Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

22 January 2024

Vulnerabilities

CISA Issues Emergency Directive to Federal Agencies on Ivanti Zero-Day Exploits

The Hacker News - January 20 2024

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Friday issued an emergency directive urging Federal Civilian Executive Branch (FCEB) agencies to implement mitigations against two actively exploited zero-day flaws in Ivanti Connect Secure (ICS) and Ivanti Policy Secure (IPS) products.

Apache ActiveMQ Flaw Exploited in New Godzilla Web Shell Attacks

The Hacker News - January 22 2024

Cybersecurity researchers are warning of a "notable increase" in threat actor activity actively exploiting a now-patched flaw in Apache ActiveMQ to deliver the Godzilla web shell on compromised hosts.

Ransomware

Tietoevry ransomware attack causes outages for Swedish firms, cities

BleepingComputer.com - January 21 2024

Finnish IT services and enterprise cloud hosting provider Tietoevry has suffered a ransomware attack impacting cloud hosting customers in one of its data centers in Sweden, with the attack reportedly conducted by the Akira ransomware gang.

Researchers link 3AM ransomware to Conti, Royal cybercrime gangs

Bleeping Computer - January 20 2024

Security researchers analyzing the activity of the recently emerged 3AM ransomware operation uncovered close connections with infamous groups, such as the Conti syndicate and the Royal ransomware gang.

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

LockBit ransomware gang claims the attack on the sandwich chain Subway
Security Affairs - January 21 2024

The LockBit ransomware gang claimed to have hacked Subway, the American multinational fast food restaurant franchise. The Lockbit ransomware group added Subway to the list of victims on its Tor data leak site and threatened to leak the stolen data on February 02, 2024 at 21:44:16 UTC. The group claims to have stolen hundreds of gigabytes of sensitive data.

Malware and threat actors

Russia-linked Midnight Blizzard APT hacked Microsoft corporate emails
Security Affairs - January 20 2024

Microsoft revealed that the Russia-linked APT Midnight Blizzard has compromised some of its corporate email accounts. Microsoft warned that some of its corporate email accounts were compromised by a Russia-linked cyberespionage group known as Midnight Blizzard.