Sep - 2024

Threatsploit Adversary Report

Edition-73

www.briskinfosec.com

Introduction :

Dear Readers,

Thank you for the huge response to our Threatsploit initiative as we step into our 7th year with the 73rd special edition this month.

Our latest report highlights some significant cybersecurity incidents and vulnerabilities that have come to light recently. One of the notable threats is the "Sitting Ducks" attack, where over a million domains have been found vulnerable to DNS hijacking due to configuration flaws. This attack underscores the importance of regular security audits and configuration checks to prevent malicious actors from exploiting such vulnerabilities.

We also cover a widespread ransomware attack that has hit hundreds of small Indian banks through C-Edge Technologies, affecting their operational capabilities and customer data security. This incident serves as a stark reminder of the increasing sophistication of ransomware attacks and the need for robust data protection measures.

In addition, the report explores a new wave of fraudulent websites using deceptive Facebook ads to scam credit card users. This phishing and fraud attack illustrate the ongoing threat posed by malicious actors who use social engineering tactics to exploit unsuspecting individuals.

Our analysis of security gaps in Windows Smart App Control reveals how design flaws can be exploited to bypass reputation-based security measures. Similarly, vulnerabilities in Roundcube Webmail highlight the dangers of inadequate input validation in email services, potentially leading to cross-site scripting attacks.

As always, the Threatsploit Adversary Report aims to provide you with timely and actionable intelligence to help you understand and mitigate these threats. By staying informed and proactive, we can better defend against the ever-evolving cyber landscape.

Stay safe and vigilant.

Best regards,
Briskinfosec Threat Intelligence Team.

- Top Cyberattacks in the Last 30 Days According to Industry
- Top 5 - Cybersecurity Podcasts to Listen
- We are exhibiting - GITEX Global 2024

Contents :

Over 1 Million Domains Vulnerable to 'Sitting Ducks' Hijacking Method

Cybercriminals use the "Sitting Ducks" attack to hijack domains by taking advantage of weaknesses in the domain name system (DNS). This attack targets domains that are poorly configured or have inadequate ownership verification. Cybercriminals can take over these domains by exploiting these DNS vulnerabilities without accessing the original owner's account. Once hijacked, cybercriminals can use the domains for malicious activities like malware distribution or spam campaigns. Since 2018, this attack has affected over 35,000 domains and is still relatively unknown compared to other hijacking methods. Organizations are advised to check their domains for vulnerabilities and use DNS providers with protections against such attacks.

Attack Type : DNS Hijacking

Cause of Issue : Configuration Flaws

Industry Type : Software Development Companies

Fake Websites Using Facebook Ads to Scam Credit Card Information

A sophisticated e-commerce scam network named ERIAKOS has been targeting mobile Facebook users with fraudulent websites that steal personal and financial data through brand impersonation and deceptive ads. The scam, detected by Recorded Future, involved 608 fake sites and primarily used ad lures and fake user comments to attract victims. The network, associated with China, poses as well-known brands and promotes fraudulent sales. This incident follows other recent scams, including a large network of fake stores called BogusBazaar and a traffic direction system (R0bl0ch0n TDS) promoting affiliate marketing scams. Additionally, researchers have discovered fake Google ads that redirect users to malicious sites that deliver malware, underscoring the ongoing threat of malvertising.

Attack Type : Fraudulent Websites

Cause of Issue : Malicious Actors

Industry Type : Software Development Companies

Ransomware Hits Hundreds of Small Indian Banks, Causing Widespread Outages

A ransomware attack on C-Edge Technologies has forced payment systems across nearly 300 small Indian local banks to temporarily shut down. The National Payment Corporation of India (NPCI) has temporarily blocked C-Edge Technologies' access to its retail payments system. The attack affects about 0.5% of the country's payment system volumes and affects around 1,500 cooperative and regional banks. In recent weeks, the RBI and Indian cyber authorities have warned Indian banks about potential cyberattacks.

Attack Type : Ransomware Attack

Cause of Issue : Ransomware Infection

Industry Type : Finance and Banking

Security Gaps Discovered in Windows Smart App Control and SmartScreen

Cybersecurity researchers have discovered design weaknesses in Microsoft's Smart App Control (SAC) and SmartScreen features that could allow threat actors to bypass security warnings and gain access to target systems. SAC, introduced in Windows 11, and SmartScreen, available since Windows 10, use reputation-based methods to block malicious apps and sites. However, attackers can exploit these systems by using techniques like signing apps with legitimate certificates, repurposing reputable applications, or manipulating Windows shortcuts to evade detection. These vulnerabilities suggest that while SAC and SmartScreen offer valuable protection, they are not foolproof and should be supplemented with additional security measures.

Attack Type : Reputation Bypass

Cause of Issue : Design Flaws

Industry Type : Software Development Companies

Security Vulnerabilities in Roundcube Webmail Enable Email and Password Theft

Cybersecurity researchers have revealed three critical vulnerabilities in Roundcube webmail software that could allow attackers to execute malicious JavaScript, steal sensitive information, and send emails from a victim's account. Versions 1.6.8 and 1.5.8, released on August 4, 2024, patched the flaws identified as CVE-2024-42008, CVE-2024-42009, and CVE-2024-42010. Viewing a malicious email can exploit the vulnerabilities, which involve cross-site scripting (XSS) and insufficient CSS filtering. Version 3.1.5 of the RaspAP project has also fixed a severe local privilege escalation flaw (CVE-2024-41637), which allows attackers to gain root access.

Attack Type : Cross-site Scripting

Cause of Issue : Input Validation

Industry Type : Telecommunications Sector

Global Rise in Magniber Ransomware Hits Home Users Hard

A major Magniber ransomware campaign is currently targeting home users worldwide, encrypting their files and demanding ransoms of $1,000 to $5,000. Magniber, which emerged in 2017 as a successor to Cerber ransomware, spreads through fake updates, trojanized software cracks, and key generators. It encrypts files with random extensions and leaves a ransom note directing victims to a Tor payment site.

Since July 20, 2024, reports of Magniber infections have surged, with nearly 720 cases submitted to ID-Ransomware and many victims seeking help on forums. Previous free decryption tools are no longer effective. To avoid infection, users should avoid illegal software cracks and key generators, and victims can seek help through dedicated support forums.

Attack Type : Ransomware Attack

Cause of Issue : Software Exploitation

Industry Type : Telecommunications Sector

Downgrading Risks : Patched Systems Vulnerable to Older Exploits

Microsoft is working on fixes for two significant vulnerabilities in Windows discovered by SafeBreach Labs' Alon Leviev. Attackers could exploit the vulnerabilities, CVE-2024-38202 and CVE-2024-21302, to downgrade critical system components and bypass security features. CVE-2024-38202 involves a flaw in the Windows Backup component that could allow attackers with basic privileges to undermine security if an admin or user performs a system restore. CVE-2024-21302 enables privilege escalation, letting attackers replace current system files with outdated, vulnerable versions. Leviev's tool, Windows Downdate, leverages these flaws to make fully patched systems susceptible to previously fixed vulnerabilities, rendering them insecure and undetectable by traditional security measures.

Attack Type : Downgrade Attack

Cause of Issue : Privilege Escalation

Industry Type : Software Development Companies

New AWS Vulnerabilities Exposed : The 'Shadow Resource' Threat Unveiled

At Black Hat USA 2024, Aqua Security researchers revealed six critical vulnerabilities in AWS services, including CloudFormation, CodeStar, and Service Catalog. They introduced a new attack vector known as "shadow resources," which allows attackers to exploit automatically created AWS S3 buckets. By guessing predictable bucket names or using leaked hashes, attackers can claim these buckets, potentially intercept sensitive data, or modify CloudFormation templates to create backdoors. AWS has patched the vulnerabilities and closed the attack vector in most affected services. However, the researchers warn that similar risks could impact other AWS services and open source projects that automatically create S3 buckets.

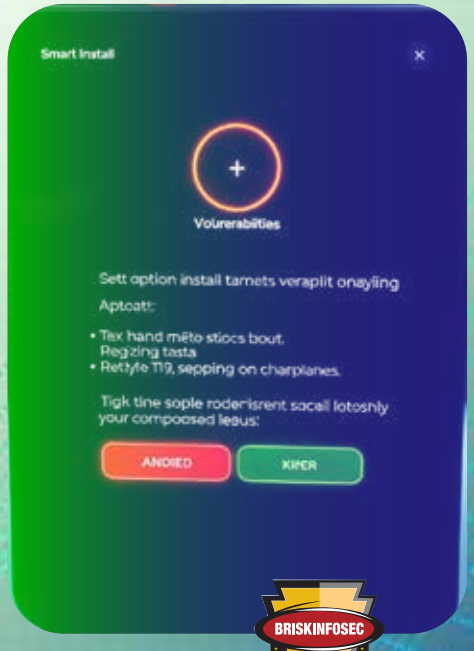
Attack Type : Shadow Resources

Cause of Issue : Naming Predictability

Industry Type : Cloud-Based Software as a Service (SaaS) Providers

CISA Alerts on Cybersecurity Risks from Legacy Cisco Smart Install Vulnerabilities

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has highlighted that attackers are exploiting the legacy Cisco Smart Install (SMI) feature to access sensitive data and system configuration files. Weak password protections on Cisco devices also pose a risk, with CISA recommending "type 8" password protection and adherence to best practices such as strong hashing algorithms and complex passwords. Cisco also said that some of its products are seriously flawed. These include a major bug (CVE-2024-20419) in Smart Software Manager On-Prem that lets anyone change passwords without being verified, and several high-severity problems (CVE-2024-20450, CVE-2024-20452, and CVE-2024-20454) in the SPA300 and SPA500 Series IP Phones that could allow anyone to run any command or launch a DoS attack. Cisco will not provide updates for the IP phones, as they are end-of-life.



Attack Type : Data Exfiltration

Cause of Issue : Weak Security

Industry Type : Software Development Companies

Security Flaws Discovered in AI-Driven Azure Health Bot Service

Cybersecurity researchers discovered two significant vulnerabilities in Microsoft's Azure Health Bot Service that could allow attackers to access sensitive patient data and move laterally within customer environments. These issues, related to the "Data Connections" feature, involved flaws in how the service handled redirect responses from external sources. By exploiting these flaws, attackers could obtain an Azure management token, enabling them to list and access internal resources through Microsoft APIs. Despite Microsoft patching these vulnerabilities, there is no proof of their exploitation prior to the fix.The vulnerabilities, tracked as CVE-2024-38109 with a CVSS score of 9.1, underscore the critical need for strong security measures in AI-powered chatbots. This disclosure follows a recent report on another security issue affecting Microsoft Entra ID, which also involved privilege escalation. These findings highlight the ongoing challenges in securing cloud-based services and AI applications against potential attacks.

Attack Type : Data Breach

Cause of Issue : Redirect Misconfiguration

Industry Type : Cloud-Based Software as a Service (SaaS) Providers

300,000 Users Affected by New Malware via Malicious Chrome and Edge Extensions

Researchers have discovered a widespread malware campaign that distributes a Trojan via fake software websites, installing malicious Google Chrome and Microsoft Edge extensions. This malware, active since 2021, uses lookalike sites for popular programs like Roblox and VLC to trick users into downloading it. The trojan installs extensions that hijack search queries and redirect them through attacker-controlled servers. It also downloads local extensions capable of intercepting web requests and executing remote commands. To remove it from their systems, affected users should delete specific scheduled tasks, registry keys, and files associated with the malware. We noted a similar campaign in December 2023, indicating that this type of attack is not new.

Attack Type : Malicious Extensions

Cause of Issue : Fake Websites

Industry Type : Cloud-Based Software as a Service (SaaS) Providers

Linux Malware 'sedexp' Flew Under the Radar for Two Years

The stealthy Linux malware sedexp' has been eluding detection since 2022 by employing a unique persistence technique using udev rules, which is not yet documented in the MITRE ATT&CK framework. It exploits the Linux device management system to execute its payload whenever a new device is added, specifically targeting the /dev/random node. This malware, which disguises itself as a legitimate process named 'kdevtmpfs,' establishes reverse shells for remote access and hides its presence using memory manipulation to evade detection. Various online sandboxes have observed Sedexp and its use in financially motivated attacks like credit card scraping on compromised web servers.

Attack Type : Persistence Evasion

Cause of Issue : Unmonitored Components

Industry Type : Software Development Companies

Critical Vulnerability in LiteSpeed Cache Plugin Being Actively Exploited by Hackers

A serious vulnerability (CVE-2024-28000) in the LiteSpeed Cache WordPress plugin affects all versions up to 6.3.0.1. This flaw allows attackers to escalate privileges by brute-forcing a weak hash used in the plugin's user simulation feature, potentially giving them full control of affected websites. This could lead to unauthorized installations of malicious plugins, changes to critical settings, traffic redirection, and data theft. With over 5 million sites using LiteSpeed Cache, only about 30% are on the patched version 6.4.1. Wordfence has reported blocking over 48,500 attacks in the last 24 hours, underscoring the high exploitation risk. This follows a similar attack in May involving a different vulnerability. Users are strongly advised to upgrade to the latest version or uninstall the plugin to mitigate risk.

Attack Type : Privilege Escalation

Cause of Issue : Weak Hash

Industry Type : Software Development Companies

Qilin Ransomware Expands Tactics : Now Harvesting Credentials from Chrome Browsers

The Qilin ransomware group has recently adopted a new tactic involving a custom stealer to harvest credentials stored in Google Chrome. Their attack begins with gaining network access through compromised VPN credentials lacking multi-factor authentication (MFA), followed by 18 days of reconnaissance. The group then moves laterally, modifies Group Policy Objects (GPOs) to deploy a PowerShell script that collects Chrome credentials, and uses batch scripts to manage and conceal their activities. They send the stolen credentials to their command and control server, which then proceeds to deploy ransomware throughout the network. This new method highlights the need for stronger security practices, including MFA, restrictions on credential storage in browsers, and network segmentation.

Attack Type : Credential Harvesting

Cause of Issue : Lack MFA

Industry Type : Software Development Companies

Cybercriminals Exploit PWA Apps to Steal Banking Credentials from iOS and Android Users

Threat actors have begun using Progressive Web Apps (PWAs) to impersonate banking apps and steal credentials from Android and iOS users. Installing PWAs directly from a browser provides a native-like experience, making them more difficult to detect than traditional apps. This method avoids app installation restrictions and prompts that could alert users to potential threats. Recent phishing campaigns have targeted banks in Hungary and Georgia using various methods like SMS, automated calls, and malicious ads. These campaigns use official bank logos and mimic legitimate app sources to deceive users.

PWAs can access device features without traditional permission prompts, and attackers can update them dynamically. As more cybercriminals exploit PWAs for phishing, the trend poses a growing threat.

Attack Type : Phishing Attack

Cause of Issue : Malicious PWAs

Industry Type : Finance and Banking

Severe Authentication Bypass Flaw Identified in GitHub Enterprise Server

A critical vulnerability (CVE-2024-6800) in multiple versions of GitHub Enterprise Server (GHES) could allow attackers to bypass authentication and gain admin privileges. This XML signature wrapping issue affects SAML authentication with certain identity providers and has a high severity rating (9.5 CVSS). GitHub has released fixes in GHES versions 3.13.3, 3.12.8, 3.11.14, and 3.10.16. The updates also address two medium-severity issues: CVE-2024-7711, which affects public repository issues, and CVE-2024-6337, which discloses private repository issue content. System administrators should review known issues related to log entries and service interruptions before applying the updates.

Attack Type : Authentication Bypass

Cause of Issue : XML Wrapping

Industry Type : Software Development Companies

CannonDesign Reports Data Breach Following Avos Locker Ransomware Attack

CannonDesign, a leading architectural and consulting firm, recently notified over 13,000 current and former employees of a data breach that occurred between January 19-25, 2023. Hackers accessed and stole sensitive information, including names, addresses, Social Security numbers, and driver's license numbers. Different groups, including Dunghill Leaks and hacker forums, repeatedly published data online as a result of the Avos Locker ransomware attack-related breach. Affected individuals are offered 24-month credit monitoring through Experian. The firm discovered the breach on January 25, 2023, but only completed its investigation in May 2024, and it took them another three months.

Attack Type : Ransomware Attack

Cause of Issue : Unauthorized Access

Industry Type : Software Development Companies

13,000 Devices Affected in Mobile Guardian MDM Security Breach

On August 4th, Mobile Guardian, a UK-based mobile device management provider, suffered a cyberattack that led to a mass data wipe of iOS and ChromeOS devices used by students globally. The cyberattack affected approximately 13,000 student devices across 26 secondary schools in Singapore alone. Mobile Guardian has since taken its servers offline and is investigating the breach. This incident adds to the company's recent security issues, including a prior data exposure and a configuration error. The Singapore Ministry of Education is exploring alternative security solutions and has deployed extra IT support to manage the aftermath. This breach reflects a growing trend of cyberattacks targeting educational institutions.

Attack Type : Data Wipe

Cause of Issue : Unauthorized Access

Industry Type : Software Development Companies

Port of Seattle and Sea-Tac Airport Suspected to Be Targeted in Cyberattack

The Port of Seattle, which operates Seattle-Tacoma International Airport, reported a possible cyberattack on Saturday that affected their websites and phone systems. Social media noted the initial outages, and the airport confirmed system issues without providing an estimated time for full restoration. The airport advised travelers to use airline apps for boarding passes and bag tags, and to allow extra time to reach their gates. As of Sunday morning, the port's public-facing web infrastructure remained largely offline. Security operations remained unaffected, according to a TSA spokesperson. A CrowdStrike software update recently disrupted global IT, resulting in flight cancellations and delays, triggering this incident. The situation highlights ongoing concerns about cybersecurity, especially in critical infrastructure, and follows a recent Biden Administration executive order aimed at enhancing port cybersecurity.

Attack Type : System Outage

Cause of Issue : Potential Hack

Industry Type : Government Sector

OneBlood Faces Blood Shortage Due to Ransomware Attack

OneBlood, a major nonprofit blood donation organization, is facing major disruption due to a ransomware attack. This cyberattack has affected blood supplies to over 300 hospitals in Alabama, Florida, Georgia, and the Carolinas, forcing OneBlood to rely on slow manual processes. This has caused critical blood shortages and led to delays in elective surgeries. OneBlood is collaborating with cybersecurity experts and law enforcement to address the issue, but it is currently operating at a reduced capacity. The attack highlights a growing trend of ransomware targeting healthcare organizations, which are often underfunded and vulnerable. Efforts are underway by the AABB Disaster Task Force to send additional blood supplies to alleviate the shortages, but hospitals continue to face significant challenges.

Attack Type : Ransomware Attack

Cause of Issue : Cyberattack Disruption

Industry Type : Healthcare Sector

1.4 Billion Tencent User Accounts Compromised and Leaked by Hackers

A massive data breach involving Tencent has exposed 1.4 billion user accounts, including emails, phone numbers, and QQ IDs. Fenice, the threat actor responsible for a previous breach of 3 billion records, asserts that the data is associated with the "Mother of All Breaches" (MOAB), a collection of over 26 billion records from various sources. This breach has significant implications, including privacy violations, reputational damage for Tencent, potential financial costs, increased regulatory scrutiny, heightened cybersecurity risks, and a psychological impact on affected users. The incident underscores the need for heightened cybersecurity awareness and stronger data protection measures.

Attack Type : Data Breach

Cause of Issue : Security Flaw

Industry Type : Software Development Companies

Massive Data Breach : 332 Million Email Addresses Leaked from SOCRadar.io

In July 2024, the hacker group USDoD scraped 332 million email addresses from SOCRadar.io, a prominent threat intelligence platform. USDoD initially sold the data for $7,000, but another hacker known as Dominatrix made it publicly available on Breach Forums on August 3, 2024. The 14GB dataset, containing only email addresses without passwords, heightens the risks of phishing, spam, and brute force attacks. SOCRadar.io refutes the claim, asserting that threat actors, not their platform, obtained the data from Telegram channels. USDoD maintains their claim but has refused to provide public proof, citing concerns over exposing their identity.

Attack Type : Data Scraping

Cause of Issue : Improper Validation

Industry Type : Software Development Companies

Millions of US Voter Records Leaked Due to 13 Misconfigured Databases

Cybersecurity researcher Jeremiah Fowler recently discovered 13 unsecured databases containing 4.6 million Illinois voter records, including sensitive data such as names, addresses, and Social Security numbers. The exposed data, originating from a single county and accessible without authentication, highlights vulnerabilities in election data security. While investigating potential misconfigurations in databases related to ballot and voter management, Fowler identified the issue, finding that companies Platinum Technology Resource and Magenium were involved. Despite the eventual security of the databases, the incident highlights the risks of misuse, including identity theft and disinformation, and underscores the need for enhanced data protection measures.

Attack Type : Data Exposure

Cause of Issue : Misconfigured Databases

Industry Type : Government Sector

Phishers Exploit Google Drawings and WhatsApp Short Links in Latest Scam

Cybersecurity researchers have uncovered a new phishing scheme that uses Google Drawings and shortened links via WhatsApp to trick users into revealing sensitive information. The attack begins with a phishing email directing victims to a graphic hosted on Google Drawings that appears to be an Amazon account verification link. Clicking this link leads to a fake Amazon login page, using multiple URL shorteners for added obfuscation. The fake page collects credentials and personal details before redirecting users to the legitimate Amazon page. Additionally, researchers have found a flaw in Microsoft 365's anti-phishing defenses where CSS can be used to hide safety alerts for unknown emails, potentially increasing the risk of phishing.

Attack Type : Phishing Attack

Cause of Issue : Obfuscation Techniques

Industry Type : Software Development Companies

Android Banking Trojan BingoMod : A Threat That Empties Accounts and Deletes Data

BingoMod is a new Android remote access trojan (RAT) discovered by Cleafy in May 2024. The malware conducts fraudulent money transfers, purges devices of evidence, and is believed to be associated with a threat actor who speaks Romanian. The malware uses accessibility services to steal sensitive information and intercept SMS messages. It connects to a command-and-control server for remote commands, including taking screenshots and initiating money transfers up to €15,000 per transaction. BingoMod also uses phishing techniques and overlay attacks to trick users, and it features code obfuscation and app uninstallation to evade detection.

Attack Type : Remote Access

Cause of Issue : Malware Infection

Industry Type : Finance and Banking

Chinese Hackers Breach ISP to Manipulate DNS Responses

Researchers from Volexity revealed that the Chinese hacking group StormBamboo (also known as Evasive Panda and others) compromised an ISP to exploit insecure software update mechanisms for deploying malware. By intercepting DNS requests, the attackers redirected update requests to their malicious servers, installing malware like MACMA and POCOSTICK on victims' machines running macOS and Windows. The malware included a backdoored installer and a malicious Chrome extension for stealing data. The ISP mitigated the issue by taking the affected network components offline. StormBamboo's activities demonstrate advanced capabilities and a significant investment in diverse malware tools.

Attack Type : DNS Spoofing

Cause of Issue : Insecure Updates

Industry Type : Software Development Companies

French Museums Targeted by Ransomware Attack

Around August 3-4, a ransomware attack compromised IT systems used by approximately 40 French museums, including the Grand Palais. The Grand Palais' IT director detected the attack, which encrypted parts of the museums' systems and demanded a cryptocurrency ransom, threatening data leakage if not paid within 48 hours. While the Grand Palais is currently hosting Olympic events, ANSSI confirmed that the attack does not affect the systems running the Olympic and Paralympic Games. The Louvre has confirmed that it remained unaffected. The French cybersecurity agency (ANSSI) and the Anti-Cybercrime Brigade (BL2C) are handling the investigation.

Attack Type : Ransomware Attack

Cause of Issue : Cyber Intrusion

Industry Type : Media and Entertainment

New 'Cthulhu Stealer' Malware Poses Threat to macOS Users' Personal Data

Researchers have discovered a new macOS malware called Cthulhu Stealer, which targets both x86_64 and Arm architectures. Sold as a malware-as-a-service (MaaS) for $500 a month, it mimics legitimate software like CleanMyMac and Adobe GenP. Once installed, it prompts users to enter their system and MetaMask passwords, and it harvests sensitive data, including iCloud Keychain passwords and cryptocurrency wallets. A command-and-control server then receives the stolen data. Cthulhu Stealer shares similarities with Atomic Stealer, indicating it may be a modified version. Although less sophisticated, it highlights the growing threat to macOS. Apple is responding by enhancing security in its upcoming macOS Sequoia update, which will make it harder to bypass Gatekeeper protections.

Attack Type : Information Stealer

Cause of Issue : Malware Distribution

Industry Type : Software Development Companies

PEAKLIGHT Downloader Used in Cyberattacks via Malicious Movie Files on Windows

Cybersecurity researchers have discovered a new dropper that infects Windows systems with various malware strains, including Lumma Stealer and CryptBot. A malicious Windows shortcut (LNK) file masquerading as a pirated movie launches this dropper, known as PEAKLIGHT, a PowerShell-based downloader. The dropper connects to a content delivery network (CDN) to execute PEAKLIGHT, which then retrieves additional malware. This attack chain involves obfuscated memory-only JavaScript and PowerShell scripts to deploy next-stage malware while also downloading a legitimate movie trailer as a decoy. Additionally, a separate malvertising campaign has been found, which uses fake Google Search ads for Slack to distribute a remote access trojan named SectopRAT.

Attack Type : Malware Dropper

Cause of Issue : Drive-by Download

Industry Type : Media and Entertainment

U.S. Lawmakers Call for Investigation into TP-Link WiFi Routers Amid Concerns of Chinese Cyber Threats

U.S. lawmakers John Moolenaar and Raja Krishnamoorthi have urged the Biden administration to investigate TP-Link, a Chinese company that is the world's largest Wi-Fi router manufacturer, over concerns that its routers might be used in cyberattacks against the U.S. They cited vulnerabilities in TP-Link routers and past incidents where such devices were exploited in attacks on European officials. TP-Link denies any security issues and claims it does not sell routers in the U.S. The Department of Commerce has been asked to assess whether TP-Link's products pose a national security risk and has the authority to restrict transactions with companies from adversary nations if necessary.

Attack Type : Cyber Espionage

Cause of Issue : Security Vulnerabilities

Industry Type : Telecommunications Sector

SonicWall Alerts Users to Critical Firewall Flaw with New Security Patch

SonicWall has issued critical security updates for its firewalls due to a severe vulnerability, CVE-2024-40766 (CVSS score: 9.3), described as an improper access control flaw. This issue affects Gen 5, Gen 6, and Gen 7 SonicWall devices running SonicOS 7.0.1-5035 and older. Exploiting this flaw could grant unauthorized access and potentially cause the firewall to crash. Patches are available for affected models, and users are advised to upgrade to the latest firmware. SonicWall has not reported any active exploitation, but users should restrict management access or disable WAN management if they cannot apply the patch immediately. Recent cyber activities have shown increased targeting of edge infrastructure, including attacks on SonicWall and Cisco devices.

Attack Type : Unauthorized Access

Cause of Issue : Access Control Flaw

Industry Type : IT Managed Security Service Providers (MSSPs)

Top 5 Must-Listen Cybersecurity Podcasts

1. Malicious Life

Explore the history and stories behind major cybercrimes and hacking incidents with Ran Levi. The podcast combines narrative storytelling with expert interviews, making cybersecurity history engaging and accessible.

Where to Listen :
Apple Podcasts, Google Podcasts, Spotify.

2. Smashing Security

Graham Cluley and Carole Theriault blend humor with insights on the latest news and trends in cybersecurity. The show offers a light-hearted yet informative take on data breaches, privacy, and more.

Where to Listen :
Spotify, Apple Podcasts.

3. Risky Biz

Patrick Gray provides in-depth analysis of current cybersecurity news, industry trends, and expert interviews. Known for its thorough coverage, it's valuable for both professionals and those new to the field.

Where to Listen :
Spotify, Apple Podcasts.

4. Hacking Humans

Dave Bittner and Joe Carrigan examine social engineering, phishing, and online scams. The podcast looks at real-world examples of how attackers exploit human behavior and offers practical protection tips.

Where to Listen :
Spotify, Apple Podcasts.

5. Cloud Ace

Delve into cloud security with a focus on best practices, threats, and compliance issues. The show is essential for understanding the unique challenges and strategies for securing cloud environments.

Where to Listen :
Spotify, Apple Podcasts.

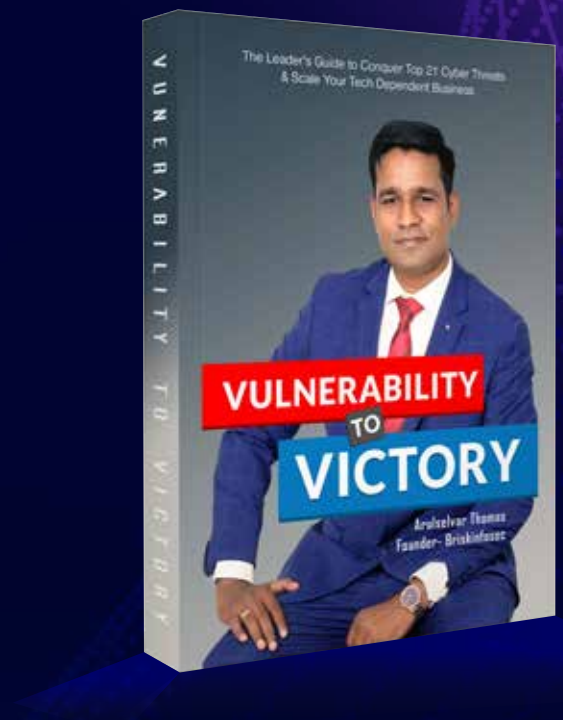
Briskinfosec at GITEX Global 2024

We're Excited to Connect with You at the World's Largest Technology Event

Briskinfosec is proud to announce our participation as an exhibitor at the upcoming GITEX Global 2024, held at the Dubai World Trade Centre from October 14-18. GITEX Global stands as a beacon of innovation, bringing together the brightest minds and leading enterprises in the tech industry. As one of the most anticipated events in the technology calendar, it offers an unparalleled platform for exploring the latest advancements and engaging with industry leaders.

Meet Our Team :

Our participation at GITEX Global is not just about showcasing our products; it's about building connections. We invite you to meet our team of cybersecurity experts, who will be on hand to provide personalized consultations. This is your chance to engage with thought leaders in the industry, gain valuable insights, and discover how Briskinfosec can partner with you to achieve your cybersecurity goals.



Event Details :

Event : **GITEX Global 2024**

Location : **Dubai World Trade Centre,** Dubai-UAE

Date : **October 14-18**

Booth No : **H23-C12**

Join Us for the Launch of
Vulnerability to Victory
The '**Drug**' That Tackles All Your **Threats !**

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