SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

December 2025 - VOL.3

The News

IN THE NEWS THIS WEEK

SonicWall Edge Access Devices Hit by Zero-Day Attacks

SonicWall on Wednesday revealed a previously unknown vulnerability in its SMA1000 remote access platform that is currently being exploited through chained attack methods. The flaw, tracked as CVE-2025-40602, is a medium-severity local privilege escalation issue within the Appliance Management Console (AMC) of the SMA1000 line. SonicWall assigned the bug a CVSS score of 6.6 and said it stems from inadequate authorization controls in the AMC component.

According to the company, attackers have been observed leveraging the new vulnerability alongside an older critical flaw, CVE-2025-23006, which affects SMA100 devices and was targeted in zero-day attacks earlier this year. SonicWall noted that exploitation of the newly disclosed issue requires either that the older critical bug remains unpatched or that an adversary already holds valid local system credentials.

The vendor did not provide details on the nature or scale of the ongoing exploitation. While SonicWall issued a statement in response to inquiries, it declined to comment directly on the attack activity involving CVE-2025-40602. The company emphasized that organizations should ensure CVE-2025-23006 is fully remediated to prevent the chained attack path.
The new vulnerability was identified by Google Threat Analysis Group researchers Clément Lecigne and Zander Work.

READ MORE >

PAGE ONE | IN THE NEWS THIS WEEK

OTHER NEWS HIGHLIGHTS

Apple Patches More Zero-Days Used in 'Sophisticated' Attack

Copilot's No-Code AI Agents Liable to Leak Company Data

Warning: WinRAR Vulnerability CVE-2025-6218 Under Active Attack by Multiple Threat Groups

The News

TOP OF THE NEWS THIS WEEK

Chrome Targeted by Active In-the-Wild Exploit Tied to Undisclosed High-Severity Flaw

Google on Wednesday released security fixes for Chrome to address three vulnerabilities, including one that the company confirmed is being actively exploited. The high-severity flaw was initially tracked only as Chromium issue 466192044, with Google withholding technical details.

\A linked GitHub commit revealed the bug affects the ANGLE graphics layer, pointing to a buffer-sizing error in its Metal renderer that could enable memory corruption or code execution. Google said an exploit is already circulating but declined to share information about attackers or targets. The update brings Chrome's total number of zero-days patched this year to eight.

Two additional medium-severity issues, in the Password Manager and Toolbar, were also fixed. Users are urged to update Chrome to version 143.0.7499.109/.110 across platforms. The exploited flaw has since been assigned CVE-2025-14174 and rated 8.8 for severity. CISA added it to its Known Exploited Vulnerabilities catalog, requiring U.S. federal agencies to patch by January 2, 2026.

READ MORE

TOP RELATED ARTICLES

Cisco Warns of Active Attacks Exploiting Unpatched 0-Day in AsyncOS Email Security Appliances

React2Shell Vulnerability Actively Exploited to Deploy Linux Backdoors

New Advanced Phishing Kits Use AI and MFA Bypass Tactics to Steal Credentials at Scale

Geo-Politics

NEWS FROM AROUND THE WORLD

China-Aligned Threat Group Uses Windows Group Policy to Deploy Espionage Malware

A newly identified China-aligned hacking group known as LongNosedGoblin has been linked to cyberattacks against government entities in Southeast Asia and Japan, with the primary goal of cyber espionage. According to Slovak cybersecurity firm ESET, the group has been active since at least September 2023 and leverages Windows Group Policy to deploy malware across networks, while using cloud services such as Microsoft OneDrive and Google Drive as command-and-control servers. The attackers employ a custom toolkit that includes NosyHistorian for collecting browser history, NosyDoor as a backdoor capable of exfiltrating and deleting files, NosyStealer for extracting browser data, NosyDownloader for loading payloads in memory, and NosyLogger for recording keystrokes. ESET first detected the group's activity in February 2024 on a Southeast Asian government system, where Group Policy was used to spread malware across multiple machines. While many victims were affected by NosyHistorian, only a subset were infected with NosyDoor, suggesting a more targeted approach, with execution guardrails limiting attacks to specific machines. The group also uses additional tools such as a reverse SOCKS5 proxy, video recording utilities, and a Cobalt Strike loader. Analysts noted similarities between LongNosedGoblin's tradecraft and other clusters like ToddyCat and Erudite Mogwai, though no definitive link has been established. In one case, a NosyDoor variant was found targeting an EU organization, this time using Yandex Disk as a command-and-control server, raising the possibility that the malware is shared among multiple China-aligned threat actors.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

North Korea-Linked Hackers Steal $2.02 Billion in 2025, Leading Global Crypto Theft

China-Linked Ink Dragon Hacks Governments Using ShadowPad and FINALDRAFT Malware

North Korea-linked Actors Exploit React2Shell to Deploy New EtherRAT Malware

Breaches

SECURITY BREACHES THIS WEEK

113,000 Impacted by Data Breach at Virginia Mental Health Authority

Virginia's Richmond Behavioral Health Authority (RBHA), a public agency providing mental health and crisis services, has disclosed a major ransomware attack that compromised the personal information of more than 113,000 individuals. The incident occurred on September 29, when portions of RBHA's network were encrypted, and was detected the following day, prompting immediate action to remove the attackers. While RBHA has stated there is no definitive evidence that personal data was accessed, the breach potentially exposed sensitive details including names, Social Security numbers, passport numbers, financial account information, and health records. In its notice, the provider urged affected individuals to remain vigilant against identity theft and fraud by monitoring account statements and credit reports.

The organization reported the breach to the US Department of Health and Human Services, confirming that 113,232 people were impacted. Although RBHA did not identify the perpetrators, the Qilin ransomware group claimed responsibility in mid-October, listing the healthcare provider on its leak site. Qilin has since published 192 gigabytes of stolen data, amounting to more than 393,000 files, intensifying concerns over the scale of the breach and its potential consequences for patients and staff.

READ MORE ›

OTHER SECURITY BREACHES

700Credit Data Breach Impacts 5.8 Million Individuals

Auto Parts Giant LKQ Confirms Oracle EBS Breach

User Data Compromised in SoundCloud Hack

Vulnerabilities

VULNERABILITIES & EXPLOITS

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

LAST WEEKS RECAP

CVE-2025-59718 - Improper verification of cryptographic signature vulnerability in Fortinet FortiOS
CVSS Score: (9.8)

CVE-2025-59719 - Improper verification of cryptographic signature vulnerability in Fortinet FortiWeb
CVSS Score: (9.8)

CVE-2025-10573 - Stored XSS in Ivanti Endpoint Manager
CVSS Score: (9.6)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

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

TARGET INDUSTRIES

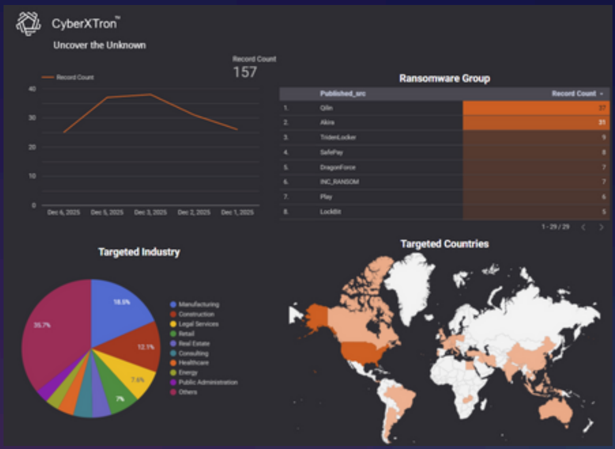
The Manufacturing sector was the primary focus, representing 18.5% of all victims.

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.



Ransomware Group

	Published_src	Record Count ▾
1.	Qilin	37
2.	Akira	31
3.	TridentLocker	9
4.	SafePay	8
5.	DragonForce	7
6.	INC_RANSOM	7
7.	Play	6
8.	LockBit	5

Dive into this interactive report to uncover hidden trends HERE!

Published Ransomware Attacks - Source: CyberXTron ThreatBolt

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.

Phishing

PHISHING NEWS THIS WEEK

Phishing Attacks Abuse Free Cloudflare Pages

Malwarebytes has issued a warning that cybercriminals are exploiting Cloudflare’s free Pages service to host phishing portals, allowing malicious sites to bypass traditional security scanners. The attackers are creating convincing fake login pages that mimic banking, insurance, and healthcare providers, designed to steal credentials, security questions, and multifactor authentication codes. Researchers note that victims often see nothing unusual beyond a strange link and a failed login attempt, while attackers benefit from free hosting, compromised redirectors, and Telegram-based data exfiltration that provide speed and resilience.

The broader trend, Malwarebytes says, is that phishing actors are increasingly relying on mainstream platforms and free web hosting to avoid detection, making their infrastructure cheap, fast, and difficult to spot. To protect against such attacks, users are advised to carefully check full domain names, avoid clicking login links in unsolicited emails or texts, and instead access institutions directly through bookmarks or typed addresses.

They should also treat unexpected security prompts with caution, especially those requesting sensitive information like card numbers or email passwords. If anything about a link or request feels suspicious, Malwarebytes urges contacting the provider through trusted official channels. The warning underscores how phishing campaigns are evolving to exploit legitimate services, raising the stakes for vigilance among both individuals and organizations.

READ MORE >

OTHER PHISHING ARTICLES

Gemini Zero-Click Vulnerability Let Attackers Access Gmail, Calendar, and Docs

Microsoft 365 users targeted in device code phishing attacks

PayPal subscriptions abused to send fake purchase emails