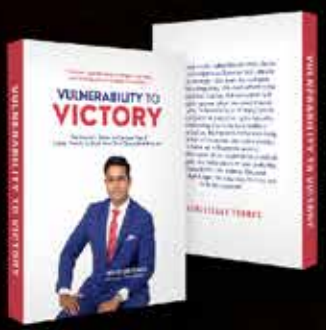
BRISKINFOSEC

CYBER TRUST & ASSURANCE

Edition - 74

Threatsploit Adversary Report

Oct - 2024



GITEX GLOBAL 14-18 OCT 2024 DUBAI WORLD TRADE CENTRE

Meet us - H23-C16C

Introduction:

Welcome to the October 2024 edition of the Threatsploit Adversary Report, where we shine a spotlight on the alarming rise of cyber threats impacting industries across the globe. This month, our focus turns to a notable cyberattack and supply chain compromise in pager devices in Lebanon, illustrating the intricate geopolitical factors that contribute to digital exploitation in today's interconnected world.

We also dive into the serious implications of Necro malware, which has infiltrated over 11 million Android devices through malicious SDKs, highlighting an urgent call for enhanced mobile app security measures. In a troubling trend, developers on Roblox are grappling with an ongoing threat from a malicious npm package designed for brandjacking, exposing vulnerabilities in widely-used platforms.

Adding to these concerns, we investigate KTLVdoor, a new breed of backdoor malware specifically targeting Chinese trading companies, underscoring the escalating risk of cyber espionage. Moreover, North Korean hackers exploiting zero-day vulnerabilities in Chrome to penetrate software development firms exemplify the growing sophistication of nation-state cyberattacks.

Our dedicated analysts have meticulously compiled insights into these pressing threats, detailing their origins, the industries affected, and the attack vectors employed. This report serves as an essential resource for cybersecurity professionals and business leaders alike.

Best wishes for a secure month ahead!

Best regards,

Briskinfosec Threat Intelligence Team.

- *Top Cyberattacks in the Last 31 Days According to Industry*
- *Top 5 YouTube Channels for Cybersecurity*
- *We are exhibiting - GITEX Global 2024*

Contents:

Cyber Attack in Lebanon: Exposing the Modern Battlefield of Warfare

A recent cyber attack in Lebanon has transformed Hezbollah's once-secure pager network into a weapon, leading to explosions that killed at least nine people and injured over 2,800. This incident highlights a new era of warfare where cyber attacks can trigger real-world destruction. Experts suspect Israeli involvement, suggesting that even outdated technologies can be vulnerable to manipulation. The attack underscores the growing significance of cyberspace in military strategies, revealing that no system is immune to cyber threats. As conflicts evolve, the potential for such attacks to disrupt societies and critical infrastructure is becoming increasingly concerning.

Attack Type : Cyber Exploitation | Cause of Issue : Device Manipulation | Industry : Telecommunication

Necro Malware Targets 11 Million Android Devices Through Google Play

Malicious advertising SDKs embedded in legitimate apps and game mods installed a new version of the Necro malware loader on 11 million Android devices. Kaspersky discovered the malware in two popular Google Play apps: Wuta Camera and Max Browser. Necro installs adware, facilitates subscription fraud, and uses infected devices as proxies for malicious traffic. It spread through official and unofficial app stores, including mods of apps like WhatsApp and Spotify. Google Play removed the infected apps, but they may still compromise many devices.

Attack Type : Supply chain attack | Cause of Issue : Malicious SDK | Industry : Mobile App Development

Roblox Developers Targeted by Malicious npm Packages Disguised as 'noblox.js'

Roblox developers are targeted by a persistent malware campaign using fake npm packages that mimic the popular "noblox.js" library to steal sensitive data. The malicious packages, like "noblox.js-async" and others, deliver stealer malware and Quasar RAT, allowing attackers remote access to systems. Techniques such as brandjacking and starjacking are used to make the packages appear legitimate. The malware also evades detection by modifying antivirus settings and establishing persistence through Windows Registry changes. The attack is part of an ongoing effort to compromise systems via the open-source ecosystem.

Attack Type : Brandjacking | Cause of Issue : Fake Packages | Industry : Software Development Companies

KTLVdoor: New Malware Targets Chinese Trading Company

The Chinese-speaking cyber threat actor Earth Lusca has deployed a new backdoor malware called KTLVdoor, targeting a trading company in China. Written in Golang, KTLVdoor is cross-platform and can operate on both Windows and Linux systems. It masquerades as a legitimate system utilities and enables various malicious tasks, including file manipulation and command execution. Notably, over 50 command-and-control servers linked to the malware are hosted on Alibaba, suggesting potential shared infrastructure with other Chinese threat actors. Earth Lusca has been active since at least 2021 and shows overlaps with groups like APT27. The full distribution methods and broader targets of KTLVdoor remain unclear.

Attack Type : Backdoor access | Cause of Issue : System exploitation | Industry : Trading company

North Korean Cybercriminals Use Chrome Zero-Day Exploit to Deploy FudModule Rootkit

A recently patched zero-day vulnerability in Google Chrome (CVE-2024-7971) was exploited by North Korean actors, known as Citrine Sleet, to deliver the FudModule rootkit. This campaign targeted cryptocurrency-related individuals and organizations through social engineering, directing victims to a malicious site that exploited the flaw for remote code execution (RCE). Citrine Sleet, part of the Lazarus Group, has previously used various Windows zero-day exploits and is known for targeting financial institutions. The attack chain also exploited another Windows kernel privilege escalation bug (CVE-2024-38106) to gain deeper system access. The incident underscores the importance of keeping systems updated and employing comprehensive security measures to detect such threats.

Attack Type : Zero-Day Exploit

Cause of Issue : RCE

Industry : Software Development Companies

Chinese Hackers Utilize GeoServer Vulnerability to Deploy EAGLEDOOR Malware Across APAC Regions

The Chinese APT group Earth Baxia targeted government and energy sectors in Taiwan and other Asia-Pacific countries using a critical vulnerability in GeoServer (CVE-2024-36401). The attack involved spear-phishing emails and malware like Cobalt Strike and EAGLEDOOR to steal data and deploy malicious payloads. The malware used various communication methods (DNS, HTTP, TCP, and Telegram) and exploited public cloud services for malicious activities. The campaign demonstrated sophisticated, multi-stage infection techniques.

Attack Type : Spear phishing

Cause of Issue : GeoServer vulnerability exploitation

Industry : Government Agencies, Energy Sector

Default Credentials in FOUNDATION Software Used by Hackers to Compromise Construction Companies

Threat actors are targeting the construction sector by exploiting vulnerabilities in FOUNDATION Accounting Software. They have been brute-forcing the software using default credentials, gaining access to high-privileged accounts like "sa" and "dba." This allows them to execute arbitrary shell commands via the MS SQL Server, which has been exposed on public networks. Huntress reported about 35,000 brute-force attempts detected on September 14, 2024, with 33 out of 500 hosts found to be publicly accessible with unchanged default credentials. Recommendations for mitigation include rotating credentials, restricting public access, and disabling the xp_cmdshell option.

Attack Type : Brute force attack

Cause of Issue : Default credentials

Industry : Construction Industry

New PondRAT Malware Concealed in Python Packages Aims at Software Developers

Threat actors linked to North Korea, specifically a group known as Gleaming Pisces, are using poisoned Python packages to deliver new malware called PondRAT. This malware is a lighter version of the previously known POOLRAT and is part of an ongoing campaign dubbed Operation Dream Job, which entices targets with job offers to download malicious software. The attackers uploaded several malicious packages to the Python Package Index (PyPI), including "real-ids," "coloredtxt," "beautifultext," and "minisound." Once installed on developer systems, these packages execute encoded instructions that download and run the malware. PondRAT has capabilities to upload and download files, execute commands, and pause operations. The campaign highlights the risks associated with using legitimate-looking open-source packages, which can lead to significant network compromises if malicious packages are successfully installed. Additionally, there are reports of North Korean threat actors submitting fake resumes to various companies, posing a serious risk to organizations with remote employees.

Attack Type : Malware Delivery

Cause of Issue : Poisoned Python Packages

Industry : Software Development Companies

Destructive Cyber Attacks by Hacktivist Group Twelve Focus on Russian Organizations

The hacktivist group Twelve, active since April 2023, targets Russian entities with destructive cyber attacks using publicly available tools. Unlike traditional ransomware groups, Twelve focuses on crippling infrastructure rather than seeking ransom. Their methods involve encrypting data and deploying wipers to ensure recovery is impossible. The group gains initial access through credential abuse and uses Remote Desktop Protocol (RDP) for lateral movement, sometimes exploiting contractors' access. Twelve is linked to the ransomware group DARKSTAR, but their goals are more aligned with hacktivism. They employ various tools for credential theft and network exploration, disguising their malware as legitimate software to evade detection. Exploiting known vulnerabilities, they use LockBit 3.0 ransomware and wiper malware reminiscent of Shamoon, emphasizing their reliance on publicly accessible malware tools.

Attack Type : Destructive Cyberattacks

Cause of Issue : Exploitation Vulnerabilities

Industry : Information Technology

Cencora's Cyber Crisis: Record $75 Million Ransom Paid to Hackers

Cencora Inc., previously known as AmerisourceBergen, suffered a major cyberattack that led to a record ransom payment of $75 million, the largest known cyber extortion payment to date. Initially demanded to pay $150 million, the company made the payment in Bitcoin in March after confirming the theft of sensitive data in February. Despite the hefty payout, there is no guarantee that the stolen data will remain private. Cencora reported $31.4 million in additional expenses related to the breach, highlighting the rising financial stakes in cyber extortion, especially in critical sectors like healthcare. Experts caution that paying ransoms may not effectively resolve the threat, as it does not ensure the stolen data's safety.

Attack Type : Ransomware

Cause of Issue : Insecure Systems

Industry : Healthcare Industry

New Strains of Malware Disrupt Security Measures

Quorum Cyber's Incident Response team has identified SharpRhino, a malware linked to the Hunters International ransomware group, which spreads via a fake Angry IP Scanner domain. SharpRhino acts as a Remote Access Trojan, allowing attackers to modify systems, deploy additional malware, and encrypt files for ransom. Hunters International has quickly become a major threat since its emergence in October 2023, conducting 134 attacks by early 2024 as a Ransomware-as-a-Service provider. Additionally, a developing trojan named BlankBot targets Turkish Android users, capturing keystrokes and recording screens. Another ransomware, CryptoKat, uses AES encryption and complicates recovery by not storing decryption keys on victims' machines. Organizations are urged to enhance cybersecurity measures to combat these threats.

Attack Type : Ransomware

Cause of Issue : Typosquatting attack

Industry : Software Development Companies

Microchip ASF Security Flaw Leaves IoT Devices Vulnerable to Remote Attacks

A critical security vulnerability, tracked as CVE-2024-7490, has been identified in the Microchip Advanced Software Framework (ASF), allowing for potential remote code execution through a stack-based overflow due to inadequate input validation. With a CVSS score of 9.5, the flaw affects ASF version 3.52.0.2574 and earlier, posing risks as the software is unsupported. There are currently no fixes available, necessitating the replacement of the vulnerable tinydhcp service. Additionally, a severe zero-click vulnerability (CVE-2024-20017) in MediaTek Wi-Fi chipsets, with a CVSS score of 9.8, also allows for remote code execution through a buffer overflow caused by unchecked packet data. A patch was released in March 2024, but the risk of exploitation has increased following the publication of a proof-of-concept exploit.

Attack Type : Remote Code Execution

Cause of Issue : Input Validation

Industry : Internet of Things (IoT)

TeamTNT Launches Cryptojacking Attack on CentOS Servers Using Rootkit

TeamTNT, a cryptojacking operation, has resurfaced with a new campaign targeting CentOS-based Virtual Private Server (VPS) infrastructures. Researchers from Group-IB reported that the attack begins with a brute force SSH attack, allowing the threat actor to upload a malicious script. This script disables security features, deletes logs, and terminates cryptocurrency mining processes. It also sets up the Diamorphine rootkit for concealing malicious activities and establishes persistent remote access to the compromised systems. The attack script checks for prior infections, modifies SSH and firewall configurations, and creates a backdoor account with root access to maintain control over the systems.

Attack Type : Cryptojacking Attack

Cause of Issue : SSH brute force

Industry : Information Technology

GitLab Resolves Critical Authentication Issue in CE and EE Editions with SAML Update

GitLab has released patches to fix a critical vulnerability (CVE-2024-45409) in its Community Edition (CE) and Enterprise Edition (EE), which could allow attackers to bypass authentication due to improper verification of the SAML Response in the ruby-saml library. This flaw, rated with a CVSS score of 10.0, enables unauthenticated users with access to any signed SAML document to forge a SAML response, allowing them to log in as arbitrary users within the vulnerable system. GitLab has urged users to enable two-factor authentication (2FA) and disallow SAML two-factor bypass to mitigate risks. While there are no confirmed exploits in the wild, GitLab has noted signs of attempted exploitation.

Attack Type : Authentication Bypass

Cause of Issue : Input Validation

Industry : Software Development Companies

BingX Faces $44 Million Loss After Cryptocurrency Theft Incident

BingX, a Singaporean crypto platform, reported a cyberattack resulting in the theft of over $44 million. The attack was detected when abnormal network access indicated a breach of BingX's hot wallet. In response, the platform suspended withdrawals and began transferring assets to mitigate losses. An audit by blockchain security firm SlowMist confirmed approximately $44.7 million in losses, with other estimates suggesting up to $48 million. BingX's chief product officer announced that the company would fully compensate for the losses using its own capital, and that trading services would continue normally. Law enforcement is also intensifying efforts to protect cryptocurrency users amid rising security incidents affecting various Asia-based crypto platforms.

Attack Type : Cryptocurrency Theft

Cause of Issue : Hot wallet compromise

Industry : Cryptocurrency industry

Ransomware Breach in Kansas County Compromises Data of Nearly 30,000 Residents

Franklin County, Kansas, reported that a ransomware attack on May 19 leaked the personal data of approximately 29,690 residents. The breach involved access to sensitive information from the County Clerk's Office, including names, Social Security numbers, driver's license numbers, and medical records. The following day, the county discovered the attack and reached out to cybersecurity experts and law enforcement. An investigation found no evidence that the stolen data was released on the Dark Web. The county has taken steps to enhance security and notified regulators about the incident. Ransomware attacks have increasingly targeted government organizations in Kansas and Missouri over the past two years.

Attack Type : Ransomware Attack

Cause of Issue : Inadequate cybersecurity

Industry : Government Sector

London High School Closes Temporarily Due to Ransomware Attack

A high school in South London, Charles Darwin School, has closed for the first half of the week following a ransomware attack that affected approximately 1,300 students. The attack was confirmed after an initial IT issue was found to be more severe than expected. All staff devices have been removed for cleansing, and students' Microsoft 365 accounts have been disabled as a precaution. A cybersecurity firm is conducting a forensic investigation, but details on the extent of the data breach remain unclear. This incident highlights a growing trend of ransomware attacks on educational institutions in the U.K., with a record number of incidents reported in recent years.

Attack Type : Ransomware Attack

Cause of Issue : Unauthorized access

Industry : Educational

Two Arrested for Allegedly Stealing and Laundering $230 Million in Cryptocurrency

Two individuals, Malone Lam (20) and Jeandiel Serrano (21) were arrested by the U.S. Department of Justice in Miami for stealing over $230 million in cryptocurrency. Since August 2024, they allegedly conspired to hack victim cryptocurrency accounts and launder the stolen funds through various exchanges and mixing services. The theft included more than 4,100 Bitcoin taken from a victim in Washington, D.C. They reportedly used the laundered money to finance luxury purchases and travel.

Attack Type : Cryptocurrency Theft

Cause of Issue : Account Compromise

Industry : Cryptocurrency industry

Europol Executes Major Takedown of iServer Phishing Scheme and Ghost Criminal Network

The Federal Communications Commission (FCC) has settled with AT&T for $13 million following an investigation into a data breach that exposed customer information from approximately 9 million wireless accounts due to a vendor's failure to protect data. The breach occurred in January 2023 and involved Customer Proprietary Network Information (CPNI) such as account numbers and email addresses, but did not include sensitive details like credit card numbers or Social Security numbers. AT&T was found to have inadequately monitored the vendor's compliance with data protection requirements. As part of the settlement, AT&T will enhance its data governance practices, implement a comprehensive Information Security Program, and conduct annual compliance audits. The company has also faced additional breaches, including a significant incident in April 2024 that compromised call logs for around 109 million customers.

Attack Type : Credential Theft

Cause of Issue : Phishing Platform

Industry : Telecommunication

Critical Vulnerability in Grafana Plugin SDK (CVE-2024-8986) Poses Risk of Sensitive Data Exposure

A critical security vulnerability, tracked as CVE-2024-8986 with a CVSS score of 9.1, has been identified in the Grafana Plugin SDK for Go. This vulnerability allows the inadvertent leakage of sensitive information, such as repository credentials, due to the inclusion of build metadata in compiled binaries. Developers often embed credentials in their repository URIs for private dependencies, leading to exposure when the plugin is built. All versions up to 0.249.0 are affected, and users are urged to upgrade to version 0.250.0 or later immediately and review any exposed credentials to mitigate potential unauthorized access.

Attack Type : Information Disclosure

Cause of Issue : Build Metadata

Industry : Software Development Companies

API Security Breaches and Bot Attacks Lead to $186bn in Global Costs

A new study by Thales reveals that increased API adoption and the rise of AI-powered bot attacks are costing global organizations between $94 billion and $186 billion annually. The report highlights that costs related to insecure APIs have surged from $12 billion in 2021 to between $35 billion and $87 billion today, while bot attacks could account for up to $116 billion in losses. Factors contributing to these security incidents include rapid API adoption, inadequate in-house expertise, and poor communication between security and development teams. Larger companies, especially those with revenues over $100 billion, face a higher proportion of these threats, which make up 26% of their security incidents compared to an average of 12%. The report emphasizes the need for organizations to integrate security strategies for both bot and API attacks to mitigate the economic impact.

Attack Type : Bot Attacks

Cause of Issue : Insecure APIs

Industry : Information Technology

MOIS-Linked UNC1860 APT Facilitates Cyber Attacks in the Middle East

An Iranian advanced persistent threat (APT) group, known as UNC1860, is likely linked to the Ministry of Intelligence and Security (MOIS) and acts as an initial access facilitator for remote network access. Mandiant has identified UNC1860's advanced toolset, including specialized backdoors and malware controllers TEMPLEPLAY and VIROGREEN, designed for gaining persistent access to high-priority networks. The group first emerged in July 2022 during ransomware attacks in Albania and has been implicated in ongoing cyber intrusions throughout the Middle East. Their tactics involve exploiting vulnerable internet-facing servers to deploy malicious payloads, while also showing overlaps with other Iranian APTs like APT34. Recent activities indicate attempts to influence U.S. elections by stealing non-public material from political campaigns.

Attack Type : APT Attack

Cause of Issue : IServer exploitation

Industry : Telecommunication

Active Cyberattacks Target Critical Vulnerability in Ivanti Cloud Appliance

Ivanti has announced that a critical security flaw, CVE-2024-8963, affecting its Cloud Service Appliance (CSA), is actively being exploited. This vulnerability has a CVSS score of 9.4 and allows remote unauthenticated attackers to access restricted functionalities. It can be exploited in conjunction with another flaw, CVE-2024-8190, which lets attackers bypass admin authentication and execute arbitrary commands. Ivanti has reported that a limited number of customers have already been compromised. In response, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added this vulnerability to its Known Exploited Vulnerabilities catalog, mandating federal agencies to implement fixes by October 10, 2024. Users are urged to upgrade to CSA version 5.0, as version 4.6 is no longer supported.

Attack Type : Remote Code Execution

Cause of Issue : Insecure Path

Industry : Information Technology

Microsoft macOS App Vulnerabilities Could Grant Hackers Full System Access

Eight vulnerabilities in Microsoft macOS apps like Outlook, Teams, Word, Excel, and OneNote could allow attackers to gain elevated privileges or access sensitive data by bypassing macOS's Transparency, Consent, and Control (TCC) framework. By injecting malicious libraries into these apps, attackers could exploit their permissions, potentially sending emails, recording audio/video, or accessing sensitive data without user knowledge. While these attacks require some initial access, they highlight the risk of trusted apps acting as proxies for unauthorized actions. Microsoft considers the flaws low-risk but has patched OneNote and Teams to address the issue.

Attack Type : Library Injection

Cause of Issue : unsigned plugins

Industry : Software Development Companies

Massive Raptor Train IoT Botnet Breaches 200,000 Devices Worldwide

Cybersecurity researchers uncovered a Chinese state-sponsored botnet called Raptor Train, which has infected over 200,000 small office/home office (SOHO) and IoT devices since 2020. Managed by the Chinese group Flax Typhoon, the botnet uses a three-tiered structure to control compromised devices like routers, IP cameras, and NAS servers. The botnet, which peaked at 60,000 active devices in June 2023, has been used for reconnaissance and potential attacks on U.S., Taiwanese, and global targets in sectors like government, military, IT, and telecommunications. Despite no DDoS attacks being detected, the U.S. Department of Justice dismantled the botnet in a law enforcement operation, seizing the infrastructure and disabling the malware from infected devices. The botnet, linked to the Beijing-based company Integrity Technology Group, utilized the Sparrow platform for control and exploitation of the infected devices.

Attack Type : Botnet Attack

Cause of Issue : Vulnerable IoT

Industry : Information Technology

Clipper Malware on the Rise: Binance Warns Cryptocurrency Holders

Binance has issued a warning about a global threat targeting cryptocurrency users with Clipper malware, also known as ClipBankers. This malware monitors clipboard activity to steal sensitive data, replacing cryptocurrency wallet addresses with those controlled by attackers, leading to financial fraud. It is primarily distributed through unofficial apps, particularly affecting Android users but also posing a risk to iOS users. The malware activity spiked in late August 2024, causing significant financial losses. Binance blocks attacker addresses and warns users to be cautious when installing software. Despite a decrease in illicit on-chain activity, cryptocurrency fraud, particularly from investment scams, has surged, with the FBI reporting over $5.6 billion in losses in 2023.

Attack Type : Clipper Malware

Cause of Issue : Unofficial Apps

Industry : Cryptocurrency Industry

Octo2 Android Banking Trojan Unveiled: Enhanced Device Takeover Features Discovered

Cybersecurity researchers have identified a new version of the Android banking trojan known as Octo, called Octo2. This enhanced malware features improved capabilities for device takeover and executing fraudulent transactions, with campaigns detected in European countries like Italy, Poland, and Hungary. Octo2, which emerged after the original source code was leaked, operates as malware-as-a-service, allowing other cybercriminals to use it for information theft. Key improvements include a Domain Generation Algorithm for resilient command-and-control operations and advanced anti-analysis techniques. The trojan is distributed via malicious apps created using an APK binding service and is not currently found on the Google Play Store. The threat level for mobile banking users has significantly increased due to Octo2's sophisticated features and customization options for various threat actors.

Attack Type : Banking trojan

Cause of Issue : Source code leak

Industry : Mobile banking

Apple Vision Pro Flaw Reveals Virtual Keyboard Inputs to Potential Attacks

A recently discovered vulnerability in Apple's Vision Pro mixed reality headset, identified as CVE-2024-40865 and dubbed GAZEploit, could allow attackers to infer text entered via the device's virtual keyboard by analyzing users' eye movements on shared avatars. This flaw, impacting the "Presence" component, was patched by Apple in visionOS 1.3 on July 29, 2024. Researchers found that by examining gaze data from virtual avatars during video calls or live streams, attackers could reconstruct keystrokes, potentially compromising sensitive information like passwords. This marks the first known attack leveraging gaze information for keystroke inference in mixed reality environments.

Attack Type : Keystroke inference

Cause of Issue : Gaze-controlled input vulnerability

Industry : Information Technology

Iran's OilRig Cyber Group Launches Advanced Malware Assault on Iraqi Government

Iraqi government networks have become the target of a sophisticated cyber attack campaign led by the Iranian state-sponsored group OilRig (also known as APT34). The attacks specifically targeted organizations such as the Prime Minister's Office and the Ministry of Foreign Affairs. The campaign involved new malware families called Veaty and Spearal, capable of executing PowerShell commands and harvesting sensitive files. Check Point's analysis revealed that the attackers used compromised email accounts for command-and-control (C2) communications and initiated the attack using deceptive files disguised as harmless documents. The sophisticated methods included DNS tunneling and custom C2 protocols, emphasizing the persistent threat posed by Iranian cyber actors in the region.

Attack Type : State-sponsored attack

Cause of Issue : Compromised emails

Industry : Government sector

Brazilian Threat Actors Target Italian Users with SambaSpy Malware in Phishing Campaign

A new malware named SambaSpy is targeting users in Italy through a phishing campaign led by a suspected Brazilian threat actor. The attack begins with phishing emails containing HTML attachments or links that deploy a Remote Access Trojan (RAT) capable of various malicious functions. If the link is clicked, users may be redirected to a legitimate invoice or a malicious web server that downloads the malware. SambaSpy can manage files, log keystrokes, and steal browser credentials. Evidence suggests the attackers may expand their operations to Brazil and Spain. This campaign highlights the growing sophistication of phishing scams in targeting sensitive information.

Attack Type : Phishing Campaign

Cause of Issue : Malware Deployment

Industry: Information Technology

Meta Penalized €91 Million for Storing User Passwords in Unsecured Plaintext Format

In March 2019, Meta stored users' passwords in plaintext, leading to an investigation by the Irish Data Protection Commission (DPC). The DPC found that Meta violated multiple GDPR rules, including not promptly notifying them about the breach and lacking proper security measures. As a result, Meta was fined €91 million ($101.56 million). Despite claiming no misuse of the passwords, the incident raised serious privacy concerns. Meta stated it took immediate action to fix the issue and informed the DPC.

Attack Type : Data Exposure

Cause of Issue : Compliance violation

Industry : Software development companies

Top 5 YouTube Channels for Cybersecurity

1. Black Hat:

Features presentations and talks from the Black Hat security conference, showcasing the latest in cybersecurity research, trends, and techniques from industry experts.

Link : https://www.youtube.com/@BlackHatOfficialYT

2. Hak5:

Known for engaging content that focuses on hacking, cybersecurity, and technology. The channel offers a variety of tutorials, reviews, and discussions on tools and techniques relevant to both beginners and seasoned professionals.

Link: https://www.youtube.com/@hak5/

3. Null Byte:

Dedicated to ethical hacking and cybersecurity education, Null Byte provides tutorials on penetration testing, security tools, and programming, making it a great resource for aspiring hackers.

Link : https://www.youtube.com/@NullByteWHT

4. IppSec:

Offers in-depth walkthroughs of various capture-the-flag challenges and vulnerable machines from platforms like Hack the Box, ideal for those looking to enhance their practical skills in penetration testing.

Link: https://www.youtube.com/@ippsec

5. LiveOverflow:

Focuses on cybersecurity education and ethical hacking with engaging tutorials, challenges, and explanations of hacking concepts, making complex topics more accessible to viewers.

Link : https://www.youtube.com/@LiveOverflow

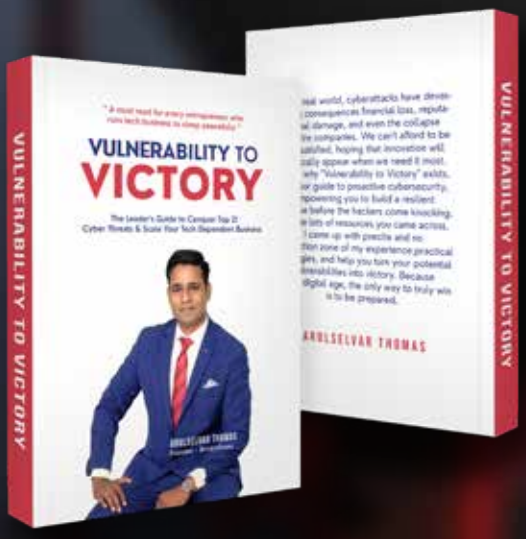
Briskinfosec at GITEX Global 2024

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-C16C

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