Scottish Cyber Coordination Centre

**TLP CLEAR**: Disclosure is not limited

# Daily threat summary

16 January 2024

## Vulnerabilities

### Windows SmartScreen flaw exploited to drop Phemedrone malware
Bleeping Computer - January 15 2024

A Phemedrone information-stealing malware campaign exploits a Microsoft Defender SmartScreen vulnerability (CVE-2023-36025) to bypass Windows security prompts when opening URL files. Phemedrone is a new open-source info-stealer malware that harvests data stored in web browsers, cryptocurrency wallets, and software like Discord, Steam, and Telegram.

### Over 178K SonicWall firewalls vulnerable to DoS, potential RCE attacks
Bleeping Computer - January 15 2024

Security researchers have found over 178,000 SonicWall next-generation firewalls (NGFW) with the management interface exposed online are vulnerable to denial-of-service (DoS) and potential remote code execution (RCE) attacks. These appliances are affected by two DoS security flaws tracked as CVE-2022-22274 and CVE-2023-0656, the former also allowing attackers to gain remote code execution.

### Latest Critical Vulnerabilities Affecting GitLab, Apple's Magic Keyboard, and Juniper Networks, Junos OS
SOCRadar - January 15 2024

In this blog post, we will shed light on the latest critical vulnerabilities, impacting GitLab, Apple's Magic Keyboard firmware, and Juniper Networks' Junos OS. GitLab Has Patched Critical Vulnerabilities, Including a Zero-Click Leading to Account Takeover (CVE-2023-7028, CVE-2023-5356) GitLab has recently rolled out security updates for both Community Edition (CE) and Enterprise Edition (EE).

## UK cyber

### Anonymous Collective Launches Cyberattack on Bahrain Over Yemen Airstrikes
The Cyber Express - January 15 2024

Scottish Cyber Coordination Centre

**TLP CLEAR**: Disclosure is not limited

The Anonymous Collective has orchestrated an alleged cyberattack on Bahrain, pointing to the country's support for the US and UK strikes on Yemen.

## Malware and threat actors

### Digital Predators of 2023: Exposing Top Cyber Threat Actors

SOCRadar - January 15 2024

In 2023, the digital landscape continued to evolve rapidly, but so did the sophistication and audacity of cyber threat actors. From ransomware to sophisticated phishing campaigns, the threat landscape has been dominated by groups that have advanced their technical capabilities and expanded their targets globally. This introduction provides a glimpse into the most dangerous threat actors of the year, each with their distinct methods and significant impacts across various sectors.

### Cybercriminals Launched Leaksmas, Exposing Massive Volumes of Compromised Data

Red Sky Alliance - X-Industry - RSS - January 15 2024

Even as the New Year approached and the world celebrated the festive Christmas season, the cybercriminal community did not pause their activities. Instead, they marked the holiday season in their unique way. On Christmas Eve, Resecurity observed multiple actors on the Dark Web releasing substantial data dumps.

### Python-Based Tool FBot Disrupts Cloud Security

Infosecurity Today - January 15 2024

Security researchers have shed light on a new Python-based hacking tool, FBot, showcasing distinct features from other cloud malware families. Discovered by the SentinelLabs team, FBot targets web servers, cloud services and Software-as-a-Service (SaaS).