SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

JULY 2025 - VOL.4

The News

IN THE NEWS THIS WEEK

Storm-2603 Exploits SharePoint Flaws to Deploy Warlock Ransomware on Unpatched Systems

Microsoft has linked the exploitation of SharePoint vulnerabilities CVE-2025-49704/49706 to Storm-2603, a suspected China-based threat actor deploying Warlock ransomware. Attackers use a web shell, scheduled tasks, and GPO modifications to gain persistence, escalate privileges, and disable defenses. Over 4600 compromise attempts have hit more than 300 organizations globally, with espionage and financial motives driving widespread intrusions.

READ MORE

Sophos and SonicWall Patch Critical RCE Flaws Affecting Firewalls and SMA 100 Devices

Sophos and SonicWall disclosed multiple critical vulnerabilities in their firewall and SMA 100 Series appliances that allow remote code execution, some even pre-auth. Sophos patched five CVEs affecting legacy components and high-availability setups, while SonicWall warned of a CVE-2025-40599 exploit linked to UNC6148's OVERSTEP backdoor. Urgent mitigations include patching, MFA enforcement, and log reviews to defend against future intrusions.

READ MORE

OTHER NEWS HIGHLIGHTS

Hive0156 Hackers Attacking Government and Military Organizations to Deploy Remcos RAT

Rise in Phishing Activity Using Spoofed SharePoint Domains With Sneaky2FA Techniques

Elephant APT Group Attacking Defense Industry Leveraging VLC Player, and Encrypted Shellcode

The News

TOP OF THE NEWS THIS WEEK

Microsoft Releases Urgent Patch for SharePoint RCE Flaw Exploited in Ongoing Cyber Attacks

Microsoft issued security updates for two critical flaws—CVE-2025-53770 and CVE-2025-53771—targeting on-premises SharePoint Servers amid active exploitation. CVE-2025-53770 enables remote code execution via unsafe deserialization, while CVE-2025-53771 is a spoofing bug rooted in path traversal. Both were tied to July's ToolShell exploit chain and patched with enhanced protections compared to earlier fixes for CVE-2025-49704/49706.

The flaws do not affect SharePoint Online and require users to apply updates to versions 2016, 2019, and Subscription Edition. Microsoft advises rotating ASP.NET machine keys and restarting IIS post-update for full protection. Over 54 entities, including banks and government bodies, have been impacted since July 18. CISA added CVE-2025-53770 to its Known Exploited Vulnerabilities (KEV) catalog.

Federal agencies are mandated to patch by July 21 to prevent further exploitation. The spoofing bug was discovered by Viettel Cyber Security and an anonymous researcher. Microsoft clarified CVE-2025-53770 is a variant of CVE-2025-49706 but emphasized the current guidance remains accurate. AMSI should be enabled with Defender Antivirus or an equivalent solution for deeper inspection.

READ MORE

TOP RELATED ARTICLES

CISA warns of hackers exploiting SysAid vulnerabilities in attacks

CISA and FBI warn of escalating Interlock ransomware attacks

Ransomware Actors Pile on 'ToolShell' SharePoint Bugs

Geo-Politics

NEWS FROM AROUND THE WORLD

Iran-Linked DCHSpy Android Malware Masquerades as VPN Apps to Spy on Dissidents

Zscaler uncovered two cyber espionage campaigns—GhostChat and PhantomPrayers—targeting the Tibetan community ahead of the Dalai Lama's 90th birthday, attributed to a China-linked threat actor. Attackers used watering hole techniques to infect victims via fake encrypted apps and celebration pages, deploying Gh0st RAT and PhantomNet for surveillance and remote control. These advanced backdoors exploited DLL sideloading and encrypted C2 traffic to stealthily exfiltrate sensitive data.

READ MORE

China-Linked Hackers Launch Targeted Espionage Campaign on African IT Infrastructure

China-linked APT41 has launched a targeted cyber espionage campaign against African government IT services, using compromised SharePoint servers and DLL sideloading to deploy Cobalt Strike. Attackers leveraged hardcoded internal infrastructure details and disguised malware delivery via GitHub-like domains to avoid detection. Their tactics blend living-off-the-land techniques with reverse shell payloads to gain persistent, covert access to victim systems.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

China's Massistant Tool Secretly Extracts SMS, GPS Data, and Images From Confiscated Phones

Operation CargoTalon Attacking Russian Aerospace & Defense to Deploy EAGLET Implant

France Says Administrator of Cybercrime Forum XSS Arrested in Ukraine

Breaches

SECURITY BREACHES THIS WEEK

Major European healthcare network discloses security breach

Zurich-based healthcare giant AMEOS Group, operating over 100 facilities across Switzerland, Germany, and Austria, disclosed a major data breach affecting patient, employee, and partner information. Despite existing safeguards, external actors accessed internal systems, prompting AMEOS to shut down all networks, notify authorities, and launch a forensic investigation. The breach—covered under GDPR Article 34—has not yet resulted in publicly leaked data, but individuals are advised to stay alert for phishing. Criminal complaints have been filed, though no ransomware group has claimed responsibility, and the attack method remains unclear. AMEOS promises updates and assures users there's no confirmed leak of individual data.

The breach potentially compromises the integrity of one of Central Europe's largest private hospital networks. Public notices warn affected parties of possible misuse of stolen contact details. The organization is reviewing and strengthening cyber defenses with external experts. Over $1.4B in annual revenue and 18,000 staff mark AMEOS as a high-value target. The company urges caution, particularly among care recipients and affiliated partners. For now, the scope of impact and identity of the threat actors remain under investigation.
The incident underscores growing risks for healthcare infrastructure across the DACH region.

READ MORE

OTHER SECURITY BREACHES

Dior begins sending data breach notifications to U.S. customers

Dell confirms breach of test lab platform by World Leaks extortion group

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2025-53770 - Microsoft SharePoint Server Remote Code Execution Vulnerability

CVSS SCORE 9.8

CVE-2025-6704 - Arbitrary file writing vulnerability in the Secure PDF eXchange (SPX)

CVSS SCORE 9.8

CVE-2025-7624- SQL injection vulnerability in the legacy (transparent) SMTP proxy of Sophos Firewall

CVSS SCORE 9.8

LAST WEEKS RECAP

CVE-2025-20337 - Critical ISE Flaw Allowing Unauthenticated Attackers to Execute Root Code
CVSS Score: (10)

CVE-2025-25257 - Critical Unauthenticated SQL Injection Vulnerability in FortiWeb
CVSS Score: (9.8)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

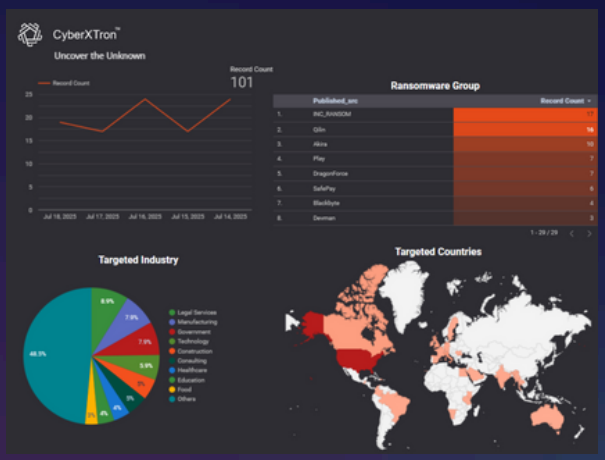
A total of 101 new victims were reported across various ransomware groups this Week.

TARGET INDUSTRIES

The Legal Services was the primary focus, representing 8.9% of all victims.

TARGET COUNTRY

The USA was the top victim country, with a total of 56 affected entities.



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.

INC. Ransom

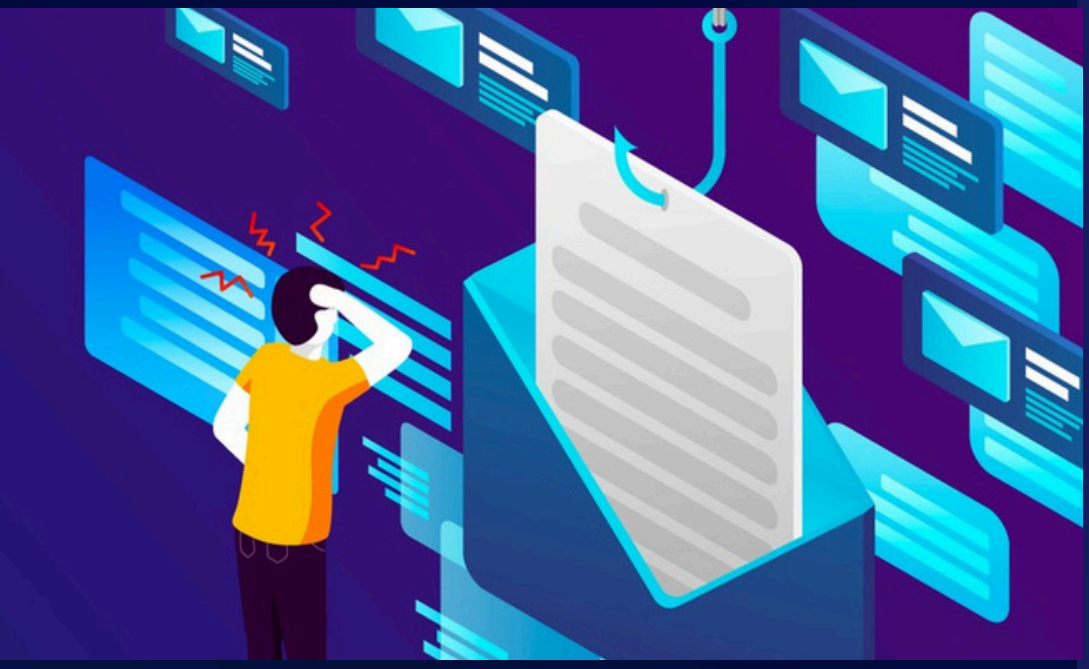
Inc. ransomware, active since July 2023, is a multi-extortion operation that steals data and threatens leaks unless victims pay to "protect their reputation." The attackers frame their extortion as a service, claiming disclosure of their methods will help secure the victim's systems.

Play

Play ransomware was first observed around June of 2022. The ransomware family's name is derived from the .play extension added to files once they have been encrypted by the ransomware.

Phishing

PHISHING NEWS THIS WEEK



Red Bull-Themed Scams Trick Job Seekers into Giving Up Credentials

Evalian's Security Operations Center (SOC) uncovered a sophisticated phishing campaign exploiting trusted platforms to bypass enterprise email defenses. Attackers impersonated Red Bull, targeting job seekers with realistic emails that passed authentication protocols like SPF, DKIM, and DMARC. Emails appeared to come from a legitimate Xero address, using "piggybacking" techniques to gain credibility. Victims were funneled through a staged attack chain involving reCAPTCHA, a fake job description, and a spoofed Facebook login page aimed at credential theft. Despite Let's Encrypt certificates giving a false sense of security, backend infrastructure traced to disposable VPS providers and low-reputation IPs revealed a broader malicious network. TLS fingerprinting and passive DNS exposed multiple domains spun up days before launch, spoofing brands and influencers—indicating scalability and intent. Evalian's SOC analyst flagged the threat manually after automated systems failed, launching a swift response that turned IOCs into protective measures for their wider customer base. The campaign showcases growing abuse of cloud platforms like SendGrid and Mailgun to deliver stealthy phishing attacks. Key defense lessons include evaluating sender reputation, inspecting certificate metadata, and correlating email, endpoint, and network telemetry. The incident reinforces that technical tools alone aren't enough; human oversight, infrastructure mapping, and behavioral analysis are crucial in defeating modern phishing tactics.

READ MORE

OTHER PHISHING ARTICLES

Surge in Phishing Attacks Exploiting Spoofed SharePoint Domains and Sneaky 2FA Tactics

Hackers fooled Cognizant help desk, says Clorox in $380M cyberattack lawsuit