Edition - 81

Threatsploit

Adversary Report

May - 2025

We are Exhibiting at

GITEX EUROPE x Berlin

AI EVERYTHING — GERMANY —

21 – 23 MAY 2025

MESSE BERLIN – SOUTH ENTRANCE –

BriskInfosec™

VULNERABILITY TO VICTORY

Booth No H5.2-A101

www.briskinfosec.com

Introduction :

Dear Readers,

This May, we bring you another edition of the Threatsploit Adversary Report, built with one goal in mind: to help you see what's really happening beneath the surface. Behind every breach is a moment when something slipped through. Whether it's a missed alert, a trusted vendor, or a tiny misstep in the cloud, everything changes in an instant.

We've covered attacks that shook some of the most established names. Trust was lost, operations stalled, and teams were left asking, how did this happen? Whether it was a phishing email that slipped past filters or a misconfigured API left wide open, each story is here to help you connect the dots before it's too late.

One story that stood out to our team was the breach that hit a major automaker. It wasn't just about data; it disrupted their manufacturing flow. Another attack targeted the Oil and Gas sector, where a vendor's compromised account became the entry point. And then there's the ransomware attack that locked researchers out of vital work in Swiss universities.

This report offers real insights into how breaches unfold, highlighting the gaps that others missed. Take a moment to share it with your teams, spark important conversations, and identify the blind spots before someone else does.

> Sometimes, the biggest lesson in cybersecurity comes not from tools or technologies but from the stories no one saw coming.

Best regards,

Briskinfosec Threat Intelligence Team.

Contents :

Phishing Attacks use Real-Time checks to Confirm Victim Emails before Credential Theft

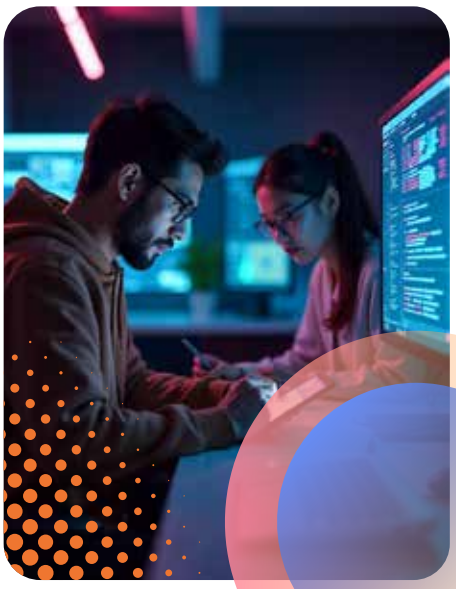
In April 2025, cybersecurity researchers identified a new phishing technique called "precision-validating phishing." This method improves credential theft by verifying victims' email addresses in real-time before displaying a fake login page. Using API or JavaScript-based validation services, attackers target only active, legitimate emails. If an email is unrecognized, victims are redirected to benign sites like Wikipedia, bypassing detection by automated security tools. This increases phishing success rates, improves data quality for resale, and complicates analysis by security researchers, as crawlers struggle with validation filters. The tactic highlights the growing sophistication of phishing attacks, stressing the need for better security measures.

Attack Type : Phishing

Cause of Issue : Phishing Mail

Industry Type : Banks and financial institutions

Evolving SparrowDoor Malware Hits Organizations in U.S. and Mexico



In July 2024, the Chinese threat group FamousSparrow targeted a U.S. trade group and a Mexican research institute using advanced versions of the SparrowDoor backdoor and, for the first time, ShadowPad malware. The attack exploited outdated Microsoft Exchange and Windows Server systems, deploying malware through a web shell on an IIS server. One SparrowDoor variant featured modular plugins for tasks like keylogging, file transfers, and remote access, while another enabled multi-threaded command execution. This cyber-espionage campaign underscores FamousSparrow's evolving tactics, focusing on compromising vulnerable organizations in the government and research sectors.

Attack Type : Cyber-Espionage

Cause of Issue : Vulnerabilities

Industry Type : Government Sector

Preloaded Malicious Apps on Chinese Android Devices Target Crypto Users

Cheap Android smartphones from Chinese manufacturers have been found with pre-installed malicious apps disguised as WhatsApp and Telegram. These trojanized apps, infected with Shibai malware, steal cryptocurrency by replacing wallet addresses in messages and scanning device images for recovery phrases. This supply chain attack embeds malware during production, with the fake devices mimicking popular models and spoofing system specs to appear legitimate. Around 40 apps were altered using LSPatch, and over $1.6 million has been stolen. The campaign primarily targets mobile and cryptocurrency users, exploiting deceptive, low-cost devices for financial theft.

Attack Type : Supply Chain

Cause of Issue : Malware

Industry Type : Mobile Device Manufacturing

Linux Systems Targeted by Chinese Threat Actors Using SNOWLIGHT and Vshell

The China-linked threat actor UNC5174 (Uteus) launched a cyber-espionage campaign targeting Linux systems, using a variant of the SNOWLIGHT malware and the open-source VShell Remote Access Trojan (RAT). SNOWLIGHT serves as a dropper, delivering the fileless, in-memory VShell RAT to enable remote control, command execution, and data exfiltration. The campaign also employed open-source tools like GOREVERSE and GOHEAVY, utilizing WebSockets for stealthy command-and-control communication. This tactic highlights a shift toward using publicly available tools to obfuscate attribution and enhance the sophistication of cyber-espionage efforts, making detection and analysis more challenging.

Attack Type : Cyber-Espionage

Cause of Issue : Malware

Industry Type : Cybersecurity Sector

Zero-Day in Fortinet Products (CVE-2024-55591) Actively Exploited to Breach Firewalls

Threat actors exploited a zero-day vulnerability (CVE-2024-55591) in Fortinet's FortiOS and FortiProxy systems, enabling unauthorized super-admin access to firewalls. By sending crafted requests to the Node.js WebSocket module, attackers bypassed authentication, created rogue admin accounts, modified firewall configurations, and set up SSL VPN tunnels for persistent access. Active since mid-November 2024, the campaign involved scanning for vulnerable devices, reconnaissance, configuration changes, and lateral network movement. The attacks targeted devices with exposed management interfaces, highlighting the importance of securing these interfaces and promptly applying available patches to prevent exploitation.

Attack Type : Exploitation

Cause of Issue : Vulnerability

Industry Type : Information Technology

WhatsApp Desktop for Windows Contains Critical Flaw, CERT-In Alerts Users

A critical vulnerability was found in older versions of WhatsApp Desktop for Windows (prior to version 2.2450.6). The issue stemmed from improper handling of MIME types and file extensions, allowing attackers to disguise malicious files as safe files like images or documents. When a user opened such a disguised file, it could execute remote code, potentially giving the attacker control over the victim's computer.

This posed a significant security risk, highlighting the importance of keeping software up to date to prevent exploitation of such vulnerabilities. Users were advised to upgrade to the latest version to mitigate the threat.

Attack Type : Remote Code Execution

Cause of Issue : MIME Mismanagement

Industry Type : Tech / Communication

GPS Spoofing Incidents Target Indian Air Force Aircraft

During a humanitarian mission over Myanmar, an Indian Air Force C-130J aircraft was targeted by a GPS spoofing attack, where false GPS signals misled the aircraft's navigation system. This caused incorrect positioning, potentially diverting the aircraft. However, the crew swiftly switched to the onboard Inertial Navigation System (INS), which doesn't rely on GPS, ensuring safe completion of the mission. The incident underscores the vulnerability of modern aircraft, including military ones, to electronic warfare tactics, highlighting the importance of backup navigation systems in countering such cyber threats.

Attack Type : Spoofing | Cause of Issue : GPS | Industry Type : Defense and Aerospace

Ransomware Attack Hits Fourlis Group, IKEA Franchise Operator

Fourlis Group, the company behind IKEA and Intersport in Greece, Cyprus, Romania, and Bulgaria, suffered a ransomware attack that disrupted its IT systems, affecting both physical stores and online services. During the Black Friday period, IKEA's online store was shut down, leading to significant sales and customer service issues. The company labeled the incident as a "malicious external action" and notified the Personal Data Protection Authority. Although no customer data was leaked, the attack resulted in a €20 million financial loss. Fourlis enlisted cybersecurity experts to help recover, highlighting the impact of cyber threats on retail businesses during peak seasons.

Attack Type : Ransomware | Cause of Issue : Data Leak | Industry Type : Healthcare

Data Breach Exposes Sensitive Information at LSC in the U.S.

Laboratory Services Cooperative (LSC) in Seattle experienced a cyberattack that exposed the personal and medical data of 1.6 million individuals. LSC, which provides lab services to health centers, including Planned Parenthood, had sensitive information such as names, medical records, insurance details, and billing data compromised. The breach occurred due to unauthorized access by an unknown attacker. After discovery, LSC hired cybersecurity experts, reported the incident to authorities, and offered free credit monitoring and identity protection. No evidence of data being shared on the dark web has been found, emphasizing the need for robust security in healthcare systems.

Attack Type : Data Breach | Cause of Issue : Unauthorized Access | Industry Type : Legal / Non-profit

Volt Typhoon Threat Actor Tied to Chinese Cyber Espionage Activities

The Deceptive Development campaign, attributed to North Korea, targets freelance software developers via job platforms like Upwork and Freelancer.com. Attackers use fake recruiter profiles to distribute malware through GitHub, GitLab, or Bitbucket, designed to steal cryptocurrency and login credentials. Key malware tools include BeaverTail and InvisibleFerret, with the latter acting as a backdoor to collect data from browsers and password managers. The campaign primarily targets developers in cryptocurrency and decentralized finance sectors, particularly in Finland, India, and the U.S., marking an evolution in North Korea's cybercrime tactics focused on cryptocurrency theft.

Attack Type : Trojan

Cause of Issue : Social Engineering

Industry Type : Cryptocurrency Sector

MURKYTOUR Malware via Fake Job Campaign

In October 2024, the Iranian-affiliated threat actor UNC2428 launched a cyber espionage campaign targeting Israeli entities. Posing as recruiters from defense contractor Rafael, they lured individuals with fake job offers and directed them to a counterfeit website. Victims downloaded a tool named "RafaelConnect.exe," which deployed a backdoor called MURKYTOUR via a launcher, LEAFPILE. This allowed persistent access to compromised systems. The operation, linked to Iran's Ministry of Intelligence and Security (MOIS) and the Black Shadow group, combined advanced social engineering with custom malware to infiltrate and surveil targeted organizations.

Attack Type : Malware

Cause of Issue : Exploitation of Human Trust

Industry Type : Defense and Aerospace

Innorix Flaws and ThreatNeedle Malware

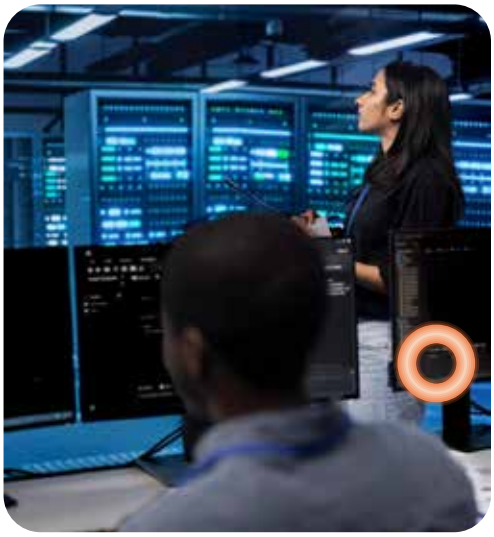
In April 2025, North Korea-linked Lazarus Group launched Operation SyncHole, targeting six South Korean organizations across multiple sectors. The group used a combination of a watering hole attack and exploitation of vulnerabilities in South Korean software, specifically CrossEX and Innorix Agent, to infiltrate systems. After breaching defenses, they deployed several malware tools, including ThreatNeedle, AGAMEMNON, wAgent, SIGNBT, and COPPERHEDGE, to facilitate data exfiltration and maintain access. The campaign, which began in November 2024, was a prolonged and highly targeted effort aimed at compromising critical industries within South Korea.

Attack Type : Advanced Persistent Threat

Cause of Issue : Innorix Agent vulnerabilities

Industry Type : Information Technology

Unmatched Vulnerability Enabling Data Breaches in Ruby Servers



In April 2025, researchers disclosed three vulnerabilities in the Rack Ruby web server, particularly affecting the Rack::Static a middleware. The most critical, CVE-2025-27610, is a path traversal flaw that allows attackers to access sensitive files outside the web directory due to a misconfigured or undefined :root parameter. CVE-2025-27111 and CVE-2025-25184 involve improper handling of carriage return line feeds (CRLF), enabling log manipulation and potential code injection. To mitigate these risks, it is advised to update Rack, remove Rack::Static if patching isn't immediate, or ensure the :root parameter points to a directory with only publicly accessible files.

Attack Type : Log Injection and Manipulation

Cause of Issue : Misconfiguration

Industry Type : Software Development

APT29 Deploys GRAPELOADER Malware

In April 2025, APT29 (Cozy Bear) launched a targeted phishing campaign against European diplomatic entities, impersonating wine-tasting event invitations. The emails contained a malicious ZIP archive named "wine.zip," which included a PowerPoint executable ("wine.exe") and two DLL files. Through DLL side-loading, the "ppcore.dll" file activated the GRAPELOADER malware.

GRAPELOADER performs system fingerprinting, establishes persistence via Windows Registry modifications, and delivers further payloads. It uses advanced anti-analysis techniques like string obfuscation and runtime API resolving. This campaign marks a shift in APT29's tactics, replacing older tools like ROOTSAW with more sophisticated and stealthy malware loaders.

Attack Type : Advanced Persistent Threat

Cause of Issue : Phishing

Industry Type : European Ministries

UK Law Firm Fined £60,000 After Client Data Leaked on Dark Web

In April 2025, the UK's Information Commissioner's Office (ICO) fined DPP Law £60,000 for a 2022 cyberattack. Attackers gained unauthorized access to an outdated administrator account without multi-factor authentication, infiltrating the firm's legacy case management system. Around 32GB of sensitive client data, including details of criminal cases, was exfiltrated and published on the dark web. DPP Law only learned of the breach from the National Crime Agency and delayed reporting to the ICO by 43 days, claiming the loss of access didn't constitute a breach. The ICO criticized the firm for inadequate security and delayed reporting, and DPP Law is appealing the fine.

Attack Type : Brute-force Attack

Cause of Issue : Weak Account Security

Industry Type : Law firm handling sensitive criminal and civil cases

Critical Vulnerability in Erlang/OTP SSH Library Exposes Devices to Remote Code Execution

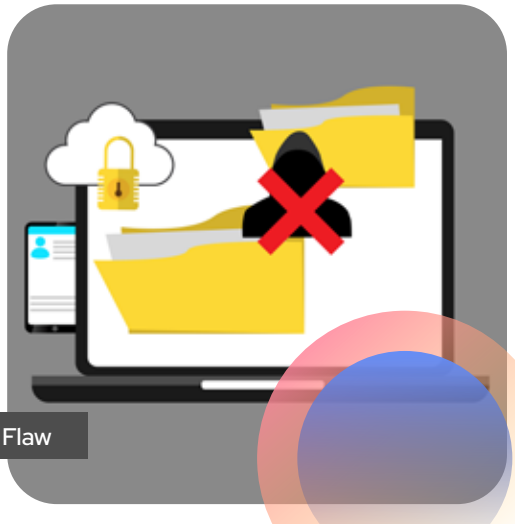
A critical vulnerability (CVE-2025-32433) has been found in Erlang/Open Telecom Platform (OTP) SSH, with a CVSS score of 10.0. It allows attackers to execute arbitrary code on affected servers without authentication by exploiting improper handling of SSH protocol messages. If the SSH daemon runs with root privileges, this could lead to full device control, data manipulation, or denial-of-service. The vulnerability affects services using Erlang/OTP's SSH library, including OT/IoT and edge computing systems. Organizations should update to patched versions OTP-27.3.3, OTP-26.2.5.11, or OTP-25.3.2.20 and restrict SSH port access as an interim measure.

Attack Type : Remote Code Execution

Cause of Issue : SSH Protocol Flaw

Industry Type : Telecommunications

New Vulnerability in Google Quick Share for Windows Enables DoS and Unauthorized File Transfers



In April 2025, cybersecurity researchers disclosed a vulnerability in Google's Quick Share for Windows, tracked as CVE-2024-10668. This flaw enables attackers to send arbitrary files to a recipient's device without consent and can cause a denial-of-service (DoS) by crashing the application. It bypasses earlier fixes for the QuickShell issue identified in August 2024. Exploitation occurs through specially crafted file names or manipulating file transfer sessions to leave unauthorized files on the victim's device. Google addressed the issue in Quick Share version 1.0.2002.2, highlighting the need for thorough patching and validation to prevent vulnerabilities from resurfacing.

Attack Type : Denial-of-Service (DoS)

Cause of Issue : File Transfer Flaw

Industry Type : Technology and Consumer Electronics

New BPFDoor Controller Enhances Hidden Lateral Movement on Linux Servers

Cybersecurity researchers have uncovered a new controller linked to the BPFDoor backdoor, enhancing its stealth and lateral movement in Linux environments. This controller enables attackers to open reverse shells, redirect connections, and monitor backdoor activity. The malware uses the Berkeley Packet Filter (BPF) to detect specific "magic packets," bypassing firewalls for covert activation. A password mechanism ensures only authorized commands are executed. Targeting sectors like telecommunications, finance, and retail in South Korea, Hong Kong, Myanmar, Malaysia, and Egypt, the attack is attributed to the Earth Bluecrow threat group, highlighting the growing risks to Linux systems.

Attack Type : Backdoor Exploitation

Cause of Issue : BPF Vulnerability

Industry Type : Telecommunications

Microsoft Patches 125 Flaws, Including Actively Exploited Windows Bug

In April 2025, Microsoft released security updates addressing 125 vulnerabilities, including CVE-2025-29824, a critical elevation of privilege flaw in the Windows Common Log File System (CLFS) Driver. This use-after-free vulnerability allows attackers with local access to execute code with SYSTEM-level privileges, enabling them to install malware and take control of affected systems. Patches for Windows 10 (both 32-bit and 64-bit) were initially unavailable, leaving many users exposed. The U.S. CISA added this flaw to its Known Exploited Vulnerabilities catalog, requiring federal agencies to apply the fix by April 29, 2025, highlighting the need for timely patch management.

Attack Type : Privilege Escalation

Cause of Issue : Use-After-Free Vulnerability

Industry Type : Windows-based Systems

DslogdRAT Malware Deployed in Japan Attacks

In December 2024, a China-linked cyber espionage group, UNC5337, exploited a zero-day vulnerability (CVE-2025-0282) in Ivanti Connect Secure (ICS), enabling remote code execution. This flaw allowed the deployment of a Perl web shell and DslogdRAT malware on systems, primarily in Japan. DslogdRAT established a connection to an external server, allowing attackers to execute commands, upload/download files, and proxy through the compromised host. The attack was part of a broader campaign using other tools like DRYHOOK and PHASEJAM. Although Ivanti patched the vulnerability in January 2025, increased scanning activity suggests future exploitation risks.

Attack Type : Zero-Day Exploitation

Cause of Issue : Zero-Day Vulnerability

Industry Type : Technology and IT Services

159 CVEs Exploited in Q1 2025

In the first quarter of 2025, cybersecurity researchers identified 159 CVEs actively exploited, up from 151 in the previous quarter. Notably, 28.3% were exploited within a day of public disclosure, indicating the rapid pace of threat actors exploiting new vulnerabilities. Most exploited flaws were found in CMS, network devices, OS, open-source software, and server software, with affected vendors including Microsoft, Broadcom, VMware, and TOTOLINK. Vulnerabilities now surpass phishing as the primary method for initial access in cyber intrusions, emphasizing the urgent need for organizations to apply security patches and maintain strong vulnerability management to mitigate risks.

Attack Type : Zero-Day Exploitation

Cause of Issue : Insufficient Vulnerability Management

Industry Type : Web Development and Hosting

OAuth Phishing Campaign Targets Ukraine Allies via Messaging Apps

"In April 2025, cybersecurity firm Volexity uncovered a sophisticated phishing campaign by Russian-linked threat actors targeting individuals and organizations related to Ukraine and human rights. The attackers impersonated European officials via Signal and WhatsApp, luring victims into meetings and directing them to legitimate Microsoft 365 login pages. By tricking users into providing OAuth codes, the attackers gained unauthorized access to Microsoft 365 accounts.

Two threat clusters, UTA0352 and UTA0355, were identified, with UTA0355 using compromised Ukrainian government emails. The attackers also exploited Microsoft Entra ID to register new devices, ensuring persistent access. This highlights evolving tactics by nation-state actors."

Attack Type : Social Engineering

Cause of Issue : Abused OAuth Login Flow

Industry Type : Human Rights Organizations

DaVita Hit by Ransomware Attack Disrupting Operations

In April 2025, DaVita Inc., a leading kidney disease treatment company, revealed it had fallen victim to a ransomware attack that encrypted parts of its IT systems. The company swiftly activated its incident response plan, isolating affected systems and involving cybersecurity experts and law enforcement. Despite the breach, patient care continued without disruption due to contingency plans. However, DaVita did not disclose whether sensitive data was compromised. Following the announcement, DaVita's stock dropped by over 3%, reflecting concerns about the financial and reputational impact of the attack. This incident underscores the growing cybersecurity risks in healthcare.

Attack Type : Ransomware

Cause of Issue : Encrypted Network

Industry Type : Healthcare Sector

4chan Hacked : Deep Breach Exposes Site's Inner Workings

In April 2025, 4chan experienced a major cyberattack, causing extended downtime and exposing sensitive internal data, including source code, moderator and janitor lists, and user permissions. The attacker gained deep access, likely exploiting outdated, unpatched software vulnerabilities. This breach raises concerns about the platform's security, as it could unmask the identities of anonymous users and moderators, challenging the site's promise of privacy. The incident highlights broader risks tied to legacy systems and the need for improved cybersecurity, especially in loosely moderated forums, reigniting debates on moderation practices, data protection, and digital security hygiene.

Attack Type : Unauthorized Access

Cause of Issue : Outdated Software

Industry Type : Online Communities

Briskinfosec at GITEX EUROPE 2025!

We are pleased to announce our participation in the inaugural GITEX EUROPE 2025, one of the most highly anticipated events in the tech and cybersecurity industry. The event will take place in Berlin from May 21–23, 2025. As a trusted cybersecurity partner for businesses in over 30 countries, Briskinfosec is bringing its global expertise and localized insights to the European stage.

Event Details

Dates : **May 21–23, 2025**

Location : **Messe Berlin, Germany**

Booth No : **H5.2 – A101**

Why Attend GITEX EUROPE 2025?

Explore innovative cybersecurity solutions to protect your business against emerging threats.
Network with industry leaders and grow your professional connections.
Gain valuable insights into the latest trends and best practices in cybersecurity.
Learn how to seamlessly integrate security into your digital transformation journey.

Visit Our Stall and Meet Our Expert Team

Our team is excited to meet you in person to discuss your unique cybersecurity challenges, share insights on the latest threat landscape, and demonstrate how Briskinfosec can help protect and future-proof your organization.

We look forward to seeing you at GITEX EUROPE 2025! Let's connect, collaborate, and shape the future of cybersecurity together.

Arulselvar Thomas
Founder & Director

Siddique
Customer Success Executive

Jayram Kumar Pothi
Chief Executive Consultant

Ransomware Attack on Change Healthcare Exposes Data of 190 Million Individuals

Change Healthcare, a major U.S. health tech provider, experienced a ransomware attack by the ALPHV/BlackCat group, compromising sensitive data of around 190 million individuals. The breach exposed personal health information, insurance details, and medical records due to system vulnerabilities. Despite containment efforts, the attackers encrypted critical data and demanded a ransom for decryption keys. The incident disrupted healthcare operations, affecting patients, providers, and insurers. Legal actions have been taken, and the attack highlights the increasing threat to healthcare infrastructure, emphasizing the need for stronger cybersecurity to protect sensitive health data.

Attack Type : Ransomware

Cause of Issue : Exploitation of System Vulnerabilities

Industry Type : Healthcare Industry

Kimsuky Exploits BlueKeep in Global Cyber Espionage Campaign

In April 2025, cybersecurity researchers discovered a campaign by North Korean group Kimsuky exploiting the BlueKeep vulnerability (CVE-2019-0708) in Microsoft Remote Desktop Services to execute remote code on vulnerable systems. Kimsuky used this to gain initial access, deploying tools like MySpy for system info and RDPWrap for persistent access.

Phishing emails with malicious files targeting CVE-2017-11882 further compromised systems. After gaining access, they used keyloggers like KimaLogger and RandomQuery to capture keystrokes. The campaign mainly targeted South Korea and Japan's software, energy, and financial sectors, with additional targets in the U.S., China, Germany, and others.

Attack Type : Remote Code Execution

Cause of Issue : Legacy Vulnerability

Industry Type : Critical Infrastructure

SuperCard X Android Malware Enables NFC Relay Attacks for Fraudulent Cashouts

In April 2025, cybersecurity researchers uncovered a new Android malware-as-a-service (MaaS) platform, SuperCard X, designed for NFC relay attacks. Targeting Italian banking customers, it uses social engineering tactics, including smishing and deceptive phone calls, to trick victims into installing malicious apps like "Verifica Carta," "SuperCard X," and "KingCard NFC." These apps capture NFC card data when the victim's card is near the infected device. The stolen data is then relayed to external servers for unauthorized transactions at PoS terminals and ATMs. The attack is believed to be orchestrated by Chinese-speaking threat actors, promoted via Telegram channels.

Attack Type : Social Engineering

Cause of Issue : Unauthorized Access

Industry Type : Financial Services

Lotus Panda Cyber Espionage Targets Southeast Asia with Custom Malware Tools

Between August 2024 and February 2025, the China-linked cyber espionage group Lotus Panda launched a targeted campaign across Southeast Asia. Their victims included a government ministry, air traffic control, telecommunications, and construction sectors. Using custom tools like credential stealers, loaders, and a reverse SSH tool, they sideloaded malicious DLLs via legitimate security software (Trend Micro, Bitdefender). They deployed an updated version of their backdoor, Sagerunex, to steal host information. Additional tools like ChromeKatz and CredentialKatz were used to extract credentials, while Zrok enabled remote access. The campaign also affected a news agency and air freight organization, signaling a broader regional focus.

Attack Type : Cyber-Espionage

Cause of Issue : Sideloading Exploits

Industry Type : Government Sector

ASUS Routers Vulnerable to Critical Remote Code Execution Flaw (CVE-2025-2492)

In April 2025, ASUS disclosed a critical security vulnerability (CVE-2025-2492) affecting routers with AiCloud enabled. The flaw, caused by improper authentication control in specific firmware versions, allows remote attackers to execute unauthorized functions. With a CVSS score of 9.2, this vulnerability is highly severe. ASUS released firmware updates for affected versions (3.0.0.4_382, 3.0.0.4_386, 3.0.0.4_388, and 3.0.0.6_102). Users are urged to update their routers immediately. For unsupported models or unpatched routers, disabling AiCloud and other internet-facing services is recommended, alongside using strong, unique passwords for network and router administration.

Attack Type : Remote Command Execution

Cause of Issue : Authentication Flaw

Industry Type : Consumer Networking Equipment

Top Critical CVEs – April 2025

1. CVE-2025-46661

IPW Systems Metazo up to version 8.1.3 allowed unauthenticated Remote Code Execution via Server-Side Template Injection in smartyValidator.php. The vulnerability has been fully patched by the supplier.

ATTACK TYPE *Server-Side Template Injection (SSTI)*

2. CVE-2025-32067

An Improper Input Validation vulnerability in Wikimedia's MediaWiki Growth Experiments Extension allows Cross-Site Scripting (XSS), affecting versions from 1.39 through 1.43 of the extension.

ATTACK TYPE Cross-Site Scripting (XSS)

3. CVE-2025-32642

A Cross-Site Request Forgery (CSRF) vulnerability in appsbd Vite Coupon permits Remote Code Inclusion. This vulnerability impacts all versions from unspecified (n/a) through 1.0.7 of the Vite Coupon application.

ATTACK TYPE Cross-Site Request Forgery (CSRF)

4. CVE-2021-47667

An OS command injection vulnerability in lib/NSSDropoff.php affects ZendTo versions 5.24-3 through 6.x before 6.10-7, enabling unauthenticated attackers to execute arbitrary commands via shell metacharacters in the tmp_name parameter during a POST /dropoff request.

ATTACK TYPE OS Command Injection

5. CVE-2024-41794

All versions of SENTRON 7KT PAC1260 Data Manager contain hardcoded credentials granting root-level remote access. If SSH is enabled, unauthenticated attackers with these credentials could gain full device access, potentially leveraging CVE-2024-41793 for exploitation.

ATTACK TYPE Remote Access

Top Critical CVEs – April 2025

6. CVE-2025-30065

Apache Parquet versions 1.15.0 and earlier have a schema parsing vulnerability in the parquet-avro module that allows arbitrary code execution. Users should upgrade to version 1.15.1, which addresses and resolves this security issue.

ATTACK TYPE Remote Code Execution

7. CVE-2025-46616

Quantum StorNext Web GUI API before version 7.2.4 contains a vulnerability that may allow Arbitrary Remote Code Execution (RCE) through file upload. Affected products include StorNext RYO, Xcellis Workflow Director, and ActiveScale Cold Storage, all before 7.2.4.

ATTACK TYPE *Arbitrary Remote Code Execution*

8. CVE-2023-40714

A relative path traversal vulnerability exists in Fortinet FortiSIEM versions 7.0.0, 6.7.0 to 6.7.2, 6.6.0 to 6.6.3, 6.5.1, and 6.5.0, allowing attackers to escalate privileges by uploading certain GUI components.

ATTACK TYPE Relative Path Traversal

9. CVE-2025-46275

WGS-80HPT-V2 and WGS-4215-8T2S lack proper authentication, potentially allowing an attacker to create an administrator account without requiring knowledge of any existing credentials.

ATTACK TYPE Missing Authentication

10. CVE-2025-45429

The Tenda AC9 v1.0 router running firmware V15.03.05.14_multi contains a stack overflow vulnerability in /goform/WifiWpsStart, which could potentially lead to remote arbitrary code execution.

ATTACK TYPE Remote Code Execution

Cyber Threats Never Sleep

Be Proactive,
Stay Protected.

+91 44 4352 4537 | +91 73059 79769
contact@briskinfosec.com | www.briskinfosec.com