
Edition-78
BRISKINFOSEC
CYBER TRUST & ASSURANCE
Threatsploit
Adversary Report
February - 2025
www.briskinfosec.com

Introduction :

Dear Readers,

Welcome to our February 2025 edition of the Threatsploit Adversary Report! In this report, we examine the ever-changing landscape of cyber threats, reveal new attack methods, and provide key insights into the latest developments. This is not just another news update; it's your guide to understanding what's happening in cybersecurity and staying aware of the evolving risks.

This month, cybercriminals have intensified supply chain attacks, sneaking fake npm packages into trusted software ecosystems and infecting thousands without immediate detection. Meanwhile, a dangerous exploit called DoubleClickjacking has emerged, enabling attackers to hijack user interactions in unprecedented ways. Additionally, a critical flaw in Nuclei has been actively exploited to bypass security defenses and execute malicious code undetected.

Privacy concerns continue to make headlines, with Apple facing a $95 million lawsuit over unauthorized Siri recordings. At the same time, FireScam malware, disguised as Telegram Premium, is stealing sensitive data from unsuspecting Android users. These threats serve as a stark reminder that cybercrime knows no boundaries, and no platform, device, or user is safe.

The digital battlefield is always shifting, but that doesn't mean we have to stay on the defensive. This edition of the Threatsploit Adversary Report equips you with critical intelligence on emerging threats and attack patterns, helping you take proactive steps to safeguard your digital world.

Best regards,
Briskinfosec Threat Intelligence Team.

Stay informed,
stay secure.

Contents :

New DoubleClickjacking Exploit Overcomes Clickjacking Defenses on Leading Websites

A new clickjacking vulnerability, called "DoubleClickjacking," has been discovered, which exploits the timing between two clicks to bypass common security protections like X-Frame-Options and SameSite cookies. The attack involves a double-click sequence where an attacker-controlled site redirects a user to a malicious page while closing the original window. This technique enables account takeovers with minimal user interaction. It targets major websites and cannot be blocked by traditional defenses. Recommendations for mitigation include client-side measures to disable critical buttons by default and for browser vendors to develop new defenses against this exploit.

Attack Type : Double Clickjacking

Cause of Issue : Timing Exploit

Industry Type : Information Technology

Apple Settles Siri Privacy Lawsuit, Offering $20 Per Affected Device

Apple has agreed to pay $95 million to settle a U.S. class action lawsuit accusing the company of invading users' privacy through unintended Siri activations, which allegedly led to private conversations being shared with third parties. The lawsuit followed a 2019 report revealing that contractors listened to Siri recordings to improve the service. Apple has denied wrongdoing but introduced measures to enhance user privacy, including opt-ins for data collection and the ability to delete Siri history. The settlement allows affected users to claim $20 per device for up to five devices.

Penalty : Privacy Violation

Cause of Issue : Accidental Activation

Industry Type : Information Technology

Nuclei Vulnerability Allows Code Execution via Signature Bypass

A high-severity vulnerability (CVE-2024-43405) has been discovered in Nuclei, an open-source vulnerability scanner, with a CVSS score of 7.4. The flaw allows attackers to bypass signature verification in templates by exploiting discrepancies between the YAML parser and regex validation. This enables attackers to inject malicious content into templates, which could lead to arbitrary code execution, data exfiltration, or system compromise. The vulnerability affects all Nuclei versions after 3.0.0 and was patched in version 3.3.2. Users are advised to avoid using untrusted templates or ensure proper validation.

Attack Type : Code Injection

Cause of Issue : Signature Bypass

Industry Type : Information Technology

Fake npm Packages Target Ethereum Developers with Hardhat Impersonation

Cybersecurity researchers have discovered several malicious npm packages impersonating the Nomic Foundation's Hardhat tool to steal sensitive data from developer systems. These packages exfiltrate private keys, mnemonics, and configuration files to attacker-controlled servers. The compromised packages exploit the Hardhat runtime environment and are designed to collect and send sensitive data. This attack highlights the complexity and security risks within the npm ecosystem, where attackers can exploit dependencies to introduce malicious code. Developers are advised to verify package authenticity and inspect source code before installation.

Attack Type : Supply Chain

Cause of Issue : Malicious Packages

Industry Type : Software Development Industry

FireScam Malware Impersonates Telegram Premium to Exfiltrate Data and Control Devices

FireScam, an Android information-stealing malware, masquerades as a fake "Telegram Premium" app distributed through a phishing site mimicking RuStore, a Russian app store. Once installed, the malware collects sensitive data such as messages, contacts, and e-commerce transactions and maintains persistence through a dropper app that prevents updates from other sources. It also receives remote commands through Firebase Cloud Messaging and exfiltrates data to a command-and-control server. Google Play Protect prevents known versions of the malware, but it can still be distributed outside of official app stores.

Attack Type : Data Exfiltration

Cause of Issue : Fake Application

Industry Type : Software Development Industry

EAGERBEE Malware Variant Targets ISPs and Government Entities with Enhanced Backdoor Features

The EAGERBEE malware framework, targeting ISPs and governmental entities in the Middle East, has been updated with new capabilities. It now includes components for deploying additional payloads, enumerating file systems, and executing shell commands. The malware, attributed to the CoughingDown group, uses a plugin-based architecture for stealth and flexibility. It has been involved in multiple cyber espionage operations, including attacks in East Asia. The framework operates primarily in memory, making detection difficult. EAGERBEE uses techniques like injecting malicious code into legitimate processes and exploiting vulnerabilities such as ProxyLogon (CVE-2021-26855) to deploy web shells.

Attack Type : Backdoor Malware

Cause of Issue : Command Injection

Industry Type : Software Development Industry

Critical Aviatrix Controller Flaw Exploited for Backdoor and Cryptominer Deployment

Aviatrix is a cloud networking company that provides a platform for managing and securing cloud infrastructure across multiple cloud providers, such as AWS, Azure, and Google Cloud. Their solutions help enterprises manage complex networking, secure cloud environments, optimize network performance, and ensure compliance in cloud environments. Aviatrix's products focus on simplifying cloud networking operations, offering features like centralized visibility, automated network provisioning, and multi-cloud networking. Their platform is particularly popular among organizations that operate in multi-cloud environments and need seamless, scalable, and secure connectivity across cloud resources.

Attack Type : Remote Execution

Cause of Issue : Input Sanitization

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

Over 4,000 Backdoors Compromised Through Expired Domains

WatchTowr Labs has hijacked over 4,000 web backdoors previously deployed by various threat actors by taking control of abandoned or expired infrastructure for as little as $20 per domain. By registering domains linked to these backdoors, they were able to track compromised hosts and potentially commandeer them. Targets included government entities and academic institutions across several countries. The backdoors, which were primarily web shells like c99shell, r57shell, and China Chopper, allowed persistent remote access for exploitation. Some of the backdoors were backdoored themselves, revealing their deployment locations and exposing attackers' mistakes.

Attack Type : Backdoor Hijacking

Cause of Issue : Expired Domains

Industry Type : Software Development Industry

Hackers Release Configurations and VPN Data for 15,000 FortiGate Devices

A new hacking group, the "Belsen Group," has leaked sensitive data, including configuration files, IP addresses, and VPN credentials, for over 15,000 FortiGate devices on the dark web. The leaked data includes folders organized by country, containing configuration dumps and VPN passwords, some in plain text. The breach is linked to a 2022 zero-day vulnerability (CVE-2022-40684) exploited before a patch was released. Although the data was collected in 2022, it still poses risks as it contains sensitive network information. FortiGate admins are advised to review and update their configurations and credentials immediately.

Attack Type : Zero-Day Exploit

Cause of Issue : Exploited Vulnerability

Industry Type : Information Technology

HuiOne Telegram Marketplace Surpasses Hydra with $24 Billion in Crypto Transactions

HuiOne Guarantee, a Telegram-based illicit marketplace, has received over $24 billion in cryptocurrency, making it the largest online marketplace of its kind. Initially created for legitimate sales, it became a hub for scams, money laundering and human trafficking. Despite distancing itself from its parent company, HuiOne Group and rebranding, the platform continues to thrive. It has facilitated various criminal activities, including online fraud, with links to North Korea's Lazarus hacking group. Additionally, HuiOne Group has launched crypto products to avoid deplatforming.

Attack Type : Online Fraud

Cause of Issue : Exploit Cryptocurrency Systems

Industry Type : Cryptocurrency

FBI Removes PlugX Malware from 4,250 Infected Computers in Extensive Operation

The FBI, authorized by the U.S. Department of Justice, removed PlugX malware from over 4,250 infected computers as part of a multi-month operation targeting a Chinese state-sponsored hacking group, Mustang Panda. This malware, which has been used since 2014, allows attackers to steal data and remotely control devices. The operation, initiated in July 2024, involved issuing a self-delete command to affected systems, ensuring no legitimate files were harmed. The attack targeted thousands of computers globally, including those in the U.S., showcasing the aggressive tactics of PRC-backed hackers.

Attack Type : Remote Access Trojan

Cause of Issue : State-Sponsored

Industry Type : Law Enforcement

European Privacy Group Files Lawsuit Against TikTok and AliExpress for Illegal Data Transfers to China

Austrian privacy non-profit None of Your Business (noyb) has filed complaints against companies like TikTok, AliExpress, SHEIN, Temu, WeChat, and Xiaomi, accusing them of violating EU data protection regulations by unlawfully transferring user data to China. Noyb argues that these companies cannot prevent the Chinese government from accessing this data, as China lacks adequate data protection laws. The complaints were filed in multiple EU countries, seeking to halt such transfers. This follows previous GDPR-related actions by noyb and coincides with other U.S. data privacy actions, including FTC actions against General Motors and GoDaddy for improper data practices.

Attack Type : Data Breach

Cause of Issue : Unauthorized Data Transfer

Industry Type : Media and Entertainment

Lumma Stealer Targeting Multiple Industries via Fake CAPTCHA Campaign

A new malware campaign is using fake CAPTCHA verification to distribute the Lumma information stealer. The attack begins when victims visit a compromised site that prompts them to run a command to download an HTA file. This file eventually leads to the execution of the Lumma payload, bypassing security systems. The campaign is global, impacting industries like healthcare, banking, and telecom. Lumma has been spreading through various methods, including counterfeit domains impersonating popular sites. Additionally, new phishing tools are emerging that evade detection, making it harder for security systems to identify threats.

Attack Type : Social Engineering

Cause of Issue : Fake CAPTCHA

Industry Type : Telecommunication Industry

HellCat and Morpheus Ransomware Affiliates Using Identical Payload Code

In late 2024 and early 2025, ransomware operations like HellCat and Morpheus saw increased activity. HellCat, known for targeting high-value entities and promoting itself in the cybercrime space, and Morpheus, which operates more discreetly, share near-identical ransomware payloads. Both use the Windows Cryptographic API for file encryption and avoid altering file extensions during the process. The samples suggest a possible overlap between affiliates or shared tools between HellCat and Morpheus. Their ransom notes are almost identical, with slight differences in contact information.

Attack Type : Ransomware

Cause of Issue : Shared Codebase

Industry Type : Pharmaceutical and Manufacturing

Star Blizzard Hackers Exploit WhatsApp to Target Diplomats and High-Value Entities

Star Blizzard, a Russian nation-state actor, launched a spear-phishing campaign targeting organizations involved in government, diplomacy, defense, and Ukraine aid. The campaign, observed in November 2024, impersonates a U.S. government official to lure victims into joining a fake WhatsApp group. Victims are tricked into scanning a malicious QR code, which links the attacker's device to their WhatsApp account, allowing the exfiltration of messages. The attack relies on social engineering rather than malware, making it harder for antivirus tools to detect. Users are advised to be cautious with unsolicited invitations and regularly check linked devices on WhatsApp for unfamiliar connections. Despite disruptions to Star Blizzard's operations in October 2024, the group has adapted and continued its activities.

Attack Type : Phishing Attack

Cause of Issue : Social Engineering

Industry Type : Government and Diplomacy

Massive Otelier Breach Compromises Millions of Hotel Bookings and Personal Data

Hotel management platform Otelier suffered a data breach after threat actors gained access to its Amazon S3 cloud storage, stealing nearly eight terabytes of data, including personal guest information and reservations for major hotel brands like Marriott, Hilton, and Hyatt. The breach, which began in July 2024 and continued through October, was caused by stolen employee credentials from an Atlassian server. The stolen data includes guest names, addresses, phone numbers, and email addresses. While passwords and billing info were not compromised, the exposed data could lead to phishing attacks. Otelier is working with cybersecurity experts to investigate and improve security.

Attack Type : Data Breach

Cause of Issue : Stolen Credentials

Industry Type : Hotel Management

Trojanized Malware Builder Targets 18,000 Script Kiddies

A Trojanized version of the XWorm RAT builder was distributed to low-skilled hackers, or "script kiddies," through platforms like GitHub, Telegram, and YouTube. Instead of being a legitimate malware builder, it secretly infected the users with a backdoor, stealing data and allowing attackers to control their devices. The malware targeted devices in countries like Russia, the U.S., India, Ukraine, and Turkey. It had a kill switch that removed the malware from many machines, but some remain compromised. CloudSEK researchers disrupted the botnet using a mass uninstall command. The incident highlights the dangers of trusting unsigned software from unreliable sources.

Attack Type : Malware Distribution

Cause of Issue : Trojanized Software

Industry Type : Information Technology

Fake Reddit Pages Deliver Lumma Stealer Malware

Hackers are using nearly 1,000 fake websites that mimic Reddit and WeTransfer to distribute Lumma Stealer malware. The fake sites trick users into downloading the malware by using deceptive branding and URLs. The malware is designed to steal sensitive data, including passwords and session tokens, which can lead to account hijacking. The campaign may begin with malvertising, SEO poisoning, or social media messages. Lumma Stealer is a powerful info-stealer malware that has been linked to high-profile attacks on companies like PowerSchool and CircleCI.

Attack Type : Phishing Attack

Cause of Issue : Fake Websites

Industry Type : Information Security

SonicWall Alerts Users to Active Exploitation of SMA1000 RCE Vulnerability

SonicWall has issued a warning about a critical pre-authentication deserialization vulnerability (CVE-2025-23006) in its SMA1000 Appliance Management Console and Central Management Console, which has been exploited as a zero-day in attacks. The flaw, with a CVSS score of 9.8, allows remote unauthenticated attackers to execute arbitrary OS commands. Affected versions include all SMA1000 firmware up to 12.4.3-02804. Users are urged to upgrade to the hotfix version 12.4.3-02854. The vulnerability poses a significant risk, especially for large organizations, government agencies, and critical service providers.

Attack Type : Remote Code Execution

Cause of Issue : Deserialization Flaw

Industry Type : Government and Critical Infrastructure

Supply Chain Attack on IPany VPN Delivers Custom Malware

South Korean VPN provider IPany was breached in a supply chain attack by the "PlushDaemon" hacking group, who trojanized the VPN installer to distribute the 'SlowStepper' malware. The malware, active from November 2023 to May 2024, infected customers globally, including a South Korean semiconductor firm and users in Japan. SlowStepper collects system data, spies via audio/video recordings, steals credentials, and runs additional payloads. ESET researchers uncovered the attack and notified IPany, leading to the removal of the malicious installer. Infected users must clean their systems to remove the malware.

Attack Type : Supply Chain

Cause of Issue : Trojanized Installer

Industry Type : Semiconductor Firm and Software Development

Wolf Haldenstein Confirms Massive Data Breach Affecting 3.4 Million

Wolf Haldenstein Adler Freeman & Herz LLP, a New York City law firm, suffered a major data breach affecting 3,445,537 individuals, exposing sensitive personal and health information. The breach, discovered on December 13, 2023, involved a cyberattack that compromised names, Social Security numbers, and medical data. After a lengthy investigation, the firm issued notifications to affected individuals, offering credit monitoring services. The breach, one of the largest at a law firm, has led Wolf Haldenstein to improve its data privacy policies and procedures.

Attack Type : Data Breach

Cause of Issue : Network Compromise

Industry Type : Healthcare Services

Botnet Hijacks 13,000 MikroTik Routers for Malspam and Attacks

A botnet consisting of around 13,000 hijacked MikroTik routers has been used to spread malware via spam campaigns. The attackers exploited misconfigured DNS records and vulnerable routers, including those affected by CVE-2023-30799, to send malicious emails that bypass email security protections. The emails contained ZIP files with obfuscated JavaScript, triggering a PowerShell script to connect to a command-and-control server. The compromised routers were turned into SOCKS proxies, making it difficult to trace the attacks. Owners are advised to update their routers and change default credentials to prevent exploitation.

Attack Type : Botnet Attack

Cause of Issue : Misconfigured DNS

Industry Type : Information Technology

UnitedHealth Reports 190 Million Affected in 2024 Data Breach

UnitedHealth revealed that the Change Healthcare ransomware attack affected 190 million Americans, nearly doubling the previous estimate of 100 million. The breach, caused by the BlackCat ransomware gang, involved the theft of sensitive health and personal data, including medical records and Social Security numbers. The attack disrupted healthcare services, including claims and prescription fulfillment. UnitedHealth paid a ransom of $22 million, but after being scammed by the attackers, additional ransom demands were made. The total financial impact of the attack is expected to reach $2.45 billion.

Attack Type : Ransomware Attack

Cause of Issue : Lack of MFA

Industry Type : Healthcare

Ransomware Groups Use Microsoft Teams to Impersonate IT Support

Ransomware gangs are using email bombing followed by impersonating IT support via Microsoft Teams calls to gain remote access and install malware on company networks. Attackers exploit Teams' default settings that allow calls and chats from external domains. Once remote access is granted, malware like RPivot and keyloggers are installed to steal data and deploy ransomware. Sophos observed two campaigns, one linked to STAC5143 and another to STAC5777, with the latter attempting to deploy Black Basta ransomware. Organizations are advised to block external Teams messages and disable Quick Assist in critical environments.

Attack Type : Email Bombing

Cause of Issue : Misconfigured Teams

Industry Type : Information Technology

Casio Hit by Ransomware, Data of 8,500 Affected in October Breach

Casio suffered a ransomware attack in October 2024, compromising the personal data of approximately 8,500 individuals, including employees, business partners, and a small number of customers. The attack, claimed by the Underground ransomware gang, involved phishing tactics that led to an IT system outage. Exposed data included names, contact details, and sensitive personal information, though no customer credit card data was affected. Casio did not pay the ransom and has worked with law enforcement and experts. While most services have been restored, some are still recovering, and the company is addressing the breach through notifications to impacted individuals.

Attack Type : Ransomware Attack

Cause of Issue : Phishing Tactics

Industry Type : Electronic Industry

62 Million Students and Teacher's Information Impacted in PowerSchool Data Breach

In January 2024, PowerSchool, a cloud-based software provider for K-12 schools, suffered a cyberattack in which hackers used stolen credentials to access their customer support portal. The breach exposed the personal data of approximately 62.4 million students and 9.5 million teachers across multiple school districts. The stolen information included Social Security numbers, medical data, and grades for some students. PowerSchool paid a ransom to prevent the data from being leaked. The company is offering two years of free identity protection and credit monitoring for those affected.

Attack Type : Ransomware Attack

Cause of Issue : Stolen Credentials

Industry Type : Education

Malicious VS Code Extension Impersonates Zoom to Steal Chrome Cookies

Cybersecurity researchers discovered a malicious Visual Studio Code extension, disguised as a Zoom app, targeting developers. Uploaded to the VS Code Marketplace in November 2024, the extension steals Google Chrome cookies and Windows registry data. It activates upon startup and communicates with a server in China. The extension uses SQL queries to extract sensitive information, including encrypted cookie data. Developers are urged to vet extensions, perform code audits, and implement strict access controls to prevent such threats. The extension has been reported to Microsoft for removal from the marketplace.

Attack Type : Malicious Extension Attack

Cause of Issue : Security Flaw

Industry Type : Software Development

QakBot-Linked BackConnect Malware Improves Remote Access and Data Collection Features

Cybersecurity researchers have uncovered a new BackConnect (BC) malware developed by threat actors linked to the QakBot loader. The BC module, used to maintain persistence and provide remote access, includes DarkVNC and IcedID (KeyHole) components. It was found alongside ZLoader malware, which has also been updated with DNS tunneling for command-and-control communications. The BC malware gathers system information and allows threat actors hands-on access to infected systems. Sophos has linked the malware to cybercriminal groups like STAC5777 and Storm-1811, which have used techniques like vishing and email bombing to deploy Black Basta ransomware.

Attack Type : Backdoor Attack

Cause of Issue : QakBot Exploitation

Industry Type : Retail and Finance Industry

Gootloader Uses SEO Manipulation to Deliver Malware

The Gootloader malware uses blackhat SEO techniques to infect users by compromising legitimate WordPress sites. It manipulates search engine results to direct victims to fake forums, where they are tricked into downloading a malicious payload. The malware's multi-stage infection involves injecting code into WordPress sites, using heavily obfuscated JavaScript, and maintaining persistence through modified plugins. Despite being discovered in 2018, Gootloader remains active, with ongoing updates to its infrastructure. Security measures include web filtering, regular WordPress updates, and user awareness about downloading documents from unfamiliar sites.

Attack Type : SEO Poisoning

Cause of Issue : Malicious Payload

Industry Type : Legal and Business Industries

IoT Botnet Targets Global Infrastructure with Massive DDoS Attacks

A newly identified IoT botnet, leveraging malware derived from Mirai and Bashlite, has been launching large-scale DDoS attacks globally since late 2024. It exploits vulnerabilities in IoT devices like routers and IP cameras, infecting them through Remote Code Execution (RCE) or weak default passwords. The botnet uses multiple DDoS attack vectors such as SYN floods and UDP floods, and targets sectors like finance, transportation, and telecommunications, particularly in North America, Europe, and Japan. To mitigate the risk, experts recommend changing default passwords, updating firmware, and isolating IoT devices on separate networks.

Attack Type : DDoS Attack

Cause of Issue : RCE Vulnerabilities

Industry Type : Finance and Transportation

Top Critical CVEs – January 2025

1. CVE-2025-21298

Score : 9.8

This is a critical zero-click vulnerability in Windows Object Linking and Embedding (OLE) technology. It enables attackers to execute arbitrary code on a victim's system by sending a specially crafted email containing a malicious Rich Text Format (RTF) document. The flaw is triggered when the victim opens or previews the email in Microsoft Outlook, leading to remote code execution without requiring any user interaction.

Impact

Exploiting this vulnerability allows attackers to execute arbitrary code on the affected system. This can result in unauthorized access, the installation of malicious software, modification or deletion of data, and exposure of sensitive information. The fact that it is a zero-click attack makes it even more dangerous, as no user interaction is needed, increasing the likelihood of successful exploitation.

2. CVE-2025-22968

Score : 9.8

This critical security vulnerability affects the D-Link DWR-M972V router, specifically firmware version 1.05SSG. The flaw allows remote attackers to execute arbitrary code via SSH using the root account without restrictions. This could enable attackers to take full control of the device, modify configurations, intercept network traffic, or deploy malware.

Impact

Successful exploitation of this vulnerability could compromise the affected router, allowing unauthorized access, modification of system settings, and potential network disruptions. Attackers could use the compromised device to launch further attacks on connected systems or exfiltrate sensitive information.

3. CVE-2025-24480

Score : 9.3

This critical vulnerability affects Rockwell Automation's FactoryTalk View Machine Edition (ME) software, particularly versions prior to 15.0. The flaw arises from insufficient input sanitization, which enables remote attackers to execute arbitrary commands or code with elevated privileges. As a result, attackers could gain control of the system, making it a significant threat to industrial automation.

Impact

Exploiting this vulnerability could grant attackers unauthorized access to the system, enabling them to modify configurations or execute malicious code. This can result in data corruption, equipment damage, and safety hazards in industrial environments. The attack could also compromise critical infrastructure, causing downtime.

Top Critical CVEs – January 2025

4. CVE-2025-0650

Score : 8.1

A critical vulnerability has been identified in the Open Virtual Network (OVN). Specially crafted UDP packets can bypass egress access control lists (ACLs) in OVN installations configured with a logical switch that has DNS records set and egress ACLs configured. This flaw can lead to unauthorized access to virtual machines and containers running on the OVN network.

Impact

Exploiting this vulnerability allows attackers to bypass security controls, potentially gaining unauthorized access to virtual machines and containers within the OVN network. This unauthorized access can result in data breaches, system compromise, and disruption of services.

5. CVE-2025-0411

Score : 7.0

This critical vulnerability in 7-Zip allows remote attackers to bypass the Mark-of-the-Web (MotW) protection mechanism. MotW is a security feature in Windows that flags files downloaded from the internet as potentially unsafe. When extracting files from a crafted archive that bears the MotW, 7-Zip fails to propagate this flag to the extracted files. This oversight enables attackers to execute arbitrary code in the context of the current user, posing significant security risks.

Impact

Exploiting this vulnerability can lead to the execution of malicious code without user consent, potentially compromising system integrity and confidentiality. The flaw is particularly concerning because it allows attackers to bypass a fundamental security feature designed to protect users from internet-based threats. Given that 7-Zip is widely used for file compression and extraction, the impact of this vulnerability is extensive.

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