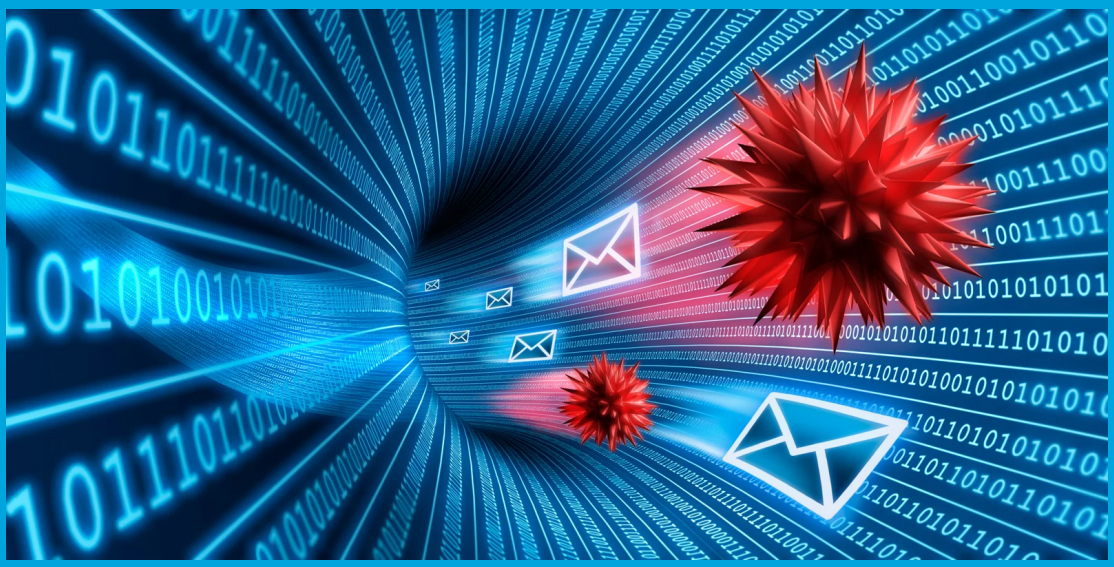
Security Newsletter

20 Mar 2023

Subscribe to this newsletter

Emotet malware now distributed in Microsoft OneNote files to evade defenses



The Emotet malware is now distributed using Microsoft OneNote email attachments, aiming to bypass Microsoft security restrictions and infect more targets. Emotet is a notorious malware botnet historically distributed through Microsoft Word and Excel attachments that contain malicious macros. If a user opens the attachment and enables macros, a DLL will be downloaded and executed that installs the Emotet malware on the device.

Once loaded, the malware will steal email contacts and email content for use in future spam campaigns. It will also download other payloads that provide initial access to the corporate network. This access is used to conduct cyberattacks against the company, which could include ransomware attacks, data theft, cyber espionage, and extortion.

While Emotet was one of the most distributed malware in the past, over the past year, it would stop and start in spurts, ultimately taking a break towards the end of 2022.

Read More

More #News

- Two U.S. Men Charged in 2022 Hacking of DEA Portal
- NordVPN open sources its Linux VPN client and libraries
- Adobe Acrobat Sign abused to push Redline info-stealing malware

#Breach Log

- Google finds 18 zero-day vulnerabilities in Samsung Exynos chipsets
- Multiple Hacker Groups Exploit 3-Year-Old Vulnerability to Breach U.S. Federal Agency
- RAT developer arrested for infecting 10,000 PCs with malware

#Patch Time!

- Microsoft Patch Tuesday, March 2023 Edition
- Microsoft shares script to fix WinRE BitLocker bypass flaw
- Mozilla Firefox gets built-in Firefox Relay controls

#Tech and #Tools

- Microsoft Warns of Large-Scale Use of Phishing Kits to Send Millions of Emails Daily
- FakeCalls Android malware returns with new ways to hide on phones
- Kaspersky releases decryptor for ransomware based on Conti source code

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