text=According%20to%20the%20U.S.%20Cybersecurity%20and%20Infrastructure%20Security,up%20to%20%241%20million%20per%20incident%20to%20remediate.* [Accessed: Jan. 19, 2024].

[9] "What is a Trojan Virus?," CyberNews, [Online]. Available: *https://cybernews.com/malware/what-is-a-trojan-virus/.* [Accessed: Jan. 20, 2024].

[10] "Emotet Botnet Disrupted in International Cyber Operation," U.S. Department of Justice, [Online]. Available: *https://www.justice.gov/opa/pr/emotet-botnet-disrupted-international-cyber-operation.* [Accessed: Jan. 20, 2024].

[11] "How One Emotet Infection Took Out This Organization's Entire Network," ZDNet, [Online]. Available: *https://www.zdnet.com/article/microsoft-how-one-emotet-infection-took-out-this-organizations-entire-network/.* [Accessed: Jan. 20, 2024].