THREATSPLOIT

Adversary Report

BRISK INFOSEC

CYBER TRUST & ASSURANCE

www.briskinfosec.com

Edition-62

Introduction :

Preface : Navigating the Cybersecurity Landscape - October 2023 Report

Welcome to the October 2023 edition of our Threatsploit Report. In this digital age, cybersecurity is no longer just a concern for IT experts; it's a topic that impacts us all. This report presents insights into 25 significant cyberattacks, breaking down how they happened, the weaknesses they exploited, and the consequences they brought.

Our aim is simple : to help you understand the world of online threats in plain language. By examining real-world incidents, we hope to provide practical lessons and foster a proactive mindset when it comes to cybersecurity. Whether you're a business leader, an IT professional, or just someone curious about online security, this report is for you.

In these pages, you won't find complex jargon or technical overload. Instead, you'll discover stories that shed light on how cyber threats affect us all. Our hope is that this knowledge will empower you to make informed decisions and better protect your digital life.

As we journey through these stories together, remember that cybersecurity is a shared responsibility. Your awareness and vigilance are essential in safeguarding our digital world. Thank you for joining us on this mission.

Best regards,

Briskinfosec Threat Intelligence Team.

Contents :

National Student Clearinghouse data breach impacts 890 schools

The U.S. educational nonprofit National Student Clearinghouse (NSC) suffered a data breach affecting 890 schools in the U.S. Attackers accessed NSC's server on May 30, 2023, and stole personal information, including names, dates of birth, Social Security numbers, and more. NSC provides services to thousands of schools and colleges. A cybercriminal group called Clop is behind the attack, demanding high ransoms, and it's expected to collect $75-100 million. Multiple U.S. federal agencies and two Department of Energy entities were also targeted

Attack Type : Data Breach

Cause of Issue : Unauthorized Access to Server

Domain Name : Software Development Companies

Hotel hackers redirect guests to fake Booking.com to steal cards

Security researchers have uncovered a multi-step information stealing campaign targeting hotels, booking sites, and travel agencies. Hackers breach these systems and then exploit their access to collect customer financial data. They create fake Booking.com payment pages to improve their success rates in obtaining credit card information. The attackers begin by establishing communication with the targeted entity, often using a fake reason, such as a medical condition, to send malicious URLs to hotel guests. These URLs lead to info-stealing malware designed to operate stealthily and collect sensitive data.In a more advanced phase of the attack, cybercriminals directly target the compromised entity's customers. They send phishing messages, appearing as legitimate requests, asking for additional credit card verification. These messages are professionally written and mimic genuine hotel interactions, reducing suspicion. The messages are sent through the booking site's message platform, making them appear trustworthy.

Victims receive links for card verification, which trigger complex JavaScript scripts designed to detect and hinder analysis.While the attackers have employed sophisticated techniques to evade detection, users should remain cautious by avoiding unsolicited links, especially those with urgent or threatening demands. Checking URLs for signs of deception is advisable. To protect against complex phishing campaigns, it's recommended to contact the company directly through official channels to verify the legitimacy of such messages.

Attack Type : Phishing Campaign

Cause of Issue : Fake Websites

Domain Name : Finance and Banking

Space and defense tech maker Exail technologies exposes database access

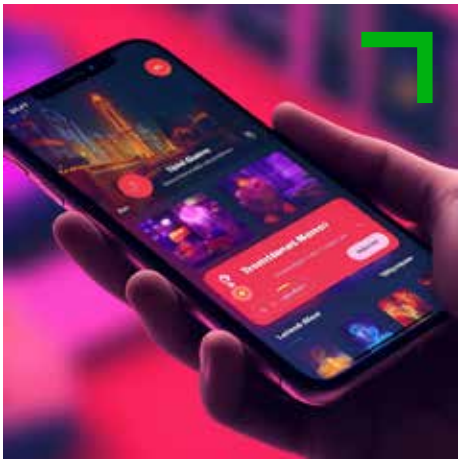
Exail, a French high-tech industrial group, inadvertently exposed a publicly accessible .env file with database credentials. This file, hosted on exail.com, could have been accessed by anyone, potentially leading to unauthorized access to sensitive data. Additionally, Exail's web server version and operating system details were exposed, making it susceptible to targeted attacks and automated scanning tools. Such vulnerabilities could have compromised security, data integrity, and the web server's operations.

Attack Type : Phishing Campaign

Cause of Issue : Fake Websites

Domain Name : Finance and Banking

T-Mobile app glitch let users see other people's account info



The T-Mobile customers had reported that an issue have araised T-Mobile customers where they could access other customers' account and billing information via the company's official mobile app. This exposed data included names, phone numbers, addresses, account balances, and credit card details. Some affected customers noted that this problem had persisted for over two weeks. T-Mobile clarified that this was not the result of a cyberattack, and their systems remained uncompromised. They attributed the incident to a temporary system glitch during a planned technology update, affecting less than 100 customers. T-Mobile has faced several data breaches in recent years, with the most recent one occurring in May 2023.Overall, while this incident was alarming, it was a system error rather than a breach, and T-Mobile promptly resolved it.

Attack Type : Data Exposure and Unauthorized Access

Cause of Issue : Server Misconfiguration

Domain Name : Telecommunications

Pizza Hut Australia hack : Data breach exposes customer information and order details

Pizza Hut's Australian branch faced a cyber attack resulting data loss of customer including delivery addresses and order details. The breach was detected in early September, prompting Pizza Hut to secure its systems, engage cybersecurity experts, and initiate an investigation. The compromised data comprises customer details, online order information, names, delivery addresses, email addresses, contact numbers, and, for registered accounts, encrypted credit card numbers and passwords. Fortunately, the breach did not disrupt operations. Pizza Hut reported the incident to the Office of the Australian Information Commissioner and estimates that approximately 193,000 customers were affected. While the company did not specify the data's timeframe, a data breaches website claimed to possess a sample of the stolen data, aligning with Pizza Hut's statement.

Attack Type : Data Breach and Unauthorized Access

Cause of Issue : Cyberattack

Domain Name : Media and Entertainment

Microsoft AI Researchers Leak 38TB of Private Data

Microsoft have accidently exposed the personal data like passwords on a public GitHub repository , a singnificant amount of data got exposed. The cloud security firm Wiz discovered this exposure. The repository, belonging to Microsoft's AI research division, was intended for open-source code and AI models but was misconfigured, granting access to the entire account. The reason behind the exposure is due to misues of the Shared Access Signature(SAS) token. Although Microsoft has invalidated the token, Wiz warns that SAS tokens pose ongoing security risks due to the lack of monitoring and governance. Microsoft has informed that there is no neeed for any action as the customer data and internal data were compromised. The have acknowledged the need for SAS token management in a better way.

Attack Type : Data Exposure

Cause of Issue : Misconfigured Shared Access Signature

Domain Name : Software Development Companies

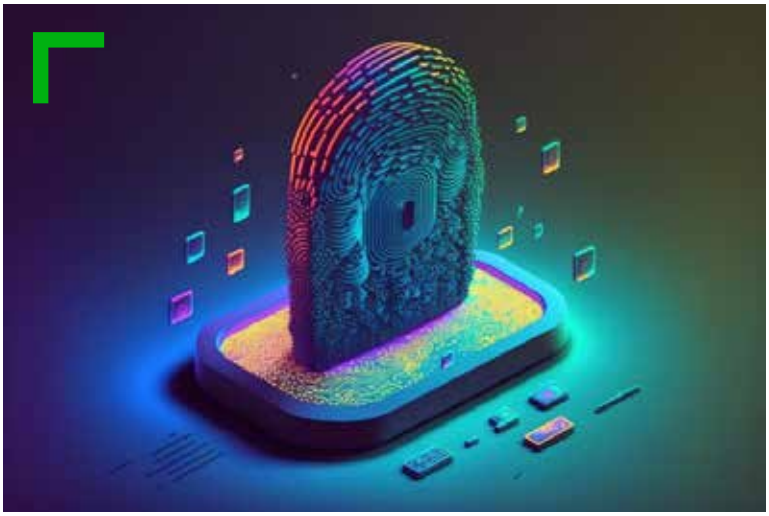
FBI hacker usdod leaks highly sensitive transunion data

A threat actor using the alias "USDoD" has claimed responsibility for leaking a large database allegedly stolen from TransUnion, a major American consumer credit reporting agency.The leaked database consist of personal information about a total of 58,505 of individuals worldwide. The senstive details consist of passport details ,credit card details from the month of March 2nd 2022. "USDoD" has a history of high-profile breaches, including recent incidents involving Airbus and the FBI. In the Airbus breach, the hacker exploited an employee's compromised account from a Turkish airline. This highlights the ongoing cybersecurity challenges posed by threat actors like "USDoD."

Attack Type : Data Breach

Cause of Issue : Unauthorized Access

Domain Name : Finance and Banking



Airbus investigates data leak allegedly involving thousands of suppliers

Airbus, the European aerospace giant, is investigating a cybersecurity incident after a hacker, known as "USDoD," posted information about 3,200 of the company's vendors on the dark web. The threat actor claims that he has got access by by compromising a Turkish airline employee's account, revealing vendor details like names, addresses, and contact information.Airbus took immediate action after confirming the incident .The threat actor is linked with the breach that occured in December 2022 of the FBI's InfraGard system and claims affiliation with the "Ransomed" ransomware group.In 2019, Airbus encountered cyberattacks aimed at its suppliers, with China suspected as the source, though denied involvement.

Attack Type : Data Breach and Unauthorized Access

Cause of Issue : Compromised Accounts

Domain Name : Media and Entertainment

Canadian Nurses Association confirms data theft after group dumps stolen info

"On 3rd April the Canadian Nurse Association has has faced some securit incident which affected their system but the operations were not affected. An investigation was conducted including the third-party expert and notified law enforcement.wo ransomware groups, Snatch and Nokoyawa, initially claimed responsibility, but Snatch later leaked 37 GB of CNA data on September 1. There has been confusion about Snatch's operations and affiliations. In a separate incident, Snatch claimed to have attacked South Africa's defense department, leaking sensitive military information. South African authorities denied a hack, attributing it to criminal syndicates aided by leaked information. Snatch asserts it stole 1.6 terabytes of data from the department."

Attack Type : Data Breach

Cause of Issue : Ransomware

Domain Name : Healthcare

MGM Resorts Confirms 'Cybersecurity Issue', Shuts Down Systems

"Hospitality and entertainment giant MGM Resorts on Monday said a "cybersecurity issue" forced the shutdown of certain computer systems, including the websites for some of the biggest Las Vegas and New York properties. Experienced a cybersecurity issue that led to the shutdown of specific computer systems, including websites for prominent Las Vegas and New York properties. The incident bears the hallmarks of a ransomware extortion attack. External cybersecurity experts and law enforcement are involved in the ongoing investigation. The incident, which started on Sunday, impacted hotel reservation systems across the United States and various IT systems on casino floors. MGM Resorts is actively working to determine the nature and scope of the issue."

Attack Type : Unauthorized Access

Cause of Issue : Ransomware

Domain Name : Media and Entertainment

AP Stylebook Breach May Have Hit Hundreds of Journalists

The Associated Press (AP) Stylebook, a popular writing guide, experienced a data breach that compromised subscribers' personal information. The breach occurred on an old AP Stylebook website maintained by an external service provider, Stylebooks.com. Threat actors accessed this legacy site between July 16 and July 22, 2023. The exposed data included names, email addresses, street addresses, phone numbers, and potentially Social Security Numbers or Taxpayer IDs. Subscribers began receiving phishing emails after the breach, leading to concerns about their personal information's security. AP is providing affected individuals with 24 months of credit monitoring and identity restoration services and mandating password changes for all AP Stylebook customers.

Attack Type : Data Breach

Cause of Issue : Phishing

Domain Name : Media Sector

Dymocks Booksellers suffers data breach impacting 836k customers

Dymocks Booksellers suffered a data breach, with customer data exposed after it was shared on hacking forums. Although there's no evidence of penetration into Dymocks' systems, the breach's full scope and duration are being investigated. Customer information, including names, email addresses, and membership details, was compromised. Dymocks reassures customers about safe online shopping but advises password changes. The data has circulated on hacking forums since June 2023, making phishing and scam attempts possible. While no passwords were exposed, changing passwords is recommended, especially if used elsewhere, and using a password manager is advised to enhance security. Customers should also be cautious of phishing emails resulting from this breach.

Attack Type : Phishing Campaign

Cause of Issue : Data Breach

Domain Name : Media and Entertainment

Hackers claim to publish prominent Israeli hospital's patient data

A ransomware attack on Mayanei Hayeshua Medical Center near Tel Aviv led to the leak of stolen data by the Ragnar Locker gang after no ransom was paid. The attack, which shut down the hospital's administrative systems, potentially exposed sensitive information of patients, including top government officials and senior rabbis. The hackers claim to possess a significant amount of personal information, internal emails, finances, medical records, and other sensitive data. They did not encrypt the files to avoid damaging medical equipment. The hospital reportedly refused to negotiate and pay the ransom, which was reported to be substantial. The incident has raised concerns about attacks on healthcare facilities and the consequences of data leaks.

Attack Type : Data Breach and Exposure

Cause of Issue : Ransomware attack

Domain Name : Healthcare

Hackers Exploit Multiple Bugs in Hotel Booking Platform

Financially motivated hackers targeted resorts and hotels using custom malware, exploiting likely zero-day flaws in popular property management software, aiming for financial gain and personal data acquisition. The attack, likely part of a coordinated effort, centered on the IRM Next Generation booking engine by Resort Data Processing. The attackers employed a variety of methods, including custom malware for covert data exfiltration, exploited vulnerabilities, and initiated the attack in the summer of 2022. The incident underscores the supply chain security challenge faced by industries, particularly smaller enterprises, relying on third-party providers for IT solutions.

Attack Type : Malware Exploitation

Cause of Issue : Supply Chain Attack

Domain Name : Software Industry

Ransomware gang claims credit for Sabre data breach

Travel booking giant Sabre is investigating a cyberattack after data purportedly stolen from the company appeared on a dark web leak site operated by the Dunghill Leak group. The group claims to have taken about 1.3 terabytes of data, including databases related to ticket sales, passenger turnover, employee information, and corporate financial data. Sabre, a provider of air passenger and booking data used by many U.S. airlines and hotel chains, is currently assessing the validity of these claims. Screenshots shared by the extortion group suggest that sensitive information, including employee records, was compromised, with some data as recent as July 2022. The identity and motives of Dunghill Leak remain largely unknown, but it is part of the ransomware and extortion landscape. Sabre had previously reported a security incident in 2017 when hackers scraped a million credit cards from its hotel reservation system.

Attack Type : Exposure of sensitive information

Cause of Issue : Data Exposure

Domain Name : Finance and Banking

Crypto Casino Stake.com Back Online After $40M Heist

Stake.com, a cryptocurrency betting platform, reported that hackers stole over $40 million in cryptocurrency from its Ethereum (ETH) and Binance Smart Chain (BSC) hot wallets. The company stated that unauthorized transactions were detected, prompting an investigation and security measures. The incident affected Ethereum and Binance Smart Chain wallets, while others remained untouched. Hot wallets, which are less secure than cold wallets, are accessible from the internet, making them vulnerable to remote attacks. Blockchain security firm Cyvers initially detected the suspicious activity, which led to the theft of $16 million worth of Ethereum, later followed by $25.6 million in BSC and Polygon from the hot wallets.

Attack Type : Data breach and theft

Cause of Issue : Blockchain Misconfiguration

Domain Name : Finance and Banking

GhostSec Leaks Source Code of Alleged Iranian Surveillance Tool

GhostSec, a hacker group, has disclosed the source code for surveillance software allegedly developed by the Iranian FANAP group, claiming it is used by the Iranian government for citizen monitoring. GhostSec has released components of the code and alleges the software includes features similar to Pegasus spyware. FANAP denies the claims, stating the software is for limited purposes and not used to recognize citizens. GhostSec obtained the source code by accessing FANAP infrastructure. The group aims to protect human rights and privacy, and its actions align with its hacktivist and vigilante background. The software reportedly includes facial recognition, car GPS tracking, and license plate recognition capabilities.

Attack Type : Exposure of sensitive information

Cause of Issue : Source Code Leakage

Domain Name : Telecommunications

Mend.io SAML Vulnerability Exposed

WithSecure has revealed a security vulnerability in Mend.io's application security platform related to its implementation of Security Assertion Markup Language (SAML) login. The vulnerability allowed a Mend.io customer to potentially access the data of other customers within the same Software-as-a-Service (SaaS) environment by guessing a valid email address. In a SAML-based Single Sign-On (SSO) system, users can access multiple applications using one set of login credentials, but the lax scoping in Mend.io's SAML login allowed a threat actor to exploit the vulnerability. Mend.io swiftly addressed the issue by implementing an additional security layer. While no active exploitation has been reported, affected organizations are encouraged to review relevant logs.

Attack Type : Unauthorized data access vulnerability

Cause of Issue : SAML Misconfiguration

Domain Name : Software Development Companie

Insurer fined $3M for exposing data of 650k clients for two years

The Swedish Authority for Privacy Protection (IMY) has fined insurer Trygg-Hansa $3 million for a data breach that exposed sensitive information of approximately 650,000 customers. The breach occurred due to an accessible backend database on Trygg-Hansa's online portal, which didn't require authentication and allowed browsing of private documents by manipulating client ID numbers in the URL. The exposed data included personal, health, financial, and contact information, as well as social security and insurance details. The breach persisted for over two years, from October 2018 to February 2021. IMY identified at least 202 cases of personal information exposure, highlighting a severe data security shortfall and leading to the substantial fine.

Domain Name : Data Exposure / Data Breach

Attack Type : Server Misconfiguration

Cause of Issue : Finance and Banking

Air Canada says hackers accessed limited employee records during cyberattack

"Air Canada reported a recent data breach involving limited employee information but assured that customer data and flight operations were unaffected. The breach was unrelated to ransomware and prompted enhanced security measures. It coincided with a suspected pro-Russia hacking group's cyberattack causing widespread disruptions at Canadian airports. While no group claimed responsibility for the Air Canada breach, Canada has faced increased cyber threats linked to its support for Ukraine. Data breaches and cyberattacks have become recurring issues for the aviation industry, impacting various airlines and related companies worldwide. A recent report indicated the transportation industry's high breach cost-per-breach, averaging $4.18 million in 2023"

Attack Type : Data Breach

Cause of Issue : Server Misconfiguration

Domain Name : Media and Entertainment

MacOS 14 Sonoma Patches 60 Vulnerabilities

Apple has released macOS 14 Sonoma, addressing over 60 vulnerabilities in the operating system. These flaws could potentially lead to the compromise of sensitive information, code execution with elevated privileges, sandbox escapes, file reading, denial-of-service attacks, privilege escalation, security bypass, file deletion, file system modification, and UI spoofing. While some vulnerabilities could be exploited remotely via specially crafted websites, many require a malicious app on the target device. Notably, one of these vulnerabilities (CVE-2023-41993) had previously been exploited as a zero-day to deliver spyware to iPhones. Apple also issued an iOS 17 update without security patches, but it updated its advisory for iOS 16.7 and iPadOS 16.7 to mention the patching of 17 additional vulnerabilities. macOS Sonoma 14 introduces various new features and improvements and is available for various Mac devices

Attack Type : Software Vulnerabilities

Cause of Issue : Multiple Exploits

Domain Name : Software Industry

Pension Firms Report 4000% Surge in Breaches

Pension providers in the UK reported a staggering 4000% increase in data breaches to the Information Commissioner's Office (ICO) in the year ending June 30, 2023. The pension sector saw cyber-attacks leading to data breaches rise from six incidents to 246, making it the hardest-hit in financial services, which overall recorded a 242% increase. Experts emphasized the need for robust cybersecurity measures and proactive reporting to the ICO to mitigate risks and protect reputation

Attack Type : Data Breach

Cause of Issue : Data Exposure

Domain Name : Finance and Banking

Briskinfosec Technology and Consulting Pvt ltd,
No : 21, 2nd Floor, Krishnama Road,
Nungambakkam, Chennai - 600034, India.

For More Info Contact Us

+91 86086 34123 | **+044 4352 4537**
contact@briskinfosec.com | **www.briskinfosec.com**