MITRE ENGENUITY | Center for Threat Informed Defense

Executive Report

Business-Critical Processes Targeted by Multiple Threat Actors

Date of Report :

February 1, 2023

Executive Summary

OneNote is increasingly being leveraged to distribute malware by cyber criminals. The reliance on sharing data via OneNote in the company to encourage collaboration makes our users susceptible to this new initial intrusion vector and threat actors are leveraging legitimate Microsoft services to send OneNote files that contain malware. Unlike traditional forms of phishing, training is unlikely to be an effective mitigation as business process involves the expectation of OneNote links to be sent via email.

Key Points

- Over the last four months there has been a large increase in the use of Microsoft OneNote documents to successfully deliver malware.
- This increase is likely attributed to Microsoft blocking macros by default in Microsoft Office applications in 2022 due to long-term abuse by threat actors.
- Employee awareness training is unlikely to substantially reduce our vulnerability to this new method of exploitation because users are conditioned to click OneNote links sent to them via Microsoft addresses.

ASSESSMENT

We now face increased risk because cyber threat actors are targeting Microsoft OneNote, which is critical to our regular business operations. OneNote abuse poses a larger risk than malicious Word or Excel documents did prior to the macro change because we did not rely on macros for business processes. The new technique is effective in bypassing detection, introducing gaps in our threat detection coverage.

- Reports show multiple OneNote malware samples are going undetected by many anti-virus vendors including our current security stack. In January 2023, Proofpoint observed over 50 OneNote campaigns delivering different undetected malware payloads. Both lures and first stage implants have effectively evaded detection.

External researchers “assess with high confidence this is one of the largest email threat landscape shifts in recent history.”

- TA577’s adoption of OneNote is an early indicator that other more sophisticated actors will begin using this technique soon. TA577 is an initial access broker that facilitates follow-on infections for additional malware including ransomware.

OUTLOOK

Increased use of this vector is likely to continue, threatening our defenses and business-critical processes. Technical mitigations are currently limited as our security tools do not currently detect malicious OneNote files and maintaining a whitelist for collaboration is likely to cause too many business interruptions. Long-term consideration should be given to adapting business processes to reduce risk exposure.

KEY INTELLIGENCE GAPS

- What is the scope and scale of OneNote delivery of malware?
- What is the breakdown of effects related to this initial intrusion vector? What is our risk exposure to those?

INTELLIGENCE REQUIREMENTS

- What vulnerabilities are currently being exploited in the wild?
- What exploited vulnerabilities can our organization detect?
- Identify and research threat actors targeting similar organizations.
- Identify and research tools and malware used by threat actors targeting similar organizations.

FEEDBACK

Please take a moment to provide feedback on this report by emailing EXAMPLE@companydomain.com; all comments are reviewed and used to enhance future reporting.

1. Rate the product's overall value:
    a. Very valuable
    b. Somewhat valuable
    c. Of limited value
    d. Not valuable
1. Rate the product's overall value:
    a. Very valuable
    b. Somewhat valuable
    c. Of limited value
    d. Not valuable
2. Rate the product's utility:
    a. Highly actionable
    b. Actionable
    c. Not actionable.
3. Rate the product's quality of analysis:
    a. High quality analysis
    b. Acceptable quality analysis

DATA SOURCES

https://www.proofpoint.com/us/blog/threat-insight/how-threat-actors-are-adapting-post-macro-world

https://www.proofpoint.com/us/blog/threat-insight/onenote-documents-increasingly-used-to-deliver-malware

https://www.rapid7.com/blog/post/2023/01/31/rapid7-observes-use-of-microsoft-onenote-to-spread-redline-infostealer-malware/

PROBABILITY MATRIX

ALMOST NO CHANCE	VERY UNLIKELY	UNLIKELY	ROUGHLY EVEN CHANCE	LIKELY	VERY LIKELY	ALMOST CERTAINLY
remote	highly improbable	improbable (improbably)	roughly even odds	probable (probably)	highly probable	nearly certain
01-05%	05-20%	20-45%	45-55%	55-80%	80-95%	95-99%