Threat Actors Using Microsoft OneNote

Summary

Recently, several malware operators have been spotted using OneNote attachments in their spam campaigns. OneNote is a powerful digital notebook tool offered by Microsoft. It provides users with a centralized location to store their thoughts, ideas, and notes in an organized manner. Cyber criminals have started new phishing campaigns delivering malicious OneNote attachments that deliver Formbook, Redline Stealer, AsyncRat or Qbot malware to unsuspecting victims.

Malware Details

- Formbook: FormBook is a well-known commercial malware, so dubbed because it has been sold "as-a-service" on hacking forums since 2016. It is designed to steal personal information from victims' devices and manipulate their devices using control commands from a C2 server. FormBook, which has been detected in the wild for over five years, is designed to steal personal information using keyloggers and form grabbers to collect victim input along with the data of some software, such as browsers, IM, Email clients, and FTP clients.
- Redline Stealer: Redline Information Stealer malware harvests information from browsers such as saved credentials, autocomplete data, and credit card information. A system inventory is also taken when running on a target machine, to include details such as the username, location data, hardware configuration, and information regarding installed security software. More recent versions of Redline added the ability to steal cryptocurrency. FTP and IM clients are also targeted by this malware family. Additionally, Redline Stealer can upload and download files, execute commands, and periodically send back information about the infected computer.
- AsyncRat: AsyncRAT is an open-source remote administration tool released on GitHub in January 2019. It's designed to remotely control computers via encrypted connection, providing complete control via functionalities such as: view and record screen, keylogger, upload, download and execute files, chat communication, persistence mechanisms, Disable Windows Defender, shutdown/restart the machine, and DOS attack.
- QBot: QBot, (a.k.a. Qakbot, Quackbot, or Pinkslipbot), is a banking Trojan discovered in 2007. Its main purpose is to steal banking credentials and other financial information. It continuously evolves with variants having worm-like capabilities, able to drop additional malware, log user keystrokes, and create a backdoor to compromised machines.

Recommendations

Threat actors are making their phishing campaigns more realistic and harder for users to detect. Users should always check the email content listed below thoroughly before clicking on any links or opening any attachments.

1. Always check the "From" email address for signs of Fraudulence.
2. Watch for misspellings or incorrect logos (ex. Southwest (legitimate branding) vs. SouthWest).
3. Be suspicious of all hyperlinks and documents.
    a. Check if the URL leads to the website you would expect based on the sender.
4. **Do NOT** open any attachments until you are 100% sure the sender is legitimate.
    a. If a user opens an attachment and there is an additional "open" button they must click on to receive attachments from the cloud, **DO NOT CLICK ON OPEN!** Immediately reach out to the sender to validate the attachment and contents.
    b. Users should avoid opening suspicious attachments or links to prevent any kind of infection.
5. Be skeptical of urgency — it's a common characteristic of phishing.
6. Be cautious of any emails that land in your inbox outside of business hours.

Conclusion

After Microsoft disabled malicious macros in Office documents in July 2022, threat actors are seeking newer options to execute code on unsuspecting targets' devices. The OneNote campaign is the latest trend in threat actors attempting to avoid detection by anti-virus solutions, increasing the likelihood of successful infections. Continue to ensure employees are vigilant with their email hygiene to prevent potential breaches.

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.