Security Newsletter

3 Apr 2023

Subscribe to this newsletter

Microsoft OneNote will block 120 dangerous file extensions

Microsoft has shared more information on what malicious embedded files OneNote will soon block to defend users against ongoing phishing attacks pushing malware. The company first revealed that OneNote will get enhanced security in a Microsoft 365 roadmap entry published three weeks ago, on March 10, following recent and ongoing waves of phishing attacks pushing malware.

Threat actors have been using OneNote documents in spear phishing campaigns since mid-December 2022 after Microsoft patched a MoTW bypass zero-day exploited to drop malware via ISO and ZIP files and finally disabled Word and Excel macros by default. Threat actors create malicious Microsoft OneNote documents by embedding dangerous files and scripts and then hiding them with design elements, as shown below.

Today, the company shared more details regarding what specific file extensions will be blocked once the new OneNote security improvements roll out. Microsoft says it will align the files considered dangerous and blocked in OneNote with those blocked by Outlook, Word, Excel, and PowerPoint.

Read More

More #News

- Fake ransomware gang targets U.S. orgs with empty data leak threats
- BingBang: How a simple developer mistake could have led to Bing.com takeover
- Hackers exploit bug in Elementor Pro WordPress plugin with 11M installs

#Breach Log

- New Money Message ransomware demands million dollar ransoms
- New AlienFox toolkit steals credentials for 18 cloud services
- 15 million public-facing services vulnerable to CISA KEV flaws

#Patch Time!

- CISA orders agencies to patch bugs exploited to drop spyware
- Microsoft pushes OOB security updates for Windows Snipping tool flaw
- SAP releases security updates fixing five critical vulnerabilities

#Tech and #Tools

- DISH slapped with multiple lawsuits after ransomware cyber attack
- 10-year-old Windows bug with 'opt-in' fix exploited in 3CX attack
- Microsoft's 'Security Copilot' Unleashes ChatGPT on Breaches

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred Group is one of the world's leading online gambling operators with business across Europe, US and Australia, offering more than 30 million customers across 9 brands a great form of entertainment in a safe, fair and sustainable environment. The company, which employs about 2,000 people, is listed on Nasdaq Stockholm Large Cap and is a member of the European Gaming and Betting Association (EGBA) and founding member of IBIA (Sports Betting Integrity Association). Kindred Group is audited and certified by eCOGRA for compliance with the 2014 EU Recommendation on Consumer Protection and Responsible Gambling (2014/478/EU). Read more on www.kindredgroup.com.

You can access the previous newsletters at https://news.infosecgur.us