Scottish Cyber Coordination Centre

Daily threat bulletin

24 April 2024

Vulnerabilities

Microsoft pulls fix for Outlook bug behind ICS security alerts

BleepingComputer - 23 April 2024 18:50

Microsoft reversed the fix for an Outlook bug causing erroneous security warnings after installing December 2023 security updates [...]

Vulnerability Exploitation on the Rise as Attackers Ditch Phishing

Infosecurity Magazine - 23 April 2024 13:01

Mandiant's latest M-Trends report found that vulnerability exploitation was the most common initial infection vector in 2023, making up 38% of intrusions.

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation: CVE-2022-38028 Microsoft Windows Print Spooler Privilege Escalation Vulnerability.

Threat actors and malware

Hackers hijack antivirus updates to drop GuptiMiner malware

BleepingComputer - 23 April 2024 11:56

North Korean hackers have been exploiting the updating mechanism of the eScan antivirus to plantbackdoors on big corporate networks and deliver cryptocurrency miners through GuptiMiner malware. [...]

North Korea-linked APT groups target South Korean defense contractors

Security Affairs - 23 April 2024 20:24

The National Police Agency in South Korea warns that North Korea-linked threat actors are targeting defense industry entities. The National Police Agency in South Korea warns that North Korea-linked threat actors are targeting defense industry entities to steal defense technology information.

CoralRaider Malware Campaign Exploits CDN Cache to Spread Info-Stealers

The Hacker News - 24 April 2024 11:20

A new ongoing malware campaign has been observed distributing three different stealers such as CryptBot Lumma C2, and Rhadamanthys hosted on Content Delivery Network (CDN) cache domains since at least February 2024.Cisco Talos has attributed the activity with moderate confidence to a threat actor tracked as CoralRaider.

Ransomware Gang Leaks Data Allegedly Stolen From Government Contractor

SecurityWeek - 23 April 2024 11:20

The LockBit ransomware gang leaks data allegedly stolen from government contractor Tyler Technologies. The post Ransomware Gang Leaks Data Allegedly Stolen From Government Contractor appeared first on SecurityWeek.