Scottish Cyber Coordination Centre

**TLP CLEAR**: Disclosure is not limited

# Daily threat summary

29 February 2024

## Vulnerabilities

### Chinese Hackers Exploiting Ivanti VPN Flaws to Deploy New Malware
The Hacker News - February 29 2024

At least two different suspected China-linked cyber espionage clusters, tracked as UNC5325 and UNC3886, have been attributed to the exploitation of security flaws in Ivanti Connect Secure VPN appliances.

### Lazarus hackers exploited Windows zero-day to gain Kernel privileges
HITBSecNews - February 29 2024

Lazarus hackers exploited Windows zero-day to gain Kernel privileges l33tdawg Thu, 02/29/2024 - 02:37

### Multiple vulnerabilities in Adobe Acrobat Reader could lead to remote code execution
Talos Intelligence Blog - February 28 2024

Cisco Talos has disclosed more than 30 vulnerabilities in February, including seven in Adobe Acrobat Reader, one of the most popular PDF editing and reading software currently available.

### Imperva Customers are Protected Against New SQL Injection Vulnerability in WordPress Plugin
Security Boulevard - RSS - February 28 2024

A critical security flaw, identified as CVE-2024-1071, was discovered in the Ultimate Member plugin for WordPress, affecting over 200,000 active installations.

## Malware and threat actors

### ALPHV/BlackCat hits healthcare after retaliation threat, FBI says
SC Magazine US - February 28 2024

The ALPHV/BlackCat ransomware gang is targeting the healthcare sector following its threats to retaliate against law enforcement interference, according to a joint advisory by the Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Agency (CISA) and Department of Health and Human Services (HHS) released Tuesday.

### Rhysida ransomware wants $3.6 million for children’s stolen data
BleepingComputer.com - February 28 2024

Scottish Cyber Coordination Centre

**TLP CLEAR**: Disclosure is not limited

The Rhysida ransomware gang has claimed the cyberattack on Lurie Children's Hospital in Chicago at the start of the month.

**Suspected Iranian cyber-espionage campaign targets Middle East aerospace, defense industries**
Record by Recorded Future - February 28 2024

An ongoing cyber-espionage campaign that uses unique malware against the aerospace, aviation and defense industries in the Middle East appears to have links to Iran, security researchers say.

**Ransomware gang claims they stole 6TB of Change Healthcare data**
Bleeping Computer - February 28 2024

The BlackCat/ALPHV ransomware gang has officially claimed responsibility for a cyberattack on Optum, a subsidiary of UnitedHealth Group (UHG), which led to an ongoing outage affecting the Change Healthcare platform.

**Lazarus hackers exploited Windows zero-day to gain Kernel privileges**
BleepingComputer.com - February 28 2024

North Korean threat actors known as the Lazarus Group exploited a flaw in the Windows AppLocker driver (appid[.]sys) as a zero-day to gain kernel-level access and turn off security tools, allowing them to bypass noisy BYOVD (Bring Your Own Vulnerable Driver) techniques.