Critical Alert: Emotet Malware

Description: Emotet is an advanced, self propagating and modular trojan, which initially appeared in 2014 as a banking trojan and is known to infect computers with an intent to steal confidential information. It was taken down in 2021 but has reappeared and currently distributes other malware or malicious campaigns. Emotet uses multiple methods for maintaining persistence and evasion techniques to avoid detection and can be spread via phishing spam emails containing malicious attachments or links.

The Australian Cyber Security Center (ACSC) advisory on the resumption of the emotet malware campaign indicated that a recent increase in the Emotet malware using the email thread 'hijacking' technique to spread itself has been observed. Using this technique the malware steals the infected victims email contacts including recent email threads and sends it to Command & Control (C&C) servers. Phishing emails are further sent to uninfected contacts using the existing email threads to make it seem real by pretending to be from the victim's email address.

One of the users reported to BtCIRT that they received an email impersonating to be from a work contact. In the email was an attachment with a password protected zip archive file (2022-04-02_1702.zip) containing an empty excel file (2022-04-02_1702.xls). This excel file with the hash (SHA-1:94994ff5ea2b7a373090ed189427a1db9e41d7d) was detected to be a windows trojan 'emotet' by microsoft and several other antivirus software. Attachments or links of any type could also be used to spread the malware.

Systems Infected as of today: Windows devices including computers and servers

Mitigation measures: Therefore, BtCIRT urges all users to be extra vigilant before clicking on links or downloading and opening attachments received through any communication medium including emails, instant messaging apps, sms, etc.

Precautions

1. Verify with the sender before clicking on any links or downloading attachment even if it appears to come from known contact.
2. If you need to click on the link or attachment always verify by submitting the link or hash of the file to VirusTotal
3. Ensure your device has all applications updated including the anti-virus software.
4. Always disable macros within MS Office unless required. When you have to, only enable macros from trusted locations and are digitally signed.
5. Say big "NO" to pirated resources including microsoft office, movies, documents and any other applications.
6. For a database of urls related to emotet visit URL haus and Feodo Tracker for list of C&C servers. Remember not to click on domain or IPs reflected in their database since those are malicious resources used to distribute malware.
7. Visit and check CISA technical alert on Emotet for more details of how the malware is operated and how to mitigate the risk related to it.

If your device has been infected

1. Immediately isolate your machine from the network
2. Update the antivirus and scan the device.
3. Patch your OS and applications if you haven't and immediately change all credentials.
4. Alert your contacts not to open any such attachments that might seem to come from you.
5. Always backup your machine periodically; it will save you when there is no other way left.

References

1. https://www.cyber.gov.au/acsc/view-all-content/advisories/advisory-2020-017-resumption-emotet-malware-campaign#:~:text=The%20ACSC%20has%20observed%20a,and%20Control%20(C2)%20server.
2. https://www.cisa.gov/uscert/ncas/alerts/aa20-280a
3. https://success.trendmicro.com/solution/1118391-malware-awareness-emotet-resurgence
4. https://www.malwarebytes.com/emotet
5. https://securitybrief.com.au/story/trickbot-takes-top-malware-spot-in-australia-emotet-returns