Edition-77

Threatsploit

Adversary Report

January - 2025

BRISKINFOSEC

CYBER TRUST & ASSURANCE

www.briskinfosec.com

Introduction :

Dear Readers,

Welcome to the January 2025 edition of the Threatsploit Adversary Report. In an era of relentless cyber threats, safeguarding digital assets is more critical than ever. This edition sheds light on the latest tactics employed by threat actors, from supply chain vulnerabilities to social engineering campaigns and typosquatting attacks. These sophisticated strategies underline the necessity for a collective and proactive approach to cybersecurity.

Organizations must embrace a culture of vigilance and resilience to withstand the constantly evolving cyber threat landscape. Building a robust security framework requires staying informed about emerging threats and understanding how adversaries exploit weak links. By proactively analyzing trends, vulnerabilities, and attack vectors, organizations can better prepare for the challenges ahead.

The real challenge lies in anticipating potential incidents and understanding the broader implications of these threats. Threat actors are leveraging weak links in industries ranging from AI to defense, exploiting everything from inadequate input validation to the proliferation of remote access vulnerabilities. Staying informed about these adversarial techniques can mean the difference between disruption and continuity.

This report provides comprehensive insights into recent attacks, highlighting key learnings to help organizations take proactive steps against an unpredictable digital landscape. By leveraging this intelligence, organizations can strengthen their defenses, reduce risks, and maintain trust in an increasingly unpredictable digital world. Together, we can outpace the adversaries.

Stay informed and stay secure!

Best regards,

Briskinfosec Threat Intelligence Team.

Report Inside :

- Top Cyberattacks in the Last 30 Days According to Industry
- Top 5 Most Affected Industries in 2024
- Top 5 Vulnerabilities of 2024
- Top 5 Affected Regions of 2024

Contents :

1. Criminals Leverage Biometric Data to Bypass KYC Protocols
2. Malicious npm Packages Impersonate Trusted Tools, Racking Up Thousands of Downloads
3. Fortinet Alerts Users to Critical Vulnerability in FortiWLM That Could Allow Admin Access Exploits
4. DarkGate Malware Deployed via Microsoft Teams and AnyDesk Exploit"
5. Bitter APT Uses WmRAT and MiyaRAT Malware in Attack on Turkish Defense Organization
6. Severe OpenWrt Vulnerability Puts Devices at Risk of Malicious Firmware Attacks
7. Authentication Bypass Vulnerability Discovered in Apache HugeGraph-Server
8. Security Flaws in McDonald's India Delivery System Expose Customer Data
9. Hapn GPS Tracker Leak Exposes Thousands of Customer Names
10. New G-Door Flaw Allows Hackers to Bypass Microsoft 365 Security via Google Docs
11. Security Vulnerabilities Discovered in Skoda Cars, Allowing Remote Tracking by Hackers
12. Cisco Breach : IntelBroker Group Dumps 2.9GB of Stolen Data
13. Malicious Android Spyware Disguised as BMI Calculator on Amazon Appstore
14. cShell Malware Targets Linux SSH Servers Using Built-in Tools for DDoS Attacks
15. BeyondTrust Addresses Critical Vulnerability in PRA and RS with Urgent Patch
16. Cybercriminals Use Webview2 to Deliver CoinLurker Malware and Bypass Security Measures
17. Cellebrite Tool Used to Unlock Journalist's Phone, Then Infected with NoviSpy Spyware
18. Critical Vulnerability in WordPress Hunk Companion Plugin Allows Malicious Plugin Installation
19. Malware Leverages Windows UI Framework to Evade EDR Systems
20. Phishing Scam : Fake Recruiters Spread Banking Trojan Through Malicious Apps
21. Hackers Leverage Microsoft MSC Files to Deploy Stealthy Backdoor in Pakistan Attack
22. Glutton Malware Targets Widely Used PHP Frameworks, Including Laravel and ThinkPHP
23. Iranian IOCONTROL Malware Targets IoT and SCADA Systems
24. Cybercriminals Leverage Google Calendar and Drawings for Phishing Campaigns
25. PUMAKIT : Advanced Linux Rootkit Employs Stealth to Avoid Detection
26. Russian APT29 Leverages RDP Proxies for Credential and Data Theft
27. EagleMsgSpy : Chinese Surveillance Spyware Exploiting Mobile Devices Since 2017
28. New $3,000 Android Trojan Targets Banks and Crypto Exchanges
29. Cybercriminals Exploit Fake Video Apps to Steal Data from Web3 Workers
30. Turla APT Group Uses Pakistani Hackers' Infrastructure to Attack Afghan and Indian Targets

Criminals Leverage Biometric Data to Bypass KYC Protocols

iProov's Q4 2024 Threat Intelligence Update reveals a dark web operation exploiting genuine identity documents and biometric data to bypass Know Your Customer (KYC) protocols. Unlike traditional identity theft, individuals willingly sell their personal information, including documents and biometric matches, to create convincing fake identities. This operation targets high-security industries, such as banking and cryptocurrency, and employs escalating attack techniques: basic (static images), mid-level (deepfakes and face-swapping), and advanced (AI-generated synthetic faces to bypass liveness detection). The findings highlight a critical vulnerability in KYC systems, as current verification methods struggle to detect genuine credentials paired with real biometric data. This evolving fraud poses a significant challenge for organizations relying on traditional identity verification technologies.

Attack Type : Biometric Spoofing

Cause of Issue : Genuine Credentials

Industry Type : Software Development Companies

Malicious npm Packages Impersonate Trusted Tools, Racking Up Thousands of Downloads

Threat actors have been observed uploading malicious typosquatted versions of popular npm packages like typescript-eslint and @types/node, tricking developers into downloading them. These counterfeit packages, such as @typescript_eslinter/eslint and types-node, deliver trojans or retrieve second-stage payloads. One package drops a trojan file disguised as a "prettier.bat" that runs on startup, while another fetches malicious scripts from Pastebin. The attack highlights the importance of securing the software supply chain and being cautious when downloading third-party libraries. Additionally, malicious VSCode extensions were also detected, mostly targeting the crypto community.

Attack Type : Typosquatting Attack

Cause of Issue : Supply Chain Vulnerability

Industry Type : Software Development Companies

Fortinet Alerts Users to Critical Vulnerability in FortiWLM That Could Allow Admin Access Exploits

Fortinet has issued advisories for two critical vulnerabilities. The first, CVE-2023-34990, is a path traversal flaw in FortiWLM that allows unauthenticated attackers to read sensitive files and potentially execute unauthorized commands. It affects FortiWLM versions 8.6.0 to 8.6.5 and 8.5.0 to 8.5.4, with fixes in versions 8.6.6 and 8.5.5. Exploiting this flaw could allow attackers to hijack web sessions and gain administrative access.

Additionally, CVE-2023-48782, an authenticated command injection flaw, can be combined with CVE-2023-34990 for remote code execution. The (space) second vulnerability, CVE-2024-48889, affects FortiManager and allows authenticate+C5d remote attackers to execute unauthorized commands via crafted requests. This flaw is fixed in versions 7.6.1 and above, with several other affected versions listed. Users are urged to update their devices to avoid exploitation.

Attack Type : Path Traversal

Cause of Issue : Input Validation

Industry Type : Software Companies

DarkGate Malware Deployed via Microsoft Teams and AnyDesk Exploit

A new social engineering campaign uses Microsoft Teams to deploy the DarkGate malware. Attackers impersonate an external supplier via Teams, instructing victims to install AnyDesk for remote access, which is then exploited to deliver malware like a credential stealer and DarkGate. DarkGate, a remote access trojan, is a malware-as-a-service offering used for activities like keylogging and screen capturing. The attack chain involves AutoIt scripts. Researchers recommend enabling multi-factor authentication, using trusted remote access tools, and thoroughly vetting third-party support providers to mitigate such risks. Additionally, phishing campaigns continue to rise, using various tactics to steal credentials and financial data, often exploiting global events for urgency.

Attack Type : Social Engineering

Cause of Issue : Remote Access

Industry Type : Software Development Companies

Bitter APT Uses WmRAT and MiyaRAT Malware in Attack on Turkish Defense Organization

A suspected South Asian cyber espionage group, Bitter (also known as TA397, APT-C-08, Hazy Tiger, and others), targeted a Turkish defense organization in November 2024 with two C++-based malware families, WmRAT and MiyaRAT. The attack used a RAR archive containing a decoy file and a hidden malicious PowerShell script, which created a scheduled task to download additional payloads. The group, active since 2013, has previously targeted countries like China, India, and Pakistan. The malware allows attackers to collect data, take screenshots, and execute commands, with MiyaRAT being used for high-value targets. The attacks are believed to be intelligence collection efforts supporting South Asian governmental interests.

Attack Type : Remote Access

Cause of Issue : Malicious Payload

Industry Type : Defense and Security

Severe OpenWrt Vulnerability Puts Devices at Risk of Malicious Firmware Attacks

A critical security vulnerability, identified as CVE-2024-54143, has been discovered in OpenWrt's Attended Sysupgrade (ASU) feature, which allows for upgrading firmware on OpenWrt devices. The flaw, with a CVSS score of 9.3, arises from a combination of command injection and a truncated 12-character SHA-256 hash used in the build process. This allows an attacker to inject arbitrary commands into the firmware build, leading to the creation of malicious firmware images that could be signed with legitimate keys.

The attacker can exploit hash collisions to replace a legitimate firmware image with a malicious one, posing a severe supply chain risk. Thevulnerability does not require authentication to exploit, and it is not clear whether it has been exploited in the wild. The issue has been fixed in ASU version 920c8a1, and users are strongly advised to update their systems to prevent potential exploitation. The vulnerability was reported by researcher RyotaK on December 4, 2024.

Attack Type : Supply Chain

Cause of Issue : Command Injection

Industry Type : Telecommunications

Authentication Bypass Vulnerability Discovered in Apache HugeGraph-Server

A security vulnerability, CVE-2024-43441, has been identified in Apache HugeGraph-Server (versions 1.0 to 1.3), an open-source graph database system. The flaw, classified as an Authentication Bypass by Assumed Immutable Data, allows attackers to bypass authentication mechanisms and gain unauthorized access to sensitive resources. This issue has been rated as important, and Apache addressed it in version 1.5.0. Users of affected versions are urged to upgrade immediately to mitigate risks. In addition to upgrading, organizations should implement strict access controls, review authentication mechanisms, and monitor server logs for suspicious activity. While there are no reports of active exploitation, the vulnerability poses a significant risk to environments where Apache HugeGraph-Server is used, especially in sectors handling sensitive data like finance and healthcare.

Attack Type : Authentication Bypass

Cause of Issue : Immutable Data

Industry Type : Software Development Companies

Security Flaws in McDonald's India Delivery System Expose Customer Data

A major security flaw in McDonald's India's McDelivery system exposed sensitive personal information of both customers and delivery drivers. Discovered by security researcher Eaton Zveare, the vulnerabilities were found in the APIs of McDelivery, used for order placement and tracking. These flaws allowed unauthorized individuals to hijack or track orders, submit feedback, and even make orders for just $0.01. The flaws also exposed full names, email addresses, phone numbers, and real-time locations of drivers, along with vehicle details and profile pictures. Zveare reported the vulnerabilities in July, and they were patched by September.

Despite McDonald's India assuring that no breach occurred, the researcher stated that the flaws impacted hundreds of millions of orders. McDonald's India (West & South) responded by emphasizing regular audits and security enhancements but did not disclose the number of affected customers. This incident follows a similar data breach in 2017, where 2.2 million customer records were exposed.

Attack Type : API Exploitation

Cause of Issue : Inadequate Authentication

Industry Type : Telecommunications Sector

Hapn GPS Tracker Leak Exposes Thousands of Customer Names

Hapn, a GPS tracking company formerly known as Spytec, exposed the names and affiliations of thousands of its customers due to a website bug discovered in November 2024. The vulnerability allowed anyone logged into a Hapn account to access sensitive data via browser developer tools. The exposed data included information on over 8,600 GPS trackers, such as IMEI numbers and customer names, as well as business affiliations. Although location data was not included, the leak raised privacy concerns, especially as some records involved individuals who may not have been aware they were being tracked. Hapn sells GPS devices for tracking valuable items and loved ones and serves corporate clients, including those in the Fortune 500. CEO Joe Besdin initially did not respond to enquiries but later confirmed the issue, stating it was resolved. The breach underscores concerns over the security of GPS tracking data and its potential misuse.

Attack Type : Data Exposure

Cause of Issue : Website Bug

Industry Type : Telecommunications Sector

New G-Door Flaw Allows Hackers to Bypass Microsoft 365 Security via Google Docs

The G-Door vulnerability allows attackers to bypass Microsoft 365 security by exploiting unmanaged Google Docs accounts created with corporate email addresses. These personal or workspace Google accounts can access third-party apps, bypassing critical security measures like Conditional Access, multi-factor authentication (MFA), and device compliance checks. The vulnerability also causes a lack of visibility in Microsoft 365 logs and exposes sensitive data to risks, as it is not subject to corporate DLP or Azure Information Protection policies. Attackers can maintain persistent access even after credential revocation, and offboarding processes may fail. To mitigate G-Door, organizations should implement strict domain verification, audit unmanaged accounts, educate users on risks, and consider third-party security solutions to monitor cross-platform access.

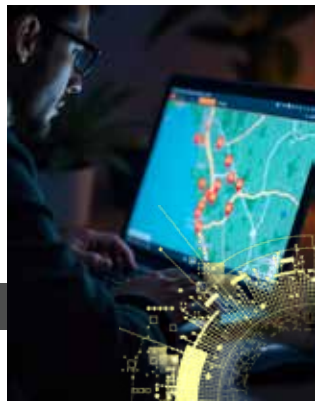
Attack Type : Authentication Bypass

Cause of Issue : Unverified Accounts

Industry Type : Software Development Companies

Security Vulnerabilities Discovered in Skoda Cars, Allowing Remote Tracking by Hackers

Security researchers from PCAutomotive have discovered 12 vulnerabilities in the infotainment system of the Skoda Superb III sedan, which could allow hackers to remotely access controls and track the car's location. These vulnerabilities, found in the MIB3 infotainment unit, could enable attackers to execute malicious code, access GPS and speed data, record conversations, and exfiltrate the owner's phone contacts stored in plaintext. While the flaws do not affect critical car systems like brakes or steering, they impact over 1.4 million vehicles. Skoda has patched the vulnerabilities, ensuring no safety risk to customers.



Attack Type : Remote Exploitation

Cause of Issue : Infotainment Vulnerabilities

Industry Type : Automobile Sector

Cisco Breach : IntelBroker Group Dumps 2.9GB of Stolen Data

On December 16, 2024, hacker IntelBroker leaked 2.9GB of data allegedly stolen from Cisco's DevHub, part of a broader breach involving 4.5TB. The breach, attributed to exposed API tokens, compromised sensitive resources like source code, hardcoded credentials, Docker builds, AWS and Azure buckets, and encryption keys from Cisco products such as IOS XE, Webex, and ISE. The breach also affected high-profile companies, including Verizon, AT&T, Microsoft, and Bank of America. Cisco confirmed the exposure but claimed its core systems were unaffected, citing a misconfigured DevHub portal. No PII or financial data was found in the leak. The incident highlights vulnerabilities in securing developer environments and the growing trend of partial data leaks to fuel demand in underground markets.

Attack Type : API Exploitation

Cause of Issue : Exposed API Token

Industry Type : Telecommunications Sector

Malicious Android Spyware Disguised as BMI Calculator on Amazon Appstore

A malicious Android spyware app, 'BMI CalculationVsn,' was found on the Amazon Appstore, disguised as a simple BMI calculator. Discovered by McAfee Labs, the app secretly performs harmful actions, including starting a screen recording service, scanning installed apps, and collecting SMS messages, including OTPs and verification codes. It was first released on October 8 and later updated with additional malicious features. Though Amazon removed the app after being notified, users who installed it must manually remove it and perform a full scan. This incident highlights the risks of third-party app stores, emphasizing the importance of installing apps from trusted publishers, carefully reviewing app permissions, and using tools like Google Play Protect for added security.

Attack Type : Spyware Infection

Cause of Issue : Malicious Permissions

Industry Type : Software Development Companies

cShell Malware Targets Linux SSH Servers Using Built-in Tools for DDoS Attacks

"ASEC has discovered a new DDoS malware strain, cShell, targeting poorly secured Linux SSH servers. The malware exploits weak SSH credentials to gain access and install tools like curl, hping3, and screen for DDoS attacks. The malware utilizes screen for managing background tasks, while hping3 is utilized to execute SYN, ACK, and UDP floods, thereby overwhelming the targeted servers. cShell is equipped with six DDoS commands and maintains communication with C&C servers to receive updates. It installs itself as a persistent service to survive reboots. Administrators are advised to secure SSH accounts with strong passwords, apply security patches, use firewalls, and monitor systems for unusual activity to defend against this threat. "

Attack Type : DDoS Attacks

Cause of Issue : Weak Credentials

Industry Type : Telecommunications Sector

BeyondTrust Addresses Critical Vulnerability in PRA and RS with Urgent Patch

BeyondTrust has disclosed a critical security vulnerability (CVE-2024-12356) in its Privileged Remote Access (PRA) and Remote Support (RS) products, with a CVSS score of 9.8. The flaw, identified as a command injection, allows unauthenticated attackers to execute arbitrary commands on affected systems as a site user. This impacts PRA and RS versions 24.3.1 and earlier. A patch has been applied to cloud instances, while on-premise users are advised to update to the latest fixes. The vulnerability was discovered after a security incident on December 2, 2024, when an API key for Remote Support SaaS was compromised. BeyondTrust is working with cybersecurity experts to investigate the incident and its impact.

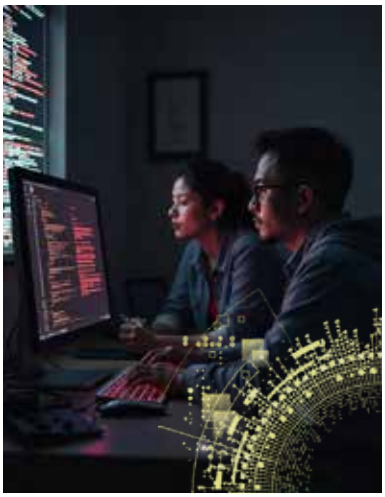
Attack Type : Command Injection

Cause of Issue : Compromised API

Industry Type : Software Development Companies

Cybercriminals Use Webview2 to Deliver CoinLurker Malware and Bypass Security Measures

Threat actors are using bogus software update lures to deliver CoinLurker, a sophisticated stealer malware. Written in Go, it uses advanced obfuscation and anti-analysis techniques to evade detection. The malware is distributed through various deceptive channels, such as fake update prompts, phishing emails, and malvertising. Once executed, CoinLurker targets cryptocurrency wallet data, including Bitcoin and Ethereum, and user credentials from platforms like Telegram and Discord. It communicates with a remote server to steal valuable information. Additionally, malicious campaigns are targeting graphic designers with Google Search ads, while a new malware family known as I2PRAT exploits the I2P network for encrypted C2 communications.



Attack Type : Malvertising Campaigns

Cause of Issue : Fake Updates

Industry Type : Software Development Companies

Cellebrite Tool Used to Unlock Journalist's Phone, Then Infected with NoviSpy Spyware

A new report by Amnesty International reveals that Serbian authorities used a combination of Cellebrite forensic tools and a previously unknown spyware called NoviSpy to compromise the phones of journalists and activists. NoviSpy, which was installed on devices during the detention of journalist Slaviša Milanov in early 2024, allows remote access to sensitive data, including location, microphone, camera, and screenshots. It targets Android phones through two apps: NoviSpyAdmin and NoviSpyAccess. Additionally, a zero-day exploit in Cellebrite's Universal Forensic Extraction Device (UFED) was found to escalate privileges on a Serbian activist's phone. Amnesty links these tools to Serbian intelligence agencies, continuing a history of using spyware on civil society members.

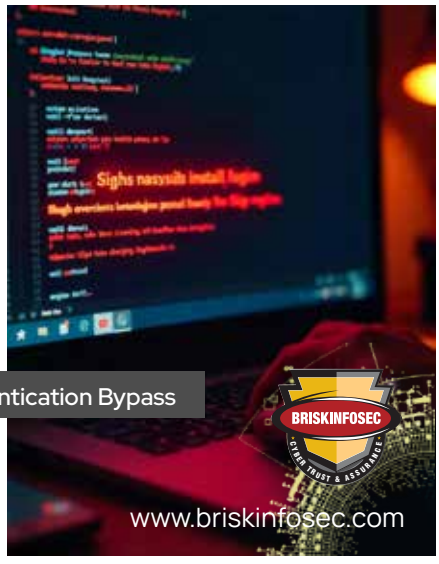
Attack Type : Spyware Infection

Cause of Issue : Tool Exploitation

Industry Type : Media and Entertainment Sector

Critical Vulnerability in WordPress Hunk Companion Plugin Allows Malicious Plugin Installation

A critical vulnerability (CVE-2024-11972) in the Hunk Companion plugin for WordPress allows attackers to install vulnerable or unauthorized plugins, enabling attacks like Remote Code Execution (RCE), SQL Injection, and Cross-Site Scripting (XSS). This flaw, affecting all versions before 1.9.0, has a CVSS score of 9.8. It exploits a bug in the plugin's script, allowing unauthenticated requests to bypass plugin installation checks. Attackers are using this flaw to install the WP Query Console plugin, which has an unpatched RCE vulnerability (CVE-2024-50498). This issue underscores the need to secure third-party plugins. Additionally, a high-severity vulnerability (CVE-2024-11205) in the WPForms plugin, affecting millions of sites, was also disclosed.



Attack Type : Remote Code Execution (RCE)

Cause of Issue : Authentication Bypass

Industry Type : Software Development Companies

Malware Leverages Windows UI Framework to Evade EDR Systems

A new attack technique uses Windows' UI Automation (UIA) framework to perform malicious activities without detection by endpoint detection and response (EDR) solutions. UIA, originally designed for assistive technologies, allows attackers to manipulate UI elements in other applications, execute commands, steal data, and redirect victims to malicious websites. This technique can also be used to read/write messages in apps like Slack and WhatsApp. It bypasses security measures, such as Windows Defender, since these actions are seen as legitimate features. Additionally, a new DCOM-based attack allows attackers to remotely write and execute malicious payloads on target systems, potentially creating backdoors, though it leaves detectable indicators of compromise.

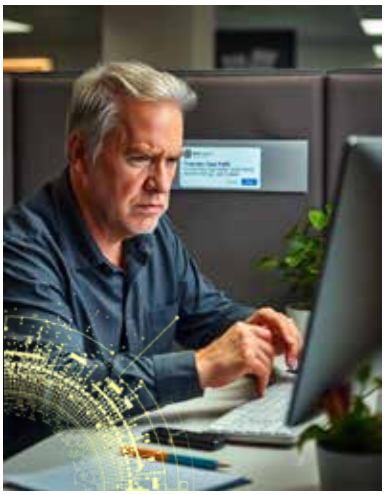
Attack Type : UI Automation Attack

Cause of Issue : Privilege Escalation

Industry Type : Software Development Companies

Phishing Scam : Fake Recruiters Spread Banking Trojan Through Malicious Apps

A sophisticated mobile phishing (mishing) campaign has been discovered, targeting users with fraudulent job offers to distribute an updated version of the Antidot banking trojan, dubbed AppLite Banker. The attackers lure victims by posing as recruiters and prompt them to download a malicious app, which then installs the trojan. The malware, capable of stealing PINs, remotely controlling devices, and displaying fake login pages for over 170 banks and social media platforms, also features keylogging, SMS theft, and call forwarding. The campaign uses social engineering tactics and manipulates Android settings to evade detection.



Attack Type : Mobile Phishing

Cause of Issue : Malicious App

Industry Type : Banking & Finance

Hackers Leverage Microsoft MSC Files to Deploy Stealthy Backdoor in Pakistan Attack

A new phishing campaign targeting Pakistan has been observed, delivering a stealthy backdoor payload through tax-themed lures. The attack, tracked by Securonix as FLUX#CONSOLE, uses MSC (Microsoft Common Console Document) files with double extensions (e.g., .pdf.msc) to deliver a dual-purpose loader and dropper. The malicious files execute JavaScript code via Microsoft Management Console (MMC), loading a backdoor DLL ("DismCore.dll") to establish remote access and exfiltrate data. A legitimate document from Pakistan's Federal Board of Revenue (FBR) is used as a decoy. Although Patchwork, a known threat actor, has previously used similar tactics, attribution remains uncertain. The attack was disrupted within 24 hours.

Attack Type : Phishing Attack

Cause of Issue : Malicious MSC Files

Industry Type : Banking & Finance

Glutton Malware Targets Widely Used PHP Frameworks, Including Laravel and ThinkPHP

Cybersecurity researchers have uncovered a new PHP-based backdoor, Glutton, linked to the Chinese nation-state group Winnti (APT41). Discovered in April 2024, Glutton targets systems in China, the US, Cambodia, Pakistan, and South Africa, aiming to exploit vulnerabilities and harvest sensitive information. The malware framework injects malicious code into PHP files, installs an ELF backdoor, and supports 22 commands for further exploitation. Uniquely, Glutton targets cybercrime forums, using compromised systems to attack other cybercriminals. It lacks typical stealth techniques, such as encrypted communications, making it less sophisticated than Winnti's usual tools. The malware demonstrates a recursive attack strategy, leveraging cybercrime resources against operators themselves.

Attack Type : Backdoor Injection

Cause of Issue : Exploited Vulnerabilities

Industry Type : Software Development Companies

Iranian IOCONTROL Malware Targets IoT and SCADA Systems

Iran-affiliated threat actors have developed a custom malware, codenamed IOCONTROL, targeting IoT and OT environments, including SCADA devices like IP cameras, routers, PLCs, and HMIs in Israel and the U.S. The malware, first documented as OrpaCrab, operates on various Linux-based platforms and is designed to execute arbitrary commands. It uses MQTT for communication and Cloudflare's DNS-over-HTTPS to evade detection. The malware aims to establish a persistent backdoor and can execute commands such as code execution, port scanning, and self-deletion. IOCONTROL is linked to the Cyber Av3ngers group, which has targeted critical infrastructure, including fuel management systems, enabling potential disruption and data theft.

Attack Type : IoT Exploitation

Cause of Issue : Malicious Malware

Industry Type : Energy and Utilities Sector

Cybercriminals Leverage Google Calendar and Drawings for Phishing Campaigns

Cybercriminals are exploiting Google Calendar and Google Drawings to launch sophisticated phishing attacks targeting over 500 million users. These attacks often involve disguised emails and calendar invites with links to malicious websites, such as fake cryptocurrency platforms. Once users click on these links, they are prompted to enter personal or financial information, leading to scams. Researchers have detected over 4,000 phishing emails in just four weeks. To protect against these threats, organizations should implement advanced email security, monitor third-party apps, and enforce multi-factor authentication. Individuals should be cautious with unexpected invites, verify links, and enable two-factor authentication. Google recommends using the "known senders" feature in Google Calendar to block phishing attempts from unfamiliar sources.

Attack Type : Phishing Attack

Cause of Issue : Exploited Trust

Industry Type : Software Development Companies

PUMAKIT : Advanced Linux Rootkit Employs Stealth to Avoid Detection

Cybersecurity researchers have discovered a new Linux rootkit called PUMAKIT, which uses advanced techniques to hide its presence and escalate privileges. It operates as a loadable kernel module (LKM) and employs a multi-stage architecture, including a dropper named "cron" and two memory-resident executables. PUMAKIT uses stealth mechanisms such as syscall hooking, hiding files and directories, and interacting with kernel functions like "prepare_creds" and "commit_creds" to alter system behavior. It activates only when specific conditions are met, such as secure boot checks or kernel symbol availability. The malware also employs unique privilege escalation methods. PUMAKIT's complexity signals an increase in sophisticated malware targeting Linux systems.

Attack Type : Kernel Rootkit

Cause of Issue : Stealth Techniques

Industry Type : Software Development Companies

Russian APT29 Leverages RDP Proxies for Credential and Data Theft

APT29, also known as "Midnight Blizzard" or "Earth Koshchei," is using 193 remote desktop protocol (RDP) proxy servers to conduct man-in-the-middle (MiTM) attacks, targeting government, military, IT, and telecommunications sectors in countries including the U.S., France, and Ukraine. The attackers exploit the PyRDP tool to intercept RDP sessions, steal credentials, data, and files, and execute malicious payloads. They gain access to victim systems by tricking users into connecting to rogue RDP servers via phishing emails. The attackers also use VPNs, TORs, and residential proxies to mask their activities. To defend against these attacks, users should avoid RDP connections from unknown sources and practice careful email security.

Attack Type : Man-in-the-middle

Cause of Issue : Phishing Emails

Industry Type : Telecommunications Sector

EagleMsgSpy : Chinese Surveillance Spyware Exploiting Mobile Devices Since 2017

Cybersecurity researchers have discovered EagleMsgSpy, a surveillance tool used by Chinese police to monitor mobile devices. Active since 2017, the Android tool collects extensive data, including chat messages, call logs, GPS location, screenshots, and audio recordings, without the user's knowledge. The software requires physical access to the target device for installation and communicates with a command-and-control server to exfiltrate data. It supports popular messaging apps like QQ, Telegram, and WhatsApp. The tool's developer, Wuhan Chinasoft Token Information Technology, has ties to Chinese law enforcement, with patents detailing data collection and analysis methods. Lookout researchers linked it to other China-based surveillance tools and noted its use by security bureaus for the surveillance of specific communities, like Tibetans and Uyghurs.

Attack Type : Surveillance Malware

Cause of Issue : Unauthorized Installation

Industry Type : Telecommunications Sector

New $3,000 Android Trojan Targets Banks and Crypto Exchanges

DroidBot, a newly discovered Android remote access trojan (RAT), targets 77 banking institutions, cryptocurrency exchanges, and national organizations. It combines hidden VNC and overlay attacks with spyware capabilities like keylogging and UI monitoring. Active since at least June 2024, DroidBot operates under a Malware-as-a-Service (MaaS) model, charging $3,000 monthly for access. It employs dual-channel communication, using HTTPS for inbound commands and MQTT for outbound data, offering flexibility and resilience. The malware, often disguised as security apps or banking software, primarily affects countries in Europe and Turkey. DroidBot uses Android's accessibility services to steal data and control devices remotely. While technically similar to other malware, its MaaS approach makes it stand out in the cybercrime landscape.

Attack Type : Remote Access

Cause of Issue : Malware Infection

Industry Type : Banking and Finance

Cybercriminals Exploit Fake Video Apps to Steal Data from Web3 Workers

Cybersecurity researchers have uncovered a scam campaign, codenamed Meeten, that uses fake video conferencing apps to deliver the Realst information stealer. The attackers pose as legitimate companies, contacting targets via Telegram to set up fake meetings. Victims are prompted to download malicious software, which steals sensitive data like cryptocurrency wallets, Telegram credentials, banking info, iCloud Keychain data, and browser cookies. The malware targets both macOS and Windows users. On macOS, it exploits system permissions, while the Windows version uses a signed installer. This attack follows similar campaigns, including one earlier this year involving counterfeit meeting apps. The use of AI by attackers to create realistic websites adds to the difficulty in detecting these scams.

Attack Type : Information Stealer

Cause of Issue : Fake Applications

Industry Type : Banking & Finance Sector

Turla APT Group Uses Pakistani Hackers' Infrastructure to Attack Afghan and Indian Targets

The Russia-linked APT group Turla has been linked to a campaign infiltrating the command-and-control (C2) servers of Pakistan-based Storm-0156 since 2022. By gaining access to Storm-0156 infrastructure, Turla deployed custom malware, including TwoDash and Statuezy, targeting Afghan government networks. This tactic mirrors previous incidents where Turla repurposed other threat actors' infrastructure, such as exploiting Iranian and Ukrainian attackers' tools. Turla's operations have expanded, including using Storm-0156's backdoors like Crimson RAT and Wainscot to further its goals. This strategy allows Turla to gather intelligence on targets of interest in South Asia with minimal effort while avoiding direct attacks, though the information gathered may not fully align with their priorities.

Attack Type : Cyber Espionage

Cause of Issue : Infrastructure Compromise

Industry Type : Government and Military

Top 5 Most Affected Industries in 2024

Healthcare :

Healthcare organizations faced a significant volume of cyberattacks due to the sensitive nature of patient data and the increasing reliance on interconnected medical devices, making them highly attractive targets for cybercriminals seeking to exploit vulnerabilities.

Finance :

The financial sector continued to be a prime target for cybercriminals driven by the high value of financial information and the constant innovation within the financial technology (FinTech) landscape, creating new opportunities for cyberattacks.

Government :

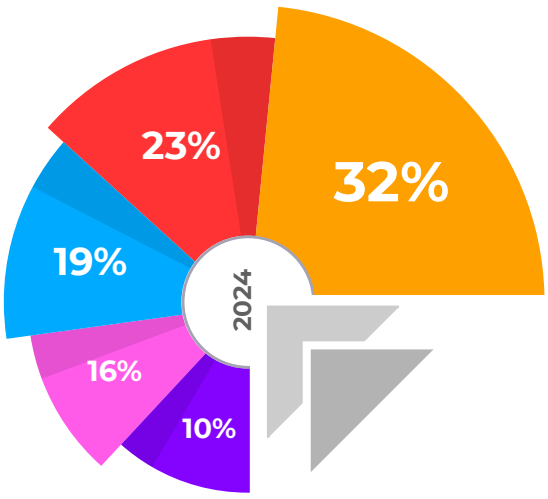
Government agencies faced persistent and sophisticated threats from nation-state actors and cybercriminal groups due to their critical role in national security and the vast amount of sensitive data they handle, making them high-value targets for espionage and disruption.

Retail :

The retail sector experienced a surge in cyberattacks driven by the increasing volume of online transactions and the growing reliance on e-commerce platforms, making customer data a highly valuable commodity for cybercriminals

Manufacturing :

The increasing digitization of manufacturing processes, including the widespread adoption of Industrial Control Systems (ICS), made this sector increasingly vulnerable to cyberattacks with potentially devastating consequences, such as production disruptions, safety hazards, and even physical damage.



- Healthcare : 32%
- Financial Services : 23%
- Government : 19%
- Retail : 16%
- Manufacturing : 10%

Top 5 Vulnerabilities of 2024

Ransomware :

Ransomware attacks remained a significant threat, with attackers employing more sophisticated techniques, such as double extortion (data theft and encryption), and demanding higher ransoms, making them increasingly disruptive and costly for organizations.

Phishing :

Social engineering attacks, particularly phishing emails and messages, continued to be a prevalent threat, with attackers utilizing AI-powered techniques to create highly convincing and personalized attacks, making them more difficult to detect and avoid.

Supply Chain Attacks :

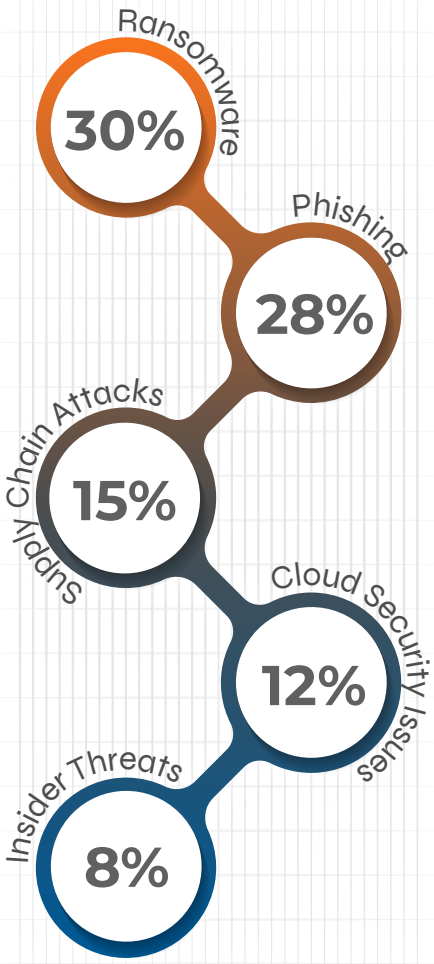
Cybercriminals exploited vulnerabilities in third-party vendors and software supply chains due to the increasing interconnectedness of modern business ecosystems, enabling them to gain access to target organizations indirectly.

Cloud Security Issues :

As cloud adoption surged, so did the number of cloud-related security incidents, driven by challenges such as misconfigurations, inadequate access controls, and insufficient data protection within cloud environments.

Insider Threats :

Malicious or unintentional actions by employees or contractors remained a significant risk, driven by factors such as human error, lack of awareness, and social engineering tactics targeting employees.



Top 5 Affected Regions of 2024

North America :

As a major economic and technological hub, North America experienced a high volume of cyberattacks due to the presence of numerous multinational corporations, critical infrastructure, and a high concentration of valuable data.

Europe :

Europe faced significant cyber threats, including those from nation-state actors and well-organized cybercriminal groups, driven by its political and economic influence on the global stage.

Asia :

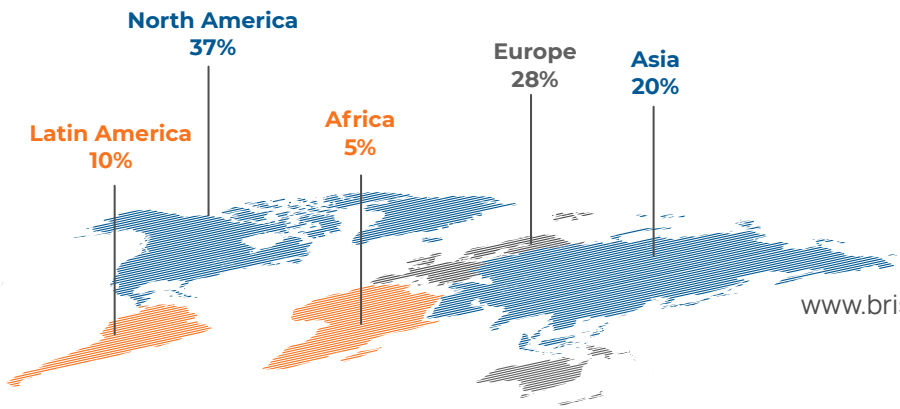
Rapid digitalization and economic growth across Asia made this region increasingly vulnerable to cyberattacks, driven by the rapid adoption of technology across various sectors and the increasing reliance on interconnected systems.

Latin America :

Organizations in Latin America faced challenges in combating cyber threats due to limited resources, evolving threat landscapes, and a lack of cybersecurity awareness and training.

Africa :

While less frequently reported, cyber threats were on the rise in Africa, driven by increasing internet penetration and digitalization, coupled with limited cybersecurity resources and infrastructure.



www.briskinfosec.com

Briskinfosec Technology and Consulting Pvt Ltd,
No : 21, 2nd Floor, Krishnama Road,
Nungambakkam, Chennai - 600034, India.

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