THREATSPLOIT

ADVERSARY REPORT

Edition-64

www.briskinfosec.com

Introduction :

In the dynamic and ever-evolving realm of cybersecurity, the "Threatsploit Adversary Report" for November 2023 stands as a crucial resource, providing a comprehensive overview of the latest threats and vulnerabilities in the digital landscape. This month's edition delves into a range of critical incidents and developments that have shaped the cybersecurity domain, offering insights into the methods and motivations of adversaries in the digital world.

Our November report highlights a series of significant cybersecurity incidents, including vulnerabilities in Windows drivers, destructive cyber attacks targeting the Iranian tech sector, and the exploitation of Apache and Citrix systems. We also uncover a sophisticated malware campaign aimed at Android users, masquerading as legitimate banking and governmental apps, and a concerning weakness in Bitcoin wallets stemming from a vulnerability known as "Randstorm."

These incidents, analyzed across various domains such as software development, finance, and biotechnology, reveal a pattern of exploitation, vulnerability, and social engineering tactics employed by cybercriminals. Each case study in the report is supplemented with detailed descriptions, references, and an assessment of the attack type and underlying causes.

As we navigate through these turbulent cyber waters, the November 2023 edition of the "Threatsploit Adversary Report" serves as a beacon, guiding cybersecurity professionals, stakeholders, and enthusiasts towards a deeper understanding of the challenges and strategies necessary for a secure digital future.

Best regards,
Briskinfosec Threat Intelligence Team.

Contents :

Researchers Find 34 Windows Drivers Vulnerable to Full Device Takeover

The research identifies 34 vulnerable Windows drivers within the Windows Driver Model (WDM) and Windows Driver Frameworks (WDF), exposing the potential for non-privileged threat actors to gain full device control, execute arbitrary code, manipulate firmware, and escalate privileges. Exploitation of drivers like AODDriver.sys, dellbios.sys, and stdcdrv64.sys could lead to kernel memory access, evading security measures like kernel address space layout randomization (KASLR) and even erasing system firmware, rendering devices unbootable. Furthermore, the study highlights WDF drivers, such as WDTKernel.sys and H2OFFT64.sys, not initially vulnerable but susceptible to being weaponized in Bring Your Own Vulnerable Driver (BYOVD) attacks by privileged threat actors to elevate privileges and disable security software, echoing concerns about expanding attack vectors beyond firmware access.

Attack Type : Exploitation

Cause of Issue : Vulnerability

Domain Name : Software Development Companies

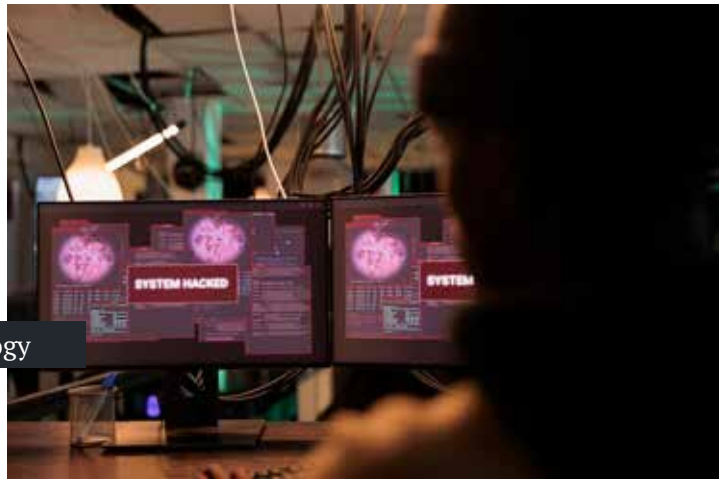
Iranian Hackers Launch Destructive Cyber Attacks on Israeli Tech and Education Sectors

Israeli higher education and tech sectors have experienced a series of destructive cyber attacks initiated in January 2023, involving previously undocumented wiper malware. These intrusions, continuing until October, are attributed to the Iranian hacking group Agonizing Serpens (also known as Agrius, BlackShadow, and Pink Sandstorm). The attacks aimed to steal sensitive data like personally identifiable information (PII) and intellectual property, followed by deploying novel wiper malware—MultiLayer, PartialWasher, and BFG Agonizer—and a bespoke tool called Sqlextractor to extract information from database servers. The attackers exploited vulnerable internet-facing web servers for initial access, utilizing web shells, conducting reconnaissance, stealing administrative credentials, lateral movement, data exfiltration using tools like WinSCP and PuTTY, culminating in deploying destructive wiper malware to render systems unusable. The group's evolution includes upgrading capabilities to bypass security measures, using a mix of known and custom tools to carry out attacks, posing a significant challenge to detection.

Attack Type : Cyberespionage

Cause of Issue : Exploitation

Domain Name : Pharmaceuticals and Biotechnology



Hackers are after vulnerable Apache and Citrix products

"Recent cybersecurity incidents highlight threats targeting Apache and Citrix vulnerabilities, urging immediate patching. Exploitation of Apache ActiveMQ and Apache Airflow flaws led to rapid attacks, including HelloKitty ransomware deployment. Cloud-managed Airflow instances by AWS and Google were left exposed initially but are now being updated. Citrix's NetScaler vulnerabilities enabled session takeovers, bypassing authentication. Excel-based malware is surging via deceptive invoices, while crypto developers faced complex attacks within trusted communities. Cloudflare's North American outage underscores infrastructure preparedness necessity, impacting critical services despite partial backup center measures."

Attack Type : Exploits

Cause of Issue : Vulnerability exploitation

Domain Name : Software Development Companies

Malicious Apps Disguised as Banks and Government Agencies Targeting Indian Android Users

A new malware campaign targeting Android smartphone users in India leverages social engineering tactics through WhatsApp and Telegram, enticing victims with fraudulent apps impersonating banks and government services. Once installed, these apps prompt users to input sensitive banking details and credentials, sending the stolen data to controlled servers. The malware also seeks permissions to intercept SMS, potentially exposing users to financial fraud. This incident highlights the risk posed by mobile banking trojans, emphasizing the need for cautious app installation and verifying app legitimacy to prevent such attacks. Additionally, recent Android malware instances, including SpyNote targeting Roblox users and Enchant focused on cryptocurrency wallets, reinforce the importance of vigilance and app source verification. Efforts by Google and Samsung to enhance security underscore the ongoing battle against Android-based threats, urging users to exercise scrutiny when downloading apps.

Attack Type : Malware

Cause of Issue : Social Engineering

Domain Name : Finance and Banking

Randstorm Exploit : Bitcoin Wallets Created b/w 2011-2015 Vulnerable to Hacking

A vulnerability termed "Randstorm()" affects Bitcoin wallets generated between 2011 and 2015, posing a risk of password recovery and unauthorized access to millions of bitcoins. This issue arises from weak cryptographic keys generated by the BitcoinJS package, reliant on the SecureRandom() function within the JSBN JavaScript library. Exploiting cryptographic weaknesses in web browsers' Math.random() implementation, attackers could exploit insufficient entropy to perform brute-force attacks and recover private keys. This underscores the susceptibility of foundational open-source dependencies and highlights supply chain risks, reminiscent of prior incidents like the Apache Log4j vulnerability. Notably, affected wallets remain vulnerable unless funds are transferred to new wallets created with updated software.

Attack Type : Exploitation

Cause of Issue : Weakness

Domain Name : Finance and Banking

27 Malicious PyPI Packages with Thousands of Downloads Found Targeting IT Experts

"An extensive threat actor campaign has targeted the Python Package Index (PyPI) repository for six months, distributing malware-laden typosquat packages disguised as popular Python libraries, infecting thousands of global users and stealing sensitive data. Employing steganography to conceal malicious payloads within innocuous image files and utilizing setup.py scripts, the attack aimed to deliver malware capable of achieving persistence, exfiltrating data, and accessing cryptocurrency wallets. Concurrently, ReversingLabs identified protest-themed npm packages embedding geopolitical messages related to conflicts in Ukraine and Israel, raising concerns about manipulation within open-source ecosystems. Additionally, revelations of thousands of leaked secrets in PyPI projects underscore the pervasive risks of exposing sensitive credentials, prompting heightened security measures and guidance from government agencies to mitigate software supply chain vulnerabilities"

Attack Type : Malware

Cause of Issue : Malicious Intent

Domain Name : Software Development Companies

Zero-Day Flaw in Zimbra Email Software Exploited by Four Hacker Groups

Multiple threat groups exploited a zero-day XSS vulnerability (CVE-2023-37580) in Zimbra Collaboration software, impacting versions before 8.8.15 Patch 41. Google TAG identified four distinct campaigns, with attacks ranging from email theft to phishing for credentials in government organizations across Greece, Moldova, Tunisia, Vietnam, and Pakistan. Exploitation involved sending malicious URLs in emails, executing scripts on victims' browsers upon clicking, and stealing email data and authentication tokens. Notably, attacks persisted even after Zimbra's patch release, emphasizing the urgency of prompt software updates and robust security measures for mail servers amidst increasing opportunistic exploitation of open-source vulnerabilities.

Attack Type : Exploitation

Cause of Issue : Vulnerability

Domain Name : Software Development Companies

Russian Cyber Espionage Group Deploys LitterDrifter USB Worm in Targeted Attacks

Russian cyber espionage actors tied to the FSB deployed the USB-propagating worm, LitterDrifter, targeting Ukrainian entities. This worm, spreading via USB drives and communicating with command-and-control servers, is suspected to be an evolution of a previous PowerShell-based worm. Employing VBS and using domains as placeholders for C&C servers, Gamaredon aimed for large-scale data collection, showing signs of global infection. In a separate instance, Russian state-sponsored hackers, APT29, exploited a WinRAR vulnerability, targeting European embassies, using phishing emails and crafted ZIP files. Ukrainian CERT unearthed a phishing campaign deploying Remcos RAT, showcasing ongoing cyber threats faced by state entities.

Attack Type : Worm

Cause of Issue : Exploitation

Domain Name : Software Development Companies

CacheWarp Attack : New Vulnerability in AMD SEV Exposes Encrypted VMs

A research team disclosed CacheWarp (CVE-2023-20592), a software fault attack affecting AMD's Secure Encrypted Virtualization (SEV) technology, enabling threat actors to infiltrate encrypted virtual machines (VMs) and perform privilege escalation. Exploiting the 'INVD' instruction, the attack allows for cache manipulation, time manipulation (timewarp), and data reset (Dropforge), ultimately granting unlimited access to the VM. AMD issued a fix via microcode update, addressing the instruction misuse. This follows previous vulnerabilities like Collide+Power, highlighting threats to CPU security despite efforts in secure execution environments.

Attack Type : Exploitation

Cause of Issue : Architectural Vulnerability

Domain Name : Finance and Banking

Vietnamese Hackers Using New Delphi-Powered Malware to Target Indian Marketers

Vietnamese threat actors behind Ducktail stealer shifted tactics, targeting Indian marketing professionals by employing Delphi-based malware in a campaign from March to October 2023. They spread malware via deceptive job-change-related archives, hijacking Facebook business accounts to run illicit ads. The malware downloads rogue components, alters browser shortcuts, and deploys extensions masquerading as legitimate Google Docs add-ons, aiding in data theft and control of open tabs. This coincides with Google's legal action against unknown individuals in India and Vietnam for distributing malware via fake generative AI tool links on social media, highlighting ongoing threats to users' credentials and privacy. Meta also observed similar deceptive browser extensions, emphasizing the persistence of such tactics across social media platforms.

Attack Type : CredentialTheft

Cause of Issue : : Deception

Domain Name : Finance and Banking

New BiBi-Windows Wiper Targets Windows Systems in Pro-Hamas Attacks

Cybersecurity researchers have cautioned about a Windows version of a wiper malware previously seen targeting Linux systems in cyber attacks aimed at Israel. Dubbed BiBi-Windows Wiper, this counterpart of BiBi-Linux Wiper was utilized by a pro-Hamas hacktivist group during the Israel-Hamas conflict. The expansion to Windows signifies an escalated threat to end-user machines and application servers, as indicated by BlackBerry. Compiled on October 21, 2023, the malware overwrites data in the C:\Users directory, deletes shadow copies, and exhibits multithreading functionality similar to its Linux variant. While it's uncertain if deployed in real-world attacks, Security Joes highlighted that BiBi-Linux Wiper is part of a larger campaign targeting Israeli entities, observing tactical parallels with a group linked to Iran called Moses Staff. This campaign, while focused on Israeli sectors, involves groups historically targeting diverse sectors and regions.

Attack Type : Data destruction

Cause of Issue : Geopolitical tensions

Domain Name : Manufacturing and Industrial Control Systems (ICS)

New 'HrServ.dll' Web Shell Detected in APT Attack Targeting Afghan Government

A new web shell, dubbed HrServ, was found targeting an unspecified Afghan government entity in a suspected APT attack. This sophisticated DLL web shell, dating back to early 2021, employs complex encoding for communication and in-memory execution. It operates through a malicious attack chain involving PAExec and creates a scheduled task masquerading as a Microsoft update. The shell responds to HTTP requests, mimicking Google services to evade detection. It has various functionalities controlled by parameters, including code execution and data manipulation. Furthermore, it deploys a memory implant to erase traces of its presence. Despite indications of financially motivated activity, its operational methods align with APT behavior. The malware author's linguistic traits suggest a non-native English speaker.

Attack Type : Web Shell

Cause of Issue : Government Targeting

Domain Name : Software Industry

Hamas-Linked Cyberattacks Using Rust-Powered SysJoker Backdoor Against Israel

Cybersecurity researchers have uncovered a Rust version of SysJoker, a cross-platform backdoor previously linked to a Hamas-affiliated threat actor targeting Israel amid regional conflicts. This updated variant, rewritten entirely in Rust, indicates significant code reworking while maintaining core functionalities. Notable changes include shifting from Google Drive to OneDrive for storing command-and-control server URLs. The backdoor, capable of executing remote commands and downloading new malware, now employs random sleep intervals, possibly to evade detection. Its utilization of OneDrive enables quick C2 address changes, aiding in avoiding reputation-based services. While unattributed, evidence suggests connections between SysJoker and Operation Electric Powder, a previous campaign against Israeli organizations, possibly involving the Hamas-linked threat actor known as Molerats. Recent analysis links SysJoker and its Rust variant to a new hacking group named WildCard, suggesting phishing campaigns to distribute trojanized software. These attacks exhibit persistent targeting of critical Israeli sectors, potentially including education and IT infrastructure. The migration to Rust possibly aims to simplify multi-platform targeting and hinder analysis

Attack Type : Backdoor Malware

Cause of Issue : Regional Conflict

Domain Name : Software Development Companies

N. Korean Hackers Distribute Trojanized CyberLink Software in Supply Chain Attack

North Korean threat actors, operating under the alias Diamond Sleet, are executing a trojanized supply chain attack, leveraging a tampered CyberLink application installer to target downstream customers. This modified installer, distributed via the company's update infrastructure, includes a malicious payload that downloads a second-stage threat. While impacting over 100 devices across multiple countries, the attackers' connections to North Korea stem from their utilization of compromised command-and-control servers. Known for targeting IT, defense, and media sectors, this group, part of the Lazarus Group, operates under various aliases and has been active since 2013. Despite the distribution of the tampered installer, no direct manipulation within target environments was observed. This incident aligns with a series of software supply chain attacks by North Korean actors, prompting warnings and advisories from South Korea and the U.K. regarding heightened threats, urging enhanced security measures to combat these sophisticated attacks.

Attack Type : Trojanized Installer

Cause of Issue : State-sponsored Targeting

Domain Name : Software Development Companies

East Texas hospital network can't receive ambulances because of potential cybersecurity incident

A hospital network in East Texas, UT Health East Texas, faces a potential cyber incident, halting ambulance access to emergency rooms since Thanksgiving Day. The network employs downtime procedures as investigations and efforts to restore computer systems continue. This incident mirrors a concerning trend of cyberattacks affecting hospitals nationwide, diverting ambulances in multiple states over recent months. Despite efforts, the network remains uncertain about the timeline for network restoration. Federal agencies like the Department of Health and Human Services and CISA, responsible for assisting hospitals in cybersecurity defense, have not yet responded to requests for comment. The ongoing struggle with cyber threats in the healthcare sector persists, highlighting vulnerabilities even amid increased attention and efforts to bolster defenses.

Attack Type : Cybersecurity Incident

Cause of Issue : Potential Breach

Domain Name : Healthcare Industry

General Electric investigates claims of cyber attack, data theft

A threat actor known as IntelBroker claimed to have breached General Electric's development environment, attempting to sell access to the company's development and software pipelines on a hacking forum. After initial unsuccessful attempts, the actor later advertised both network access and allegedly stolen data, including DARPA-related military information from GE Aviation. General Electric acknowledged the claims and is investigating the potential data leak. IntelBroker, known for previous successful cyberattacks, was involved in high-profile breaches, including accessing sensitive information from DC Health Link, leading to widespread media coverage and a congressional investigation into the breach's cause, involving a misconfigured server that exposed the data online

Attack Type : Data Breach

Cause of Issue : Network Access

Domain Name : Energy and Utilities

Alert : F5 Warns of Active Attacks Exploiting BIG-IP Vulnerability

F5 issued a warning following active exploitation of a critical security vulnerability, CVE-2023-46747, in BIG-IP systems. This flaw allows unauthenticated attackers to execute arbitrary system commands through the management port, affecting multiple software versions. Additionally, threat actors are leveraging CVE-2023-46748, an authenticated SQL injection flaw, chained with the first vulnerability, enabling the execution of arbitrary system commands. The company observed attackers exploiting these vulnerabilities, urging users to check for compromise indicators. The Shadowserver Foundation reported attempts of CVE-2023-46747 exploitation since October 30, emphasizing the urgency of applying patches. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added these flaws to its list of actively exploited vulnerabilities, mandating patch application by November 21, 2023, for federal agencies.

Attack Type : Command Execution

Cause of Issue : Software Vulnerability

Domain Name : Software Development Companies

New Ransomware Group Emerges with Hive's Source Code and Infrastructure

The emergence of Hunters International, inheriting assets from the defunct Hive ransomware group, signals a shift in the threat landscape. While the Hive group ceased operations earlier in 2023, their core developers passed on source code and infrastructure, allowing Hunters International to emerge. The new group focuses on data exfiltration alongside encryption, distinguishing itself as a data extortion outfit. Adopting Rust-based foundations, the ransomware has undergone simplification, improving encryption processes and minimizing verbosity. However, the true extent of their threat potential remains uncertain as Hunters International aims to establish its prowess and attract proficient affiliates in the cybersecurity sphere.

Attack Type : Data Extortion

Cause of Issue : Source Code Transfer

Domain Name : Software Industry

Alert: 'Effluence' Backdoor Persists Despite Patching Atlassian Confluence Servers

Cybersecurity researchers discovered the "Effluence" backdoor through an exploited Atlassian Confluence flaw (CVE-2023-22515). This persistent threat allows remote access and unauthorized admin account creation. A subsequent flaw (CVE-2023-22518) worsened the situation. Effluence enables covert entry, data theft, and even manipulating server logs, posing a severe threat across Atlassian products, potentially affecting JIRA and Bitbucket

Attack Type : Remote Access

Cause of Issue : Atlassian Security Flaw

Domain Name : Software Development Companies

GoTitan Botnet Spotted Exploiting Recent Apache ActiveMQ Vulnerability

Threat actors are exploiting a critical vulnerability in Apache ActiveMQ (CVE-2023-46604) to distribute malware including GoTitan, a botnet for DDoS attacks, and PrCtrl Rat, a remote access trojan. The attacks involve dropping payloads onto breached servers, launching various malware such as GoTitan designed for DDoS attacks. Another threat, PrCtrl Rat, establishes remote control over the infected system but its motive remains unclear. These exploits highlight ongoing security risks within vulnerable Apache ActiveMQ servers.

Attack Type : Exploitation

Cause of Issue : Vulnerability

Domain Name : Apache Server

Design Flaw in Google Workspace Could Let Attackers Gain Unauthorized Access

A critical vulnerability in Google Workspace's domain-wide delegation (DWD) feature allows threat actors to exploit privilege escalation, potentially granting unauthorized access to Workspace APIs without requiring super admin privileges. Named DeleFriend, this design flaw permits manipulation of existing delegations in Google Cloud Platform (GCP) and Workspace, bypassing the need for super admin credentials. Despite Google disputing it as a design flaw, the issue lies in how domain delegation relies on service account identifiers (OAuth IDs) rather than specific private keys. Threat actors, leveraging this weakness, can create numerous JSON web tokens, aiming to identify successful combinations of private key pairs to enable domain-wide delegation. Successful exploitation enables unauthorized actions across Gmail, Drive, and other Workspace services, impacting every identity within the domain. Hunters provided a proof-of-concept to detect misconfigurations, emphasizing the severe consequences of such exploits on Workspace's security.

Attack Type : Privilege Escalation

Cause of Issue : Design Flaw

Domain Name : Software Industry

N. Korean Hackers 'Mixing' macOS Malware Tactics to Evade Detection

North Korean threat actors are blending RustBucket and KANDYKORN macOS malware elements, using RustBucket as a conduit for KANDYKORN. SentinelOne found connections, tying ObjCShellz to RustBucket. SwiftLoader, linked to Lazarus, now distributes KANDYKORN, echoing a trend of North Korean groups sharing tactics. Their updated SwiftLoader variant, disguised as "EdoneViewer," likely fetches KANDYKORN. Andariel, a Lazarus subgroup, was tied by AhnLab Security to attacks exploiting an Apache ActiveMQ flaw to deploy NukeSped and TigerRAT backdoors.

Attack Type : Hybridization

Cause of Issue : Tool Mixing

Domain Name : Data Breach

MGM Resorts : Slot machines go down in cyber-attack on firm

MGM Resorts encountered operational disruptions due to a recent cyber-attack, impacting systems for slot machines, online bookings, and digital keys. Guests faced inconveniences such as room key malfunctions, leading to the distribution of physical keys, and disruptions in various services like reservations, payments, and account logins. The company initiated an investigation with cybersecurity experts' assistance, law enforcement was notified, and specific systems were shut down to protect data. Although the attack's nature and extent are still being investigated, the resorts' essential operations, including dining, entertainment, and gaming, remained functional. However, the company's main website and resort-specific sites were inaccessible, redirecting visitors to contact via phone or third-party websites. MGM Resorts previously faced a cybersecurity breach in 2019, where customer records were compromised, raising concerns about potential data theft in the current incident.

Attack Type : Cyber-Attack

Cause of Issue : Cybersecurity Breach

Domain Name : Healthcare domain

Boeing Says Business Hit By "Cyber Incident" After Ransomware Threat

Boeing, a major defense and aerospace contractor, disclosed an ongoing investigation into a cyber incident affecting parts of its distribution business, following a threat from the Lockbit cybercrime gang. The gang claimed to have stolen sensitive data and threatened to release it if a ransom wasn't paid by a specific date. Boeing emphasized that the incident did not affect flight safety and reassured ongoing cooperation with law enforcement and regulatory authorities. Some webpages related to the affected division were temporarily down due to technical issues.

Lockbit, a prominent ransomware group, has a history of encrypting systems and extorting sensitive data. However, it remains uncertain what specific information Lockbit may have obtained from Boeing. Security experts caution against expecting data deletion even if ransom is paid, highlighting potential risks associated with data exposure. The potential impact on defense-related information remains unspecified, and neither Boeing nor the U.S. Cybersecurity and Infrastructure Security Agency (CISA) commented on this aspect.

Attack Type : Ransomware

Cause of Issue : Cyber Extortion

Domain Name : Manufacturing and Industrial Control Systems (ICS)

Okta Discloses Broader Impact Linked to Support System Breach

Okta revealed an extension of the breach's impact, acknowledging additional threat actor activity related to the October 2023 incident involving their support case management system. The breach led to the download of names and email addresses of all users within the Okta customer support system, affecting most Okta Workforce Identity Cloud and Customer Identity Solution customers, excluding specific separate environments. Although Okta reported no evidence of immediate misuse, they alerted customers to potential risks of phishing and social engineering while implementing new security measures. The company continues its investigation, promising notifications to affected individuals. The breach's origins remain unclear, but previous attacks by the Scattered Spider group on Okta's systems underscore the group's sophisticated methods, notably infiltrating systems within an hour and affiliating with ransomware operations. This ongoing activity emphasizes the group's expertise in navigating both cloud and on-premises environments.

Attack Type : Data Breach

Cause of Issue : Breach in support system

Domain Name : (SaaS) Providers

Briskinfosec Technology and Consulting Pvt ltd,

No : 21, 2nd Floor, Krishnama Road,

Nungambakkam, Chennai - 600034, India.

Office : +044 4352 4537 | Mobile : +91 86086 34123

contact@briskinfosec.com | www.briskinfosec.com