Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

14 March 2024

Vulnerabilities

DarkGate Malware Exploits Recently Patched Microsoft Flaw in Zero-Day Attack
The Hacker News - March 14 2024

A DarkGate malware campaign observed in mid-January 2024 leveraged a recently patched security flaw in Microsoft Windows as a zero-day using bogus software installers. “During this campaign, users were lured using PDFs that contained Google DoubleClick Digital Marketing (DDM) open redirects that led unsuspecting victims to compromised sites hosting the Microsoft Windows SmartScreen bypass

CVE-2024-23672: Apache Tomcat: WebSocket DoS with incomplete closing handshake
Open Source Security - March 13 2024

Denial of Service via incomplete cleanup vulnerability in Apache Tomcat.
It was possible for WebSocket clients to keep WebSocket connections open leading to increased resource consumption.

Mysterious Werewolf hits defense industry with new RingSpy backdoor
Bi-Zone Blog - March 13 2024

The criminal group gains initial access through phishing emails with a compressed executable that unleashes RingSpy, an original remote access backdoor.

Malware and threat actors

Hackers Hiding Keylogger, RAT Malware in SVG Image Files
BankInfoSecurity - March 13 2024

New Campaign Evades Security Tools to Deliver Agent Tesla Keylogger and XWorm RAT
Threat actors are using image files or Scalable Vector Graphics files to deliver ransomware, download banking Trojans or distribute malware.

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

PixPirate Android malware uses new tactic to hide on phones
BleepingComputer.com - March 13 2024

The latest version of the PixPirate banking trojan for Android employs a previously unseen method to hide from the victim while remaining active on the infected device even if its dropper app has been removed. [...]

Stanford University failed to detect ransomware intruders for 4 months
The Register - Security - March 13 2024

27,000 individuals had data stolen, which for some included names and social security numbers Stanford University.

Stormous Gang - Stopped the Flow
Red Sky Alliance - X-Industry - RSS - March 13 2024

The Stormous ransomware gang has taken credit for an attack on a major Belgian beer producer this week.

Acer Philippines disclosed a data breach after a third-party vendor hack
Security Affairs - March 13 2024

Acer Philippines disclosed a data breach after employee data was leaked by a threat actor on a hacking forum.

EquiLend Employee Data Breached After January Ransomware Attack
HackRead - March 13 2024

By Waqas Some reports suggest that LockBit ransomware gang is behing the EquiLend data breach.

Israeli Universities Hit by Supply Chain Cyberattack Campaign
Dark Reading - March 13 2024

Iranian hacktivist group known as Lord Nemesis and Nemesis Kitten targeted an academic sector software firm in Israel to gain access to its customers.