Threatsploit Adversary Report

Edition-66

Feb-2024

Report Insights

- Top Cyberattacks in the Last 30 Days According to Industry
- Top 5 Cybersecurity Movies to Watch on OTT
- Top 5 Cybersecurity Blogs to Read
- Top 5 Cybersecurity Podcasts

BRISK INFOSEC
CYBER TRUST & ASSURANCE

www.briskinfosec.com

Introduction :

Dear Readers,

Welcome to the February 2024 edition of Briskinfosec's Threatsploit Adversary Report, marking our 66th edition. This month, we are thrilled to introduce enhanced features that significantly elevate the depth and breadth of our cybersecurity insights.

Our commitment to keeping you informed about the ever-evolving cyber threat landscape remains unwavering. In this edition, we have meticulously increased the visibility and insights of each attack. You will notice more detailed analyses, reflecting the complexities and nuances of current cybersecurity challenges. Our aim is to provide you with a clearer understanding of each threat, empowering you with the knowledge to better protect your digital assets.

Furthermore, we're excited to blend the worlds of entertainment and cybersecurity education. This edition includes a special feature on the 'Top 5 Cybersecurity Movies'. These selections are not just thrilling cinematic experiences but also provide valuable lessons and insights into the cybersecurity arena. We believe that learning can be both informative and enjoyable, and these movies are a testament to that philosophy.

We hope that these enhancements will not only enrich your reading experience but also strengthen your cybersecurity posture. As always, we are grateful for your continued trust and engagement with our reports. Together, let's stay one step ahead in this dynamic and challenging cyber landscape.

Thank you for your unwavering support.

Best regards,
Briskinfosec Threat Intelligence Team.

SCAN TO READ

Report Insights

- Top Cyberattacks in the Last 30 Days According to Industry
- Top 5 Cybersecurity Movies to Watch on OTT
- Top 5 Cybersecurity Blogs to Read
- Top 5 Cybersecurity Podcasts

Sea Turtle Cyber Espionage Campaign Targets Dutch IT and Telecom Companies

Sea Turtle, a Turkish threat actor, has initiated a cyber espionage campaign targeting telecommunication, media, ISPs, IT-service providers, and Kurdish websites in the Netherlands. The group focuses on supply chain and island-hopping attacks, collecting politically motivated information, including data on minority groups and political dissidents. The stolen information is likely to be exploited for surveillance and intelligence gathering.

Sea Turtle, also known as Cosmic Wolf, Marbled Dust, Teal Kurma, and UNC1326, was first documented in 2019 for state-sponsored attacks in the Middle East and North Africa. The group uses DNS hijacking and has been active since 2017. In 2023, they were found using a Linux/Unix reverse TCP shell called SnappyTCP for attacks. The group remains stealthy, employing defense evasion techniques, and organizations are advised to enhance security measures, including strong password policies and 2FA, to mitigate risks.

Attack Type : Supply Chain Attacks

Cause of Issue : Cyber Espionage

Domain Name : Telecommunications

Today's biggest threats against the energy grid

The U.S. energy grid faces increasing risks from physical threats such as storms and solar storms, with a 77% rise in physical attacks in 2022. Cybersecurity threats are also on the rise, with the energy sector being the fourth most attacked industry in 2022, making up 10.7% of all cyberattacks. Russia's invasion of Ukraine has heightened concerns, especially regarding cyberattacks from groups like Killnet. Attacks on energy companies include data theft, extortion, ransomware, and DDoS threats. Upgrading technology and adopting modern, cloud-based solutions are recommended to reduce vulnerabilities in the aging infrastructure of the energy grid.

Attack Type : Physical and Cyber Attacks

Cause of Issue : Grid Vulnerabilities

Domain Name : Energy and Utilities

New Terrapin Flaw Could Let Attackers Downgrade SSH Protocol Security

SCAN TO READ

Researchers from Ruhr University Bochum have uncovered a vulnerability named Terrapin (CVE-2023-48795) in the Secure Shell (SSH) cryptographic protocol. This "first-ever practically exploitable prefix truncation attack" allows an attacker in an active adversary-in-the-middle position to downgrade SSH connection security by manipulating the extension negotiation message. The vulnerability affects various SSH client and server implementations, including OpenSSH, PuTTY, and FileZilla.

Exploiting this flaw could lead to intercepting sensitive data or gaining control over critical systems. Patches have been released, but nearly 11 million internet-exposed SSH servers remain vulnerable, with the U.S. having the highest instances, followed by China, Germany, Russia, Singapore, and Japan.

Attack Type : Prefix Truncation

Cause of Issue : SSH Vulnerability

Domain Name : (SaaS) Providers

SCAN TO READ

Unifying Security Tech Beyond the Stack : Integrating SecOps with Managed Risk and Strategy

The current state of cybersecurity faces challenges such as talent retention issues, leadership focus, inadequate board engagement, and organizational silos. The lack of alignment between SecOps, risk management, and cybersecurity strategy results in vulnerabilities and a heightened risk of cyberattacks. The use of multiple, unintegrated tools exacerbates these issues, making it difficult to keep up with threats.

A disjointed approach increases the risk and impact of cyber incidents, leading to misallocation of resources and delayed response times. To address these challenges, organizations need a unified approach, integrating managed risk, managed strategy, and a Security Operations Center (SOC) into a cohesive ecosystem for a robust cybersecurity posture.

Attack Type : Prefix Truncation

Cause of Issue : Cybersecurity Challenges

Domain Name : Software Companies

North Korea's Cyber Heist : DPRK Hackers Stole $600 Million in Cryptocurrency in 2023

North Korean state-sponsored hackers targeted cryptocurrency platforms, stealing over $600 million in 2023, constituting nearly a third of all crypto funds stolen globally. Despite a 30% reduction from 2022, DPRK-affiliated attacks were ten times more damaging than non-linked incidents. These attacks, totaling about $3 billion since 2017, serve as a vital revenue source for the sanctions-hit nation, funding weapons programs.

The hackers employ social engineering to compromise private keys, transfer assets to controlled wallets, and convert them to hard currency using OTC brokers. Continuous vigilance and innovation are crucial to counter North Korea's evolving hacking strategies.

Attack Type : Cryptocurrency Theft

Cause of Issue : Loss of Theft

Domain Name : Finance and Banking

Threatsploit Adversary Report
Feb-2024

X-Force 2022 insights : An expanding OT threat landscape

The OT cyber threat landscape is rapidly expanding, with increasing incidents of vulnerability scanning, phishing, and malspam attacks targeting operational technology (OT) environments. The manufacturing industry remains the most attacked, accounting for 23% of total incident response cases, followed by electric utilities (13%), and oil and gas/transportation (8%). Phishing continues to be the predominant initial access vector, constituting 78% of incidents. Vulnerability scanning, weak encryption, and brute force attempts are the most common network attack methods. The Emotet Trojan delivered through malspam is the top threat, comprising 44% of incidents, with a notable shift from ransomware attacks observed in 2021.

Attack Type : OT Cyber Threats

Cause of Issue : OT Vulnerabilities

Domain Name : Energy and Utilities

BRISK INFOSEC
CYBER TRUST & ASSURANCE

US mortgage lender loanDepot confirms ransomware attack

LoanDepot, a leading U.S. mortgage lender, confirmed a ransomware attack that resulted in data encryption. The company, with over $140 billion in serviced loans, experienced system issues over the weekend, affecting the payment portal. While recurring automatic payments will be processed, making new payments through the portal is not possible. The extent and impact of the incident are under investigation, and it's unclear which ransomware group was involved. Customers are advised to be vigilant against potential phishing attacks and identity theft due to the sensitive nature of the compromised data.

Attack Type : Ransomware Attack

Cause of Issue : Data Encryption

Domain Name : Finance and Banking

www.briskinfosec.com

Turkish hackers Sea Turtle expand attacks to Dutch ISPs, telcos

SCAN TO READ

The Turkish state-backed cyber espionage group Sea Turtle, known for its DNS hijacking and man-in-the-middle attacks, has expanded its operations to the Netherlands. Analysts at Hunt & Hackett observed Sea Turtle's activity targeting telcos, media, ISPs, and Kurdish websites, with a focus on acquiring economic and political intelligence aligning with Turkish interests.

The group uses compromised cPanel accounts and recently introduced a new tool called 'SnappyTCP' for basic command and control capabilities. Sea Turtle's tactics, classified as moderately sophisticated, pose a significant threat, and mitigation recommendations include strict network monitoring, MFA implementation, and minimizing SSH exposure.

Attack Type : Espionage, DNS Hijacking

Cause of Issue : State-backed cyber espionage

Domain Name : Telecommunications

One Year After the Colonial Pipeline Attack, Regulation Is Still a Problem

Colonial Pipeline cyberattack prompts federal mandates for operational technology (OT) cybersecurity. TSA issues mandatory directives for all U.S. pipeline operators without prior notice, leading to confusion and concerns about feasibility. Pipeline operators struggle to comply with overly prescriptive and complex rules, with some suggesting that TSA lacks the expertise and tools needed for effective cybersecurity regulation. Calls for the Federal Energy Regulatory Commission (FERC) to handle pipeline cybersecurity regulations gain support, anticipating changes and improved collaboration with the industry in future regulations.

Attack Type : Ransomware Response

Cause of Issue : Mandatory Directives

Domain Name : Energy and Utilities

BRISK INFOSEC
CYBER TRUST & ASSURANCE

Capital Health attack claimed by LockBit ransomware, risk of data leak

LockBit ransomware claims responsibility for a cyberattack on Capital Health hospital network in November 2023. The gang threatens to leak seven terabytes of sensitive medical data and negotiation chats tomorrow if ransom demands are not met. Capital Health, a healthcare service provider in New Jersey, has restored its systems, and operations have returned to normal. LockBit, known for targeting healthcare networks, avoided encrypting files to prevent interference with patient care but stole over 10 million files.

Attack Type : Ransomware Extortion

Cause of Issue : Ransomware attack

Domain Name : Healthcare

Cyberattack Hits Maldives Government : Websites Recover Amid Diplomatic Tensions

Maldives experienced a cyberattack, affecting official websites like the President's office, Foreign Ministry, and Tourism Ministry. The disruption followed derogatory remarks about India's Prime Minister made by three Maldivian ministers. The attack caused temporary unavailability, and the government attributed it to "technical issues." Speculations suggest a connection to diplomatic tensions, but concrete evidence is lacking.

Attack Type : Web Disruption

Cause of Issue : Diplomatic Tensions

Domain Name : Telecommunications

Google : Malware abusing API is standard token theft, not an API issue

SCAN TO READ

Malicious actors are reportedly exploiting an undocumented Google Chrome API to generate new authentication cookies after the previously stolen ones have expired. Multiple information-stealing malware operations, including Lumma, Rhadamanthys, Stealc, Medusa, RisePro, and Whitesnake, are said to be using this technique to gain unauthorized access to users' Google accounts. Google downplays the issue, stating it is a regular case of malware-based cookie theft, but security researchers argue that restricting access to the API would be a more effective solution to prevent abuse by malware operations.

Attack Type : Cookie Theft

Cause of Issue : Undocumented API

Domain Name : (SaaS) Providers

NoName on Rampage! Claims DDoS Attacks on Ukrainian Government Sites

NoName ransomware group claims to have targeted various Ukrainian government websites, including Accordbank, Zaporizhzhya Titanium-Magnesium Plant, and State Tax Service, among others. The alleged attack resulted in disruptions and connectivity issues for some websites, displaying "403 forbidden" and other error messages. The NoName group has previously targeted Finnish government websites as well, indicating a trend of hacktivist groups engaging in cyberattacks amid geopolitical tensions.

Attack Type : Ransomware, DDoS

Cause of Issue : Ransomware attack

Domain Name : Telecommunications

Personal, pregnancy details of Midwives of Windsor patients breached

A data breach involving email has exposed personal and pregnancy information of clients of the Midwives of Windsor in Ontario. The breach, which occurred in April 2023, was reported to Ontario's Information and Privacy Commissioner months before clients were notified. The compromised data includes names, addresses, email addresses, telephone numbers, dates of birth, pregnancy information, treatment/diagnosis details, prescription information, patient IDs, and health insurance information. The breach has been reported to law enforcement, and an investigation is ongoing.

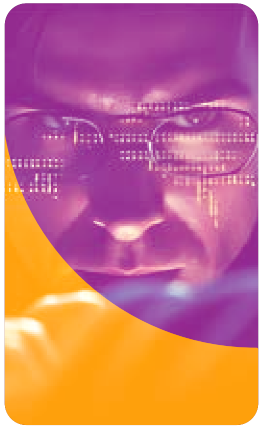
Attack Type : Email Breach

Cause of Issue : Email Compromise

Domain Name : Healthcare

A Cyber Attack Hit the Beirut International Airport

Cyber attackers targeted Beirut International Airport, breaching the Flight Information Display System. The hackers displayed a message warning of war, attributing it to Hezbollah and Iran. The cyber attack disrupted the Baggage Handling System, requiring manual inspection with police dogs. The incident is linked to rising tensions between Israel and Lebanon, but no hacker group has claimed responsibility.



Attack Type : Airport Disruption

Cause of Issue : Escalating Tensions

Domain Name : Industrial Control Systems (ICS)

Russian Hackers Were Inside Ukrainian Telecoms Giant for Almost a Year

SCAN TO READ

Russian hackers infiltrated the systems of Ukraine's largest telecom operator, Kyivstar, in a severe cyberattack starting in May of the previous year. The attack, causing widespread service outages for approximately 24 million users in December, aimed to inflict psychological harm and gather intelligence. The hackers accessed personal information, phone locations, SMS messages, and Telegram accounts. The Ukrainian military was unaffected due to different systems. The Security Service of Ukraine attributed the attack to the Russian military intelligence unit, Sandworm. Investigations are ongoing to determine the method of compromise and malware used. Kyivstar, in collaboration with authorities, restored all services by December 20.

Attack Type : Cyber Espionage

Cause of Issue : Cybersecurity Breach

Domain Name : Telecommunications

Stealthy AsyncRAT malware attacks targets US infrastructure for 11 months

Over the past 11 months, a sophisticated cyber campaign has been spreading the AsyncRAT malware to targeted individuals and organizations, particularly focusing on key infrastructure entities in the U.S. The campaign involves hundreds of unique loader samples and more than 100 domains, with attackers using tactics like hijacked email threads and obfuscated scripts to evade detection. The malware's loader employs anti-sandboxing measures and a domain generation algorithm to avoid analysis and maintain stealth. While the specific threat actors remain unidentified, AT&T Alien Labs has provided indicators of compromise and detection signatures to help organizations identify and mitigate this ongoing AsyncRAT campaign.

Attack Type : Targeted Malware

Cause of Issue : Cyber Espionage

Domain Name : Telecommunications

SCAN TO READ

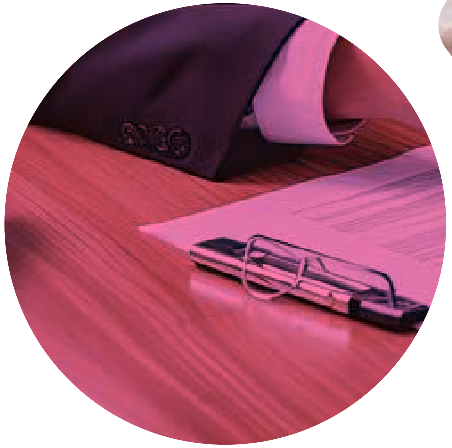
Mortgage firm loanDepot cyberattack impacts IT systems, payment portal

LoanDepot, a top U.S. mortgage lender, grapples with a cyberattack, forcing IT system shutdowns. They urge customers to pay via phone amid online portal issues. Suspected ransomware attack heightens data security worries, mirroring past industry breaches, highlighting cybersecurity risks.

Attack Type : Ransomware

Cause of Issue : Cyberattack Disruption

Domain Name : Finance and Banking



SEC X (Twitter) Account Hacked, Spreads Fake News About Bitcoin ETFs

The official Twitter account of the U.S. Securities and Exchange Commission (SEC) was hacked, leading to a false announcement of Bitcoin ETF approval, causing market excitement and panic. The agency quickly clarified the hack and disavowed the tweet. Cybersecurity experts emphasized the ongoing threat of social media account compromise. Despite the incident, the SEC is still expected to review Bitcoin ETF applications, sparking debates on online information reliability and government social media platform security.

Attack Type : Social Engineering

Cause of Issue : Social Media Hack

Domain Name : Software Development Companies

X Account of Google Cybersecurity Firm Mandiant Hacked in Crypto Scam

Mandiant, a cybersecurity firm owned by Google, had its Twitter account compromised, leading to a cryptocurrency scam targeting its 122,000 followers. Hackers posed as the Phantom crypto wallet, offering fake airdrops. Despite regaining control, restoring the account proved challenging due to Twitter's restrictions. This incident reflects a trend of high-profile Twitter hacks for cryptocurrency scams, including notable figures like Barack Obama and Elon Musk. Security precautions include safeguarding private keys and using strong passwords.

Attack Type : Twitter Crypto Scam

Cause of Issue : Twitter Breach

Domain Name : Software Companies

Three ways to Supercharge Your Software Supply Chain Security

This article underscores three key strategies for enhancing Software Supply Chain Security: protecting sensitive data, utilizing Software Composition Analysis (SCA) tools, and integrating ethical hacking in development. These measures aim to bolster security, ease compliance, and reduce risks throughout the supply chain, ensuring more robust and trustworthy software for users and regulators.

Attack Type : Supply Chain Attacks

Cause of Issue : Redundant Repetition

Domain Name : Software Companies

Cybercriminals share Millions of Stolen Records During Holiday Break

During the holiday season, cybercriminals conducted a major event called "Leaksmus" on the Dark Web, leaking 50 million records of sensitive personal data worldwide. These leaks, tagged "Free Leaksmas," aimed to attract new clients and foster mutual support among criminals. Breaches included both recent and older incidents, with notable targets such as Peruvian telecom provider Movistar and Swedish fintech company Klarna. Known threat actors like SeigedSec and "Five Families" were involved in distributing stolen data. Cybercriminals also offered discounts on stolen payment data to lure new buyers, highlighting the ongoing focus on exploiting personal information for fraudulent purposes.

Attack Type : Data Breach

Cause of Issue : Summary Length

Domain Name : Finance and Banking

Attackers Abuse Google OAuth Endpoint to Hijack User Sessions

SCAN TO READ

CloudSEK's Pavan Karthick M outlined a critical exploit discovered by "Prisma," allowing persistent Google cookie generation via token manipulation. Infostealers like Lumma and Rhadamanthys adopted it, spreading rapidly. The exploit targets Google's "MultiLogin" OAuth endpoint, regenerating cookies even after password resets. Lumma's encryption of tokens makes detection difficult, highlighting the need for advanced defense strategies against evolving cyber threats.

Attack Type : Persistent OAuth

Cause of Issue : Undocumented Endpoint

Domain Name : Software Development Companies

TensorFlow CI/CD Flaw Exposed Supply Chain to Poisoning Attacks

The TensorFlow machine learning framework had CI/CD misconfigurations that could be exploited for supply chain attacks. Vulnerabilities in GitHub Actions workflows on self-hosted runners allowed attackers to upload malicious releases and gain remote code execution. These issues were fixed after disclosure in December 2023. Similar vulnerabilities were found in other projects like Chia Networks, Microsoft DeepSpeed, and PyTorch, posing risks to AI/ML companies reliant on self-hosted runners for CI/CD processes.

Attack Type : Supply Chain Attack

Cause of Issue : Misconfigured CI/CD

Domain Name : Software Development Companies

New Docker Malware Steals CPU for Crypto & Drives Fake Website Traffic

A new attack campaign targets vulnerable Docker services, deploying XMRig cryptocurrency miners and 9Hits Viewer software for profit. It's the first known use of 9Hits as malware. Attackers exploit Docker hosts, deploy malicious containers from Docker Hub, and use 9Hits to generate traffic credits while XMRig exhausts CPU resources. Legitimate workloads suffer, highlighting evolving adversary tactics for financial gain.

Attack Type : Containerized Malware

Cause of Issue : Docker Vulnerabilities

Domain Name : Software Development Companies

SCAN TO READ

New Findings Challenge Attribution in Denmark's Energy Sector Cyberattacks

Cyber attacks hit Denmark's energy sector in May 2023, exploiting Zyxel firewall vulnerabilities and deploying Mirai botnets. Forescout's investigation revealed two separate waves of attacks, unrelated to the Russia-linked Sandworm group. The second wave targeted unpatched Zyxel firewalls in a broader campaign, lasting from February to October 2023 across Europe and the U.S. SektorCERT couldn't confirm Sandworm's involvement, highlighting the challenge of attribution in cyber attacks.

Attack Type : Targeted Exploitation

Cause of Issue : Attribution Challenge

Domain Name : Software Development Companies

DDoS Attacks on the Environmental Services Industry Surge by 61,839% in 2023

In Q4 2023, the environmental services sector saw a staggering 61,839% spike in HTTP-based DDoS attacks, coinciding with COP 28. The cryptocurrency industry remained the top target, while the U.S. and China were the main sources of attack traffic. Attacks on Palestinian and Taiwanese websites surged amidst geopolitical tensions. DDoS attacks became longer and more sophisticated, targeting multiple IP destinations. Cloudflare warned of the growing threat from unsecured API endpoints.

Attack Type : HTTP DDoS

Cause of Issue : Cybersecurity Threat

Domain Name : Industrial Control Systems (ICS)

CISA : AWS, Microsoft 365 Accounts Under Active 'Androxgh0st' Attack

The FBI and CISA have issued an alert regarding a malware campaign targeting Apache webservers and Laravel websites. The threat, called "Androxgh0st," exploits known vulnerabilities to steal credentials for popular applications like AWS and Microsoft 365. The malware scans for Laravel .env files containing sensitive information and can deploy web shells. Organizations are advised to patch vulnerabilities, limit exposure of internet-facing systems, and review credentials stored in .env files for unauthorized access.

Attack Type : Web Credential Theft

Cause of Issue : Credential Theft

Domain Name : (SaaS) Providers

North Korean Hackers Weaponize Fake Research to Deliver RokRAT Backdoor

In December 2023, ScarCruft, a threat actor linked to North Korea's Ministry of State Security, targeted media organizations and experts in North Korean affairs with a sophisticated campaign. They employed decoy documents and multi-stage infection sequences to deliver the RokRAT backdoor, posing as legitimate organizations to expand their targets and avoid detection. This strategic effort aimed to gather intelligence and understand international perceptions of North Korea for decision-making purposes.

Attack Type : Spear-phishing Campaign

Cause of Issue : Cyber Espionage

Domain Name : (SaaS) Providers

Apache ActiveMQ Flaw Exploited in New Godzilla Web Shell Attacks

Cybersecurity experts have observed a surge in malicious activity exploiting a vulnerability (CVE-2023-46604) in Apache ActiveMQ. Threat actors are using the Godzilla web shell to gain control over compromised systems, evading detection with its concealed JSP code. This exploit allows for various malicious actions, including ransomware deployment and DDoS attacks. Users are urged to update to the latest ActiveMQ version to protect against these threats.

Attack Type : Web Shell Attack

Cause of Issue : ActiveMQ Vulnerability

Domain Name : Industrial Control Systems (ICS)

SCAN TO READ

40,000 Attacks in 3 Days : Critical Confluence RCE Under Active Exploitation

A critical flaw, CVE-2023-22527, affects older versions of Atlassian Confluence Data Center and Server, allowing remote code execution by unauthenticated attackers. Over 40,000 exploitation attempts from 600 IPs, primarily Russian, have been recorded within days of disclosure. The flaw permits arbitrary code execution, prompting opportunistic scanning for vulnerable servers.

Attack Type : Remote Code Execution

Cause of Issue : Software Vulnerability

Domain Name : Software Development Companies

Water services giant Veolia North America hit by ransomware attack

Veolia North America faced a ransomware attack impacting its Municipal Water division's systems, leading to temporary shutdowns but no disruption to water services. Limited personal data exposure was reported, amid a broader trend of cyber threats against water facilities globally. Authorities have issued guidance to enhance cybersecurity defenses in the water sector.

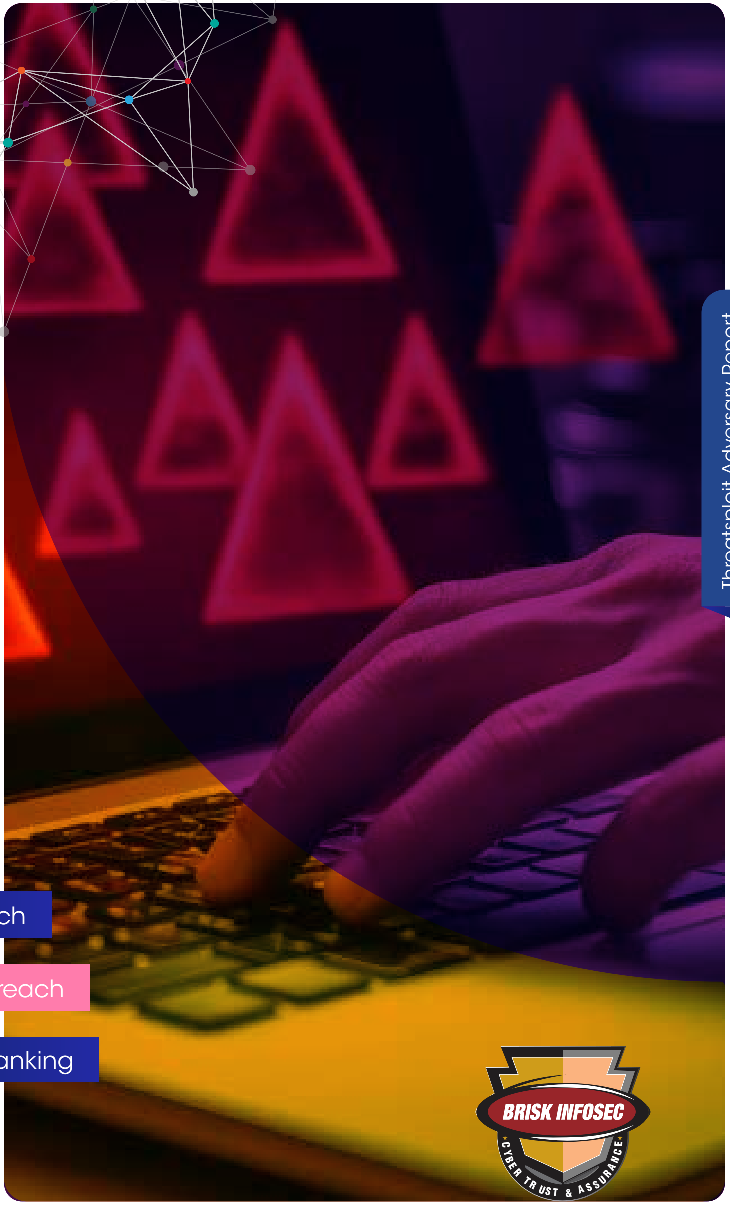
Attack Type : Ransomware Breach

Cause of Issue : Cybersecurity Breach

Domain Name : Industrial Control Systems (ICS)

LoanDepot cyberattack causes data breach for 16.6 million people

LoanDepot, a prominent U.S. mortgage lender, recently disclosed a ransomware attack that occurred on January 6, affecting approximately 16.6 million individuals. The attack led to system shutdowns and disruptions in customer portals, including payment processing delays. The company confirmed the breach days later, offering affected individuals free credit monitoring and identity protection services. While progress has been made in restoring systems, the investigation is ongoing, and the specific types of stolen personal information have not been disclosed. This incident follows a previous data breach in August 2022. As loanDepot stores sensitive financial data, affected individuals should be vigilant against phishing and identity theft attempts.



Attack Type : Ransomware Breach

Cause of Issue : Cybersecurity Breach

Domain Name : Finance and Banking

AllaKore RAT Malware Targeting Mexican Firms with Financial Fraud Tricks

A spear-phishing campaign targeting Mexican financial institutions is underway, deploying a modified version of the AllaKore RAT. This campaign, attributed to a Latin America-based threat actor, has been active since 2021. The RAT is tailored to steal banking credentials for financial fraud. Large companies with revenues over $100 million are targeted across various sectors. The malware, delivered via ZIP files, grants attackers capabilities like keylogging and remote control. The threat actor's ties to Latin America are indicated by the use of Mexico Starlink IPs and Spanish-language instructions. Additionally, Lamassu Douro bitcoin ATMs were found vulnerable to attacks, allowing physical access to steal user assets, though these issues were addressed in October 2023.

Attack Type : Financial Phishing

Cause of Issue : Cybersecurity Threat

Domain Name : Finance and Banking

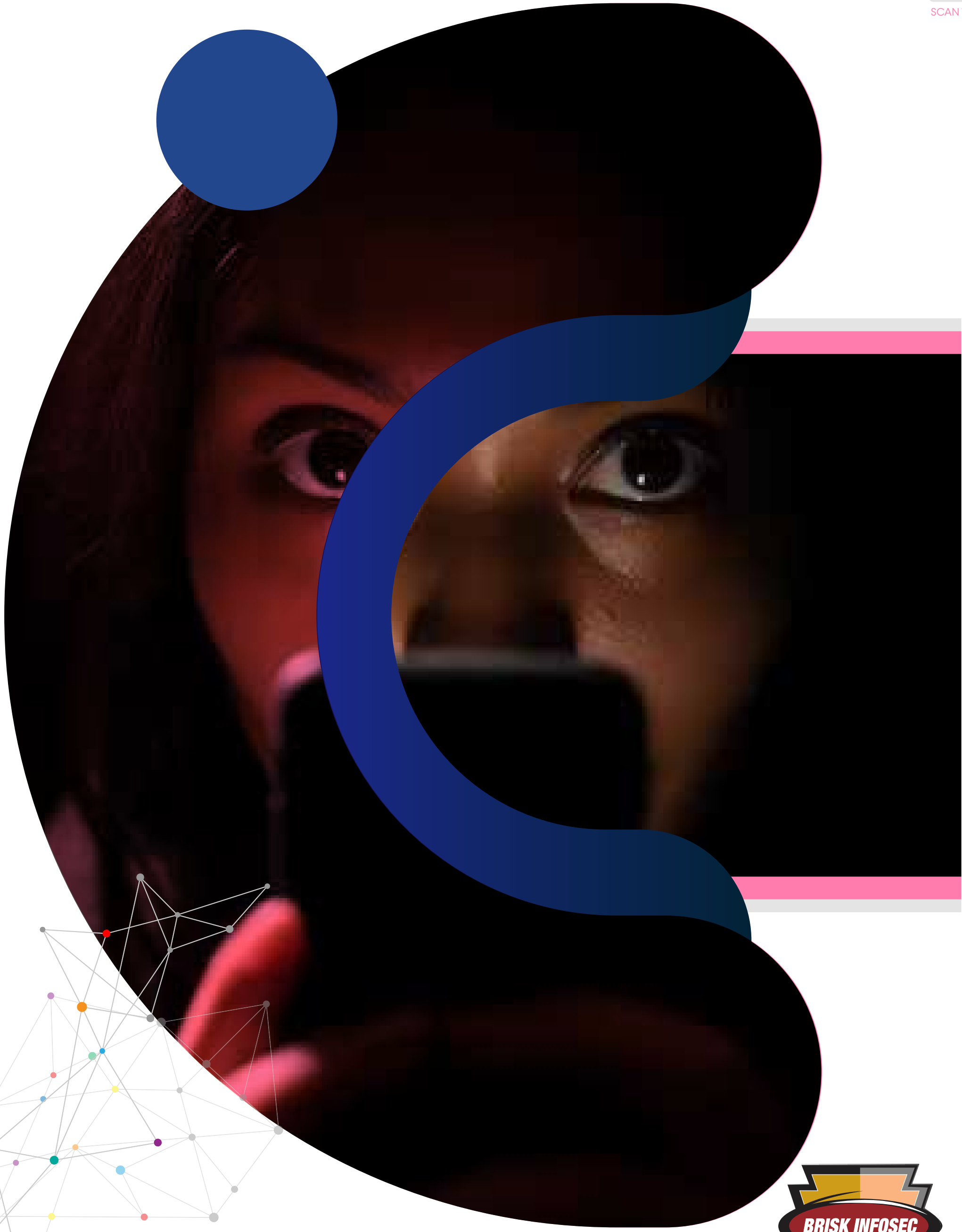
Malicious Ads on Google Target Chinese Users with Fake Messaging Apps

A malvertising campaign dubbed FakeAPP targets Chinese-speaking users by luring them to download messaging apps like Telegram, WhatsApp, and LINE, which are redirected to bogus websites containing Remote Administration Trojans (RATs). The campaign, traced to Nigeria-based advertiser accounts, aims for quantity over quality, constantly pushing new payloads. Additionally, phishing attacks using the Greatness platform have spiked, targeting Microsoft 365 users with personalized credential harvesting pages. The phishing emails spoof trusted sources and induce urgency, while Greatness, available for $120 per month, facilitates attacks at scale. South Korean companies have also been targeted with phishing lures impersonating tech firms like Kakao to distribute malware via malicious Windows shortcut files.

Attack Type : Malvertising & Phishing

Cause of Issue : Cybersecurity Threats

Domain Name : Private Sector Business



Top 5

Cybersecurity Movies

SCAN TO READ

1. Hackers (1995) A classic cyberpunk film following a group of hackers who uncover a conspiracy, exploring themes of hacking and cybercrime.

Available on Amazon Prime and Google Play.

Rating : **6.3/10** (IMDb)

2. The Matrix (1999) A sci-fi masterpiece intertwining reality and virtual worlds, touching on themes of hacking, artificial intelligence, and control.

Available on Netflix and HBO Max

Rating : **8.7/10** (IMDb)

3. WarGames (1983) A thriller about a young computer whiz accidentally hacking into a military supercomputer, highlighting the unintended consequences of hacking.

Available on Amazon Prime and iTunes.

Rating : **7.1/10** (IMDb)

4. Sneakers (1992) A blend of comedy and suspense, focusing on ethical hacking and security testing, with a diverse team of experts.

Available on Disney+ and Hulu.

Rating : **7.1/10** (IMDb)

5. Who Am I (2014) A German techno-thriller film that follows a young computer whiz who becomes involved with an underground hacking group. The movie explores themes of identity, hacking, and the consequences of online actions.

Available on Amazon Prime, Netflix, and Google Play.

Rating : **7.6/10** (IMDb)

BRISK INFOSEC
CYBER TRUST & ASSURANCE

TOP 5 BLOGS

1. Host Header Attack

Protect your web applications from Host Header Injection (HHI) attacks. Learn how attackers exploit vulnerabilities and implement mitigation strategies effectively.

Views : **28809**

2. Getting Started with Frida

Explore the dynamic instrumentation toolkit Frida and its applications in mobile app security testing. Learn about installation, commands, and setting up Frida on various platforms. Discover essential Frida flavors and tools for effective security assessments.

Views : **25721**

3. Red vs Blue vs Purple vs Orange vs Yellow vs Green vs White Cybersecurity Team

Discover the roles and responsibilities of Red, Blue, Yellow, Purple, Orange, Green, and White cybersecurity teams in the industry. Learn how each team contributes to offensive and defensive security operations, maximizes performance, and ensures software and applications are free from security issues.

Views : **21830**

4. SQL Injection - Using Burp Suite

Discover SQL injection vulnerabilities, exploitation techniques, and prevention measures. Learn how Burp Suite aids in exploitation and manual testing. Benefit from Briskinfosec's expert security assessments for robust protection against cyber threats.

Views : **16267**

5. FTP Penetration Testing

Explore FTP penetration testing, vulnerabilities, and defense strategies. Learn how Briskinfosec strengthens network security with practical solutions. Discover case studies illustrating successful security assessments.

Views : **11943**

SCAN TO READ

BRISK INFOSEC
CYBER TRUST & ASSURANCE

TOP 5 CYBERSECURITY PODCASTS

SCAN TO READ

1.Security Now!

Hosted by Steve Gibson and Leo Laporte, it covers the latest security news and trends, offering insights into the world of cybersecurity.

Listen On

Available on Twit.Tv

2. Darknet Diaries

Narrates real-life hacking and cybersecurity stories, providing a captivating and informative look into the world of cybercrime.

Listen On

darknetdiaries.com and various podcast platforms.

3. The CyberWire

Offers daily news briefings and interviews covering a wide range of cybersecurity topics, keeping listeners informed about the latest developments.

Listen On

Thecyberwire.com and various podcast platforms.

4. Hacking Humans

Explores the human element of security, discussing social engineering techniques and how people are manipulated into compromising security.

Listen On

Thecyberwire.com and various podcast platforms.

5. Risky Business

A weekly podcast discussing the latest cybersecurity news, vulnerabilities, and breaches, providing practical insights for professionals.

Listen On

Risky.biz and various podcast platforms.

BRISK INFOSEC

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