Scottish Cyber Coordination Centre

Daily threat bulletin

16 July 2024

Vulnerabilities

Hackers use PoC exploits in attacks 22 minutes after release

BleepingComputer - 13 July 2024 12:16

Threat actors are quick to weaponize available proof-of-concept (PoC) exploits in actual attacks, sometimes as quickly as 22 minutes after exploits are made publicly available.

Microsoft fixes bug causing Windows Update automation issues

BleepingComputer - 13 July 2024 11:15

Microsoft has resolved a known issue caused by the June 2024 KB5039302 preview update, causing update problems when using Windows Update automation scripts on Windows 11 systems.

Ransomware groups target Veeam Backup & Replication bug

Security Affairs - 15 July 2024 22:42

Multiple ransomware groups were spotted exploiting a vulnerability, tracked as CVE-2023-27532, in Veeam Backup & Replication. The vulnerability CVE-2023-275327 (CVSS score of 7.5) impacts the Veeam Backup & Replication component. An attacker can exploit the issue to obtain encrypted credentials stored in the configuration database, potentially leading to gaining access to the backup infrastructure hosts.

CISA Warns of Actively Exploited RCE Flaw in GeoServer GeoTools Software

The Hacker News - 16 July 2024 10:31

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Monday added a critical security flaw impacting OSGeo GeoServer GeoTools to its Known Exploited Vulnerabilities (KEV) catalog, based on evidence of active exploitation. GeoServer is an open-source software server written in Java that allows users to share and edit geospatial data.

Critical Exim Mail Server Vulnerability Exposes Millions to Malicious Attachments

The Hacker News - 12 July 2024 17:21

A critical security issue has been disclosed in the Exim mail transfer agent that could enable threat actors to deliver malicious attachments to target users' inboxes. The vulnerability, tracked as CVE-2024-39929, has a CVSS score of 9.1 out of 10.0. It has been addressed in version 4.98.

Threat actors and malware

New BugSleep malware implant deployed in MuddyWater attacks

BleepingComputer - 15 July 2024 15:19

The Iranian-backed MuddyWatter hacking group has partially switched to using a new custom-tailored malware implant to steal files and run commands on compromised systems.

New HardBit Ransomware 4.0 Uses Passphrase Protection to Evade Detection

The Hacker News - 15 July 2024 11:40

Cybersecurity researchers have shed light on a new version of a ransomware strain called HardBit that comes packaged with new obfuscation techniques to deter analysis efforts."Unlike previous versions, HardBit Ransomware group enhanced the version 4.0 with passphrase protection.

SEXi Ransomware Rebrands as 'APT Inc.,' Keeps Old Methods

darkreading - 15 July 2024 21:24

The cybercrime group demands ransoms of varying degrees, from thousands to even millions of dollars in some cases, 2 bitcoin per encrypted customer.

Beware of the Latest Phishing Tactic Targeting Employees

Security Boulevard - 15 July 2024 17:43

Found in Environments Protected By: Google, Outlook 365, Proofpoint By Sabi Kiss, Cofense Phishing Defense Center Phishing attacks are becoming increasingly sophisticated, and the latest attack strategy targeting employees highlights this evolution. In this blog post, we'll dissect a recent phishing attempt that impersonates a company's Human Resources (HR) department, and we'll provide detailed insights.

DarkGate, the Swiss Army knife of malware, sees boom after rival Qbot crushed

The Register - 16 July 2024 01:15

Meet the new boss, same as the old boss The DarkGate malware family has become more prevalent in recent months, after one of its main competitors was taken down by the FBI.

CRYSTALRAY Cyber-Attacks Grow Tenfold Using OSS Tools

Infosecurity Magazine - 15 July 2024 17:15

The Sysdig Threat Research Team (TRT) has revealed significant developments in the activities of the SSH-Snake threat actor. The group, now referred to as CRYSTALRAY, has notably expanded its operations, increasing its victim count tenfold to more than 1500.

UK incidents

UK cyber-boss slams China's bug-hoarding laws

The Register - 15 July 2024 01:03

The interim CEO of the UK's National Cyber Security Centre (NCSC) has criticized China's approach to bug reporting.

Scottish
Cyber
Coordination
Centre