Scottish Cyber Coordination Centre

# Daily Threat Bulletin

19 May 2025

## Vulnerabilities

### U.S. CISA adds Google Chromium, DrayTek routers, and SAP NetWeaver flaws to its Known Exploited Vulnerabilities catalog

Security Affairs - 17 May 2025 09:02

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds Google Chromium, DrayTek routers, and SAP NetWeaver flaws to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added Google Chromium, DrayTek routers, and SAP NetWeaver flaws to its Known Exploited Vulnerabilities (KEV) catalog.

### Researchers Expose New Intel CPU Flaws Enabling Memory Leaks and Spectre v2 Attacks

The Hacker News - 16 May 2025 15:38

Researchers at ETH Zürich have discovered yet another security flaw that they say impacts all modern Intel CPUs and causes them to leak sensitive data from memory, showing that the vulnerability known as Spectre continues to haunt computer systems after more than seven years.

## Threat actors and malware

### Ransomware gangs increasingly use Skitnet post-exploitation malware

BleepingComputer - 16 May 2025 11:00

Ransomware gang members increasingly use a new malware called Skitnet ("Bossnet") to perform stealthy post-exploitation activities on breached networks. [...]

### Experts found rogue devices, including hidden cellular radios, in Chinese-made power inverters used worldwide

Security Affairs - 18 May 2025 09:52

Chinese "kill switches" found in Chinese-made power inverters in US solar farm equipment that could let Beijing remotely disable power grids in a conflict. Investigators found "kill switches" in Chinese-made power inverters in US solar farm equipment. These hidden cellular radios could let Beijing remotely cripple power grids during a conflict.

### New HTTPBot Botnet Launches 200+ Precision DDoS Attacks on Gaming and Tech Sectors

The Hacker News - 16 May 2025 18:07

Cybersecurity researchers are calling attention to a new botnet malware called HTTPBot that has been used to primarily single out the gaming industry, as well as technology companies and educational institutions in China.

### Fileless Remcos RAT Delivered via LNK Files and MSHTA in PowerShell-Based Attacks

The Hacker News - 16 May 2025 14:26

Cybersecurity researchers have shed light on a new malware campaign that makes use of a PowerShell-based shellcode loader to deploy a remote access trojan called Remcos RAT.”Threat actors delivered malicious LNK files embedded within ZIP archives, often disguised as Office documents,” Qualys security researcher Akshay Thorve said in a technical report.

### Russian APT Exploiting Mail Servers Against Government, Defense Organizations

SecurityWeek - 16 May 2025 11:11

Russia-linked APT28 has been exploiting mail server vulnerabilities against government and defense entities since September 2023.

### Russian Espionage Operation Targets Organizations Linked to Ukraine War

Infosecurity Magazine - 16 May 2025 11:15

In Operation RoundPress, the compromise vector is a spearphishing email leveraging an XSS vulnerability to inject malicious JavaScript code into the victim’s webmail page

## UK related

The inside story of a council held to ransom in cyber-attack

BBC News - 19 May 2025 02:26

The BBC investigates one of the most damaging ranswomare attacks on a UK local council.

### UK Cyber Vacancies Growing 12% Per Year

Infosecurity Magazine - 16 May 2025 12:00

An analysis by Robert Walters found there are around 17,000 cybersecurity vacancies in the UK currently, with organizations struggling to fill open positions