Threatsploit Adversary Report

Edition-68

BRISKINFOSEC

CYBER TRUST & ASSURANCE

www.briskinfosec.com

APR'2024

Introduction :

Dear Readers,

Welcome to April month's edition of Threatsploit, where we dissect the cyber threats that have been lurking around the corners of our digital lives. This month, we're taking a closer look at the cybersecurity incidents that have not only shaped our understanding of the digital threat landscape but also set the stage for proactive defenses in the months to come. Here's a peek into the intriguing, sometimes alarming, yet always enlightening world of cyber threats that were identified last month.

When Your Tools Turn Against You : Imagine the tools you rely on for software development becoming the very channels through which threats infiltrate. That's exactly what happened with JetBrains TeamCity, as BianLian ransomware actors exploited its vulnerabilities. It's a stark reminder of the importance of scrutinizing the security of the tools in our arsenal.

A New Era of Tunneling : The QEMU emulator, a tool admired for its utility, was ingeniously manipulated as a tunneling tool by attackers. This instance reveals a sophisticated approach to bypassing security measures, prompting us to rethink our defense strategies against such innovative threats.

Unlikely Allies in Cybercrime : The digital underworld saw an unusual alliance between GhostSec and Stormous, uniting to launch ransomware attacks. This development in the cybercrime ecosystem signifies a new level of threat, especially for the finance and banking sectors, and underscores the need for collective vigilance.

Your Visit, Their Weapon : In a surprising turn of events, hacked WordPress sites have been turning visitors' browsers into tools for brute-force attacks. This scenario brings to light the unforeseen risks of merely visiting a website, urging us to be more cautious about our digital footprints.

Apple Steps Up : On a positive note, Apple's swift action to release critical updates against actively exploited vulnerabilities is commendable. It serves as a vital lesson in the importance of staying updated and protected against emerging threats.

As we navigate through the complexities of these cyber threats, it's clear that staying informed is our best defense. Each incident is a puzzle piece in understanding the broader cyber threat landscape, providing us with insights to better protect our digital realms.

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 Games
- Top 5 Cybersecurity Comic Books to Read

BianLian Threat Actors Exploiting JetBrains TeamCity Flaws in Ransomware Attacks

BianLian ransomware actors are exploiting vulnerabilities in JetBrains TeamCity software to deploy their ransomware. They use CVE-2024-27198 or CVE-2023-42793 to gain initial access. BianLian, which shifted to extortion-only attacks in 2023, implants a custom Go-based backdoor tailored to each victim. Recently, they've utilized a PowerShell version of the backdoor for infiltration. This PowerShell backdoor establishes communication with a command-and-control server, enabling attackers to execute arbitrary actions. Meanwhile, VulnCheck highlighted a critical flaw (CVE-2023-22527) in Atlassian Confluence, exploited to deploy various malware, including ransomware and remote access trojans.

Attack Type : Ransomware Exploitation

Cause of Issue : TeamCity Vulnerabilities

Domain Name : Software Development Companies

QEMU Emulator Exploited as Tunneling Tool to Breach Company Network

Threat actors have utilized the open-source QEMU emulator as a tunneling tool in a cyber attack targeting a large company, enabling communication between virtual machines and remote servers. Kaspersky researchers discovered this tactic, emphasizing the need for multi-level protection to counter increasingly sophisticated attacks blending legitimate tools with malicious intent. By leveraging QEMU's networking capabilities, attackers establish covert channels, underscoring the importance of robust endpoint security and specialized solutions against complex, targeted threats.

Attack Type : Tunneling Emulator

Cause of Issue : Misused Emulator

Domain Name : Software Development Companies

GhostSec and Stormous Launch Joint Ransomware Attacks in Over 15 Countries

GhostSec, a cybercrime group, has been linked to a Golang variant of the ransomware GhostLocker, along with Stormous. They operate double extortion attacks across various sectors worldwide, offering a RaaS program called STMX_GhostLocker. Their arsenal includes tools like GhostPresser for WordPress site breaches, demonstrating their evolving tactics, as reported by Cisco Talos. They are part of The Five Families coalition, targeting businesses in numerous countries and industries, with a focus on technology, education, and government sectors. Talos discovered new tools used by GhostSec, including a deep scan toolset and GhostPresser for XSS attacks, further enhancing their capabilities.

Attack Type : Double Extortion

Cause of Issue : Ransomware-as-a-Service

Domain Name : Finance and Banking

Hacked WordPress Sites Abusing Visitors' Browsers for Distributed Brute-Force Attacks

Sucuri reports distributed brute-force attacks on WordPress sites via malicious JavaScript injections targeting innocent visitors. Attackers exploit compromised sites to brute-force other WordPress sites using common passwords. This shift from crypto drainers to brute-force attacks may stem from profit motives. Concurrently, a critical flaw in 3DPrint Lite plugin (CVE-2021-4436) enables deployment of the Godzilla web shell. Additionally, SocGholish campaign distributes JavaScript malware through modified legitimate plugins, aiming to deploy remote access trojans for ransomware attacks.

Attack Type : Brute-force Injection

Cause of Issue : Compromised Sites

Domain Name : Telecommunications Sector

Apple Issues Critical Updates for Actively Exploited Zero-Day Flaws

Apple released security updates addressing actively exploited vulnerabilities (CVE-2024-23225, CVE-2024-23296) allowing bypassing kernel memory protections. iOS 17.4, iPadOS 17.4, iOS 16.7.6, and iPadOS 16.7.6 include fixes. Three zero-days have been addressed by Apple this year. CISA added CVE-2023-21237 (Android) and CVE-2021-36380 (Sunhillo SureLine) to its Known Exploited Vulnerabilities catalog. Exploitation details vary, from targeted Android attacks to Mirai botnet leveraging CVE-2021-36380.

Attack Type : Memory Corruption

Cause of Issue : Kernel Vulnerability

Domain Name : Telecommunications Sector

New Banking Trojan CHAVECLOAK Targets Brazilian Users via Phishing Tactics

A new banking trojan called CHAVECLOAK targets users in Brazil through phishing emails containing PDF attachments. The trojan uses DLL side-loading to execute malware, stealing sensitive information and monitoring banking activity. Meanwhile, Copybara Android Banking Trojan targets the U.K., Spain, and Italy, employing smishing and vishing tactics to perform unauthorized banking transfers. Threat actors utilize a centralized web panel named 'Mr. Robot' to manage phishing campaigns and deploy malware. Sophisticated techniques like geofencing, device fingerprinting, and APK customization are employed to evade detection and steal credentials.

Attack Type : Phishing Malware

Cause of Issue : Social Engineering

Domain Name : Finance and Banking

How Cybercriminals are Exploiting India's UPI for Money Laundering Operations

A sophisticated money laundering scheme in India involves the use of the XHelper Android app to manage a network of money mules recruited via Telegram. Chinese cybercriminals exploit Indian UPI services to initiate illegal transactions, with proceeds funneled back to China. XHelper facilitates mule management, offering features for tracking earnings, recruiting agents, and training mules. Europol's global crackdown led to over 1,000 arrests and the identification of thousands of money mules and recruiters. This scheme underscores a broader trend of increasing mobile malware activity, particularly on Android devices, as reported by Kaspersky.

Attack Type : Money Mule

Cause of Issue : Financial Exploitation

Domain Name : Finance and Banking

Lazarus Hackers Exploited Windows Kernel Flaw as Zero-Day in Recent Attacks

The Lazarus Group exploited CVE-2024-21338, a zero-day Windows Kernel flaw, to gain kernel-level access and disable security software. This allowed them to execute their FudModule rootkit, bypassing security checks. The vulnerability, introduced in Windows 10 version 1703, facilitated direct kernel object manipulation. Lazarus Group's sophisticated tactics highlight their ongoing evolution and cross-platform focus, posing significant cybersecurity challenges. This incident underscores the group's status as a prolific and advanced persistent threat actor, showcasing their complex and stealthy malware tools like FudModule.

Attack Type : Kernel Escalation

Cause of Issue : Privilege Escalation

Domain Name : Software Development Companies

LockBit Ransomware Hacker Ordered to Pay $860,000 After Guilty Plea in Canada

Mikhail Vasiliev, a Russian-Canadian national, has been sentenced to nearly four years in jail in Canada for his involvement in the LockBit ransomware operation. He pleaded guilty to eight counts of cyber extortion and other charges, characterized as a "cyber terrorist" motivated by greed. Vasiliev attempted to extort ransom payments from Canadian companies during the pandemic, and he must pay back over $860,000 in restitution. LockBit suffered a major setback in February 2024 with its infrastructure seized and key affiliates arrested. Additionally, Roman Sterlingov was convicted for operating Bitcoin Fog, a long-running cryptocurrency mixer used for money laundering.

Attack Type : Ransomware Extortion

Cause of Issue : Illicit online Activity

Domain Name : Government Sector

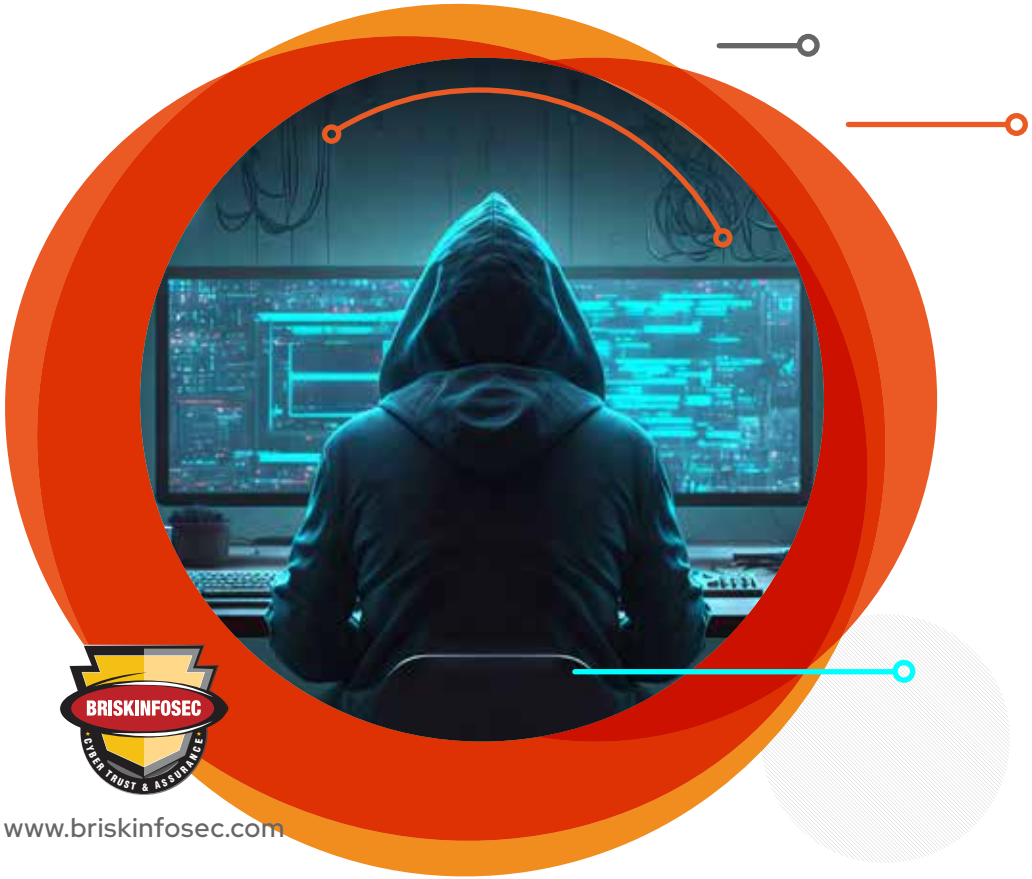
RedCurl Cybercrime Group Abuses Windows PCA Tool for Corporate Espionage

RedCurl, a Russian-speaking cybercrime group, exploits Windows' Program Compatibility Assistant to execute malicious commands, as revealed by Trend Micro. Their attacks involve phishing emails with malicious attachments, leveraging cmd.exe to download utilities, including curl, and using Impacket for unauthorized command execution. This underscores ongoing threats from RedCurl, while another Russian group, Turla, employs a new wrapper DLL named Pelmeni to deploy the Kazuar backdoor, masquerading as legitimate software libraries.

Attack Type : Phishing Malware

Cause of Issue : Exploited Vulnerability

Domain Name : Software Development Companies



Russian Hackers Use 'WINELOADER' Malware to Target German Political Parties

Recent cyber attacks, linked to APT29 (Midnight Blizzard) and Russia's SVR, targeted diplomatic entities using wine-tasting phishing lures. Mandiant identified the use of WINELOADER malware, notably targeting German political parties in February 2024, marking a strategic shift for APT29. The phishing campaign, disclosed by Zscaler ThreatLabz, uses German-language dinner invitations containing malicious ZIP files hosting ROOTSAW dropper, which deploys WINELOADER. WINELOADER communicates with attacker-controlled servers via DLL side-loading, sharing traits with other APT29 families. This expansion aligns with SVR's interest in political intelligence and coincides with espionage charges against German military officer Thomas H for allegedly spying for Russian intelligence.

Attack Type : Wine-tasting Phishing

Cause of Issue : Cyber Espionage

Domain Name : Government Sector

French Employment Agency Data Breach Could Affect 43 Million People

France's government unemployment agency, France Travail, formerly known as Pole Emploi, suffered a recent data breach potentially impacting up to 43 million people. The breach, which occurred between February 6 and March 5, 2024, resulted in the theft of personal information of job seekers, including names, social security numbers, contact details, and agency-specific identifiers. Passwords and financial information were not compromised. This is not the agency's first data breach, as a similar incident occurred in August 2023. Additionally, recent cyberattacks targeting other French services have been reported, indicating a broader trend of cyber threats against the country's institutions.

Attack Type : Data Breach

Cause of Issue : Information Compromise

Domain Name : Media and Entertainment

Akira's breach of Nissan impacts 100K people

In December 2023, Nissan was targeted in a cyberattack by the Akira ransomware cartel, impacting various aspects of its operations, including customer data. Approximately 100,000 individuals, including customers, dealers, and employees, were affected, with sensitive information like government IDs and personal details being compromised. Nissan has initiated contact with those affected and is offering credit monitoring and identity protection services. The attackers, Akira, are known for demanding ransom payments and leaking data if not paid.

Attack Type : Ransomware Breach

Cause of Issue : Ransomware Data Loss

Domain Name : Manufacturing and Industrial Control Systems (ICS)

Critical XSS Flaw Discovered in WP Statistics Impacting 600K Sites

A critical Cross-Site Scripting (XSS) vulnerability (CVE-2024-2194) in WP Statistics plugin, allowing attackers to inject malicious code via the URL parameter. With over 600,000 installations, the flaw poses severe risks, enabling unauthorized script execution and potential data theft or site compromise. Update promptly to patched versions to prevent potential exploitation.

Attack Type : Cross-Site Scripting

Cause of Issue : Input validation

Domain Name : Software Development Companies

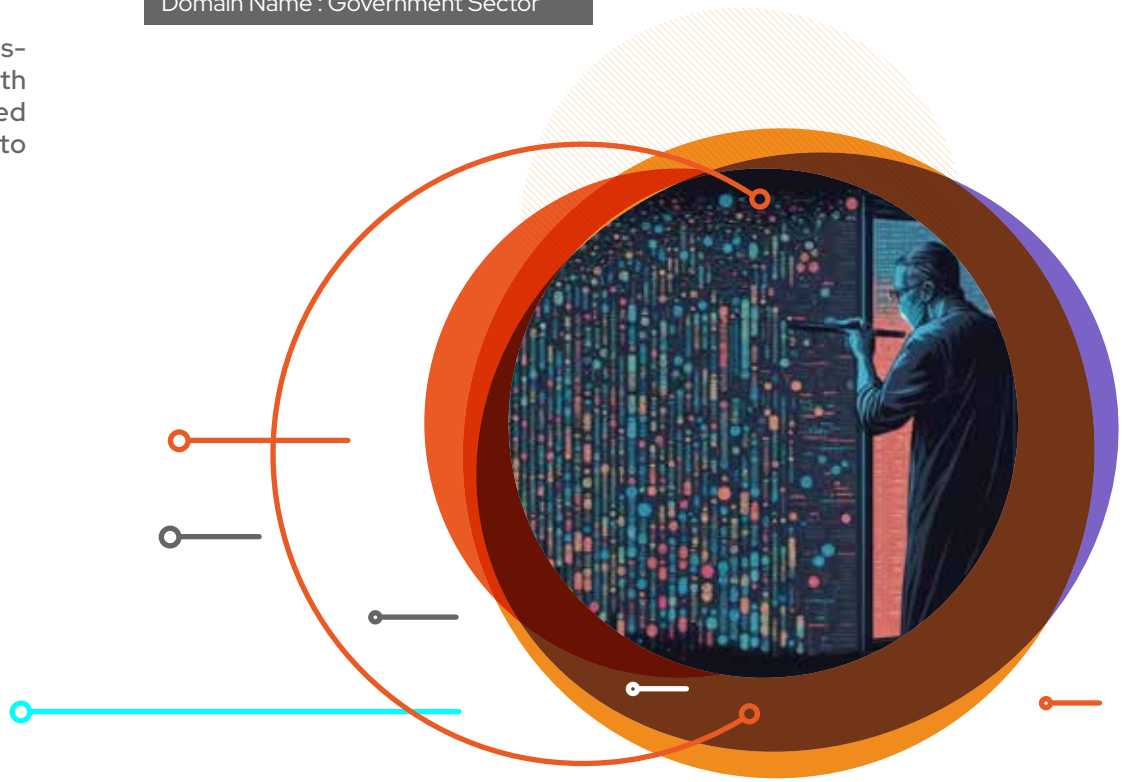
Chinese Earth Krahang hackers breach 70 orgs in 23 countries

A sophisticated hacking campaign attributed to the Chinese APT group 'Earth Krahang' has targeted 116 organizations across 45 countries since early 2022. Primarily focusing on government entities, the attackers exploit vulnerabilities like CVE-2023-32315 and CVE-2022-21587 to deploy web-shells and spear-phishing emails. Once inside the network, they use compromised infrastructure for further attacks, deploying malware like Cobalt Strike and XDealer to gain command execution and data collection capabilities. Trend Micro researchers suggest a possible connection between Earth Krahang and the Chinese company I-Soon, indicating a dedicated task force for cyberespionage on government entities.

Attack Type : Cyberespionage Campaign

Cause of Issue : Vulnerability Exploitation

Domain Name : Government Sector



AT&T says leaked data of 70 million people is not from its systems

AT&T denies data breach after hacker attempts to sell alleged 2021 breach data. Another actor leaks data for free, including sensitive details like names, addresses, and social security numbers. Some data confirmed accurate by cybersecurity researchers, raising concerns for AT&T customers about potential targeted attacks like phishing and SIM swapping. Customers advised to be cautious of communications claiming to be from AT&T and to verify legitimacy directly with the company.

Attack Type : Data Breach

Cause of Issue : Unauthorized Access

Domain Name : Telecommunications Sector

Riverview School District latest to be hit with online security incident

The Riverview School District recently experienced a security incident, leading to disruptions in teachers' internet access and the use of district-issued devices. Superintendent Neil English stated uncertainty regarding a security breach but emphasized caution. The district's technology department is investigating, with limited details provided to parents. This incident adds to a string of cyberattacks targeting educational and government entities, including recent breaches in Allegheny County, Carnegie Mellon University, and Butler County. Such attacks have seen a significant increase in recent years, with substantial financial implications for affected institutions.

Attack Type : Cybersecurity Breach

Cause of Issue : Cybersecurity Vulnerability

Domain Name : Finance Sector

Henry County undergoes cyber attack

Henry County infrastructure experienced a cyber-attack affecting its Computer Aided Dispatch and Records Management System, though 9-1-1 and public safety radio remained unaffected. The county's Information Systems department activated its Cyber Response Plan and initiated an investigation with industry experts and government agencies. Public safety agencies are using contingency measures while systems are being restored securely. There's no evidence of data compromise, but affected individuals are advised to monitor their personal information.

Attack Type : Cyber Intrusion

Cause of Issue : Cyber - Attack

Domain Name : Telecommunication Sector

Fujitsu Hacked – Attackers Infected The Company Computers With Malware

Fujitsu Limited discovered malware on operational computers, prompting immediate action to isolate affected systems and enhance monitoring. Approximately 130,000 employees support customers globally. The company initiated an internal investigation, revealing potential unauthorized access to sensitive information. Fujitsu implemented stringent security measures, including isolating impacted computers and reinforcing surveillance. They are conducting a thorough investigation to determine the intrusion method and potential data leak. Individuals and customers potentially affected have been contacted, and the breach reported to regulatory authorities. As of now, no misuse of leaked information has been reported. Fujitsu apologizes for any inconvenience and is committed to security, privacy, transparency, and maintaining trust.

Attack Type : Data Breach

Cause of Issue : Malware Intrusion

Domain Name : Information and communication technology

Discount retailer Giant Tiger says customer data was compromised in third-party breach

Giant Tiger, a discount retailer based in Ottawa, announced that some customer contact information was compromised in a security incident involving a third-party vendor used for managing customer communications. The breach, discovered on March 4 and confirmed by March 15, affected various groups of customers, with different levels of information exposed. This includes names, email addresses, phone numbers, and street addresses for loyalty members and online shoppers. The company emphasized that no payment information or passwords were compromised and that its store systems were unaffected. They have engaged cybersecurity experts to investigate the incident and are advising affected customers to be vigilant against potential phishing attempts. This breach adds Giant Tiger to a growing list of Canadian organizations facing cybersecurity incidents, including Indigo, LCBO, and government entities.

Attack Type : Third-Party Breach

Cause of Issue : Third-party Vulnerability

Domain Name : Software Development Companies

Spa Grand Prix email account hacked to phish banking info from fans

Hackers hijacked the official contact email for the Belgian Grand Prix event, sending fraudulent emails offering a €50 voucher for tickets to the Formula 1 race. The emails directed recipients to a fake website where they were asked for personal and banking information. The race organizer, SPA GP, responded promptly, warning customers and implementing additional security measures. They filed a complaint with Belgian cyber police and plan to file a civil claim. The number of impacted individuals and extent of data access are still unclear. SPA GP reassured that their official website and ticketing system remain secure.

Attack Type : Phishing Scam

Cause of Issue : Email Hijacking

Domain Name : Finance and Banking

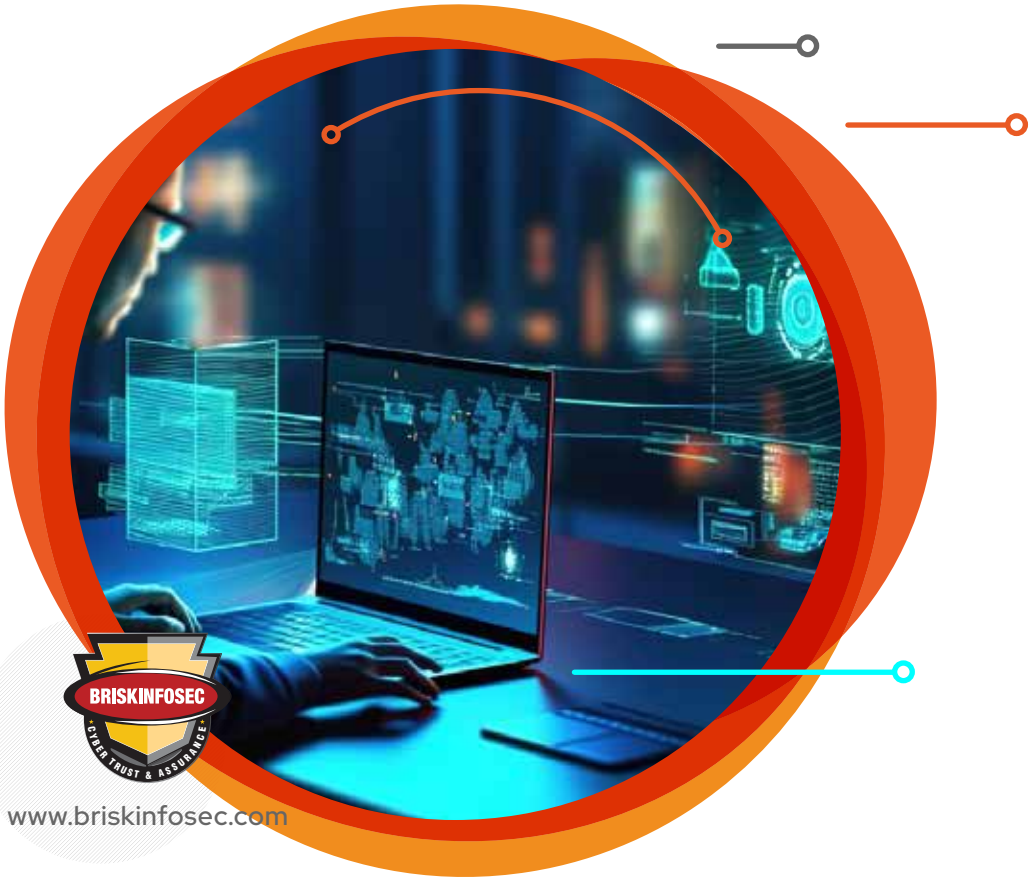
Mintlify says customer GitHub tokens exposed in data breach

Mintlify, a documentation startup, suffered a data breach on March 1st due to a vulnerability in its systems, exposing 91 customers' GitHub tokens. These tokens allow access to users' source code repositories. Mintlify notified affected users and is collaborating with GitHub to investigate potential misuse. The breach was disclosed publicly last week, sparking discussions on Reddit and Hacker News. Mintlify is deprecating private tokens to prevent future incidents. Despite initially labeling the discovery as a bug bounty report, Mintlify's co-founder describes it as a malicious attack. Investigations suggest the leaked token may not have been used, but further analysis is ongoing with GitHub and affected customers.

Attack Type : Supply Chain Attack

Cause of Issue : System Vulnerability

Domain Name : Software Development Companies



Acer confirms Philippines employee data leaked on hacking forum

Acer Philippines confirmed that employee data was stolen in an attack on a third-party vendor managing the company's employee attendance data. The stolen data was leaked on a hacking forum by a threat actor known as 'ph1ns'. The attacker claimed it was a pure data theft attack without ransomware involvement and provided evidence of wiping data from breached servers. Acer verified the authenticity of the data but clarified it wasn't acquired directly from their systems. They assured no customer data was affected, and their systems remained uncompromised. Acer notified authorities and initiated an investigation. This incident adds to previous security lapses, including breaches in 2023, 2021, and 2021, involving technical manuals, customer data, and a REvil ransomware attack.

Attack Type : Vendor Breach

Cause of Issue : Third-party Vulnerability

Domain Name : Software Development Companies

Over 2,300,000 records of Family Entertainment Business Were Exposed in Data breach

Jeremiah Fowler, a cybersecurity researcher, uncovered a non-password protected database belonging to Kids Empire, a US operator of recreational centers. The exposed database contained over 2.3 million documents including reservations, injury waivers, receipts, and digital gift cards, potentially exposing personally identifiable information (PII) of customers. Fowler promptly notified Kids Empire, and the database was secured after three weeks of exposure. The breach posed risks of identity theft and targeted phishing attacks. Fowler recommends proactive security measures, such as encryption, regular security updates, and dedicated channels for data and privacy issues. He emphasizes the importance of awareness and preparedness in mitigating potential damage during data breaches. Fowler clarifies that his actions are ethical and limited to verification and notification purposes, with no data downloaded.

Attack Type : Data Exposure

Cause of Issue : Inadequate security

Domain Name : Media and Entertainment

Hackers Claim Accessing 740GB of Data from Viber Messaging App

Messaging app Viber faces potential data breach claims by a pro-Palestinian hacktivist group, Handala Hack, who allege to have accessed 740GB of data, including Viber's source code. The hackers demand 8 Bitcoin (approximately $583,000) as ransom. Viber, owned by Rakuten since 2014, denies the breach but confirms an investigation is underway. If verified, this could be a significant breach involving personal messages, call logs, contact details, and financial information, posing serious risks to Viber users. Handala Hack is known for targeting Israeli entities and their allies and has utilized sophisticated techniques, including phishing emails and SQL injection attacks, to disrupt political messages. Viber users are advised to change passwords, beware of phishing attempts, and stay updated on official communications regarding the alleged breach. In an update, a Viber spokesperson dismissed Handala Hack's claims, stating no evidence of intrusion or data compromise was found upon investigation.

Attack Type : Sophisticated Breach

Cause of Issue : Alleged Breach

Domain Name : Software Development Companies

Hospitals Lobby Feds to Clarify Breach Duties in UHG Attack

In February, a cyberattack hit Change Healthcare, affecting thousands of healthcare organizations. The American Hospital Association (AHA) urges the Department of Health and Human Services (HHS) to ensure UnitedHealth Group handles breach notifications. HHS OCR is investigating if PHI was breached and if HIPAA rules were followed. AHA wants UnitedHealth Group and Change Healthcare to handle notifications to simplify the process. Legal experts suggest it's unlikely HHS will designate UnitedHealth Group solely responsible, but it would ease pressure on healthcare providers. Change Healthcare is restoring services gradually, with some already back online and others expected soon.

Attack Type : Cyber Breach

Cause of Issue : Ransomware

Domain Name : Healthcare Sector

A bug in an Irish government website that exposed COVID-19 vaccination records took 2 years to publicly disclose

Two years after discovering a vulnerability in the Irish Health Service Executive's (HSE) COVID-19 vaccination portal, security researcher Aaron Costello revealed that the portal exposed the vaccination records of approximately one million residents. The vulnerability, discovered in December 2021, allowed any user to access the health information of others, including vaccination details and internal HSE documents. Although the HSE fixed the issue promptly upon notification, Costello's attempts to coordinate public disclosure were met with resistance from government departments. Despite the breach not requiring a report to the Data Protection Commission, Costello believed in the importance of public disclosure to enhance overall security measures.

Attack Type : Data Exposure

Cause of Issue : Data breach

Domain Name : Government Sector

Greensboro College Data Breach: 52,000 Affected in Ransomware Attack, Lawsuit Filed

Greensboro College faces a class action lawsuit following a data breach affecting over 52,000 individuals, caused by a ransomware attack in August 2023. Abigail Hedgecock filed the lawsuit, alleging the college failed to safeguard personal information and delayed notifying affected individuals. The breach exposed sensitive data including names, Social Security numbers, and health information, raising concerns about repeated security lapses at the institution. Plaintiffs seek compensation for damages and equitable relief to improve data protection measures. Greensboro College has initiated internal investigations and security enhancements in response but must undertake a fundamental reassessment of cybersecurity infrastructure. Affected individuals are advised to monitor accounts for suspicious activity and consider proactive measures such as fraud alerts or credit freezes

Attack Type : Ransomware Attack

Cause of Issue : Data Breach

Domain Name : Education Sector

Top 5 Cybersecurity Games

BRISKINFOSEC
CYBER TRUST & ASSURANCE

www.briskinfosec.com

1. Hacknet

A realistic hacking simulation game that uses real UNIX commands and simulates a network environment, allowing players to understand the basics of hacking and cybersecurity principles through immersive gameplay.

Official website : https://www.hacknet-os.com/

2. Cyberpunk 2077

While not purely a cybersecurity game, it features a dystopian future with themes around hacking, data theft, and corporate espionage, offering insights into potential future cyber threats.

Official website: https://www.cyberpunk.net/in/en/

3. Watch Dogs 2

A game that combines adventure and hacking in a massive open world. Players use their skills to manipulate systems and gather information, highlighting the power of cyber warfare in society.

Official website : https://www.ubisoft.com/en-gb/game/watch-dogs/watch-dogs-2

4. Grey Hack

A multiplayer hacking simulator game that simulates a network and system hacking based on real-world vulnerabilities and tools, offering a sandbox environment to learn cybersecurity tactics

Official website : https://store.steampowered.com/app/605230/Grey_Hack/

5. Uplink

Players take the role of a freelance hacker in the late 21st century, performing jobs for major corporations. Its gameplay focuses on hacking and social engineering.

Official website: https://www.introversion.co.uk/introversion/

www.briskinfosec.com

Top 5 Cybersecurity Comic Books

1. "Snow Crash" by Neal Stephenson

While originally a novel, its graphic novel adaptation brings to life a future where information is the most valuable commodity, and cyber warfare is prevalent

Where to buy : https://bit.ly/SnowCrash_NealStephenson

2. "Transmetropolitan" by Warren Ellis

This comic book series follows a gonzo journalist fighting against political corruption in a cyberpunk future, highlighting themes of information control and surveillance.

Where to buy : https://bit.ly/Transmetropolitan_by_WarrenEllis

3. "The Private Eye" by Brian K. Vaughan

Set in a future after the "cloud" bursts, leaking everyone's personal information into the public domain, this comic explores themes of privacy, data security, and surveillance.

Where to buy : https://bit.ly/PrivateEye_by_BrianKVaughan

4. "Hacktivist" by Alyssa Milano, Jackson Lanzing, and Collin Kelly

Inspired by real-world events, it follows two social media moguls who secretly double as hackers for social change, tackling themes of cyber activism and surveillance.

Where to buy : https://bit.ly/Hacktivist_by_AlyssaMilano

5. "Watchmen" by Alan Moore and Dave Gibbons

A groundbreaking graphic novel that explores themes of power, morality, and the human condition through the lens of masked vigilantes.

Where to buy : https://tinyurl.com/WatchmenInternationalEdition

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