Guess Who's Back (Back Again): Emotet Returns After Three Months of Silence

After a brief hiatus, Emotet threat actors have re-commenced operations as of early March 2023. Originally tracked as a banking trojan, Emotet has evolved into a multi-purpose dropper/downloader malware. Emotet derives its success based on the sheer volume of spam emails it sends, with some campaigns ranging in the millions. Using a phishing technique known as email hijacking, attackers insert themselves into existing business conversations or initiate new email conversations based on information previously gathered. This makes it appear that the malicious email is from a trusted source and can contribute to a higher success rate as victims are more prone to open the malicious emails. Additionally, operators create a sense of urgency by utilizing topics such as invoices for services.

In recent activity, Emotet creators have adopted binary padding as an evasion technique, purposefully inflating the files to over 500MB to make it harder for antivirus solutions to scan and detect them as malicious. These emails contain a ZIP file (.zip) attachment that includes an infected Word document that prompts the user to enable macros. Once enabled, it downloads the Emotet Digital Link Library (DLL) from an external site and loads it to memory. In some instances, embedded links have been used, however in this campaign they have not been included. After Emotet is loaded, it waits for instructions from a remote command and control server, which typically includes downloading additional payloads to include ransomware.

As Microsoft moves to disable macros by default, we anticipate Emotet operators to shift to a new format for delivery of the malware. Historically, Emotet operators have targeted organizations in healthcare, government, banking, and education industries, with small businesses and individuals being impacted the most.

The Critical Start Cyber Threat Intelligence (CTI) team will continue to monitor the situation and work closely with the Threat Detection Engineering (TDE) team and the SOC to implement any relevant detections. For future updates, the CTI team will post via ZTAP® Bulletins and on the Critical Start Intelligence Hub.

References:

1. https://www.darkreading.com/threat-intelligence/emotet-resurfaces-yet-again-after-three-month-hiatus
2. https://cofense.com/blog/emotet-sending-malicious-emails-after-three-month-hiatus/
3. https://www.bleepingcomputer.com/news/security/emotet-malware-attacks-return-after-three-month-break/
4. https://www.trendmicro.com/en_us/research/23/c/emotet-returns-now-adopts-binary-padding-for-evasion.html