Nov – 2024 Edition – 75

Threatsploit

Adversary Report

BRISKINFOSEC
CYBER TRUST & ASSURANCE

www.briskinfosec.com

Introduction

Dear Readers,

Welcome to the November edition of the Threatsploit Adversary Report, your essential monthly resource for understanding the ever-evolving landscape of cyber threats worldwide. Each issue of Threatsploit is dedicated to providing security professionals, organizations, and enthusiasts with the latest insights into emerging threats, major incidents, and vulnerabilities impacting diverse sectors.

A recently discovered zero-day vulnerability in Mozilla Firefox allows attackers to execute remote code on unpatched computers, underscoring the critical need for timely patch management and strong security practices to safeguard essential software.

Ransomware attacks continue to affect businesses, with a notable incident involving Casio last month that compromised sensitive customer data. This highlights ransomware gangs' growing focus on large corporations, emphasizing the importance of robust defenses.

The financial sector faces escalating risks, with breaches impacting major investment organizations and exposing vast amounts of personal and financial information. These incidents stress the importance of rigorous data security measures to protect customer information and uphold organizational trust.

Designed as a comprehensive yet actionable guide, the Threatsploit Adversary Report is more than just a collection of incidents; it serves as a single, authoritative source of intelligence that empowers readers to navigate complex threat landscapes. In a digital world where the stakes are constantly rising, our mission is to streamline access to critical security intelligence, helping you strengthen your defenses and create a secure environment for your organization.

Stay informed, stay vigilant, and leverage these insights to bolster your organization's cybersecurity posture against current and emerging threats, ensuring preparedness for whatever challenges lie ahead.

Best Regards,

Briskinfosec Threat Intelligence Team

Contents

Immediate Action Needed Firefox Zero-Day Vulnerability Exposes Users

A critical security vulnerability in Firefox and Firefox Extended Support Release (ESR), tracked as CVE-2024-9680, with a CVSS score of 9.8, has been announced by Mozilla. A use-after-free bug in the Animation Timeline component, which allows remote code execution, is currently being exploited in active attacks in the wild. The flaw was discovered by ESET researcher Damien Schaeffer. Firefox versions 131.0.2, 128.3.1 ESR, and 115.16.1 ESR have been updated to address the vulnerability. Users are urged to update their browsers to the latest versions to mitigate potential attacks, including watering holes or drive-by download methods. An emergency update for Tor Browser (version 13.5.7) has also been released by the Tor Project to address the same issue. Mozilla responded swiftly, resolving the problem within 25 hours of responsible disclosure.

Attack Type : Remote code execution | Cause of Issue : Use-after-free bug | Industry : Software Development Companies

National Public Data Declares Bankruptcy Following Major Data Breach Impacting Millions

A major data breach exposed the personal information of approximately 300 million individuals, including 270 million Social Security numbers. National Public Data, a data broker for Jerico Pictures, filed for Chapter 11 bankruptcy. The breach, which occurred in April, involved names, dates of birth, addresses, phone numbers, and additional sensitive information. Numerous lawsuits, regulatory challenges from the FTC and more than 20 states, and demands for credit monitoring have been faced. Jerico Pictures has indicated that its debts cannot be repaid. Coverage was declined by the company's insurance provider following the breach, leaving it with less than $75,000. Although significant revenue was generated in 2022 and 2023, most of it had been spent on bulk data purchases and payments to its owner, Salvatore Verini.

Attack Type : Data theft | Cause of Issue : Inadequate Security | Industry : Banking and Finance

Casio Suffers Ransomware Attack, Exposing Customer Data

Casio confirmed a ransomware attack earlier this month, resulting in the theft of sensitive data, including information on employees, contractors, business partners, and interviewees, as well as some technical and company data. Although credit card details remain secure, there may have been access to customer data as well. The ransomware group Underground claimed that the attack resulted in over 200 GB of stolen data. Storm-0978 (RomCom), a cybercriminal group associated with Russia, links Underground. Casio is still assessing the extent of the damage, with some systems remaining unusable, and has not disclosed if a ransom was demanded.

Attack Type : Ransomware Attack | Cause of Issue : Data Breach | Industry : Media and Entertainment

Personal Data of 77,000 Fidelity Customers Exposed in Recent Breach

A data breach at Fidelity Investments compromised personal information, including Social Security numbers and driver's licenses, impacting over 77,000 customers. The breach occurred between August 17 and 19, when a third party accessed data through two newly created customer accounts. Fidelity detected the unauthorized activity on August 19 and took immediate action to terminate access. The firm emphasized that there was no access to customer accounts or funds. The attorneys general of Maine, Massachusetts, and New Hampshire have reported the breach, but they did not disclose further details about how the accounts allowed access to such a large amount of data.

Attack Type : Account compromise | Cause of Issue : Fraudulent access | Industry : Banking and Finance

Internet Archive Hit by Third Cyberattack, API Token Mismanagement Exploited

The Internet Archive suffered its third major cyberattack in October 2024, with hackers exploiting unrotated API tokens to access the organization's Zendesk support platform, potentially compromising user data, including personal identification documents. This follows two earlier breaches: an October 9 hack using an exposed GitLab token that affected 31 million users and a subsequent DDoS attack. Despite the Internet Archive's efforts to improve security, the repeated incidents have raised concerns about its ability to protect its data. Users are advised to monitor their accounts for suspicious activity.

Attack Type : API exploitation | Cause of Issue : Unrotated tokens | Industry : Media and Entertainment

Over 115,000 Texans Personal Data Exposed in DPS Security Breach

The Texas Department of Public Safety (DPS) reported a significant data breach involving the personal information of 115,071 Texans. The exposed data includes names, addresses, Social Security numbers, driver's license numbers, and government-issued ID numbers. Despite the breach, DPS has yet to notify the affected individuals. The Texas Office of the Attorney General disclosed this information, but further details from DPS are still pending. This incident follows a similar case in December 2022, where DPS mistakenly sent at least 3,000 replacement driver's licenses to a Chinese organized crime group. The group used stolen information to target Asian Texans, creating fraudulent Texas.gov accounts.

Attack Type : Data breach | Cause of Issue : Security lapse | Industry : Government Sector

Astaroth Banking Malware Makes a Comeback in Brazil with Spear-Phishing Tactics

A spear-phishing campaign in Brazil is distributing the Astaroth banking malware (Guildma) through obfuscated JavaScript, affecting industries such as manufacturing, retail, and government agencies. Malicious emails are being used to impersonate official tax documents, exploiting the urgency of personal income tax filings to trick users into downloading ZIP archives that contain harmful Windows shortcuts. These shortcuts utilize mshta.exe to execute obfuscated commands and connect to a command-and-control server. Despite being an older banking trojan, the resurgence of Astaroth presents significant threats, including long-term damage to consumer trust, regulatory fines, and increased operational costs due to business disruptions and recovery efforts. To mitigate these risks, strong password policies should be enforced, multi-factor authentication (MFA) should be used, software should be kept updated, and the principle of least privilege (PoLP) should be applied.

Attack Type : Spear-phishing attack | Cause of Issue : Obfuscated JavaScript | Industry : Software Development Companies

Hackers Compromise MoneyGram, Exposing Customer Data and Transaction Details

A cyberattack was confirmed by MoneyGram on September 20, resulting in the theft of customers' personal information and transaction data. A week-long outage of the company's website and app was caused by the unauthorized access. Names, contact information, dates of birth, national IDs, and a limited number of Social Security numbers were included in the stolen data. Additionally, transaction details and, for some consumers, information related to criminal investigations were compromised. An investigation into the breach is currently being conducted by MoneyGram, and U.K. data protection regulators have been notified as required by law.

Attack Type : Data breach | Cause of Issue : Cyberattack compromise | Industry : Banking and Finance

Customer Data Compromised in Ransomware Incident Involving Debt Collection Agency, Says Comcast

A ransomware attack on Financial Business and Consumer Solutions (FBCS), a debt collection agency used by Comcast until 2020, resulted in the personal data of over 237,000 customers being compromised. Initially, it was reported by FBCS to Comcast in March that no customer data was affected; however, it was later admitted in July that customer information, including names, addresses, Social Security numbers, dates of birth, and Comcast account details, had been accessed during the attack that occurred between February 14 and February 26, 2024. More than 4 million individuals had their personal information accessed, as confirmed by FBCS. Affected parties included CF Medical, which reported that over 620,000 individuals' health and personal information had been stolen, and Truist Bank, which stated that customer names, addresses, account numbers, and Social Security numbers were compromised. The incident remains unclaimed by any major ransomware group.

Attack Type : Ransomware attack | Cause of Issue : Data breach | Industry : Finance and Banking

CISA Warns of Active Exploits Targeting Ivanti Security Flaw

A remote code execution vulnerability (CVE-2024-29824) in Ivanti Endpoint Manager (EPM) has been alerted by CISA, as it is being actively exploited by hackers. This flaw, which was first disclosed by Trend Micro's Zero Day Initiative in April and patched by Ivanti in May, allows malicious code to be executed on unpatched servers by unauthenticated attackers. It has been mandated by CISA that all federal agencies update vulnerable systems by October 23 to mitigate risks. Ivanti, which is served by over 40,000 corporate clients, confirmed that a limited number of customers were targeted, although specifics about any data breaches were not disclosed. This alert follows previous incidents in which vulnerabilities in Ivanti's Connect Secure VPN solution were exploited by hackers.

Attack Type : Remote Code Execution | Cause of Issue : Unpatched Vulnerability | Industry : Government Sector

Ransomware Actors Capitalize on LockBit's Infamy to Intimidate Victims

Recent research by Trend Micro highlights the emergence of new ransomware that is exploited for data exfiltration using Amazon S3 Transfer Acceleration, with its identity disguised as the notorious LockBit variant. The malware, developed in Golang, has hard-coded AWS credentials embedded and is capable of targeting both Windows and macOS. Files are encrypted and renamed while being exfiltrated to the cloud before a LockBit-themed ransom note is displayed. Meanwhile, significant activity from the Mallox variant is observed, which has a known cryptographic flaw allowing some victims' files to be decrypted. The Akira ransomware is actively targeting sectors like manufacturing, benefiting from a decline in LockBit's activity and utilizing various vulnerabilities for infiltration. Overall, ransomware attacks are considered a critical threat, although some metrics indicate a slight decrease in overall incidents.

Attack Type : Ransomware attack | Cause of Issue :Cloud exploitation | Industry : Software Development Companies

Phishing Campaigns Leverage Gophish Framework to Distribute Remote Access Trojans

A new phishing campaign targeting Russian-speaking users is being employed with the Gophish toolkit to deliver two remote access Trojans (RATs): DarkCrystal RAT (DCRat) and a newly identified variant called PowerRAT. Malicious documents and HTML files that require user interaction to initiate infection are utilized in this campaign. Phishing emails that imitate services like Yandex Disk and VK are sent, with the infection being initiated when macros are enabled in a malicious Word document by victims. A PowerShell loader and rogue HTML application are involved in the subsequent malware execution, while DCRat is designed for data theft and remote control. The use of evolving phishing tactics, including virtual hard disk files to evade detection, is illustrated by this campaign.

Attack Type : Phishing Campaign | Cause of Issue : Targeted phishing

Industry : Information technology

Vulnerability in Styra's OPA Leaks NTLM Hashes to Remote Threats

A recently patched security flaw in Styra's Open Policy Agent (OPA), tracked as CVE-2024-8260, could have allowed the leakage of NTLM hashes from local user accounts. This medium-severity vulnerability, with a CVSS score of 6.1/7.3, was caused by improper input validation, which enabled unauthorized access when a Universal Naming Convention (UNC) path was improperly used as an argument. For exploitation, an initial foothold would be required, along with the ability to initiate SMB traffic over port 445. The flaw was addressed in version 0.68.0 on August 29, 2024. Additionally, another NTLM-related privilege escalation vulnerability in Microsoft's Remote Registry Service was highlighted by Akamai, emphasizing ongoing concerns regarding NTLM's susceptibility to relay attacks. It is planned by Microsoft to retire NTLM in favor of Kerberos for improved security.

Attack Type : Credential leakage | Cause of Issue : Input validation | Industry : Information technology

Globe Life Faces Extortion After Customer Data Theft

Globe Life, a major insurance provider, has been reported as being extorted by hackers who stole sensitive customer data from its subsidiary, American Income Life Insurance Company. The breach involves personally identifiable information, including names, addresses, and, in some cases, Social Security numbers. While about 5,000 individuals are confirmed as affected, it is believed that the total number could be much higher given the company's large policyholder base. The attack is characterized as extortion-focused, not involving ransomware, and some information has been leaked to short sellers and plaintiffs' attorneys. Federal law enforcement has been notified about the incident by Globe Life.

Attack Type : Data extortion | Cause of Issue : Data breach | Industry : Banking and Finance

Cybercriminals Target Docker API Servers for Illicit SRBMiner Crypto Mining

Exploited by bad actors, exposed Docker remote API servers are being targeted for the deployment of the SRBMiner crypto miner for illicit XRP mining, with the gRPC protocol over h2c being utilized to evade security measures. The attack is initiated through the discovery of public-facing Docker APIs and the checking of HTTP/2 upgrades, followed by the sending of gRPC requests to manage Docker functionalities. Additionally, the same method is employed by attackers to deploy the perfctl malware via a Base64-encoded payload. It is recommended by researchers that strong access controls be implemented to secure Docker APIs, that unusual activities be monitored, and that container security best practices be followed.

Attack Type : API exploitation | Cause of Issue : Exposed interfaces

Industry : Software Development Companies

Attackers Target Roundcube Webmail XSS Flaw to Capture User Credentials

Unknown threat actors are exploiting a now-patched vulnerability (CVE-2024-37383) in the Roundcube webmail software to launch phishing attacks aimed at stealing user credentials. The flaw, a cross-site scripting (XSS) vulnerability, allows attackers to execute JavaScript by tricking victims into opening malicious emails. Discovered by Positive Technologies, the attack targeted a governmental organization in a CIS country, exfiltrating credentials to a remote server. The vulnerability was patched in Roundcube versions 1.5.7 and 1.6.7. While not widely used, Roundcube remains a target due to its prevalence in government agencies.

Attack Type : Phishing Campaign | Cause of Issue : XSS Vulnerability | Industry : Government

Malware Disguised as Google Meet Pages Targets Users in ClickFix Campaign

Threat actors are exploiting fake Google Meet web pages in a malware campaign called ClickFix, targeting Windows and macOS systems. They use deceptive error messages to trick users into executing malicious PowerShell code, resulting in the installation of infostealers like StealC, Rhadamanthys, and Atomic. The campaign has been linked to groups such as Slavic Nation Empire and Scamquerteo, suggesting shared resources. Additionally, it targets WordPress sites using malicious plugins, leading to significant infections. The rise of open-source infostealers poses new challenges for cybersecurity professionals. More than 6,000 WordPress sites have reportedly been compromised through these tactics.

Attack Type : ClickFix Campaign | Cause of Issue : User Deception | Industry : Information Technology

Exploited npm Packages Threaten Ethereum Wallet Security with SSH Access

Several malicious packages have been identified by cybersecurity researchers on the npm registry that are designed to harvest Ethereum private keys and gain remote access to victims' machines via SSH. The packages, which are intended to impersonate the legitimate ethers library, include names such as ethers-mew and ethers-web3, and are believed to have been released by accounts for testing purposes. Unlike previous threats that were triggered upon installation, active use in code is required for these packages to execute their malicious actions. The ethers-mew package is capable of modifying the root user's SSH configuration to allow attackers to have persistent access. After being discovered, these packages were quickly removed by their authors.

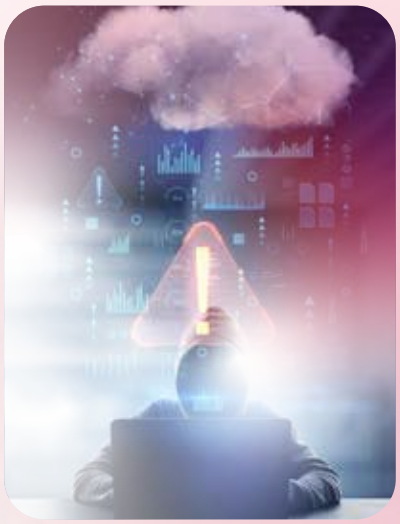
Attack Type : Supply chain | Cause of Issue : Malicious packages | Industry : Software Development Companies

Cisco Releases Critical Update for ASA and FTD Software Vulnerability Amid Ongoing Attacks

Updates have been released by Cisco to address a security flaw, tracked as CVE-2024-20481, in its Adaptive Security Appliance (ASA) that affects the Remote Access VPN (RAVPN) service. The vulnerability, which has been assigned a CVSS score of 5.8, can be exploited by unauthenticated attackers to trigger a denial-of-service (DoS) condition by overwhelming the service with VPN authentication requests. Although no direct workarounds are available, it is recommended by Cisco that logging be enabled, threat detection be configured, and unauthorized connection attempts be blocked. The flaw has been exploited in a larger brute-force campaign targeting various VPN and SSH services.

Attack Type : Denial-of-Service | Cause of Issue : Resource exhaustion | Industry : Software Development Companies

CISA Alerts on Ongoing Exploitation of Microsoft SharePoint Flaw



CISA has added the CVE-2024-38094 vulnerability, a deserialization flaw in Microsoft SharePoint, to its Known Exploited Vulnerabilities Catalog due to active exploitation. Rated "Important" with a CVSS score of 7.2, this vulnerability allows unauthorized remote code execution by exploiting untrusted data. Organizations, especially federal agencies under BOD 22-01, are urged to address this and similar vulnerabilities promptly to enhance cybersecurity resilience and protect sensitive information. CISA emphasizes the importance of timely remediation to reduce exposure to cyberattacks.

Attack Type : Remote Code Execution | Cause of Issue : Untrusted Deserialization | Industry : Software Development Companies

Advanced Qilin.B Ransomware Variant Introduced with Enhanced Encryption and Stealth Tactics

An advanced version of the Qilin ransomware, referred to as Qilin.B, has been discovered by cybersecurity researchers at Halcyon. AES-256-CTR encryption is supported for systems with AESNI capabilities, while Chacha20 is retained for those without. RSA-4096 with OAEP padding is used to secure encryption keys. The ransomware, noted initially in mid-2022, has evolved from Golang to Rust. A ransomware-as-a-service scheme has been established, allowing affiliates to receive 80% to 85% of ransom payments. Credential theft from Google Chrome has been included in recent attacks, indicating a shift from typical double extortion tactics. Enhanced encryption methods, evasion techniques, and disruption of backup systems are employed by Qilin.B, marking it as a significant threat. Similar advancements have been noted in the new Embargo ransomware, which utilizes the MDeployer loader and MS4Killer EDR-killing tool, both written in Rust. Ransomware attacks have impacted 389 U.S. healthcare institutions this fiscal year, with substantial financial losses reported.

Attack Type : Ransomware attack | Cause of Issue : Evasion tactics | Industry : Finance and Banking

AWS CDK Flaw Poses Serious Risk of Account Takeover for Users

A significant vulnerability in the AWS Cloud Development Kit (CDK) was uncovered by cybersecurity researchers, which could lead to account takeover due to predictable naming conventions for S3 buckets and IAM roles created during bootstrapping. Bucket names that many users default to can be easily guessed by attackers, potentially allowing unused buckets to be claimed and CloudFormation templates to be manipulated for executing malicious actions within the victim's AWS account. The issue was addressed by AWS in CDK version 2.149.0, and users were urged to customize bucket names and update to the latest version. The necessity of keeping AWS account IDs private and using unique identifiers for resources was underscored by this incident. Additionally, a separate report from Symantec highlighted security risks posed by mobile apps that hard-coded cloud service credentials, further exposing user data.

Attack Type : S3 Bucket Sniping | Cause of Issue : Insecure Defaults | Industry : Software Development Companies

New Variants of Grandoreiro Banking Malware Introduce Enhanced Evasion Techniques

New variants of the Grandoreiro banking malware are being reported, having been adapted to bypass anti-fraud measures despite recent actions taken by law enforcement. It has been revealed by Kaspersky's analysis that tactics such as domain generation algorithms, ciphertext stealing, and mouse tracking are now being employed, particularly targeting banking customers in Mexico. Since its emergence in 2016, credentials have been stolen from 1,700 financial institutions across 45 countries by Grandoreiro, which is operated on a malware-as-a-service model. Following the arrests of some gang members, the malware has fragmented into two codebases, with updated samples being detected that utilize larger file sizes to evade detection. Key features, including user activity monitoring, evasion of security software, and rerouting of cryptocurrency transactions, have been noted. The ongoing evolution of Grandoreiro is highlighting the sophistication of cyber threats, especially in the LATAM region, where users are also being targeted by other banking trojans like Mispadu and Silver Oryx Blade.

Attack Type : Banking Malware | Cause of Issue : Evolving tactics | Industry : Finance and Banking

LinkedIn Fined €310 Million by Irish Regulator for GDPR Breaches

LinkedIn was fined €310 million by Ireland's Data Protection Commission (DPC) for violating GDPR by using behavioral analysis of user data for targeted ads without adequate consent. The investigation, triggered by a complaint in 2018, found LinkedIn breached transparency and fairness requirements under GDPR. Specifically, LinkedIn did not obtain clear user consent or provide enough information before processing members' data, using "legitimate interests" as a legal basis. LinkedIn now has three months to comply with GDPR requirements. Meanwhile, Austrian privacy group noyb has filed a similar complaint against Pinterest for default tracking without user consent.

Penalty : Data Privacy Violation | Cause of Issue : Inadequate consent | Industry : Software Development Companies

Microsoft Uncovers macOS Flaw Allowing Unauthorized Access to Safari Privacy Settings

Microsoft has revealed a security flaw, "HM Surf" (CVE-2024-44133), in Apple's macOS Transparency, Consent, and Control (TCC) framework, which allows attackers to bypass user privacy settings and access sensitive data. The flaw specifically affects Apple's Safari browser, allowing unauthorized access to data such as browsed pages, camera, microphone, and location by modifying configuration files. Although the vulnerability was patched in macOS Sequoia 15, Microsoft noted potential exploitation by known macOS adware, AdLoad. Microsoft is also collaborating with other browser vendors to enhance protections.

Attack Type : Privacy Bypass | Cause of Issue : TCC Misconfiguration | Industry : Software Development Companies

Fortinet Issues Alert on Serious FortiManager Flaw Facing Ongoing Attacks

A critical vulnerability (CVE-2024-47575) in FortiManager has been disclosed by Fortinet, rated 9.8 on the CVSS scale, which allows arbitrary code to be executed by remote unauthenticated attackers via specially crafted requests. Multiple FortiManager versions and certain older FortiAnalyzer models with specific configurations are affected by this flaw. Active exploitation has been reported by the threat group UNC5820, with configuration data being exfiltrated from compromised devices. Over 4,000 exposed FortiManager admin portals have been identified, primarily in the U.S. Immediate patching is recommended by Fortinet, and workarounds have been provided for various versions. This vulnerability has been added to the U.S. CISA's Known Exploited Vulnerabilities catalog, with a mandate for federal agencies to address it by November 13, 2024. Significant risks posed by this vulnerability to enterprise security are highlighted by experts.

Attack Type : Remote Code Execution | Cause of Issue : Missing Authentication | Industry : Software Development Companies

Cybercriminals Exploit EDRSilencer Tool to Evade Detection and Conceal Malicious Actions

Threat actors are leveraging the open-source EDRSilencer tool to evade detection by endpoint detection and response (EDR) solutions. Detected by Trend Micro, EDRSilencer blocks outbound traffic from various EDR processes, making it difficult for security software to send telemetry. The tool utilizes the Windows Filtering Platform (WFP) to dynamically identify and inhibit running EDR processes, allowing malware to operate undetected. This trend aligns with the increasing use of EDR-bypassing tools among ransomware groups, highlighting the ongoing challenge of disabling security measures for successful attacks.

Attack Type : Detection Evasion | Cause of Issue : EDR Tampering | Industry : Software Development Companies

VMware Releases vCenter Server Patch to Mitigate Critical RCE Security Flaw

Updates have been released by VMware to address a critical security flaw in the vCenter Server, tracked as CVE-2024-38812, which could lead to remote code execution due to a heap overflow vulnerability in the DCE/RPC protocol. The flaw was initially patched on September 17, 2024, but further updates were required for versions 8.0 U3d, 8.0 U2e, and 7.0 U3t, as well as VMware Cloud Foundation versions 5.x, 5.1.x, and 4.x. Although no evidence of exploitation has been found, users are urged to update to mitigate potential threats. The vulnerability was reported by researchers at a cybersecurity competition in China.

Attack Type : Remote Code | Cause of Issue : Heap Overflow | Industry : Software Development Companies

TrickMo Trojan Enhances Capabilities to Steal Android PINs and Unlock Patterns

New variants of the Android banking trojan TrickMo have been discovered, featuring undocumented capabilities to steal a device's unlock pattern or PIN. This malware, first identified in 2019 and linked to the TrickBot cybercrime group, can remotely control infected devices, steal SMS-based OTPs, and capture credentials through deceptive overlay screens. Recent updates include improved evasion techniques and permission-granting methods for unauthorized transactions. TrickMo uses a fake UI to mimic the device's unlock screen, capturing user inputs and sending them to an attacker-controlled server. The threat poses significant risks to both personal and corporate data, with a 29% increase in mobile banking malware attacks reported from June 2023 to April 2024, especially targeting India.

Attack Type : Banking Trojan | Cause of Issue : Malicious UI | Industry : Information Technology

SideWinder APT Launches Covert Multi-Stage Assault on Middle Eastern and African Targets

An advanced persistent threat (APT) group known as SideWinder, suspected to have ties to India, has launched attacks against high-profile targets in the Middle East and Africa. This group employs a multi-stage infection process using spear-phishing emails to deliver a new toolkit called StealerBot, which facilitates espionage activities. Targets include government, military, and infrastructure sectors across multiple countries. Despite appearing low-skilled, their operations reveal significant capabilities. Additionally, another group, Transparent Tribe (APT36), is also increasing its activities, particularly against Linux systems used in Indian government sectors.

Attack Type : Spear-phishing | Cause of Issue : Vulnerabilities in Software/Social Engineering | Industry : Government and Military

Delta Takes Legal Action Against CrowdStrike Following Widespread Flight Disruptions

Delta Air Lines has sued cybersecurity firm CrowdStrike in Georgia state court following a major global outage in July that led to 7,000 flight cancellations and affected 1.3 million customers. Delta claims the incident, caused by a faulty software update from CrowdStrike, resulted in over $500 million in losses. CrowdStrike has responded, stating that Delta's claims are unfounded and reflect a misunderstanding of cybersecurity. The incident prompted an investigation by the U.S. Transportation Department, and a CrowdStrike executive previously apologized for the software failure.

Attack Type : Operational disruption | Cause of Issue : Faulty software update | Industry : Aviation

FBI and CISA Probe Chinese-Linked Telecom Breaches Targeting Trump and Harris Devices

U.S. agencies, including the FBI and CISA, are investigating alleged breaches by Chinese hackers targeting telecommunications companies, which compromised devices linked to Vice President Kamala Harris' campaign, former President Donald Trump, and vice presidential candidate JD Vance. The group, known as Salt Typhoon, accessed systems at major carriers like AT&T and Verizon, raising concerns about the potential extent of the data breaches. This investigation highlights ongoing cybersecurity threats to political figures amid increasing disinformation campaigns, including recent Russian efforts to undermine election integrity.

Attack Type : Data breach | Cause of Issue : Unauthorized access | Industry : Telecommunication

Change Healthcare Ransomware Attack Exposes Data of Over 100 Million Americans

In February, a ransomware attack on Change Healthcare resulted in the theft of private health information from over 100 million individuals, marking one of the largest data breaches in U.S. history. The attack, attributed to the Russian-speaking gang ALPHV/BlackCat, caused significant disruptions across the healthcare sector. UnitedHealth Group (UHG), which owns Change Healthcare, is still notifying affected individuals as investigations continue. The breach exposed sensitive personal and health information, including Social Security numbers and medical records, due to inadequate cybersecurity measures, specifically the lack of multi-factor authentication. Lawmakers are now scrutinizing UHG's handling of data security, especially given its substantial profits and extensive data collection practices.

Attack Type : Ransomware Attack | Cause of Issue : Credential Theft | Industry : Healthcare Industry

Top 5 Ransomware Families

Ransomhub

Ransomhub is a notorious ransomware-as-a-service (RaaS) platform that provides affiliates with tools to encrypt data and demand ransoms. It leverages advanced techniques to avoid detection, making it particularly challenging for organizations to defend against.

Play

Known for its custom encryption methods, Play ransomware is relatively new but has rapidly risen in notoriety. It avoids traditional extensions and uses unique markers in encrypted files, making detection and recovery difficult.

Lockbit 3.0

An evolution of previous Lockbit versions, Lockbit 3.0 is known for its double-extortion tactics, where sensitive data is stolen and encrypted, forcing victims to pay for both the return of data and confidentiality.

Meow

Originally targeting poorly secured databases, Meow ransomware has developed techniques to infiltrate systems via unsecured or misconfigured cloud storage. Its simplicity in targeting and fast-spreading capabilities make it a serious threat.

Hunters

The Hunters ransomware family has gained infamy for its highly targeted attacks on large organizations. Known for thorough network infiltration, Hunters often bypass traditional security measures to cause maximum disruption.

Top 5 targeted countries by Ransomware

Top 5 Targeted Industries by Ransomware

Thanks for Reading

Stay Secure ! Stay Vigilant !

Briskinfosec Technology and Consulting Pvt Ltd,
No : 21 , 2nd Floor, Krishnama Road,
Nungambakkam, Chennai - 600034, India.
Office : +91 44 4352 4537 | Mobile : +91 86086 34123
contact@briskinfosec.com | www.briskinfosec.com