



## Daily Threat Bulletin

5 January 2026

### Vulnerabilities

#### [Over 10K Fortinet firewalls exposed to actively exploited 2FA bypass](#)

BleepingComputer - 02 January 2026 12:01

Over 10,000 Internet-exposed Fortinet firewalls are still vulnerable to attacks exploiting a five-year-old two-factor authentication (2FA) bypass vulnerability. [...]

#### [Thousands of ColdFusion exploit attempts spotted during Christmas holiday](#)

Security Affairs - 03 January 2026 11:59

GreyNoise observed thousands of attacks targeting about a dozen Adobe ColdFusion vulnerabilities during the Christmas 2025 holiday. GreyNoise reports a coordinated campaign exploiting about a dozen Adobe ColdFusion vulnerabilities, with thousands of attack attempts observed during the Christmas 2025 holiday.

#### [RondoDox Botnet Exploiting React2Shell Vulnerability](#)

SecurityWeek - 02 January 2026 12:12

In December, the botnet's operators focused on weaponizing the flaw to compromise vulnerable Next.js servers.

### Threat actors and malware

#### [Hackers claim to hack Resecurity, firm says it was a honeypot](#)

BleepingComputer - 03 January 2026 16:34

The ShinyHunters hacking group claims it breached the systems of cybersecurity firm Resecurity and stole internal data, while Resecurity says the attackers only accessed a deliberately deployed honeypot containing fake information used to monitor their activity. [...]

#### [Trust Wallet links \\$8.5 million crypto theft to Shai-Hulud NPM attack](#)

BleepingComputer - 02 January 2026 10:19

Trust Wallet believes the compromise of its web browser to steal roughly \$8.5 million from over 2,500 crypto wallets is likely related to an "industry-wide" Sha1-Hulud attack in November. [...]

#### [Sedgwick discloses data breach after TridentLocker ransomware attack](#)

Security Affairs - 05 January 2026 07:50



Scottish  
Cyber  
Coordination  
Centre

Sedgwick confirmed a cyber incident at its federal contractor unit after TridentLocker claimed to steal 3.4GB of data. Sedgwick is a leading global claims management and risk services provider operating in the insurance and risk solutions sector. It employs roughly 33,000 people worldwide, across more than 80 countries.

### **Two U.S. cybersecurity professionals plead guilty in BlackCat/Alphv ransomware case**

Security Affairs - 02 January 2026 23:33

Two U.S. cybersecurity professionals pleaded guilty to charges tied to their roles in BlackCat/Alphv ransomware attacks. The U.S. cybersecurity professionals Ryan Goldberg and Kevin Martin pleaded guilty to charges tied to their roles in BlackCat/Alphv ransomware attacks that occurred in 2023.

### **Cybercriminals Abuse Google Cloud Email Feature in Multi-Stage Phishing Campaign**

The Hacker News - 02 January 2026 15:44

Cybersecurity researchers have disclosed details of a phishing campaign that involves the attackers impersonating legitimate Google-generated messages by abusing Google Cloud's Application Integration service to distribute emails.

### **Adobe ColdFusion Servers Targeted in Coordinated Campaign**

SecurityWeek - 02 January 2026 11:11

GreyNoise has observed thousands of requests targeting a dozen vulnerabilities in Adobe ColdFusion during the Christmas 2025 holiday.