Threatsploit

Adversary Report

December - 2024

Edition-76

BRISKINFOSEC

CYBER TRUST & ASSURANCE

www.briskinfosec.com

Introduction :

Dear Readers,

Welcome to the December edition of the Threatsploit Adversary Report, your authoritative resource for comprehensive insights into the rapidly evolving cybersecurity threat landscape. As technology continues to advance, so do the complexities and sophistication of cyber adversaries. This report serves as a critical guide, equipping organizations with the information they need to effectively mitigate and respond to emerging threats.

This month, we investigate key incidents that underscore the urgency of robust cybersecurity strategies. Our coverage includes a high-profile ransomware attack targeting a major healthcare provider, resulting in operational disruptions and the exposure of sensitive patient data. We also examine a notable supply chain breach that compromised critical oil and gas operations, revealing the cascading risks inherent in interconnected systems.

Additionally, this edition highlights a phishing campaign aimed at financial institutions, exploiting human vulnerabilities to gain access to sensitive information. A zero-day vulnerability exploited in widely deployed IT systems also comes under scrutiny, emphasizing the importance of timely patching. The issue concludes with an analysis of a DDoS attack targeting government infrastructure, showcasing the persistent threats faced by public sector entities.

The Threatsploit Adversary Report aims to go beyond merely informing readers; it strives to provide actionable intelligence to empower proactive defense measures. In a dynamic threat environment, staying ahead requires a blend of vigilance, preparedness, and collaboration. Let this report be your strategic ally in navigating the complexities of cybersecurity.

Thank you for trusting the Threatsploit Adversary Report as your partner in safeguarding the digital domain. Together, we can drive resilience and build a secure cyber future.

Stay safe and vigilant.

Best regards,
Briskinfosec Threat Intelligence Team.

Report Inside :

- Top Cyberattacks in the Last 30 Days According to Industry

Contents :

Texas Oilfield Supplier Hit by Ransomware Attack, Leading to Operational Disruptions

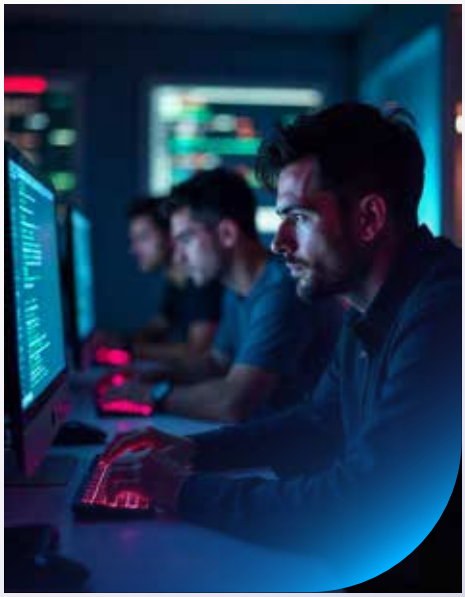
Newpark Resources, a key supplier for oilfields, experienced a ransomware attack on October 29, which disrupted access to some internal systems, including financial and operational reporting. Despite the attack, the company's manufacturing and field operations continued using downtime procedures. The company has not yet determined the financial impact but believes it won't significantly affect its operations. The oil and gas industry, a frequent target of ransomware attacks, has faced similar incidents in the past, leading to increased cybersecurity regulations.

Attack Type : Ransomware Attack

Cause of Issue : System Disruption

Industry Type : Oil and Gas Industry

CISA Alerts on Exploited Critical Vulnerability in Palo Alto Networks



CISA warned that attackers are exploiting a critical vulnerability (CVE-2024-5910) in Palo Alto Networks Expedition, a migration tool, allowing remote attackers to reset admin credentials on exposed servers. This flaw, patched in July, can lead to unauthorized access to sensitive data. A proof-of-concept exploit combining this flaw with another vulnerability (CVE-2024-9464) can enable attackers to execute arbitrary commands and take over firewalls. CISA added the vulnerability to its Known Exploited Vulnerabilities Catalog, and U.S. federal agencies must secure affected systems by November 28. Palo Alto recommends rotating credentials after applying security updates.

Attack Type : Command Injection

Cause of Issue : Authentication Flaw

Industry Type : Information Technology

Ransomware Attack Disrupts Georgia Hospital's Access to Record System

Memorial Hospital and Manor in Bainbridge, Georgia, was hit by a ransomware attack that disrupted access to its Electronic Health Record system. The hospital discovered the attack over the weekend and is working on recovery, using paper-based processes temporarily. The Embargo ransomware gang claimed responsibility, threatening to leak 1.15 terabytes of stolen data unless a ransom is paid. The Embargo is a new ransomware group known for its sophisticated tactics, including targeting healthcare organizations. Similar attacks have impacted other hospitals, with ransom payments averaging around $4 million.

Attack Type : Ransomware Attack

Cause of Issue : Data Encryption

Industry Type : Healthcare Domain

Microsoft warns Chinese hackers use Quad7 botnet for credential theft

Microsoft has warned that Chinese threat actors are using the Quad7 botnet, which consists of compromised SOHO routers, to carry out password-spray attacks and steal credentials. The botnet targets devices from brands like TP-Link, ASUS, Ruckus, Axentra, and Zyxel, using custom malware for remote access via Telnet. Once credentials are stolen, attackers use them to breach networks, deploy remote access tools (RATs), and exfiltrate data for cyber espionage. The exact method of compromising the routers is still unclear, though an OpenWRT zero-day has been observed in some attacks.

Attack Type : Password Spray

Cause of Issue : Compromised Routers

Industry Type : Software Industry

Russian Hackers Use NTLM Flaw to Deliver RAT Malware in Phishing Attacks

A newly patched Windows NTLM vulnerability, CVE-2024-43451, was exploited as a zero-day by a suspected Russia-linked group UAC-0194 in cyberattacks targeting Ukraine. The flaw allows NTLMv2 hash theft via minimal interaction with malicious URL files. Attackers sent phishing emails from a compromised Ukrainian government server, prompting victims to download a malicious file from an official site. This triggered the download of Spark RAT malware, enabling Pass-the-Hash attacks for lateral movement. CERT-UA also linked related phishing campaigns to financial theft using LiteManager software, targeting enterprise accountants.

Attack Type : Phishing Exploitation

Cause of Issue : NTLM Vulnerability

Industry Type : Financial Industry

Hamas-Linked WIRTE Group Launches SameCoin Wiper Attacks on Israel

A hacking group called WIRTE, linked to Hamas, has expanded its operations to conduct disruptive cyberattacks against Israeli entities during the Israel-Hamas conflict. These attacks include phishing campaigns and the deployment of malware like the SameCoin Wiper and IronWind downloader. The group also targets other Middle Eastern countries, including Jordan and Egypt. WIRTE uses deceptive files and phishing emails to spread malware, often exploiting geopolitical tensions. Their tools can spy on systems, erase data, or disrupt operations. Some phishing emails impersonated legitimate organisations to trick victims. Despite the ongoing conflict, WIRTE has maintained a persistent and versatile campaign of espionage and sabotage.

Attack Type : Cyber Espionage

Cause of Issue : Phishing Emails

Industry Type : Public Sector

NSO Group Continues Using WhatsApp to Deploy Pegasus Spyware Despite Meta's Legal Action

Legal documents from an ongoing legal battle between Meta's WhatsApp and NSO Group reveal that NSO Group exploited multiple vulnerabilities in WhatsApp to install the Pegasus spyware. One key attack vector, known as "Erised," was a zero-click exploit that compromised devices without user interaction. The group also used the CVE-2019-3568 vulnerability to install Pegasus, affecting thousands of devices. Despite WhatsApp's defence measures, NSO Group developed new methods to bypass these protections. The documents also highlight NSO's central role in operating the spyware, contradicting their claims that clients manage it. NSO insists its tools are for fighting crime and terrorism.

Attack Type : Spyware Implant

Cause of Issue : WhatsApp Exploits

Industry Type : Information Technology

New 'ToxicPanda' Malware Exploits Android Banking Apps for Fraudulent Transactions

The ToxicPanda Android banking malware has infected over 1,500 devices, enabling attackers to conduct fraudulent banking transactions through on-device fraud (ODF). Linked to a Chinese-speaking threat actor, it shares similarities with the TgToxic malware but introduces new commands while lacking features like Automatic Transfer System (ATS). ToxicPanda masquerades as legitimate apps like Google Chrome and abuses Android accessibility services to bypass two-factor authentication (2FA), steal data, and remotely control devices. Its command-and-control (C2) panel enables attackers to manage victim devices and perform real-time unauthorized transactions.

The malware appears to be in early development, with ongoing refinements. Additionally, similar malware like HookBot targets institutions such as PayPal and Coinbase, using overlay attacks and spreading via WhatsApp links under a malware-as-a-service model. These threats highlight increasing exploitation of Android accessibility features by cybercriminals.

Attack Type : Banking Trojan

Cause of Issue : Accessibility Abuse

Industry Type : Banking and Financial Services

Over 2,000 Palo Alto Networks Devices Compromised in Active Exploitation Campaign

A campaign exploiting Palo Alto Networks' security flaws, CVE-2024-0012 (authentication bypass) and CVE-2024-9474 (privilege escalation), has compromised around 2,000 devices, primarily in the U.S. and India. These vulnerabilities allow attackers to modify configurations, execute arbitrary code, and deploy malware, such as PHP-based web shells. The flaws are actively exploited, with both manual and automated scanning observed. Users are urged to apply patches immediately and restrict management interface access to trusted internal IPs to mitigate risks.

Attack Type : Privilege Escalation

Cause of Issue : Vulnerable Interfaces

Industry Type : Information Technology

Ngioweb Botnet Powers NSOCKS Proxy Network Using Infected IoT Devices

The Ngioweb malware is being used to power a residential proxy service called NSOCKS, which is primarily fueled by IoT devices and small office/home office routers. The botnet, which is responsible for infecting over 20,000 devices, is being sold on a proxy marketplace for as little as $0.20 to $1.50 per 24-hour access. NSOCKS allows cybercriminals to route malicious traffic through proxies, enabling anonymity and global targeting of entities like .gov or .edu domains. The botnet has also been leveraged in credential-stuffing attacks and DDoS campaigns. The malware uses a two-tier architecture for infection, deploying via vulnerabilities in routers and IoT devices.

Attack Type : Botnet Proxy

Cause of Issue : IoT Compromise

Industry Type : Telecommunications

300 US Water Systems Vulnerable to Potential Cyber Attacks

A report from the EPA's Office of Inspector General reveals that over 300 drinking water systems in the U.S. are vulnerable to cybersecurity threats, potentially affecting 110 million people. The vulnerabilities could lead to service disruptions, denial-of-service attacks, and customer data compromise. The assessment covered over 1,000 water systems and identified critical issues such as poor IT hygiene, email security flaws, and external open portals. 97 systems were found to have severe issues, while 211 others had medium to low-severity vulnerabilities. The report highlights a lack of coordinated cybersecurity reporting and response strategies within the EPA.

Attack Type : Denial of Service

Cause of Issue : Vulnerabilities

Industry Type : Water Systems

Helldown Ransomware Targets VMware and Linux Systems in New Variant

Cybersecurity researchers have identified a new Linux variant of the Helldown ransomware, which targets industries like IT services, telecommunications, manufacturing, and healthcare. Initially exploiting Zyxel firewalls to gain access, the ransomware carries out credential harvesting, lateral movement, and ultimately encrypts files, using techniques like data exfiltration and double extortion. While the Windows version shares similarities with other ransomware strains like LockBit 3.0 and DarkRace, the Linux variant lacks sophisticated anti-debugging mechanisms and primarily focuses on encrypting virtual machine files. Helldown's activities highlight the evolving nature of ransomware groups, with many targeting both Windows and Linux systems in various sectors.

Attack Type : Ransomware Attack

Cause of Issue : Exploiting Vulnerabilities

Industry Type : IT Services

Critical Vulnerability in WordPress Security Plugin Grants Admin Access

A critical authentication bypass vulnerability (CVE-2024-10924) has been discovered in the 'Really Simple Security' WordPress plugin, affecting both free and Pro versions. The flaw allows remote attackers to gain full administrative access to websites by bypassing two-factor authentication (2FA) due to improper handling of authentication parameters. The vulnerability impacts plugin versions 9.0.0 to 9.1.1.1. It can be exploited using automated scripts, posing a significant security risk. A fix was released in version 9.1.2, and website administrators are urged to update to this version to mitigate the issue.

Attack Type : Remote Takeover

Cause of Issue : Authentication bypass

Industry Type : Software Development Companies

T-Mobile Compromised in Major Chinese Cyber-Espionage Attack on U.S. Telecoms

T-Mobile's network was compromised in a Chinese cyber-espionage campaign, part of a broader attack targeting multiple U.S. and international telecoms, attributed to the Chinese hacker group Salt Typhoon. The attackers sought to monitor high-value intelligence targets, including U.S. officials and politicians, by exploiting vulnerabilities in telecom infrastructure. Although T-Mobile confirmed no significant impact on customer data, the breach raised national security concerns. The group also accessed information from systems used to comply with U.S. surveillance orders. The FBI and CISA are investigating the breaches, which are believed to have lasted for several months.

Attack Type : Cyber-Espionage

Cause of Issue : Exploited Vulnerabilities

Industry Type : Telecommunications

Git Configuration Breach Compromises 15,000 Credentials and Clones 10,000 Private Repositories

The EMERALDWHALE cyber campaign targets exposed Git configurations to steal credentials, clone private repositories, and extract cloud credentials. The attackers have collected over 10,000 private repositories and 15,000 stolen credentials, which were stored in an Amazon S3 bucket before being taken down. The campaign uses tools like MZR V2 and Seyzo-v2 to exploit exposed Git and Laravel files. The stolen data is sold on underground marketplaces, highlighting the growing market for cloud service credentials. The attack emphasizes the need for more robust secret management to secure environments.

Attack Type : Credential Theft

Cause of Issue : Exposed Git Configuration Files

Industry Type : Software Development Companies

Synology Issues Urgent Patch for Zero-Click RCE Vulnerability Impacting Millions of NAS Devices

Synology has addressed a critical zero-day vulnerability (CVE-2024-10443) impacting its DiskStation and BeePhotos NAS devices. Dubbed RISK:STATION, the flaw allows unauthenticated, zero-click remote code execution, giving attackers root-level access. This affects millions of devices, risking data theft and malware deployment. The vulnerability was demonstrated at Pwn2Own Ireland 2024. Affected versions include BeePhotos 1.0 and 1.1, and Synology Photos 1.6 and 1.7. Users are urged to upgrade to the latest patched versions to protect their devices.

Attack Type : Remote Code Execution

Cause of Issue : Authentication Bypass

Industry Type : Information Technology

North Korean Hackers Deploy Hidden Risk Malware to Target Crypto Firms on macOS

A North Korean-linked threat group, BlueNoroff, has targeted cryptocurrency-related businesses with a multi-stage malware campaign called "Hidden Risk." The campaign uses phishing emails, disguised as fake news about cryptocurrency trends, to deliver a malicious app mimicking a PDF. Once executed, the app installs a backdoor on macOS devices, stealing cryptocurrency-related credentials and utilizing novel persistence techniques. The malware is signed with a valid Apple developer ID, which was later revoked. This campaign is part of a broader strategy by North Korean hackers to exploit the cryptocurrency sector, using social engineering and malware to steal sensitive data.

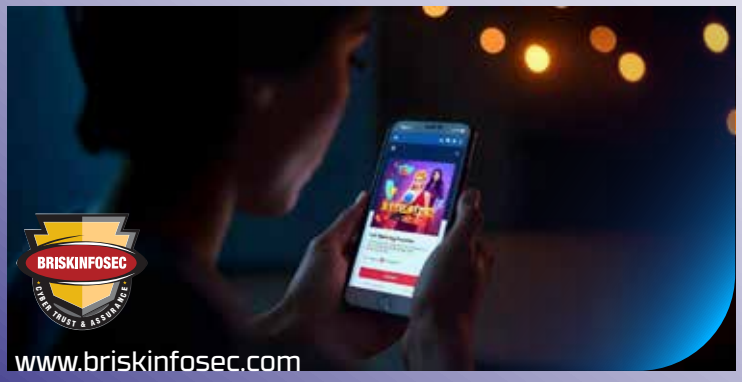
Attack Type : Phishing Attack

Cause of Issue : Credential Theft

Industry Type : Cryptocurrency Sector

NodeStealer Malware Exploits Facebook Ads to Steal Credit Card Information

The Python-based NodeStealer malware has been updated to target Facebook Ads Manager accounts, extracting budget details, credit card data from browsers, and access tokens via the Facebook Graph API. Developed by Vietnamese threat actors, it uses social engineering, malvertising campaigns, and Telegram for data exfiltration. Additionally, phishing campaigns leveraging techniques like ClickFix and fake CAPTCHAs are delivering malware such as RATs and stealers, posing significant risks of financial fraud and security breaches.



Attack Type : Information Stealing

Cause of Issue : Malware Infection

Industry Type : Software Development Companies

IcePeony and Transparent Tribe Use Cloud Tools in Attacks on Indian Entities

High-profile entities in India are being targeted by two cyber espionage groups: Pakistan-based Transparent Tribe and China-nexus IcePeony. Transparent Tribe uses ElizaRAT, a Windows RAT, and ApoloStealer to exfiltrate files, abusing cloud services like Telegram and Google Drive for command-and-control. IcePeony focuses on SQL injections, web shells, and credential theft, with tools like IceCache and IceEvent. Both groups are intensifying their attacks, with Transparent Tribe expanding its malware arsenal and IcePeony targeting government, academic, and political organizations in India, Mauritius, and Vietnam.

Attack Type : Cyber Espionage

Cause of Issue : Credential Theft

Industry Type : Government Sector

Gelsemium APT Exploits Linux with WolfsBane Backdoor

The China-aligned APT group Gelsemium has been linked to a new Linux backdoor called WolfsBane, discovered in cyberattacks targeting East and Southeast Asia. WolfsBane, a Linux adaptation of the group's older Windows malware Gelsevirine, is designed for cyber espionage, targeting sensitive data and maintaining stealthy, persistent access.

ESET also identified another implant, FireWood, which employs a rootkit for hiding activities. The exact initial access vector remains unclear but is suspected to involve web application vulnerabilities. This marks Gelsemium's first documented use of Linux malware, highlighting a growing trend of APT groups targeting Linux systems as security measures improve on Windows platforms.

Attack Type : Backdoor Deployment

Cause of Issue : Web Exploitation

Industry Type : Government Sector

Zero-Day Attacks Target Mac Users, Apple Issues Security Fixes

Apple released security updates for macOS, iPhones, and iPads to address two active zero-day vulnerabilities. These flaws were exploited in cyberattacks targeting Intel-based Macs and were reported by Google's Threat Analysis Group. The vulnerabilities were related to WebKit and JavaScriptCore, which power the Safari browser and web content. Attackers could exploit these bugs by tricking users into processing malicious web content, leading to arbitrary code execution. This could result in malware installation on vulnerable devices. Although the attackers' identity is unclear, a government-backed actor is suspected. Users are urged to update their devices immediately to mitigate risks.

Attack Type : Arbitrary Code Execution

Cause of Issue : WebKit Vulnerabilities

Industry Type : Information Technology

Attackers Exploit Unsecured Jupyter Notebooks for Illegal Sports Streaming

Malicious actors are exploiting misconfigured JupyterLab and Jupyter Notebooks to hijack servers and conduct illegal sports piracy. Using the tool FFmpeg, they capture live sports streams, redirect them to their servers, and broadcast them on illegal platforms like ustream.tv. This exploitation not only facilitates piracy but also risks compromising data science operations, leading to potential data theft, corruption, and financial damage. The campaign was discovered by Aqua after monitoring honeypots.

Attack Type : Stream Piracy

Cause of Issue : Exploiting Misconfiguration

Industry Type : Sports Broadcasting Industry

FBI and CISA Confirm Chinese Cyber Espionage Campaign Targeting US Telecom Networks

A US government investigation revealed a large-scale cyber espionage campaign by Chinese-affiliated hackers targeting US telecommunications companies. The hackers infiltrated networks to steal customer call records, access private communications of government and political figures, and copy data related to US law enforcement requests. The FBI and CISA are providing technical assistance and encouraging other potential victims to report the incident. The campaign has raised concerns about the security of US telecom infrastructure, with further investigations expected. The Chinese government has not yet issued an official statement.

Attack Type : Cyber Espionage

Cause of Issue : Entertainment Industry

Industry Type : Telecommunications

Typosquatting PyPI Package 'Fabrice' Exfiltrates AWS Keys from Developers

Researchers have discovered a malicious package called "fabrice" on PyPI, which typosquats the legitimate "fabric" library. Over 37,100 downloads occurred since its release in March 2021, with the package designed to steal AWS credentials and create backdoors. On Linux, it executes shell scripts, while on Windows, it runs a Visual Basic Script and a Python script to download malicious files. The ultimate goal is to exfiltrate AWS access and secret keys. The attack highlights the risks of typosquatting and credential theft from developers.

Attack Type : Typosquatting Attack

Cause of Issue : Credential Theft

Industry Type : Information Technology

AndroxGh0st Malware Leverages Mozi Botnet to Exploit IoT and Cloud Services

The AndroxGh0st malware, a Python-based tool, is exploiting various vulnerabilities in internet-facing applications, including CVEs in Cisco, Dasan GPON routers, Atlassian Jira, and others, to gain access and establish control. Initially targeting Laravel applications, AndroxGh0st now also deploys the Mozi botnet, which uses remote code execution and credential-stealing techniques to maintain access. The integration of Mozi enhances AndroxGh0st's ability to infect IoT devices and expand its operations. The combined botnet uses shared command infrastructure, suggesting a high level of coordination between the two, potentially under the same cybercriminal group.

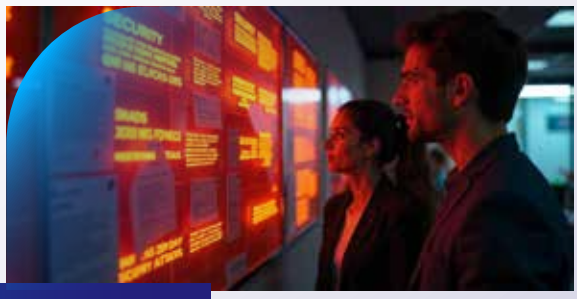
Attack Type : Botnet Exploitation

Cause of Issue : Unpatched Vulnerabilities

Industry Type : Cloud-based SaaS Providers

Unpatched Fortinet Flaw Abused by DEEPDATA Malware to Extract VPN Credentials

BrazenBamboo, a Chinese threat actor, has exploited an unpatched zero-day flaw in Fortinet's FortiClient for Windows to extract VPN credentials using a malware framework called DEEPDATA. Disclosed by Volexity, DEEPDATA includes plugins for credential theft, data exfiltration, and post-exploitation tasks. The malware targets various applications like WhatsApp, Telegram, and browsers, expanding its capabilities beyond earlier spyware like LightSpy.DEEPDATA works with other tools like DEEPPOST for file exfiltration and shares similarities with LightSpy, which has variants for Windows, macOS, and iOS. The malware uses sophisticated methods for persistence and communication, indicating development by a private enterprise likely tasked with supporting government-linked cyber-espionage. Despite reporting the flaw to Fortinet in July 2024, the vulnerability remains unpatched.



Attack Type : Credential Theft

Cause of Issue : Unpatched Vulnerability

Industry Type : Information Technology

Bitfinex Hacker Gets 5-Year Sentence for $10.5 Billion Bitcoin Laundering Scheme

Ilya Lichtenstein was sentenced to five years for hacking Bitfinex in 2016, stealing nearly 120,000 bitcoins (valued at $10.5 billion). He exploited a vulnerability in Bitfinex's multi-signature withdrawal system and laundered the funds with his wife, Heather Morgan, who will be sentenced on November 18. They used techniques like chain hopping, mixing services, and fake identities to conceal the theft. The couple's purchase of Walmart gift cards helped investigators trace the stolen funds. Separately, Daren Li pleaded guilty to laundering $73.6 million from cryptocurrency scams and faces up to 20 years in prison.

Attack Type : Data Breach

Cause of Issue : Security Vulnerability

Industry Type : Financial Services

Critical Vulnerability in PostgreSQL Exposes Environment Variables to Exploitation

A high-severity vulnerability (CVE-2024-10979) in PostgreSQL could allow unprivileged users to alter environment variables, potentially leading to arbitrary code execution or information disclosure. The flaw, which affects versions 12.21 to 17.1, involves incorrect control of environment variables in PostgreSQL's PL/Perl. This flaw can be exploited to change sensitive variables like PATH, enabling attackers to execute malicious code. The issue has been fixed in newer PostgreSQL versions, and users are advised to apply patches, restrict extensions, and follow best security practices to mitigate the risk.

Attack Type : Code Execution

Cause of Issue : Environment Variables

Industry Type : Information Technology

North Korean Hackers Use AI Scams and Malware to Steal $10M via LinkedIn

The North Korea-linked threat group, Sapphire Sleet, has stolen over $10 million in cryptocurrency through social engineering campaigns on LinkedIn. Posing as recruiters and job seekers, the group lures targets by pretending to be interested in their companies, then delivers malware via AppleScript or Visual Basic Script files. The malware allows the attackers to steal credentials and cryptocurrency. Sapphire Sleet, active since at least 2020, is associated with APT38 and BlueNoroff. North Korean IT workers, using fake profiles and AI tools, facilitate these attacks, and the group has earned at least $370,000 through these efforts.

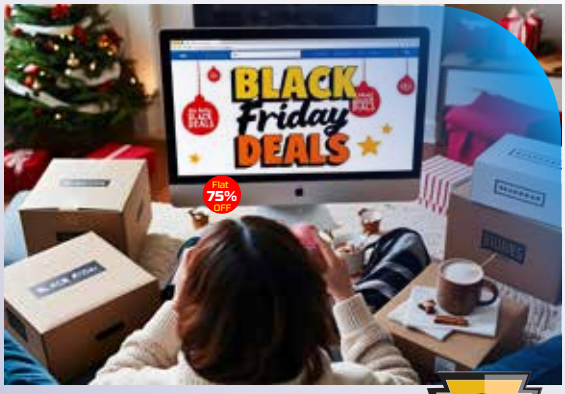
Attack Type : Social Engineering

Cause of Issue : Malware Download

Industry Type : Information Technology

Phishing Campaign Targets Black Friday Shoppers with Fake Discount Sites

A phishing campaign targeting e-commerce shoppers in Europe and the U.S. has been observed ahead of the Black Friday shopping season. The attackers, believed to be a Chinese threat actor group called SilkSpecter, use fake websites mimicking legitimate brands like IKEA and North Face to steal personal and financial information. The phishing sites promote fake discounts and use tools like Google Translate, trackers, and Stripe for fraudulent transactions. Victims are also asked for phone numbers, likely to conduct follow-up smishing and vishing attacks. The campaign is believed to spread via social media and search engine poisoning.



Attack Type : Phishing Campaign

Cause of Issue : Fake Discounts

Industry Type : E-commerce

Vulnerability to Victory

A Cybersecurity Guide for Business Leaders

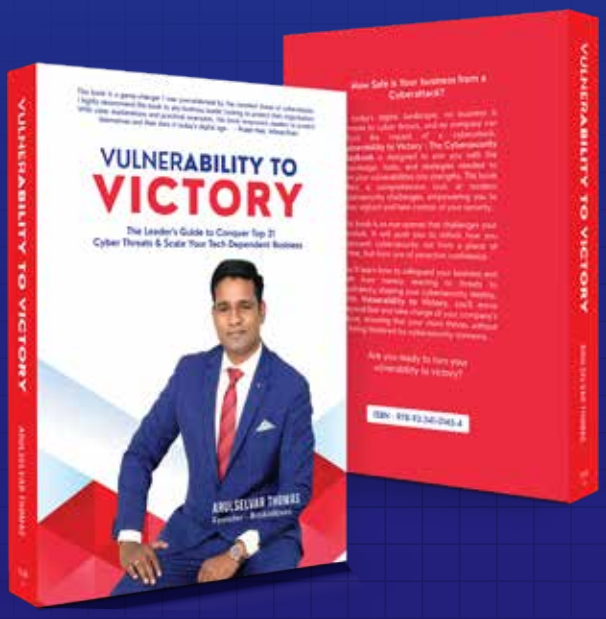
Arulselvar Thomas, the visionary founder of Briskinfosec, has authored a compelling new book, **"Vulnerability to Victory,"** now available on Amazon. Officially launched on 24th October 2024, at GITEX Global, one of the world's premier technology events, this book has already received widespread acclaim for its depth, practical insights, and transformative approach to cybersecurity

Recognition from Industry Leaders

Prominent voices across the cybersecurity and technology sectors have praised the book for its relevance and applicability, highlighting its pivotal role in shaping strategic approaches to today's ever-evolving security challenges.

"This book is a game-changer I was overwhelmed by the constant threat of cyberattacks. I highly recommend this book to any business leader looking to protect their organization. With clear explanations and practical examples, this book empowers readers to protect themselves and their data in today's digital age."
- Prabh Nair, InfosecTrain

"This book bridges the gap between technical jargon and real-world cybersecurity consequences, making it an essential read for anyone involved in incident response and investigations."
- Dr Deepak Kumar (D3) Cyber Intelligence & Forensics Professional



A must-read for cybersecurity professionals at any stage, this book offers practical insights and strategies to tackle today's security challenges.

Available Now On Amazon

Stay with us
Secure your consistency
Elevate your future

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