Scottish
Cyber
Coordination
Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

28 March 2024

Vulnerabilities

DarkGate Malware Campaign Exploits Patched Microsoft Flaw

Security Boulevard - RSS - March 27 2024

The Zero Day Initiative (ZDI) by Trend Micro uncovered a phishing campaign that exploited a patched Microsoft flaw to infect devices with DarkGate malware. CVE-2024-21412 was the Microsoft patch that was exploited by using fake software installers.

Google: Spyware vendors behind 50% of zero-days exploited in 2023

BleepingComputer.com - March 27 2024

Google's Threat Analysis Group (TAG) and Google subsidiary Mandiant said they've observed a significant increase in the number of zero-day vulnerabilities exploited in attacks in 2023, many of them linked to spyware vendors and their clients.

Google reports a significant surge in zero-day vulnerabilities in 2023

SiliconANGLE - March 27 2024

A new report released today by Google LLC’s Threat Analysis Group and Google-owned Mandiant warns that zero-day exploits have become more common amid a rise in nation-state hackers. The report, “We’re All in this Together: A Year in Review of Zero-Days Exploited In-the-Wild in 2023,” detailed 97 zero-day vulnerabilities observed by Google in 2023, up from […] The post Google reports a significant surge in zero-day vulnerabilities in 2023 appeared first on SiliconANGLE.

Malware and threat actors

Extensive APT31 targeting detailed

SC Magazine US - March 27 2024

Attacks deployed by Chinese state-backed threat operation APT31 against numerous U.S. and Western politicians, journalists, foreign policy experts, and dissidents between 2015 and 2024 also involved the targeting of their family members as part of the group's cyberespionage efforts, according to CyberScoop. Malicious emails with tracking links, which when clicked would reveal key device, network, and IP information, have been sent by APT31 to the family members of their targets, with the Chinese hackers later using the obtained information to facilitate reconnaissance efforts against higher-value targets, an unsealed indictment from U.S. prosecutors revealed.

INC Ransom stole 3TB of data from the National Health Service (NHS) of Scotland

Security Affairs - March 27 2024

The INC Ransom extortion group hacked the National Health Service (NHS) of Scotland and is threatening to leak three terabytes of alleged stolen data. The INC Ransom extortion gang added the National Health Service (NHS) of Scotland to the list of victims on its Tor leak site. The cybercrime group claims to have stolen three terabytes of data and is threatening to leak them. Scotland’s NHS, or National Health Service, is the publicly funded healthcare system serving Scotland. It provides a wide range of healthcare services, including hospitals, general practitioners (GPs), mental health services, and community healthcare. The Scottish Government oversees the NHS in Scotland, and it operates separately from the NHS systems in England, Wales, and Northern Ireland.