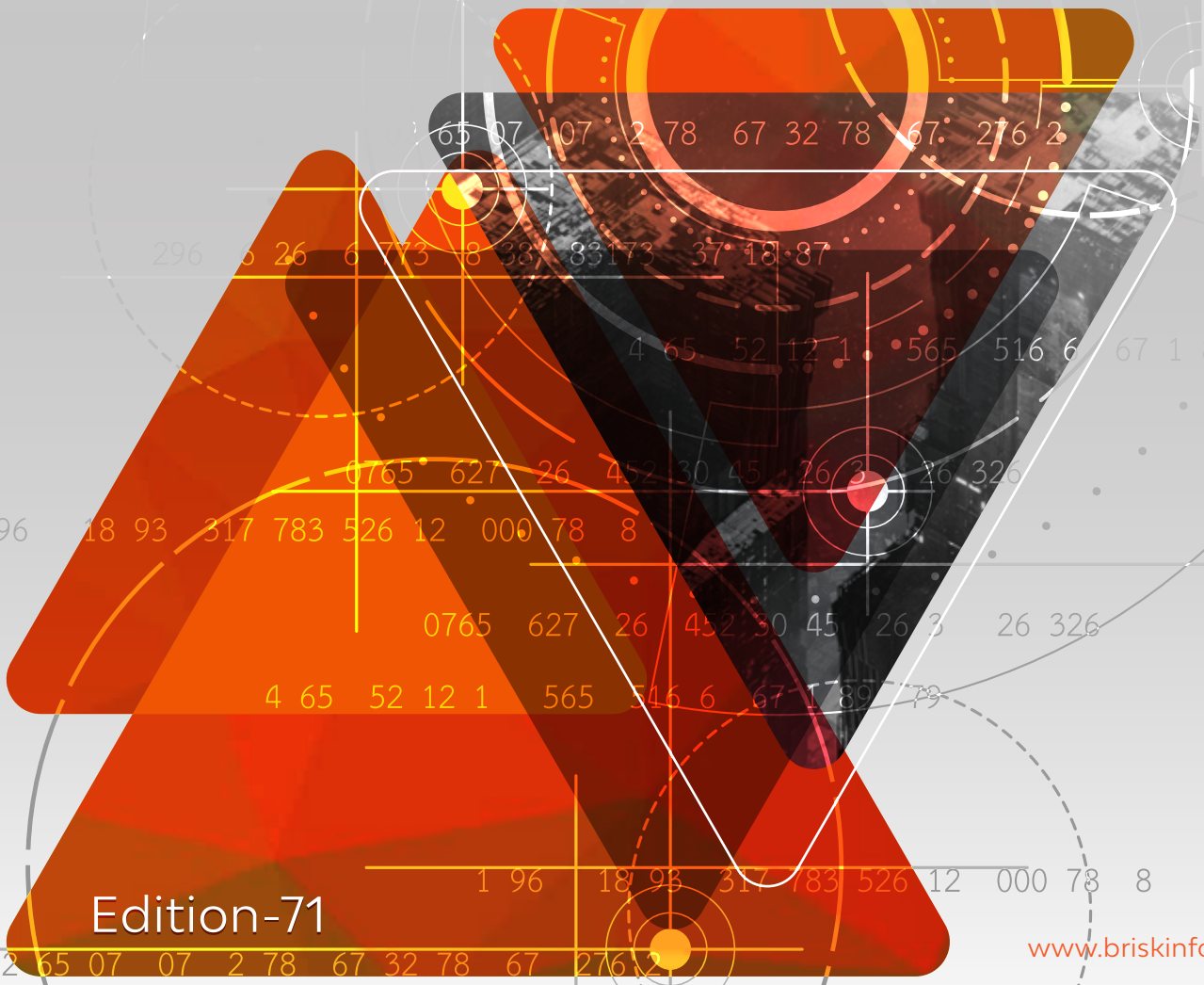
THREATSPLOIT

ADVERSARY REPORT

July - 2024



Edition-71

www.briskinfosec.com

INTRODUCTION :

Dear Readers,

As technology keeps changing fast, the cybersecurity world gets more complicated and riskier. Welcome to the July 2024 edition of the Threatsploit Adversary Report. We're here to keep you updated on the latest cybersecurity developments and threats.

This month, we cover the biggest cybersecurity incidents from the past month across various sectors like technology, finance, healthcare, and government. These incidents show how cyber threats affect many areas of our lives. We'll talk about complex cyber-espionage operations, new types of dangerous software, and tricky tricks used in social media to steal data.

We analyze these threats in detail to show you how cyber attackers work and what weaknesses they use. Our goal is to give you a clear picture of the current cyber threat landscape so you can stay informed about how hackers operate.

Explore our detailed descriptions of each incident to learn more about these threats and what they mean for you. The Threatsploit Adversary Report is here to help you understand the challenging world of cybersecurity so you can stay alert and ready.

Thank you for joining us as we work to keep you ahead of cybersecurity risks.

Best regards,

Briskinfosec Threat Intelligence Team.

Report Inside :

CONTENTS :

CYBER INCIDENT: CLINICAL IMPACT IN SOUTH EAST LONDON

In early June, Synnovis, a pathology lab serving NHS trusts in south-east London, suffered a ransomware attack, severely disrupting blood test processing. NHS London declared a regional incident, coordinating efforts to mitigate the effects, including reallocating surgeries, rerouting blood tests, and boosting blood supplies. Over 800 operations and 700 appointments were rescheduled at King's College Hospital and Guy's and St Thomas' trusts in the first week alone. Despite efforts to restore services, significant disruption is expected to persist. The NHS urges patients to seek emergency care normally and attend scheduled appointments unless notified otherwise.

Attack Type : Ransomware Cyberattack

Cause of Issue : Cybersecurity Breach

Industry Type : Health Care Domain

NICERAT MALWARE TARGETS SOUTH KOREAN USERS VIA CRACKED SOFTWARE

A newly identified malware, NiceRAT, has emerged as a significant threat primarily targeting South Korean users. This malware spreads by masquerading as cracked software or license verification tools for popular programs such as Microsoft Windows and Office. NiceRAT is especially insidious because it advises users to disable anti-malware programs during distribution, making detection difficult.NiceRAT operates via a botnet utilizing NanoCore RAT and Discord for command-and-control purposes. This functionality allows threat actors to steal sensitive data from infected devices effectively. Notably, the malware's development includes both an open-source and premium version, suggesting it operates under a malware-as-a-service model. Meanwhile, there has been a resurgence of the Bondnet cryptocurrency mining botnet, which uses modified legitimate tools for command-and-control operations. This resurgence underscores the ongoing evolution and sophistication of cyber threats leveraging legitimate software for malicious purposes.

Attack Type : Malware Propagation

Cause of Issue : Software Exploitation

Industry Type : Software Development Companies

PAKISTANI HACKERS USE DISGOMOJI MALWARE IN INDIAN GOVERNMENT CYBER ATTACKS

In 2024, a cyber espionage campaign targeting Indian government entities has been linked to a UTA0137, a Pakistan-based threat actor, was identified. This actor employs a malware named DISGOMOJI. The application is written in Golang and utilizes Discord for command and control through the use of emojis. DISGOMOJI infects Linux systems through spear-phishing emails that contain malicious Golang binaries. It captures information, executes commands, and exfiltrates data using emojis like for command execution, for taking screenshots, Upload a file from the victim's device to the channel, Upload a file from the victim's device to transfer [.]sh, Download a file to the victim's device, Download a file hosted on oshi[.]at to the victim's device, Find and exfiltrate files matching the following extensions : CSV, DOC, ISO, JPG, ODP, ODS, ODT, PDF, PPT, RAR, SQL, TAR, XLS, and ZIP, Gather all Mozilla Firefox profiles on the victim's device into a ZIP archive, Terminate the malware process on the victim's device, Inform the attacker that the command is being processed, Inform the attacker that the command has been executed. The campaign also employs tools.

Attack Type : Cyber Espionage

Cause of Issue : Cyber Vulnerabilities

Industry Type : Telecommunications

CELEBRITY TIKTOK ACCOUNTS ARE COMPROMISED USING A ZERO-CLICK ATTACK VIA DMS

TikTok has encountered significant security challenges, including a recent zero-click attack exploiting a messaging flaw. This sophisticated attack allowed threat actors to gain control of prominent accounts without any user interaction. Attackers have also exploited prior vulnerabilities, resulting in unauthorized data access and account takeovers. These incidents have heightened concerns about user privacy, particularly given TikTok's ownership by a Chinese company. Efforts to mitigate risks and restore affected accounts are ongoing; however, TikTok remains a frequent target for malicious activities. For instance, individuals have exploited incidents like the "Invisible Challenge" to disseminate malware, thereby jeopardizing user security. The global community has responded with scrutiny, resulting in bans imposed by various countries. These actions reflect ongoing debates surrounding TikTok's data handling practices and concerns over its potential for facilitating propaganda.

Attack Type : Zero-click account takeover

Cause of Issue : Messaging Vulnerability

Industry Type : Media and Entertainment

CDK GLOBAL OUTAGE CAUSED BY BLACKSUIT RANSOMWARE ATTACK

CDK Global, a prominent SaaS provider serving car dealerships, experienced a significant IT outage following a ransomware attack attributed to the BlackSuit gang. The attack, which targeted CDK's systems across North America, severely disrupted operations and necessitated the use of manual processes by affected dealerships. CDK Global has initiated negotiations with the hackers to obtain a decryption and prevent potential data leaks. The BlackSuit gang, which emerged in 2023 as a successor to the Royal ransomware group, has garnered attention for its targeting of organizations on a global scale. The incident underscores the persistent threat posed by ransomware groups like BlackSuit and highlights the critical need for robust cybersecurity measures and incident response protocols within organizations.

Attack Type : Ransomware Attack

Cause of Issue : Cybersecurity Breach

Industry Type : Telecommunications

MILITARY-THEMED EMAIL SCAM SPREADS MALWARE TO INFECT PAKISTANI USERS

Cybersecurity researchers at Securonix have identified a new phishing campaign dubbed PHANTOM#SPIKE, targeting individuals in Pakistan. This campaign employs military-themed phishing documents that contain password-protected ZIP files. Upon extraction, these ZIP files reveal a CHM file alongside a hidden executable named ""RuntimeIndexer.exe."" When the user opens the CHM file, it deceives them by displaying benign content like meeting minutes. Simultaneously, the hidden executable (""RuntimeIndexer.exe"") operates as a stealthy backdoor, enabling remote access to compromised machines. This backdoor functionality allows attackers to execute commands, gather system information, and exfiltrate sensitive data to a remote server.PHANTOM#SPIKE stands out for its use of straightforward yet effective techniques to establish persistent access and execute malicious activities on infected systems.

Attack Type : Phishing Backdoor

Cause of Issue : Social Engineering

Industry Type : Telecommunications

OYSTER BACKDOOR SPREADING VIA TROJANIZED POPULAR SOFTWARE DOWNLOADS

Recent Rapid7 findings highlight a malvertising campaign that uses fake websites to distribute trojanized installers for popular software like Google Chrome and Microsoft Teams. These installers deliver a backdoor known as Oyster, associated with the Russian-linked ITG23 group behind TrickBot. The malware allows remote access and gathers host information while attempting to disguise itself by installing legitimate software afterward. Simultaneously, email phishing campaigns have identified a group named Rogue Raticate, which is deploying Net Support RAT via PDF decoys. Additionally, a new phishing-as-a-service platform called ONNX Store offers sophisticated tools like QR code phishing and 2FA bypass mechanisms to target Microsoft 365 credentials.

Attack Type : Malvertising Campaign

Cause of Issue : Software exploitation

Industry Type : Software Development Companies

CHINESE HACKERS DEPLOY SPICERAT AND SUGARGHOST IN GLOBAL ESPIONAGE CAMPAIGN

A Chinese-speaking threat actor known as SneakyChef is responsible for a cyber espionage campaign. Operating since at least August 2023, the campaign utilizes malware such as SugarGhost and SpiceRAT to target government entities across Asia, EMEA, and the US. Tactics include spear-phishing with lures like scanned government documents, employing techniques like Windows Shortcut files, and self-extracting archives for initial infection. The operation, also named Operation Diplomatic Specter by Palo Alto Networks, highlights a significant cybersecurity threat focused on governmental and AI-related sectors globally.

Attack Type : Targeted Spear-Phishing

Cause of Issue : Cyber Espionage

Industry Type : Software Development Companies

CHINESE CYBER ESPIONAGE TARGETS TELECOM

Symantec's Threat Hunter Team identified a cyber espionage campaign targeting telecom operators in an undisclosed Asian country since 2021, possibly starting in 2020. The attackers, believed to be associated with Chinese groups like Mustang Panda and RedFoxtrot, used custom backdoors such as COOLCLIENT and QUICKHEAL to infiltrate networks, steal credentials, and potentially gather sensitive data. The campaign also targeted a telecom services company and a university in a different Asian country. Motives range from intelligence gathering to the potential disruption of critical infrastructure.

Attack Type : Targeted Cyber Espionage

Cause of Issue : State-Sponsored Espionage

Industry Type : Telecommunications

COMMANDO CAT: A NOVEL CRYPTOJACKING ATTACK ABUSING DOCKER REMOTE API SERVERS

The Commando Cat attack campaign targets exposed Docker remote API servers to deploy cryptocurrency miners. Attackers exploit Docker's vulnerabilities using images from the Commando project, starting with the benign cmd.cat/chattr image. They break out of containers using chroot and volume binding to access host systems and deploy malware via scripts that download binaries. Indicators like specific User-Agent strings and DropBear SSH on port 3022 help detect their presence. To prevent such attacks, mitigation entails securing Docker configurations, using trusted images, and following container security best practices.

Attack Type : Container breakout

Cause of Issue : Exposed API

Industry Type : Software Development Companies

HACKER CLAIMS TO HAVE 30 MILLION CUSTOMER RECORDS FROM AUSTRALIAN TICKET SELLER GIANT TEG

A hacker claims to have stolen data from TEG, an Australian live events and ticketing company, and sells it on a hacking forum. The data allegedly includes details of 30 million users, such as full names, genders, dates of birth, usernames, hashed passwords, and email addresses. Ticketek, owned by TEG, had previously disclosed a data breach affecting Australian customers, but it claimed no customer accounts were compromised due to password encryption. However, the hacker's advertised data potentially impacted names, dates of birth, and email addresses. TechCrunch verified the legitimacy of some data samples by attempting to create accounts with published email addresses. The breach may involve a cloud platform, possibly Snowflake, but Snowflake denies any direct responsibility, attributing such incidents to customer misconfigurations and a lack of multi-factor authentication.

Attack Type : Data Breach

Cause of Issue : Third-party Vulnerability

Industry Type : Media and Entertainment

“ CHANGE HEALTHCARE ” CONFIRMS RANSOMWARE HACKERS STOLE MEDICAL RECORDS ON A ‘SUBSTANTIAL PROPORTION’ OF AMERICANS

UnitedHealth Group owned Change Healthcare, a major U.S. health tech company, suffered a ransomware attack in February. This incident led to widespread disruptions in healthcare services across the country for weeks. The attackers stole sensitive personal and medical information, affecting a significant portion of the American population. This data breach included names, addresses, dates of birth, Social Security numbers, medical records, insurance details, and financial information. Change Healthcare confirmed it paid a ransom to prevent the publication of stolen data. The attack cost UnitedHealth roughly $870 million. Notifications to affected individuals are expected to begin in late July.

Attack Type : Ransomware Attack

Cause of Issue : Security Lapse

Industry Type : Health Care Domain

EXCOBALT CYBER GANG TARGETS RUSSIAN SECTORS WITH A NEW GORED BACKDOOR

ExCobalt, a cybercrime group linked to the notorious Cobalt Gang, has targeted Russian organizations with sophisticated cyber espionage tactics using tools like the newly identified GoRed backdoor. This group, active since at least 2016, employs methods such as compromising contractors and supply chain attacks to gain initial access. They target a wide range of sectors, including government, IT, metallurgy, mining, software development, and telecommunications. ExCobalt's arsenal includes well-known tools and exploits like Metasploit, Mimikatz, and Linux privilege escalation vulnerabilities. Their operations are characterized by continuous evolution and adaptation, demonstrating significant expertise in bypassing security controls and maintaining persistence in compromised environments.

Attack Type : Cyber Espionage

Cause of Issue : Supply Chain

Industry Type : Software Development Companies

HACKER CLAIMS A BREACH OF INDIA’S EMIGRATE LABOR PORTAL

A hacker claims to have accessed and is selling a database from India's eMigrate portal, managed by the Ministry of External Affairs. Users' personal details, such as names, emails, phone numbers, dates of birth, addresses, and passport information, are included in the data. TechCrunch verified the authenticity of some data entries, including that of an Indian government ambassador. Whether the data came from a recent breach or an earlier incident remains uncertain. India's CERT-In is investigating, but the Ministry of External Affairs has not responded to inquiries. This incident follows previous cybersecurity issues affecting Indian government services.

Attack Type : Data Breach

Cause of Issue : Security Vulnerability

Industry Type : Government Sector

110,000 WEBSITES ARE AFFECTED BY HIJACKED POLYFILL SUPPLY CHAIN ATTACK

Google has blocked ads for e-commerce sites using Polyfill.io due to a supply chain attack. A Chinese company, Funnel, acquired the domain and modified the JavaScript library to redirect users to malicious sites. Over 110,000 websites embedding in the library are affected. The original creator, Andrew Betts, advised immediate removal, stating that most web features now have universal support. Cloudflare and Fastly offered alternative endpoints. Concerns include reliance on Funnel for security, as evidenced by malware injections redirecting to harmful sites. Additional security issues involve a critical flaw in Adobe Commerce and Magento websites, potentially leading to remote code execution.

Attack Type : Supply Chain Attack

Cause of Issue : Domain Acquisition

Industry Type : Software Development Companies

NEW MEDUSA MALWARE VARIANTS TARGET ANDROID USERS IN SEVEN COUNTRIES

The Medusa banking trojan, also known as TangleBot, has resurfaced with new, compact variants targeting countries including France, Italy, the US, and others since May. These variants require fewer permissions and focus on initiating fraudulent transactions directly from compromised Android devices. Initially discovered in 2020, Medusa offers capabilities like keylogging and SMS manipulation. Recent campaigns identified by Cleafy involve lighter variants deployed via SMS phishing, using dropper apps like fake Chrome browsers and 4K Sports streaming apps. Medusa's central infrastructure manages these campaigns, linking them to several botnets. The latest Medusa variant minimizes its footprint but still uses Android's Accessibility Services, enabling actions like overlaying screens and capturing screenshots.

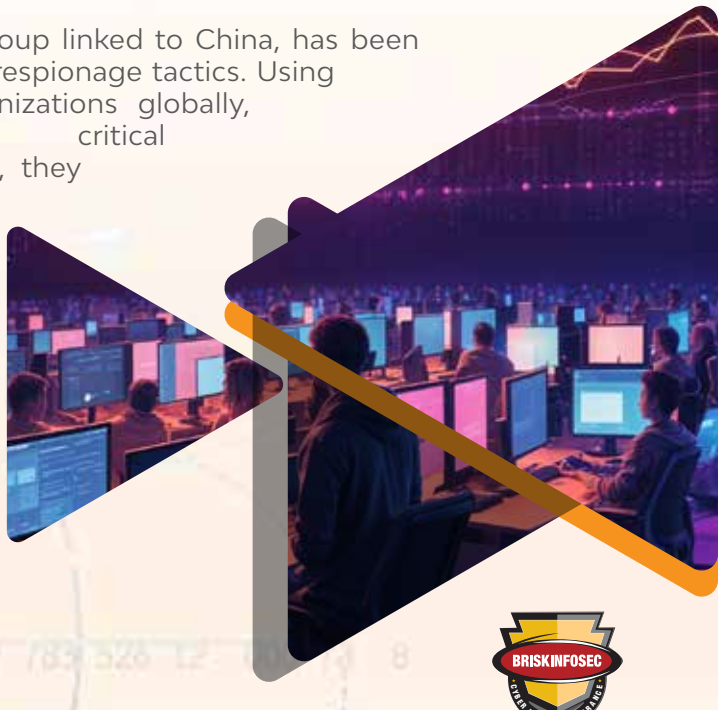
Attack Type : Banking Trojan

Cause of Issue : Android Malware

Industry Type : Software Development Companies

CHINESE CYBERSPIES EMPLOY RANSOMWARE IN ATTACKS FOR DIVERSION

ChamelGang, an advanced persistent threat (APT) group linked to China, has been employing ransomware alongside sophisticated cyberespionage tactics. Using CatB ransomware, they targeted high-profile organizations globally, including government entities and critical infrastructure, between 2021 and 2023. Additionally, they utilized BestCrypt and BitLocker to encrypt files in separate attacks, impacting organizations primarily in North America, South America, and Europe. These tactics not only aim to disrupt operations but also obscure attribution, blending cyberespionage with ransomware for strategic advantage.



Attack Type : Cyberespionage Ransomware

Cause of Issue : Attribution Obscurity

Industry Type : Software Development Companies

PLUGINS ON WORDPRESS.ORG WERE BACKDOORED IN A SUPPLY CHAIN ATTACK

A threat actor injected malicious PHP scripts into the source code of several WordPress plugins, compromising them. These scripts allowed the creation of unauthorized admin accounts on affected websites and injected SEO spam. Wordfence identified the breach and promptly notified the plugin developers, resulting in the release of patches. The breach affected five plugins: Social Warfare, Blaze Widget, Wrapper Link Element, Contact Form 7 Multi-Step Addon, and Simply Show Hooks. Users are advised to update to the patched versions and conduct thorough malware scans if suspicious activity is detected, such as new admin accounts or traffic to the attacker's IP address (94.156.79 [.]8).

Attack Type : Supply Chain

Cause of Issue : Source Code

Industry Type : Software Development Companies

MASSIVE BSNL DATA BREACH EXPOSES MILLIONS TO SIM CARD CLONING AND FINANCIAL FRAUD

BSNL, the state-owned telecom provider, has experienced a major data breach orchestrated by hacker 'kiberphant0m'. The breach compromised over 278GB of sensitive information, including IMSI numbers, SIM details, HLR data, DP card information, and SOLARIS server snapshots. The stolen data, valued at $5,000, poses significant risks such as SIM cloning, identity theft, privacy violations, financial fraud, and targeted scams. BSNL users are advised to monitor their accounts for unusual activity, enable two-factor authentication, and be cautious of phishing attempts. Experts recommend BSNL enhance security measures, conduct audits, and deploy advanced threat detection technologies to mitigate future risks.

Attack Type : Data Breach

Cause of Issue : Security Vulnerability

Industry Type : Telecommunications Sector

NEW CREDIT CARD SKIMMER TARGETS WORDPRESS, MAGENTO, AND OPENCART SITES

Caesar Cipher Skimmer, a new credit card web skimmer, has recently targeted popular content management systems like WordPress, Magento, and OpenCart. This malware infiltrates e-commerce websites to steal payment information by modifying crucial files like WooCommerce's "form-checkout.php" to embed malicious code disguised as Google services. The skimmer uses a Caesar cipher to obfuscate its payload and often masquerades as innocuous files like "style.css" or "css.php" to avoid detection. Attackers also exploit vulnerabilities in plugins like WPCode to inject malicious scripts. These incidents highlight the importance of maintaining CMS and plugin updates, strong passwords, and regular security audits to prevent such attacks.

Attack Type : E-commerce Web Skimming

Cause of Issue : Website Vulnerabilities

Industry Type : Software Industry

LEVI'S SUFFERS FROM A CREDENTIAL STUFFING ATTACK: STEPS TO SECURE YOUR ONLINE IDENTITY

Levi's experienced a credential stuffing attack on June 13, compromising 72,231 customer accounts. While no fraudulent transactions occurred, attackers accessed PII like names, emails, addresses, and partial payment details. Levi's enforced password resets and urges customers to verify their account information. They recommend using strong, unique passwords and monitoring for compromised credentials. Foresiet offers digital security solutions, emphasizing dark web monitoring, threat intelligence, and brand protection to prevent data breaches and cyber threats.

Attack Type : Credential Stuffing

Cause of Issue : Compromised Credentials

Industry Type : Textile Industry

RUSSIAN POWER COMPANIES, IT FIRMS AND GOVERNMENT AGENCIES HIT BY THE DECOY DOG TROJAN

The cybersecurity company Positive Technologies has identified a series of cyber attacks named Operation Lahat, conducted by an advanced persistent threat (APT) group known as HellHounds. Since at least 2021, this group has targeted Russian organizations with a malware known as Decoy Dog, initially a Linux-based trojan, but now showing evidence of a Windows version. Decoy Dog, a variant of the Pupy RAT, uses DNS tunnelling for command-and-control communication and can move between controllers to evade detection. HellHounds gained initial access through compromised SSH credentials and have infiltrated sectors including IT, government, space, and telecom. Despite using modified open-source tools, they've successfully maintained covert access within targeted organizations.

Attack Type : Persistent APT

Cause of Issue : Cyber Espionage

Industry Type : Software Development Companies

SNOWFLAKE WARNS: TARGETED CREDENTIAL THEFT CAMPAIGN HITS CLOUD CUSTOMERS

The cloud computing and analytics company Snowflake confirmed that a coordinated campaign targeted some of its customers. The attackers used stolen credentials obtained through malware to access databases configured with single-factor authentication. Snowflake, along with CrowdStrike and Mandiant, emphasized that there's no evidence of a platform vulnerability or compromised credentials of Snowflake personnel. They urged customers to implement multi-factor authentication (MFA) and restrict network access to trusted locations. Both U.S. and Australian cybersecurity agencies issued alerts advising organizations to watch for suspicious activities and follow Snowflake's security recommendations.

Attack Type : Credential Stuffing

Cause of Issue : Credential Compromise

Industry Type : Cloud-Based Software as a Service

A PROMPT INJECTION FLAW IN VANNA AI EXPOSES DATABASES TO RCE ATTACKS

The Vanna.AI library, a Python-based machine learning tool for querying SQL databases using natural language prompts, has revealed a critical security flaw (CVE-2024-5565, CVSS score 8.1). The vulnerability stems from prompt injection in the "ask" function, enabling attackers to execute arbitrary commands. This could lead to remote code execution due to the library's integration with Plotly for visualizing SQL query results. Following responsible disclosure, Vanna has released a hardening guide, advising users to sandbox environments when using Plotly integration. The incident underscores the risks associated with AI models like Vanna when used without robust security measures, emphasizing the need for vigilant governance in AI applications.

Attack Type : Prompt Injection

Cause of Issue : Prompt Handling

Industry Type : Software Development Companies

CRITICAL SQLI VULNERABILITY FOUND IN THE FORTRA FILECATALYST WORKFLOW APPLICATION

A critical security vulnerability, CVE-2024-5276, has been discovered in Fortra FileCatalyst Workflow versions 5.1.6 Build 135 and earlier. This flaw allows attackers to execute SQL injection attacks, potentially gaining unauthorized access to and manipulating the application database. To address the issue, Fortra has released a patch to version 5.1.6, build 139. sers are advised to disable specific services or restrict access as temporary measures until they are patched. Cybersecurity firm Tenable disclosed the vulnerability and also published a proof-of-concept exploit that demonstrated the exploitability via user-supplied jobID parameters in the application's URL endpoints.

Attack Type : SQL Injection

Cause of Issue : Input Sanitization

Industry Type : IT Industry

NEW ATTACK TECHNIQUE EXPLOITS MICROSOFT MANAGEMENT CONSOLE FILES

Threat actors have been exploiting a new attack method using specially crafted management saved console (MSC) files to achieve full code execution through the Microsoft Management Console (MMC). Dubbed "GrimResource" by Elastic Security Labs, this technique leverages vulnerabilities in MMC libraries, enabling adversaries to execute arbitrary code, including deploying malware like PASTALOADER and Cobalt Strike. The approach bypasses traditional security measures and has gained traction since Microsoft's default macro disabling Office files from the internet. Notably, the method exploits an unpatched cross-site scripting (XSS) flaw in the apds.dll library, reported to Microsoft and Adobe in 2018.

Attack Type : Console File Exploitation

Cause of Issue : MMC Library Vulnerability

Industry Type : Software Development Companies

REBRANDED KNIGHT RANSOMWARE TARGETS HEALTHCARE AND BUSINESSES WORLDWIDE

RansomHub, a new ransomware strain, has emerged as an updated version of Knight ransomware, which itself evolved from Cyclops. It employs double extortion tactics across various platforms and uses phishing for distribution. After Knight's shutdown, RansomHub surfaced with similar code and tactics, targeting notable entities. It recruits affiliates from other defunct ransomware groups and operates with speed and expertise. The rise of RansomHub reflects a broader trend of ransomware resurgence in 2023, marked by code reuse and operational overlaps in the cyber underground.

Attack Type : Ransomware Resurgence

Cause of Issue : Cybersecurity Vulnerabilities

Industry Type : Health Care Domain

KRAKEN CRYPTO EXCHANGE HIT BY $3 MILLION THEFT EXPLOITING ZERO-DAY FLAW

Kraken experienced a security breach due to a flaw that allowed users to artificially inflate their account balances. A security researcher, later revealed to be from CertiK, discovered the flaw but instead of reporting it properly, exploited it with others to steal $3 million. They demanded a ransom from Kraken to return the funds, prompting Kraken to label the incident as extortion. Kraken eventually returned all stolen funds and distributed them to its users via a USDT airdrop.

Attack Type : Account Balance Manipulation

Cause of Issue : UI Change

Industry Type : Banking & Finance Sector

NORTH KOREAN HACKERS TARGET BRAZILIAN FINTECH WITH SOPHISTICATED PHISHING TACTICS

Since 2020, North Korean cyber espionage groups, including UNC4899 and PAEKTUSAN, have significantly targeted Brazil's government, aerospace, technology, and financial sectors. Their tactics include social engineering via job offers and phishing emails, as well as trojanized apps and malware to target cryptocurrency and fintech companies. These groups have also impersonated recruiters and HR directors to distribute malware through phishing campaigns and counterfeit software packages, aiming to steal credentials and sensitive information. The activities highlight North Korea's increasing focus on Brazil amid its emergence as a regional power.

Attack Type : Social Engineering Phishing

Cause of Issue : State-sponsored Espionage

Industry Type : Banking & Finance Sector

HACKERS BASED IN CHINA EXPLOIT A FORTINET FLAW, INFECTING 20,000 SYSTEMS WORLDWIDE

State-sponsored threat actors linked to China exploited a critical security flaw (CVE-2022-42475) in Fortinet FortiGate systems between 2022 and 2023. They gained access to 20,000 systems globally, including those of Western governments, international organizations, and defence companies. Before its disclosure, the attackers exploited a zero-day vulnerability to infect 14,000 devices. They used a backdoor named COATHANGER to maintain access and potentially deploy more malware. This incident highlights ongoing vulnerabilities in edge devices and their attractiveness to cyber attackers.

Attack Type : Supply Chain Attack

Cause of Issue : Security Vulnerability

Industry Type : Software Development Companies

TEAMVIEWER'S CORPORATE NETWORK WAS BREACHED IN AN ALLEGED APT HACK

TeamViewer, a popular remote access software provider, reported a breach within its corporate IT environment on June 26, 2024. Upon detecting irregularities, the company initiated investigations with cybersecurity experts. TeamViewer emphasized that customer data in the product environment was unaffected, though their internal systems were compromised. Security alerts from NCC Group and Health-ISAC linked the breach to the Russian state-sponsored hacking group known as Midnight Blizzard. TeamViewer is currently investigating the incident and addressing concerns about potential network access vulnerabilities.

Attack Type : Cyberespionage

Cause of Issue : Security Breach

Industry Type : Software Development Companies

START-UP'S SCRAMBLE TO ASSESS THE FALLOUT FROM THE EVOLVE BANK DATA BREACH

Evolve Bank and Trust suffered a cyberattack and data breach that affected its retail customers and fintech partners. The attack, attributed to the LockBit ransomware gang, resulted in the illegal posting of customer data on the dark web. Several fintech companies, including Affirm, Marqeta, and Melio, are investigating the breach to determine potential impacts on their customers. Evolve is currently managing the repercussions of the incident, which affects multiple companies reliant on its banking services.

Attack Type : Ransomware Breach

Cause of Issue : Cybersecurity Lapse

Industry Type : Banking and Finance

GRANDOREIRO MALWARE CAMPAIGN : A GLOBAL THREAT TO BANKING SECURITY

The Grandoreiro banking trojan, initially identified in 2016, has re-emerged as a major global threat despite law enforcement efforts. Operating on a Malware-as-a-Service model, it targets over 1,500 banks across 60+ countries, employing advanced techniques to evade detection. Its capabilities include phishing campaigns mimicking legitimate organizations, sophisticated system infiltration methods, and extensive data collection. Mitigation strategies against Grandoreiro emphasize multi-layered defences, such as email filtering, network surveillance, DNS filtering, and endpoint security enhancements. Organizations are urged to bolster cybersecurity measures to combat this persistent and adaptable threat effectively.

Attack Type : Banking Trojan

Cause of Issue : Cybersecurity Vulnerability

Industry Type : Banking and Finance

CYBERSECURITY TV SHOWS

1. Mr. Robot

Follows Elliot Alderson, a cybersecurity engineer and hacker, as he navigates through complex plots involving corporate corruption and cybercrime.

Where to Watch : Watch on Amazon Prime Video

2. Black Mirror

An anthology series exploring the dark and often dystopian aspects of modern society and technology, touching on themes like privacy, surveillance, and ethical implications of new technologies.

Where to Watch : Watch on Netflix

3. Scorpion

Follows genius Walter O'Brien and his team of brilliant misfits who use their extraordinary talents to tackle global threats involving cybersecurity and high-tech challenges.

Where to Watch : Available on Amazon Prime Video

4. StartUp

Focuses on a group of entrepreneurs who launch a digital currency startup, exploring the intersections of technology, crime, and govC ernment intrigue.

Where to Watch : Watch on Crackle

5. Person of Interest

Centers on a former CIA operative and a reclusive billionaire who use artificial intelligence to predict and prevent crimes, dealing with themes of surveillance, AI ethics, and cybersecurity.

Where to Watch : Watch on Netflix

HIGH SEVERITY CVES OF 2024

1. CVE-2024-32962

XML-crypto, up to version 4.0.0, doesn't properly check who signed documents. This lets attackers re-sign files with fake certificates, fooling the system. Version 6.0.0 fixes this issue.

https://www.cve.org/CVERecord?id=CVE-2024-32962

2. CVE-2024-37902

DeepJavaLibrary (DJL), a Java deep learning framework, had a security issue in versions 0.1.0 to 0.27.0. It allowed archived files to overwrite system files using absolute paths. DJL 0.28.0 fixes this; users should update for security.

https://www.cve.org/CVERecord?id=CVE-2024-37902

3. CVE-2024-37228

InstaWP Connect versions up to 0.1.0.38 have a vulnerability that allows 'Code Injection' due to inadequate control over code generation.

https://www.cve.org/CVERecord?id=CVE-2024-37228

4. CVE-2024-35746

BuddyPress Cover, from version n/a to 2.1.4.2, has a vulnerability that allows 'Code Injection' through unrestricted uploading of files with dangerous types.

https://www.cve.org/CVERecord?id=CVE-2024-35746

5. CVE-2024-33566

OrderConvo, up to version 12.4, has a security issue where OS Command Injection can occur due to missing authorization checks.

https://www.cve.org/CVERecord?id=CVE-2024-33566

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