Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

SC3 Daily threat summary

7th March 2024

Vulnerabilities

Apple's 17.4 emergency update patches two iPhone zero-days
SC Magazine US - March 6 2024

VMware Releases Security Advisory for Multiple Products
CISA Current Activity - March 6 2024

VMware released a security advisory to address multiple vulnerabilities in ESXi, Workstation, Fusion, and Cloud Foundation. A cyber threat actor could exploit one of these vulnerabilities to take control of an affected system. CISA encourages users and administrators to review the following VMware security advisory and apply the necessary updates: VMSA-2024-0006

CISA Adds Two Known Exploited Vulnerabilities to Catalog
CISA Current Activity - March 6 2024

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. **CVE-2024-23225** Apple iOS and iPadOS Memory Corruption Vulnerability **CVE-2024-23296** Apple iOS and iPadOS Memory Corruption Vulnerability These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise.

Malware and threat actors

ALPHV ransomware gang fakes own death, fools no one
Malwarebytes Labs Blog - March 6 2024

For the second time in only four months, all is not well on the ALPHV (aka BlackCat) ransomware gang's dark web site. Gone are the lists of compromised victims. In their place, a veritable garden of law enforcement badges has sprouted beneath the ominous message "THIS WEBSITE HAS BEEN SEIZED." The ALPHV ransomware dark web site has a new look So far, so FBI, but all is not what it seems.

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

[Europol, DOJ, NCA deny involvement in recent AlphV/BlackCat 'shutdown']
Record by Recorded Future - March 6 2024

[FBI: Critical infrastructure menaced by spike in ransomware]
The Register - Security - March 6 2024

Jump in overall cybercrime reports, $60M-plus reportedly lost to extortionists alone Digital crimes potentially cost victims more than $12.5 billion last year, according to the FBI's latest Internet Crime Complaint Center (IC3) annual report. ...

[A Ransomware That Doesn't Extort Money WinDestroyer & Its Origin]
CYFIRMA - March 6 2024

EXECUTIVE SUMMARY The CYFIRMA research team has identified a destructive malware; WinDestroyer. The ransomware lacks ransom demands, pointing to non-financial...

[Alert: GhostSec and Stormous Launch Joint Ransomware Attacks in Over 15 Countries]
The Hacker News - March 6 2024

The cybercrime group called GhostSec has been linked to a Golang variant of a ransomware family called GhostLocker. "TheGhostSec and Stormous ransomware groups are jointly conducting double extortion ransomware attacks on various business verticals in multiple countries," Cisco Talos researcher Chetan Raghuprasad said in a report shared with The Hacker News.

[Spinning YARN - A New Linux Malware Campaign Targets Docker, Apache Hadoop, Redis and Confluence]
Cado Security - March 6 2024

Introduction Cado Security Labs researchers have recently encountered an emerging malware campaign targeting misconfigured servers running the following web-facing services: Apache Hadoop YARN, Docker, Confluence and Redis The campaign utilises a number of...