Threatsploit Adversary Report

Edition-67

MAR’2024

BRISKINFOSEC

CYBER TRUST & ASSURANCE

www.briskinfosec.com

Introduction :

Dear Readers,

Welcome to the March 2024 edition of Briskinfosec's Threatsploit Adversary Report, marking our 67th edition. This month, we're excited to introduce upgraded features that significantly enrich our cybersecurity insights.

The Threatsploit Report for March 2024 offers a comprehensive overview of the latest cyber threats, vulnerabilities, and notable security incidents that have influenced the cybersecurity landscape in the past month. This report is tailored to provide insights into the evolving threat landscape, empowering businesses, cybersecurity professionals, and stakeholders to effectively comprehend and address the challenges presented by cyber adversaries.

Key highlights from the report include :

Job Board Hacks by ResumeLooters : A new threat actor, ResumeLooters, has been exploiting job boards to steal millions from unsuspecting job seekers through sophisticated SQL Injection attacks. This campaign highlights the importance of robust security practices to prevent data breaches and financial loss.

Cloudflare's Nation-State Breach : Cloudflare faced a significant security breach, likely perpetrated by nation-state hackers, compromising sensitive data due to credential mismanagement. This incident underscores the critical need for stringent access controls and vigilance against sophisticated cyber espionage efforts.

Shift in KV-Botnet Operations : Following an FBI takedown, operators behind the KV-botnet, known for being used by Chinese state-sponsored actors, have shifted tactics. This development emphasizes the adaptive nature of cyber threat actors and the need for continuous monitoring and threat intelligence to combat evolving cyber threats.

Cyber Intrusion at Kyivstar : Ukraine's largest mobile carrier, Kyivstar, suffered a cyber intrusion, leading to significant service disruptions. This attack, attributed to cyber sabotage, demonstrates the vulnerabilities in critical infrastructure and the potential impacts of cyberattacks on national security.

Each incident in the report is detailed with descriptions of the attack types, causes of the issues, domains affected, and reference links to further information. This report serves as a valuable resource for understanding the dynamic and complex nature of cyber threats, offering actionable insights for enhancing cybersecurity resilience.

Thank you for your unwavering support.

Best regards,
Briskinfosec Threat Intelligence Team.

Report Inside :

- ★ Top Cyberattacks in the Last 30 Days According to Industry
- ★ Top 5 Cybersecurity Documentaries
- ★ Top 5 Cybersecurity Books to Read
- ★ Most Popular Cybersecurity Framework

Hackers Exploit Job Boards, Stealing Millions of Resumes and Personal Data

A new threat actor named ResumeLooters has been targeting employment agencies and retail companies in the Asia-Pacific (APAC) region since early 2023. They use SQL injection attacks to steal sensitive data, including resumes, from job search platforms. The stolen data, containing over 2 million unique email addresses, is sold on Telegram channels. ResumeLooters also employs cross-site scripting (XSS) infections to harvest administrator credentials. Their modus operandi involves using tools like sqlmap, Metasploit, and BeEF. The campaign is financially motivated, and compromised websites are primarily located in India, Taiwan, Thailand, Vietnam, China, Australia, and Turkey. The group's persistence and experimentation with various attack methods highlight the importance of improved security practices.

Attack Type : SQL Injection

Cause of Issue : Poor security practices

Domain Name : Telecommunications

Cloudflare Breach : Nation-State Hackers Access Source Code and Internal Docs

Cloudflare experienced a likely nation-state attack between November 14 and 24, 2023, where stolen credentials were used to access its Atlassian server. The attacker gained access to documentation and some source code, targeting systems related to network configuration, backups, identity management, and remote access. About 120 code repositories were viewed, with 76 potentially exfiltrated. The attack utilized credentials stolen from Okta's system in October 2023, and Cloudflare failed to rotate these credentials. Precautionary measures included rotating over 5,000 production credentials, segmenting systems, and forensic analysis. CrowdStrike conducted an independent assessment, and Cloudflare terminated all malicious connections.

Attack Type : Nation-state infiltration

Cause of Issue : Credential Mismanagement

Domain Name : (SaaS) Providers

www.briskinfosec.com

FBI Warns U.S. Healthcare Sector of Targeted BlackCat Ransomware Attacks

The U.S. government warns of a resurgence in BlackCat ransomware attacks targeting healthcare. Despite law enforcement actions, the group regained control and continues operations. They're targeting critical infrastructure and are suspected in recent attacks. The government offers rewards for information. LockBit also returns. Exploits in ConnectWise software are leveraged by threat actors. Remote access software vulnerabilities are exploited, with thousands of exposed hosts. Ransomware groups employ sophisticated tactics, like custom deployment tools and selling network access. A Linux-specific ransomware threat has emerged, raising concerns about its spread and impact.

Attack Type : Ransomware resurgence

Cause of Issue : Cybersecurity threats

Domain Name : Healthcare Sector

Ukraine's largest mobile carrier Kyivstar down following cyberattack

Kyivstar, Ukraine's largest telecommunications provider, suffered a cyberattack, causing mobile and internet service disruptions. The company reported the incident to authorities, who have initiated criminal proceedings. While the exact source remains unconfirmed, suspicions point towards Russian hackers due to the ongoing conflict. Despite the outage, Vodafone Ukraine's roaming service remains available for affected users. Ukrainian telecommunication firms have implemented a system of free internal roaming to mitigate service disruptions. The outage has also affected the air raid alert network, impacting timely notifications for incoming bombing attacks.

Attack Type : Cyber intrusion

Cause of Issue : Cyberattack, sabotage

Domain Name : Telecommunications

Lazarus Exploits Typos to Sneak PyPI Malware into Dev Systems

North Korean hackers uploaded four malware-containing packages to PyPI, targeting developers. These packages, named pycryptoenv, pycryptoconf, quasarlib, and swapmempool, mimicked legitimate ones to exploit typos during installation. The malware, disguised as a test script, ultimately executes a Windows executable file called Comebacker, connecting to a command-and-control server. This campaign mirrors a previous attack on npm registry by Phylum, indicating a trend of targeting developers. JPCERT/CC warns users to be vigilant during software installation to avoid downloading malicious packages.

Attack Type : Supply chain attack

Cause of Issue : Malicious packages

Domain Name : Software Development Companies

BRISKINFOSEC

CYBER TRUST & ASSURANCE

www.briskinfosec.com

Budworm hackers target telcos and govt orgs with custom malware

The Budworm cyber-espionage group has been observed targeting a Middle Eastern telecommunications firm and an Asian government entity with a new variant of its 'SysUpdate' backdoor. This variant, deployed via DLL sideloading, evades detection by launching within a legitimate program process. Budworm's toolkit includes publicly available tools for actions like credential dumping and network mapping. Telecom companies have become common targets for state-sponsored hacking groups, with recent instances of custom malware installations providing backdoor access. Budworm has a history of targeting high-value entities since 2013, employing tactics such as abusing Windows BitLocker and setting up fake sites to distribute malware.

Attack Type : Cyber espionage

Cause of Issue : State-sponsored hacking

Domain Name : Telecom Infiltration

Hackers could have enslaved 3 million toothbrushes for DDoS attack

Reports of three million smart toothbrushes being infected and used in a DDoS attack on a Swiss company were debunked, highlighting concerns over the security of IoT devices. While vulnerabilities in connected devices pose real risks, skepticism arises due to the lack of concrete evidence in the toothbrush incident. Cybersecurity experts emphasize the constant threat posed by cybercriminals targeting IoT devices and the importance of keeping devices updated to mitigate risks.

Attack Type : Alleged DDoS

Cause of Issue : Insecure IoT

Domain Name : Software Development Companies

66%

organizations reported being targeted by ransomware, with the average ransom payout rising from $812,380 in 2022 to $1,542,333.

In 2023

36.4% of emails are categorized as “unwanted”.

Iran and Hezbollah Hackers Launch Attacks to Influence Israel-Hamas Narrative

Hackers backed by Iran and Hezbollah launched cyber attacks to undermine public support for the Israel-Hamas war. Tactics included destructive attacks, hack-and-leak operations, phishing campaigns, and information operations. Iranian groups like GREATRIFT and Charming Kitten targeted Israel with malware and phishing. Hamas-linked actors targeted Israeli software engineers with malware and spyware. The conflict saw retaliatory cyber operations from both sides, with Microsoft reporting Iranian cyberattacks in support of Hamas and against Israel's allies. Collaboration among Iranian-affiliated groups and Hezbollah cyber units was observed. The U.S. also reportedly conducted a cyber attack against an Iranian military ship.

Attack Type : Cyber Warfare

Cause of Issue : State-sponso tacks

Domain Name : Software Development Companies

BRISKINFOSEC

CYBER TRUST & ASSURANCE

www.briskinfosec.com

U.S. Sanctions 6 Iranian Officials for Critical Infrastructure Cyber Attacks

The U.S. Treasury Department's Office of Foreign Assets Control (OFAC) imposed sanctions on six Iranian intelligence officials associated with the Iranian Islamic Revolutionary Guard Corps Cyber-Electronic Command (IRGC-CEC) for attacking critical infrastructure entities. These officials, including Reza Lashgarian, are accused of hacking programmable logic controllers manufactured by Unitronics, posing a threat to sensitive targets like water systems. The sanctions follow revelations by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) regarding Iranian threat actors targeting the Municipal Water Authority of Aliquippa. Additionally, another pro-Iranian group, Homeland Justice, claimed responsibility for attacking Albania's Institute of Statistics (INSTAT).

Attack Type : Cyber espionage

Cause of Issue : Iranian cyberattacks

Domain Name : Networking Sector

Newest Ivanti SSRF zero-day now under mass exploitation

The Ivanti Connect Secure and Ivanti Policy Secure server-side request forgery (SSRF) vulnerability, tracked as CVE-2024-21893, is being actively exploited by multiple attackers. This zero-day flaw allows attackers to bypass authentication and access restricted resources on vulnerable devices. Threat monitoring service Shadowserver has detected 170 distinct IP addresses attempting to exploit the vulnerability, indicating a significant shift in attackers' focus. The U.S. Cybersecurity & Infrastructure Security Agency (CISA) has ordered federal agencies to disconnect all affected appliances until patched.

Attack Type : Server-side request forgery

Cause of Issue : Zero-day Vulnerability

Domain Name : SaaS providers

74% financial and insurance attacks compromised clients' personal details.

200% surge in voice scams from 2022 to 2023 has caused a seismic shift in the landscape of digital crimes.

BRISKINFOSEC CYBER TRUST & ASSURANCE

www.briskinfosec.com

AnyDesk Hacked : Popular Remote Desktop Software Mandates Password Reset

Remote desktop software provider AnyDesk experienced a cyber attack on its production systems, prompting a security audit and certificate revocation. While the incident is not a ransomware attack, AnyDesk revoked all passwords and urged users to update their software and passwords. The company emphasized that there is no evidence of end-user systems being affected. Additionally, cybersecurity firm Resecurity found threat actors selling AnyDesk customer credentials on the dark web, potentially for technical support scams and phishing. AnyDesk assured users that its software from official sources remains safe to use, with no malicious modifications to its source code detected.

Attack Type : Supply chain

Cause of Issue : Cyber Attack

Domain Name : Wireless Communication

www.briskinfosec.com

Ransomware attack forces 100 Romanian hospitals to go offline

A ransomware attack has targeted the Hipocrate Information System (HIS) used by 100 hospitals across Romania, leading to the encryption of their systems. While 25 hospitals have confirmed data encryption, 75 others have taken their systems offline as a precaution. The attackers demanded a ransom of 3.5 BTC (approximately €157,000), and doctors have resorted to manual record-keeping as systems remain offline. The Romanian Ministry of Health and cybersecurity experts are investigating the incident, with the ransomware variant identified as Backmydata. No evidence of data theft has been found so far, and the software service provider, RSC, has not issued a public statement.

Attack Type : Ransomware Encryption

Cause of Issue : Ransomware attack

Attack Type : Pharmaceuticals and Biotechnology

New RustDoor macOS malware impersonates Visual Studio update

A new macOS malware, dubbed RustDoor, written in Rust, is being distributed as a Visual Studio update. It provides backdoor access to compromised systems and is linked to infrastructure used by the ALPHV/BlackCat ransomware gang. The malware communicates with command and control servers and has various capabilities, including executing shell commands, exfiltrating data, and establishing persistence on the system. It has been active for at least three months and comes in multiple variants, posing challenges for detection by security products.

Attack Type : MacOS Backdoor

Cause of Issue : Malware Distribution

Attack Type : Software Development Companies

New Mispadu Banking Trojan Exploiting Windows SmartScreen Flaw

The Mispadu banking Trojan, targeting users in Mexico, exploits a patched Windows SmartScreen flaw to infiltrate systems via phishing emails. This variant, part of the LATAM banking malware family, uses internet shortcut files to bypass security warnings. Recent attacks also involve DarkGate and Phemedrone Stealer malware. Mexico has seen a surge in campaigns delivering information stealers and RATs, notably from financially-motivated groups like TA558. Additionally, the FIN7 group employs DICELOADER, a custom downloader, and AhnLab uncovers new cryptocurrency mining campaigns using booby-trapped archives and game hacks.

Attack Type : Phishing exploit

Cause of Issue : Security Vulnerabilities

Domain Name : Finance and Banking

Critical Flaw in Zoom Windows Apps Allows Privilege Elevation

Zoom disclosed a critical privilege escalation vulnerability, CVE-2024-24691, with a severity score of 9.6, affecting various Windows versions of its products. The flaw could allow unauthenticated users to escalate privileges via network access. Researchers from Zoom's Offensive Security division reported the issue, but it's unclear if it has been exploited in the wild. Other vulnerabilities, including improper input validation issues and information disclosure flaws, were also patched in the update. Users are advised to update to the latest versions to mitigate these security risks.

Attack Type : Improper Sanitization

Cause of Issue : Privilege Escalation

Domain Name : (SaaS) Providers

Microsoft's February 2024 Patch Tuesday Addresses Two Zero-day Vulnerabilities

The February 2024 Patch Tuesday updates from Microsoft address several vulnerabilities, including two zero-day flaws. One affects Internet Shortcut Files, allowing attackers to bypass security checks, while the other impacts Windows SmartScreen, enabling code execution. Additionally, patches were released for three critical vulnerabilities and 66 other issues of varying severity. Users are advised to manually check for updates to ensure all fixes are applied promptly.

Attack Type : Feature bypass

Cause of Issue : Security Vulnerabilities

Attack Type : Software Development Companies

Hacker arrested for selling bank accounts of US, Canadian users

A 31-year-old Ukrainian cybercriminal was arrested for running a sophisticated cybercrime operation that targeted American and Canadian users. He distributed trojanized software through his websites, infecting victims' devices and stealing sensitive data, which he sold on the dark web. The suspect, active since 2017, also engaged in phishing, earning at least $92,000 from his illegal activities. Authorities seized his assets, including a luxury SUV, and he faces up to 8 years in prison for multiple violations of Ukraine's Criminal Code. Users are advised to exercise caution when downloading software and use ad-blockers to mitigate malvertising threats.

Attack Type : Malware Distribution

Cause of Issue : Cybercrime Operation

Attack Type : Finance and Banking

BRISKINFOSEC
CYBER TRUST & ASSURANCE

www.briskinfosec.com

U.S. takes down Russian botnet of routers

The U.S. has taken down a Russian botnet comprised of compromised routers, targeting APT28/Fancy Bear. Default password negligence allowed access. Also, a $10 million reward is offered for AlphV/BlackCat ransomware intel. ESET patches vulnerabilities, Rhysida ransomware is unlocked, and Kryptina ransomware code is now freely available. Mandiant reports on Hamas and Iranian cyber activities in the Middle East. Livall helmets had a security flaw allowing real-time location tracking.

Attack Type : Router Compromise

Cause of Issue : Default Passwords

Attack Type : Pharmaceuticals and Biotechnology

Cyberattacks on Hospitals Are Likely to Increase, Putting Lives at Risk, Experts Warn

Cybersecurity experts are warning of increased cyberattacks on hospitals, exemplified by recent incidents like the one at Lurie Children's Hospital in Chicago. Attackers, often from foreign countries, demand hefty ransoms, causing disruptions in medical care. Last year saw a significant rise in such attacks, with hospitals facing financial and operational challenges. The government is urged to take stronger action, including banning ransom payments, while hospitals are advised to bolster their cybersecurity measures. The Department of Health and Human Services plans to revise HIPPA regulations and may tie cybersecurity requirements to Medicaid and Medicare funding. However, rural hospitals may struggle due to limited resources. The aftermath of cyberattacks can be prolonged, affecting patient care and hospital operations. Lurie Hospital, for instance, has been offline for two weeks, impacting surgeries and patient services. Even after restoration, full recovery may take months.

Attack Type : Ransomware Attacks

Cause of Issue : Cybersecurity Vulnerabilities

Attack Type : Pharmaceuticals Industry

BRISKINFOSEC
CYBER TRUST & ASSURANCE

www.briskinfosec.com

HiveForce Labs revealed three zero-day vulnerabilities in Apache

HiveForce Labs recently unveiled alarming findings in cybersecurity, detecting five attacks and six vulnerabilities in just a week, along with identifying two active adversaries. Notably, they disclosed three zero-day vulnerabilities affecting Apache, Microsoft Windows SmartScreen, and Fortinet FortiOS SSL-VPN. One attack by UAC-0027 targeted Ukrainian entities, while Mispadu info stealer now targets Mexican regions via CVE-2023-36025. Additionally, Volt Typhoon threatens U.S. critical infrastructure with advanced tactics, highlighting the escalating global threat of cyberattacks.

Attack Type : Zero-day Vulnerabilities

Cause of Issue : Cybersecurity Threats

Domain Name : (SaaS) Providers

Russian-Linked Hackers Target 80+ Organizations via Roundcube Flaws

Winter Vivern, also known as TA473 and UAC0114, a threat actor aligned with Belarus and Russia, has been identified in a cyber espionage campaign targeting over 80 organizations primarily in Georgia, Poland, and Ukraine. They exploited cross-site scripting (XSS) vulnerabilities in Roundcube webmail servers from October 2023, aiming to collect intelligence on European political and military activities. Winter Vivern's sophisticated methods involve social engineering and exploiting Roundcube flaws to exfiltrate user credentials to a command-and-control server. Recorded Future also found evidence of Winter Vivern targeting Iranian embassies in Russia and the Netherlands, as well as the Georgian Embassy in Sweden, indicating broader geopolitical interests.

Attack Type : Cross-site Scripting (XSS)

Cause of Issue : Cyber espionage

Domain Name : Energy and Utilities

BRISKINFOSEC
CYBER TRUST & ASSURANCE

www.briskinfosec.com

Iranian Hackers Target Middle East Policy Experts with New BASICSTAR Backdoor

Charming Kitten, an Iranian cyber threat group, has targeted Middle East policy experts with a new backdoor named BASICSTAR. They use fake webinar portals and sophisticated social engineering tactics, posing as reputable organizations like the Rasanah International Institute for Iranian Studies. The attacks involve compromised email accounts and serve different malware depending on the victim's operating system, such as POWERLESS for Windows and NokNok for macOS. Charming Kitten is linked to Iran's IRGC and has a history of deploying various backdoors and malware to gather sensitive information. Recorded Future uncovered IRGC's use of contracting companies with ties to Iranian intelligence and military organizations to target Western countries, exporting surveillance and offensive technologies.

Attack Type : Targeted phishing

Cause of Issue : Cyber Espionage

Domain Name : Finance Sector

Bangladesh election commission's app hacked during general elections, claims EC

During Bangladesh's 12th general election, the Election Commission's mobile app, "Smart Election Management BD," was targeted by hackers from Ukraine and Germany, causing a slowdown in its functioning. Users complained about the malfunction, prompting an investigation that confirmed the cyberattack's source. Bangladesh EC Secretary, Md Jahangir Alam, confirmed the attack, stating that it affected the app's real-time voting information service.

Attack Type : Cyber intrusion

Cause of Issue : Public Sector Malfunction

Domain Name : Government Sector

Meta Warns of 8 Spyware Firms Targeting iOS, Android, and Windows Devices

Meta Platforms released their Adversarial Threat Report for Q4 2023, revealing actions taken against eight surveillance firms in Italy, Spain, and the U.A.E. The spyware targeted various devices and platforms, collecting sensitive information and enabling device functionalities. Additionally, Meta removed over 2,000 accounts, Pages, and Groups exhibiting coordinated inauthentic behavior from China, Myanmar, and Ukraine. Countermeasures include new security features in Messenger and WhatsApp. Furthermore, recent discoveries include Patternz, a surveillance tool leveraging advertising data, and MMS Fingerprint, a mobile network attack allegedly utilized by NSO Group.

Attack Type : Surveillance infiltration

Cause of Issue : Surveillance Proliferation

Domain Name : Software Development Companies

BRISKINFOSEC

CYBER TRUST & ASSURANCE

www.briskinfosec.com

Anatsa Android Trojan Bypasses Google Play Security, Expands Reach to New Countries

An Android banking trojan named Anatsa, also known as TeaBot and Toddler, has expanded its campaign to Slovakia, Slovenia, and Czechia. It spreads through innocuous apps on the Google Play Store, gaining control over devices to steal credentials and conduct fraudulent transactions. In a recent November 2023 campaign, dropper apps bypassed security measures, including Android 13's restrictions, targeting Samsung devices specifically. These campaigns are focused and maximize fraud in specific regions. Additionally, a separate campaign impersonating a cryptocurrency wallet service distributes the SpyNote remote access trojan. Google has removed the malicious apps from the Play Store, and users are protected by Google Play Protect.

Attack Type : Android Banking Trojan

Cause of Issue : Android Malware

Domain Name : Software Industry

VMware Alert : Uninstall EAP Now - Critical Flaw Puts Active Directory at Risk

VMware has identified critical flaws in its Enhanced Authentication Plugin (EAP), urging immediate uninstallation. These vulnerabilities enable attackers to trick users into relaying service tickets and hijack sessions. Users connecting to VMware vSphere via the vSphere Client are affected. VMware won't patch the issues and recommends removing the plugin to mitigate risks. Additionally, Joomla! faces XSS flaws potentially leading to remote code execution. Salesforce's Apex language is also vulnerable, allowing unauthorized data access and manipulation, posing serious business risks.

Attack Type : Session Hijacking

Cause of Issue : Arbitrary Authentication

Domain Name : Software Development Companies

Raspberry Robin Worm Rides on New One-Day Flaws to Launch Stealthy Attacks

A new version of the Raspberry Robin worm has surfaced, exploiting two new one-day vulnerabilities to conduct stealthy attacks since October 2023, targeting organizations globally. Notably, it has extended its reach to the financial and insurance sectors in Europe. The attack flow involves dropping malicious files via Discord, activating the worm upon execution, and leveraging exploits for Microsoft Streaming Service Proxy and Windows TPM Device Driver to escalate privileges. The operators employ evasion tactics, including process termination and API routines, to hinder analysis. With an evolving nature, organizations are urged to remain vigilant and stay informed about associated indicators of compromise to mitigate risks effectively.

Attack Type : Stealthy Exploitation

Cause of Issue : Security Vulnerabilities

Attack Type : Software Industry

"Security used to be an inconvenience sometimes, but now it's a necessity all the time."

– Martina Navratilova.

BRISKINFOSEC

CYBER TRUST & ASSURANCE

www.briskinfosec.com

ResumeLooters Steal Millions of Unique Emails from Multiple Sites

ResumeLotters, a threat group, executed a large-scale attack campaign from November to December 2023, targeting 65 websites, predominantly in Asia-Pacific. They employed SQL injection and Cross-Site Scripting (XSS) tactics to pilfer over two million unique emails, primarily from recruitment and retail platforms. Utilizing penetration testing tools like sqlmap and Acunetix, they breached databases and deployed malicious scripts on legitimate sites. The stolen data, including personal information of job seekers, was circulated for sale on Chinese-speaking hacking forums. With over 70% of victims in India, Taiwan, Thailand, and Vietnam, organizations globally are urged to bolster their security measures against such threats.

Attack Type : Database Breach

Cause of Issue : Database Vulnerabilities

Attack Type : Software Industry

27% 27% of healthcare cyber incidents involved backdoor attacks.

36% 36% of healthcare facilities reported an increase in medical complications owing to ransomware attacks(2023-2024).

39% 39% of UK businesses reported suffering a cyber attack in 2022.

45% Cloud-based data breaches made up 45% of all breaches.

74% 74% of all breaches are due in part to human error, privilege misuse, use of stolen credentials, or social engineering.

In 2023

In the first quarter of 2023, we witnessed a massive 600% increase in cyber incidents targeting cryptocurrency firms.

New Coyote Trojan Targets 61 Brazilian Banks with Nim-Powered Attack

The Coyote banking trojan targets 61 Brazilian banking institutions, utilizing the Squirrel installer and a unique combination of Node.js and Nim programming languages for distribution and execution. Coyote monitors user activities, contacts actor-controlled servers for commands, and performs various malicious actions, including capturing screenshots and logging keystrokes. The trojan's use of Nim adds complexity, reflecting evolving sophistication in the threat landscape. Additionally, Brazilian authorities have taken action against similar malware operations, while a new Python-based information stealer targets Vietnamese users.

Attack Type : Banking Trojan

Cause of Issue : Malicious Distribution

Domain Name : Banking Sector

Data breach at French healthcare services firm puts millions at risk

French healthcare services firm Viamedis suffered a cyberattack resulting in the exposure of policyholders' and healthcare professionals' data. The breach exposed sensitive information such as social security numbers and health insurance details. Viamedis has notified impacted parties, filed complaints with authorities, and initiated investigations. The breach affected 84 healthcare organizations covering 20 million insured individuals. The company's General Director stated that the breach resulted from a phishing attack, not ransomware. The incident has disrupted certain healthcare services, impacting providers like Malakoff Humanis.

Attack Type : Phishing Breach

Cause of Issue : Phishing attack

Domain Name : Health care

www.briskinfosec.com

Top 5 Cybersecurity Documentaries

1. Zero Days (2016)

Explores the Stuxnet virus and its implications for cyber warfare, providing insights into the covert world of state-sponsored cyber-attacks.

Available on Hulu and Amazon Prime

Rating : 7.7/10 (IMDb)

2. Citizenfour (2014)

A real-life thriller documenting Edward Snowden's revelation about NSA surveillance, revealing the challenges and sacrifices of whistleblowers.

Available on HBO Max and Amazon Prime

Rating : 8/10 (IMDb)

3. The Great Hack (2019)

Examines the impact of data-driven political campaigns and the role of companies like Cambridge Analytica in manipulating public opinion.

Available on Netflix and Hulu

Rating : 7/10 (IMDb)

4. Terms and Conditions May Apply (2013)

Reveals the consequences of agreeing to online terms and conditions, shedding light on privacy concerns in the digital age.

Available on Amazon Prime and iTunes

Rating : 7.3/10 (IMDb)

5. CyberWar (2016)

A documentary series delving into various aspects of cyber warfare, from nation-state attacks to cybercrime and espionage.

Available on Amazon Prime

Rating : 7.7/10 (IMDb)

BRISKINFOSEC

CYBER TRUST & ASSURANCE

www.briskinfosec.com

Top 5 Cybersecurity Books

Available on Amazon

1. "The Art of Deception"

by Kevin D. Mitnick

Explores the human side of security, detailing social engineering tactics and strategies employed by hackers.

Rating : 4.2/5 (Goodreads)

2. "Hacking : The Art of Exploitation"

by Jon Erickson

Provides hands-on insights into hacking techniques, focusing on the practical aspects of ethical hacking.

Rating : 4.3/5 (Goodreads)

3. "Ghost in the Wires"

by Kevin D. Mitnick

An autobiographical account of Kevin Mitnick's life as a hacker, detailing his experiences and the cat-and-mouse game with law enforcement.

Rating : 4.14/5 (Goodreads)

4. "The Web Application Hacker's Handbook"

by Dafydd Stuttard and Marcus Pinto

A comprehensive guide to understanding and securing web applications, covering common vulnerabilities and attack techniques.

Rating : 4.25/5 (Goodreads)

5. "Countdown to Zero Day"

by Kim Zetter

Investigates the Stuxnet attack on Iran's nuclear facilities, providing an in-depth look at the world of cyber espionage and state-sponsored attacks.

Rating : 4.17/5 (Goodreads)

BRISKINFOSEC

CYBER TRUST & ASSURANCE

www.briskinfosec.com

Most Popular Cybersecurity Framework

1. NIST

(National Institute of Standards and Technology)

Provides a comprehensive set of guidelines, standards, and best practices for managing cybersecurity risks.

2. OWASP

(Open Web Application Security Project)

Focuses on improving the security of software applications, particularly web applications, through community-led projects, documentation, and tools.

3. MITRE ATT&CK

(MITRE Adversarial Tactics, Techniques, and Cyber Kill Chain)

Describes the tactics and techniques used by attackers during various stages of a cyberattack, helping organizations understand and improve their defensive strategies.

4. FIRST

(Forum of Incident Response and Security Teams)

A global organization that promotes cooperation and coordination among incident response and security teams, offering guidance and resources for handling cybersecurity incidents.

5. PTES

(Penetration Testing Execution Standard)

Provides a standard methodology for conducting penetration tests, ensuring consistency and thoroughness in testing the security of systems and networks.

BRISKINFOSEC

CYBER TRUST & ASSURANCE

www.briskinfosec.com

BRISKINFOSEC

CYBER TRUST & ASSURANCE

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