

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

January 2026 - VOL.1

The News

IN THE NEWS THIS WEEK



Attackers Exploit Zero-Day in End-of-Life D-Link Routers

Attackers are actively exploiting a zero-day vulnerability, tracked as CVE-2026-0625 (CVSS 9.3), in multiple discontinued D-Link DSL gateway devices to execute arbitrary shell commands. The affected products have been end-of-life for years and no longer receive security updates, prompting D-Link to urge organizations to retire and replace them with supported models.

D-Link learned of the flaw in mid-December 2025 after VulnCheck observed active exploitation in production environments involving a compromised CGI library. The vulnerability is a command injection issue in the dnscfg.cgi endpoint, which fails to properly validate user input, allowing attackers to inject malicious commands disguised as DNS settings. Due to variations in firmware implementations, the full list of affected models remains unclear, though past exploitation has targeted devices such as the DSL-2740R, DSL-2640B, DSL-2780B, and DSL-526B.

The flaw poses serious risk because these devices typically sit at the network perimeter, giving attackers an entry point to steal data, establish persistence, or pivot deeper into internal networks. The incident highlights the broader danger of continuing to operate obsolete hardware, a recurring issue with D-Link devices that have been exploited long after support ended. Security agencies like CISA have repeatedly added vulnerabilities in discontinued D-Link products to their known exploited list, underscoring the need for organizations to phase out end-of-life technologies despite cost or operational constraints.

[READ MORE >](#)

OTHER NEWS HIGHLIGHTS

Two Chrome Extensions Caught Stealing ChatGPT and DeepSeek Chats from 900,000 Users

Kimwolf Android Botnet Infects Over 2 Million Devices via Exposed ADB and Proxy Networks

DarkSpectre Browser Extension Campaigns Exposed After Impacting 8.8 Million Users Worldwide

The News

TOP OF THE NEWS THIS WEEK



Veeam Patches Critical RCE Vulnerability with CVSS 9.0 in Backup & Replication

Veeam has released security updates for multiple vulnerabilities in its Backup & Replication software, including a critical remote code execution flaw tracked as CVE-2025-59470 with a CVSS score of 9.0. The issue allows users with Backup Operator or Tape Operator roles to execute arbitrary code as the postgres user by abusing malicious interval or order parameters. Although these roles are already highly privileged, successful exploitation could lead to full system compromise.

Veeam noted that it considers the issue high severity but said the risk of exploitation is reduced when customers follow its recommended security guidelines. In addition to the critical flaw, three other vulnerabilities were patched, enabling various forms of remote code execution or file writes as root or postgres users by abusing configuration files or input parameters. These weaknesses further highlight the risks associated with misused or overly permissive backup-related roles.

All four vulnerabilities affect Veeam Backup & Replication version 13.0.1.180 and earlier 13.x builds and have been fixed in version 13.0.1.1071. While there is no evidence of active exploitation, Veeam urges customers to apply the updates promptly, especially given the history of threat actors targeting vulnerabilities in backup and recovery software.

[READ MORE >](#)

TOP RELATED ARTICLES

Critical LangChain Core Vulnerability Exposes Secrets via Serialization Injection

LastPass 2022 Breach Led to Years-Long Cryptocurrency Thefts, TRM Labs Finds

Personal LLM Accounts Drive Shadow AI Data Leak Risks

Geo-Politics

NEWS FROM AROUND THE WORLD



HIGHLIGHTS FROM AROUND THE WORLD

Cyberattacks Likely Part of Military Operation in Venezuela

US Cyber Pros Plead Guilty Over BlackCat Ransomware Activity

Sprawling 'Operation Sentinel' Neutralizes African Cybercrime Syndicates

DDoS Powers Affiliate-Driven Hactivist Attacks

NoName057(16), a pro-Russian hactivist group active since 2022, is conducting politically motivated DDoS campaigns against government, media, and institutional websites linked to Ukraine and Western interests. The group relies on a custom tool called DDoSia, which is distributed through a volunteer model that allows individuals with minimal technical skill to participate. Its operations often align with major geopolitical events, such as sanctions or military aid announcements, which the group frames as justification for retaliatory cyberattacks.

According to SOCRadar, NoName057(16) operates more like an organized community than a traditional covert botnet. Campaigns follow a structured playbook: targets are selected, supporters are mobilized through propaganda on platforms like Telegram and X, and attack parameters are distributed via command-and-control servers.

While the attacks are generally disruptive rather than destructive, the group's strength lies in persistence, coordination, and efficiency. DDoSia employs application-layer techniques, multivector attacks, and evasion methods to bypass CDNs and strain origin servers, even with moderate traffic volumes. The tool has evolved into a sophisticated, multiplatform system with encrypted C2 channels and detection avoidance features, reinforcing NoName057(16)'s ability to repeatedly cause short-term service outages, particularly for public sector organizations with limited DDoS defenses.

[READ MORE >](#)

Breaches

SECURITY BREACHES THIS WEEK



OTHER SECURITY BREACHES

Qilin Ransomware Group Attack Hits Sugawara Laboratories and CSV Group

Akira Ransomware Targets BUHLMANN GROUP

DragonForce Strikes Barnes & Jones in Ransomware Attack

Space Agency Confirms Breach — Hackers Claim 200 GB Of Data Stolen

The European Space Agency (ESA) has confirmed a security breach affecting a limited number of external science servers used for unclassified collaborative engineering work. While classified and mission-critical systems were not impacted, threat actors claim to have exfiltrated up to 200GB of data. ESA has launched an internal forensic investigation and implemented short-term remediation measures, though it remains unclear exactly how the compromise occurred or what data was definitively accessed.

Security experts warn the incident highlights broader risks facing the rapidly growing space sector, now valued at over \$600 billion globally. Attackers do not always rely on zero-day vulnerabilities; unpatched systems, social engineering, and human error can be sufficient. According to external analysis, the stolen data may include private Bitbucket and JIRA repositories, source code, and API tokens, suggesting attackers potentially had access for days and could have mapped development pipelines or uncovered hardcoded credentials.

The breach underscores the inherent tension between open collaboration and strong security in multinational scientific environments. Experts caution that expanding partnerships, cloud services, and shared infrastructure significantly increase the attack surface, raising the risk of follow-on or supply-chain attacks. ESA has notified relevant stakeholders and stated that further updates will be provided once the forensic analysis is complete.

[READ MORE >](#)

Vulnerabilities



VULNERABILITIES & EXPLOITS

CVE-2026-21858 - N8N Unauthenticated Remote Code Execution vulnerability

CVSS SCORE 10

CVE-2025-59470 - Veeam remote code execution vulnerability

CVSS SCORE 10

LAST WEEKS RECAP

CVE-2025-20393 - Cisco Multiple Products Improper Input Validation Vulnerability
CVSS Score: (10)

CVE-2025-37164 - HP OneView Improper Control of Generation of Code ('Code Injection') Vulnerability
CVSS Score: (10)

CVE-2025-14174 - Google Chromium Out of Bounds Memory Access Vulnerability
CVSS Score: (8.8)

CVE-2025-43529 - Apple Multiple Products Use-After-Free WebKit Vulnerability
CVSS Score: (8.8)

Ransomware



WEEKLY RANSOMWARE ROUNDUPS

TOP THREAT ACTORS

Qilin

Qilin is a ransomware-as-a-service operation linked to Russia, encrypting and stealing data for ransom. Active since October 2022, it has targeted organizations like The Big Issue and Yanfeng.

Akira

Akira is a ransomware strain that appeared in March 2023, targeting over 250 organisations including BHI Energy, Nissan Australia, Tietoevry, and Stanford University. Operating as ransomware-as-a-service, it earned up to \$42 million by April 2024.

Clop

Clop ransomware first emerged in 2019, when it became a prevalent threat to organizations and businesses. Clop ransomware encrypts the victims files and threatens to leak the confidential information if no ransom is paid.



OVERVIEW

A total of 157 new victims were reported across various ransomware groups this Week.

TARGET INDUSTRIES

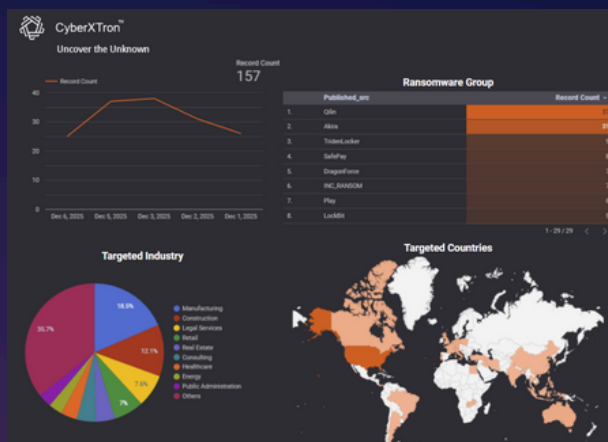
The Manufacturing sector was the primary focus, representing 18.5% of all victims.

TARGET COUNTRY

The USA had the highest number of victims, with 93 in total.

TOP GROUP

The Qilin Group was the most active, claiming 37 victims.

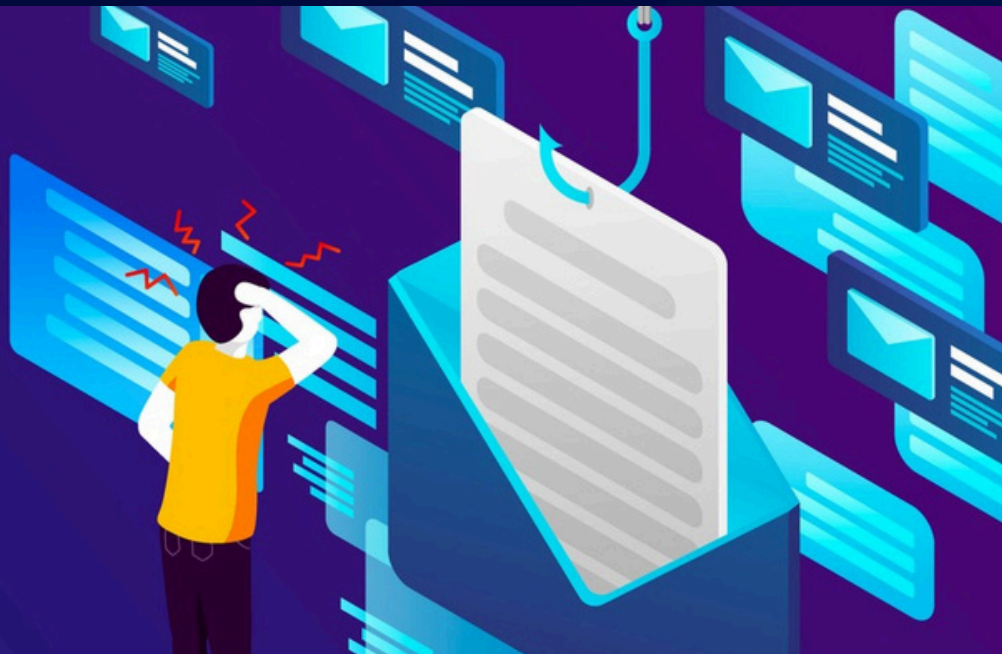


Dive into this interactive report to uncover hidden trends [HERE!](#)

Published Ransomware Attacks - Source: CyberXTron ThreatBolt

Phishing

PHISHING NEWS THIS WEEK



Microsoft Warns Misconfigured Email Routing Can Enable Internal Domain Phishing

Threat actors are abusing complex email routing configurations and weak spoofing protections to impersonate organizations' own domains, making phishing emails appear as if they were sent internally. Microsoft reports that attackers use this method to deliver a wide range of phishing lures, including voicemails, shared documents, HR communications, and password reset notices, often via phishing-as-a-service platforms such as Tycoon 2FA. Although the technique is not new, its use has surged since May 2025, affecting organizations across many industries.

These attacks primarily target tenants with misconfigured mail routing, such as MX records that pass through on-premises Exchange servers or third-party services before reaching Microsoft 365. This setup creates exploitable gaps that allow spoofed emails to bypass protections. Successful attacks can result in credential theft, data exfiltration, and business email compromise, including financial scams involving fake invoices, W-9 forms, and fraudulent bank documentation.

Microsoft blocked more than 13 million malicious emails linked to the Tycoon 2FA kit in October 2025 alone, highlighting the scale of the threat. To reduce risk, organizations are advised to enforce strict DMARC reject and SPF hard-fail policies, correctly configure third-party connectors, and disable Direct Send if unnecessary. Tenants with MX records pointing directly to Microsoft 365 are not vulnerable to this specific attack vector.

[READ MORE >](#)

OTHER PHISHING ARTICLES

[Fake Booking Emails Redirect Hotel Staff to Fake BSoD Pages Delivering DCRat](#)

[Cybercriminals Abuse Google Cloud Email Feature in Multi-Stage Phishing Campaign](#)

[Hackers abuse Google Cloud to send trusted phishing emails](#)