THREATSPOLIOT ADVERSARY REPORT

Edition 60

www.briskinfosec.com

Introduction :

Welcome to the latest "Threadsploit Report," where we explore the world of cybersecurity vulnerabilities and exploits in our interconnected digital age.

In this edition, we delve into over 15 cyber incidents, highlighting the evolving tactics of threat actors and the vulnerabilities modern organizations face. We begin by examining a case in the automotive sales industry, where a data exposure incident at a Suzuki dealership reminds us of the importance of safeguarding our digital footprints.

Moving on to identity and access management, we uncover the story of a nation-state intrusion into JumpCloud's network. This case underscores the need not only for strong digital defenses but also swift threat response.

In000 the healthcare sector, we detail the consequences of lax cybersecurity through the "Egypt's Ministry of Health : Medical Data Breach" exposé. This incident highlights the profitable nature of cybercrime and the urgency to bolster our defenses.

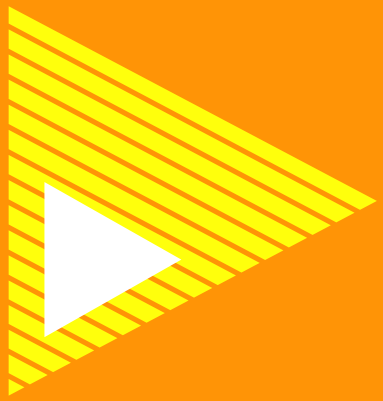
However, this report is more than a list of attacks. It's a source of empowerment, providing you with insights to understand the changing threat landscape, knowledge to enhance your defenses, and the ability to recognize potential dangers.

In a world where technology drives progress, we must collectively ensure that progress isn't hijacked by malicious forces. The "Threadsploit Report" is a testament to this commitment. These stories remind us that the battle against cyber threats is ongoing and requires vigilance, readiness, and collaboration.

Thank you for joining us on this journey. Let's equip ourselves with knowledge and rise to the challenges ahead, securing the digital frontier for ourselves and future generations.

Best regards,

Briskinfosec Threat Intelligence Team.



Contents :

Sporty Suzuki : Shame the dealer left your data exposed

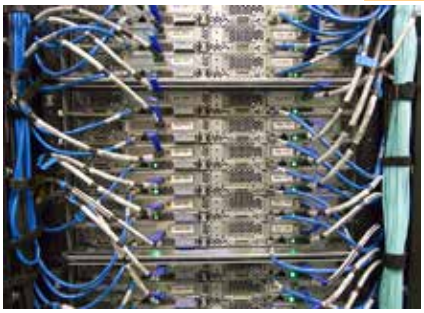
The Cybernews research team recently discovered two Suzuki-authorized dealer websites that were leaking sensitive information. Files that should have been kept secret and confidential were made public. Passwords and secret tokens for accessing user data, company management tools, or administering websites might have been obtained by anyone. The first dealership is open in Brazil, a country with a population of 214.3 million people and a high crime rate. Bahrain, an island country in the Middle East with a population of 1.46 million, is home to the second auto dealer. This isn't the first time vehicle dealers have encountered cybersecurity issues. Last year, ransomware infiltrated the UK's second-largest vehicle dealer, which had 160 shops. SMTP credentials would have allowed attackers to send fraudulent emails to users of the suzukiveiculos.com.br and suzukibahrain.com websites via the official email address of the domains. Database credentials enable attackers to readily access the database's contents, which are likely to contain user information. Attackers would need to first seize control of the web server or get a foothold in the network.

Attack Type : Data leakage

Cause of Issue : Insufficient security measures

Domain Name : Insufficient security measures

JumpCloud claims that nation-state hackers broke into its systems



JumpCloud, an identity and access management company, claims it has reset clients' API keys after nation-state hackers hacked its servers. JumpCloud, a directory platform that enables companies to identify, authorise, and manage users and devices, informed clients last week that it had reset their API credentials "out of an abundance of caution" owing to an ongoing, unnamed security incident. According to JumpCloud, a nation-state actor got unauthorised access to its networks and targeted a "small and specific" set of clients. JumpCloud CISO Bob Phan stated in his findings that the first observed anomalous activity happened on June 27, which was linked back to a spearphishing operation carried out by the threat actor on June 22. At the time, the corporation stated that it saw no evidence of customer effect. JumpCloud announced two weeks later, on July 5, that it observed odd behaviour in their commands framework for a small number of clients, revealing that some users were affected. The company then reset all admin API keys and began notifying affected clients.

Attack Type : Spearphishing

Cause of Issue : Unauthorized access to servers

Domain Name : Cloud services

Egypt's Ministry of Health claims a hacker stole sensitive medical records

An 'established' threat actor claimed to have two million stolen data records from Egypt's Ministry of Health and Population. On July 25, 2023, cyber threat intelligence service SOCRadar and dark web monitoring firm Falcon Feeds discovered the allegation on the hacker site Popürler. The database, according to the threat actor's post, contains extensive, personal patient information such as names, IDs, decision and national numbers, phone numbers, addresses, procedure classification details, diagnoses, and treatment details. To back up his claim, the hacker gave a sample of the dataset, which included data on 1000 persons.

This threat actor, who was "known last week for selling databases allegedly belonging to Indonesian entities," also invited possible purchasers to contact them using the Telegram chat service. According to SOCRadar's dark web surveillance platform, "evidence points to financial gain as the primary motivation behind these actions." According to evidence obtained by Infosecurity, the same hacker forum user claimed to be selling millions of data records as a result of various breaches in 2021 and 2022.

Attack Type : Data Breach

Cause of Issue : Security Vulnerability

Domain Name : Health care

A data breach occurred at a dating app with 50 million users

Jeremiah Fowler, a cybersecurity researcher, found and reported to vpnMentor a non-password secured database containing around 2.3 million records. Further examination revealed that these records were linked to several dating applications stored in a single database. The database appears to have a large number of user records, which include customer names, account numbers, emails, passwords, and other information. The database contains about 600 compressed server logs in total. I discovered a vast number of email addresses while reviewing a single server record. Given the small sample size, it is probable that the remaining files include many more emails. If this information falls into the wrong hands, all of these people may become victims of spam, phishing attempts, or other malware infestations.

A dating app data breach, like any other, can endanger the privacy and security of its users. Users of dating apps are frequently required to give sensitive information, such as sexual preferences or medical issues. This information could be used to discriminate against individuals or to blackmail them. Furthermore, compromised personal information such as users' true names and email addresses may make them a target for cyber criminals. It is unknown how long the database was exposed or whether anyone else had access to these photographs, information, and server logs. We publish our findings for educational objectives as well as to highlight the real-world concerns associated with data exposure. Users who have used these or other dating apps and fear their personal information has been compromised should be wary of any strange behaviour.

Attack Type : Data Breach

Cause of Issue : Misconfiguration of the Database

Domain Name : Social Media

A VirusTotal data leak exposes the personal information of certain registered customers

Data connected with a subset of VirusTotal registered customers, including their names and email addresses, were accidentally posted to the malware scanning platform by an employee. Der Spiegel and Der Standard were the first to report on the security breach, which included a database of 5,600 names in a 313KB file. VirusTotal apologised on Friday for the recent customer data exposure incident, stating that it was caused by an employee accidentally uploading a CSV file to the platform on June 29, 2023, that contained information pertaining to its Premium account customers, specifically their names, associated VirusTotal group names, and group administrators' email addresses.

Attack Type : Data Breach

Cause of Issue : Accidental uploading of files by employee

Domain Name : Malware scanning platform

Deutsche Bank says that a supplier compromise exposed customer information

Deutsche Bank AG reported to BleepingComputer that a data breach on one of its service providers exposed the data of its clients in a suspected MOVEit Transfer data-theft assault. "We have been notified of a security incident at one of our external service providers, which operates our account switching service in Germany," said a spokeswoman for the company. According to the bank, the security failure revealed only a small amount of personal data. The number of clients affected has not been determined, however Deutsche Bank stated that they have all been informed of the immediate impact and what safeguards they should take about their exposed data. Meanwhile, the bank is examining the causes of the data leak and taking focused action to improve its data security procedures in the future to avoid such instances affecting its consumers. According to Deutsche Bank, fraudsters cannot access accounts using the disclosed data, although they may attempt to make unauthorised direct debits. As a result of this danger, the bank has extended the term for unauthorised direct debit refunds to 13 months, giving customers plenty of opportunity to detect, report, and get reimbursement for unauthorised transactions.

Attack Type : Data Breach

Cause of Issue : External service providers

Domain Name : Banking and Financial Services

Bangladesh's government website exposes personal information about its inhabitants

Jeremiah Fowler, a cybersecurity researcher, found and reported to vpnMentor a non-password secured database containing around 2.3 million records. Further examination revealed that these records were linked to several dating applications stored in a single database. The database appears to have a large number of user records, which include customer names, account numbers, emails, passwords, and other information. The database contains about 600 compressed server logs in total. I discovered a vast number of email addresses while reviewing a single server record. Given the small sample size, it is probable that the remaining files include many more emails. If this information falls into the wrong hands, all of these people may become victims of spam, phishing attempts, or other malware infestations.

Attack Type : Data Breach

Cause of Issue : Security vulnerability

Domain Name : Public Sector

Unreleased Shows and Scripts at Risk from a 500GB Nickelodeon Data Leak

Nickelodeon is beloved by millions around the world, but recent internet rumours imply that the renowned children's entertainment network has been the victim of a huge data breach or leak. Approximately 500GB of data, including unpublished television series, scripts, and other documents, has been compromised, according to multiple internet forums and tweets. According to reports, Nickelodeon's legal staff acted quickly, aggressively pursuing Digital Millennium Copyright Act (DMCA) takedowns. Simply revealing the substance of the leak has resulted in serious consequences for those involved. According to reports, the hacked data came from Nickelodeon's "consumer products and experience" section. Unauthorised individuals gained access to the Nickelodeon animation department's sensitive content due to a system authentication flaw. Although the leak was discovered on Discord in January 2023, Nickelodeon has since rectified the issue and patched the gateway.

On June 29th, a Twitter user going by the handle @GhostyTongue revealed information on the supposed leak at Nickelodeon's animation department. Two persons engaged in the leak, known by their Discord nicknames "BowDown" and "IncidentalSeventy," have reportedly faced repercussions from either police authorities or Nickelodeon itself, according to @GhostyTongue. Several private groups, according to their account, have been exchanging chunks of the leaked files, with trusted users having access to more extensive dumps comprising assets such as PSDs, scripts, and animation files.

Attack Type : Data Breach

Cause of Issue : System authentication flaw in Nickelodeon

Domain Name : Entertainment Sector

A data breach at Pepsi Bottling Ventures affected 28,000 people

A data leak at independent bottling company Pepsi Bottling Ventures affected over 28,000 people. The data breach, discovered on January 10, occurred between December 23, 2022, and January 19, 2023, and resulted in an unauthorised party accessing the company's employees' personal, financial, and health information. On February 10, Pepsi Bottling Ventures started informing the impacted individuals that the attackers gained access to certain systems containing their personal information, but did not reveal how many individuals were affected. In conjunction with a public announcement regarding the incident, Pepsi Bottling Ventures recently informed the Maine Attorney General's Office that the attackers had access to the personal information of more than 28,000 individuals.

Names, addresses, email addresses, financial account information, ID numbers, driver's licence numbers, Social Security numbers, digital signatures, medical history records, and health insurance information, according to the company, have been hacked. Pepsi Bottling Ventures claims to have enhanced its network's security and initiated a company-wide password reset to secure all employee and partner accounts on its network. The company claims it is unaware of any exploitation of the hacked information, but such data is frequently sold or shared on underground cybercrime portals and subsequently used in phishing and other forms of assaults.

Attack Type : Data Breach

Cause of Issue : Unauthorised access to company systems

Domain Name : Beverage Company

Employee and customer data were compromised at India's largest IT retailer

Poorvika recently identified a non-password secured data leak in the records and file names. Employee data such as religion, sex, date of birth, marital status, family dependents, and other PII were included in the records. The database was closed to the public the same day after a responsible disclosure notice was sent to Poorvika. However, they never responded to my observations. Poorvika claims to be India's largest electronics retailer, specialising in mobile phones and mobile-related accessories. Poorvika was formed in 2004 and has since grown to become one of the country's leading mobile merchants, with over 500 stores in 43 cities. Poorvika also has an online store where you can buy cellphones, laptops, desktops, smart gadgets, and technology accessories. Poorvika appears to be involved in more than one data-exposure event.

In March 2023, a Twitter user claimed that the SiegedSec hacker organisation got a database from Poorvika Mobiles, an Indian shop. The purported database contains 15 GB of Poorvika account data, financial information, personnel data, PII, and other information. This amount of data is less than the 725.8 GB that I discovered was freely accessible to everyone with an internet connection.

Attack Type : Data Breach

Cause of Issue : Non-password secured database access

Domain Name : Retail Sector

Data Breach on TikTok, Instagram, and Yahoo

A new purported data leak involving the TikTok database has been discovered by the SOCRadar Dark Web Team. The leaked data is said to be in JSON format and came from tiktok.com. The data amount is claimed to be 178GB, however the timing of the leak is uncertain. During the same week, another threat actor released the identical supposed leak on a separate forum. This threat actor claimed that the data is from 2022, implying that it may contain older records. SOCRadar's dark web analyst has identified an alleged Instagram database leak. According to reports, the hacked data contains approximately 17 million JSON records containing usernames, email addresses, phone numbers, addresses, and names. The nature of the data shows that it was obtained from open source. The SOCRadar Dark Web Team has discovered a fresh suspected database sale involving the IMJUVE Instituto Mexicano de la Juventud. The threat actor claims to be selling complete access to the database of the website "imjuventud[.]gob[.]mx," claiming to have all leaked databases available. They also state that they have over 3,000 recordings for sale. A new purported database leak for Yahoo! accounts has been discovered by a SOCRadar researcher. The researcher identified evidence of a possible compromise of Yahoo! account data. More information, such as the scale of the leak and the precise information exposed, has yet to be released.

Attack Type : Data Breach

Cause of Issue : Vulnerabilities in databases

Domain Name : Social Media

AVrecon, a new SOHO router botnet, has spread to 70,000 devices across 20 countries

For more than two years, a new malware strain has been secretly targeting small office/home office (SOHO) routers, penetrating over 70,000 machines and establishing a botnet with 40,000 nodes spread across 20 nations. "AVrecon is now one of the largest SOHO router-targeting botnets ever seen," according to the business. "The goal of the campaign appears to be the establishment of a covert network to enable a variety of criminal activities ranging from password spraying to digital advertising fraud." The compromised system then establishes contact with a new server, known as the secondary C2 server, to await further commands. Lumen claims to have identified 15 such distinct servers that have been operational since at least October 2021. It's worth noting that notorious botnets like Emotet and QakBot use tiered C2 infrastructure. According to KrebsOnSecurity on July 25, 2023, AVrecon is the "malware engine" behind a service called SocksEscort, which rents hacked residential and small business devices to cybercriminals looking to conceal their true location online. It is linked to a Moldovan national named Adrian Crismaru.

Attack Type : Botnet

Cause of Issue : Malware targeting SOHO routers

Domain Name : Cybersecurity Domain

Atera Windows Installer Zero-Days expose users to Privilege Escalation Attacks

Zero-day vulnerabilities in the Atera remote monitoring and management software's Windows Installers might be used to execute privilege escalation attacks. The holes, identified by Mandiant on February 28, 2023, were assigned the numbers CVE-2023-26077 and CVE-2023-26078, and were fixed in Atera versions 1.8.3.7 and 1.8.4.9, released on April 17, 2023 and June 26, 2023, respectively. "The ability to initiate an operation from an NT AUTHORITYSYSTEM context can present potential security risks if not properly managed," according to security researcher Andrew Oliveau. "For example, attackers can use misconfigured Custom Actions running as NT AUTHORITYSYSTEM to execute local privilege escalation attacks." Both weaknesses exist in the MSI installer's repair mechanism, which might result in actions being conducted from an NT AUTHORITYSYSTEM context even when initiated by a standard user.

According to the Google-owned threat intelligence group, Atera Agent is vulnerable to a local privilege escalation attack via DLL hijacking (CVE-2023-26077), which might then be exploited to acquire a Command Prompt as the NT AUTHORITYSYSTEM user. CVE-2023-26078, on the other hand, is concerned with the "execution of system commands that trigger the Windows Console Host (conhost.exe) as a child process," resulting in the display of a "command window, which, if executed with elevated privileges, can be exploited by an attacker to perform a local privilege escalation attack." The announcement comes as Kaspersky sheds further light on a now-patched, serious privilege escalation weakness in Windows (CVE-2023-23397, CVSS score: 9.8) that has been actively exploited in the wild by threat actors via a specifically constructed Outlook task, mail, or calendar event.

Attack Type : Privilege Escalation

Cause of Issue : Zero-day vulnerabilities in software

Domain Name : IT Domain

Clop is currently leaking data stolen from clearweb sites during MOVEit attacks

The Clop ransomware gang is emulating the ALPHV ransomware group's extortion strategy by constructing Internet-accessible webpages dedicated to specific victims, making it simpler to disclose stolen data and increasing victim pressure to pay a ransom. When a ransomware gang assaults a business target, it steals data from the network before encrypting files. This stolen data is used as leverage in double-extortion attempts, informing victims that if a ransom is not paid, the data will be leaked. Ransomware data leak sites are typically located on the Tor network, which makes it more difficult for law officials to seize their infrastructure or shut down the website. However, this hosting approach has its own set of problems for ransomware operators, as it requires a specialised Tor browser to access the sites, search engines do not index the leaked data, and download rates are often quite slow. To address these challenges, the ALPHV ransomware operation, also known as BlackCat, launched a new extortion method last year by constructing clearweb websites to release stolen data, which were advertised as a way for employees to check if their data had been exposed. A clearweb website is hosted directly on the Internet, as opposed to anonymous networks such as Tor, which require specialised software to access. This new way makes it easy to obtain the data and will almost certainly result in it being indexed by search engines, further spreading the exposed information.

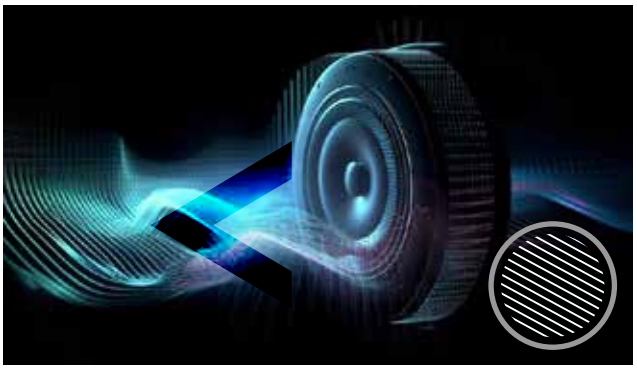
Attack Type : Ransomware

Cause of Issue : Double-extortion ransomware attacks

Domain Name : Cybersecurity Domain

Amazon has agreed to pay a $25 million fine for Alexa privacy violations involving children

Amazon has agreed to pay a $25 million fine to settle allegations of violations of children's privacy laws connected to the company's Alexa voice assistant service, according to the US Justice Department and the Federal Trade Commission (FTC). Since May 2018, Amazon has provided Alexa voice-activated products and services aimed at children under the age of 13. In May 2023, the Federal Trade Commission (FTC) and the United States Department of Justice (DOJ) charged Amazon with breaking children's privacy laws, including the FTC Act, the Children's Online Privacy Protection Act (COPPA), and the COPPA Rule. Amazon was charged for failing to comply with parents' requests to erase their children's voice recordings and geolocation data. According to the complaint, Amazon "failed to honour parents' requests that it delete their children's voice recordings for a significant period of time by continuing to retain the transcripts of those recordings and failing to disclose that it was doing so, also in violation of COPPA."Furthermore, the corporation should have destroyed consumers' voice and geolocation data upon request, but instead chose to keep that data for future usage. The FTC fined Epic Games $245 million (down from a planned $520 million penalty) in March 2022 for violating children's privacy rules and using misleading tactics known as dark patterns to trick millions into making inadvertent in-game purchases.



Attack Type : Privacy laws

Cause of Issue : FTC Act and COPPA

Domain Name : Technology Domain

Passports of FIA World Endurance Championship drivers have been leaked

On June 16th, our analysts discovered two Google Cloud Storage buckets that were misconfigured, resulting in public exposure. Both had over 1.1 million files when combined. Among them were hundreds of FIA World Endurance Championship (FIA WEC) drivers' passports, government-issued IDs, and driver's licences. Two publicly accessible storage buckets containing 1.1 million data were uncovered by the Cybernews investigative team. The public availability of such databases means that anyone can simply access and exploit sensitive data. The is closed information includes driver's licences, passports, and government-issued identification cards. The disclosed documents belonged to endurance racers at the top of their game.

Many have been racing for a long time, and others have even won various phases of the competition. We have decided not to reveal their identities out of caution. The exposed storage buckets are from the fiawec (.) com website, which is controlled by the Le Mans Endurance management team. Following the correspondence with Cybernews, the vulnerable datasets were secured and, as of this writing, are not leaking data. An occurrence in which personal data is disclosed without authorization, on the other hand, is a violation of the General Data Protection Regulation (GDPR). Cybernews has requested an official response from both the corporation and the local data protection authorities (CNIL in France). CNIL stated that it had "not received any complaints or reports about this case," and we have yet to hear back from the corporation.

Attack Type : Data Leak

Cause of Issue : Misconfiguration of Cloud Storage

Domain Name : Motorsport Domain

Three tax preparation firms shared 'extraordinarily sensitive data about taxpayers with Meta, according to lawmakers

Over the course of at least two years, three huge tax preparation services submitted "extraordinarily sensitive" information on tens of millions of taxpayers to Facebook parent company Meta, according to a group of congressional Democrats. Some of that data, they claim, was subsequently utilised by Meta to develop targeted advertising for its own users, other businesses, and to train Meta's algorithms. The Democrats' report urges federal agencies to investigate and even sue H&R Block, TaxAct, and TaxSlayer for the volume of information they shared with the social media behemoth. Seven legislators, in a letter to the leaders of the IRS, the Department of Justice, the Federal Trade Commission, and the IRS watchdog, said their findings "reveal a shocking breach of taxpayer privacy by tax prep companies and Big Tech firms.

" According to the study, taxpayer data was also shared with Google via its own tracking tools, though the company told lawmakers that it never used the information to track people on the internet. Senators Elizabeth Warren, Ron Wyden, Richard Blumenthal, Tammy Duckworth, Bernie Sanders, Sheldon Whitehouse, and Rep. Katie Porter all signed the letter to federal agencies. Legislators demanded that the agencies "immediately open an investigation into this incident."

Attack Type : Data Breach

Cause of Issue : Sharing sensitive taxpayer data with Meta

Domain Name : Financial Sector

The BlackLotus UEFI Bootkit Source Code has been leaked on GitHub

The source code for the BlackLotus UEFI bootkit has been made public on GitHub, however it has been modified from the original virus. The bootkit, which was designed exclusively for Windows, first appeared on hacker forums in October of last year, boasting APT-level capabilities such as secure boot and user access control (UAC) bypass, as well as the ability to disable security software and defence measures on victim PCs. BlackLotus can be used to load unregistered drivers and has been spotted abusing CVE-2022-21894, a year-old Windows vulnerability, to disable secure boot even on fully patched PCs. Microsoft offered resources in April to assist threat hunters in identifying BlackLotus infections. The NSA issued recommendations in June to assist organisations in hardening their systems against the danger.

The BlackLotus source code, which was uploaded on GitHub on Wednesday, has been stripped of the 'Baton Drop' exploit targeting CVE-2022-21894, and now employs the bootlicker UEFI firmware rootkit, although the rest of the original code is still present. According to Alex Matrosov, CEO of firmware security startup Binarly, the public availability of the bootkit's source code poses a considerable risk because it may be integrated with additional flaws and generate new attack chances.

Attack Type : Bootkit

Cause of Issue : Leaked BlackLotus UEFI bootkit source code

Domain Name : Cybersecurity Domain

A critical MikroTik RouterOS vulnerability exposes more than 500,000 devices to hacking

Remote malicious actors could exploit a severe privilege escalation vulnerability in MikroTik RouterOS to execute arbitrary code and seize complete control of susceptible devices. The vulnerability, identified as CVE-2023-30799 (CVSS score: 9.1), is estimated to expose about 500,000 and 900,000 RouterOS systems to exploitation via their web and/or Winbox interfaces, respectively, according to VulnCheck in a Tuesday report."CVE-2023-30799 does require authentication," according to security researcher Jacob Baines. "In reality, the vulnerability is a simple privilege escalation from admin to'super-admin,' resulting in access to any function."

Obtaining credentials for RouterOS installations is simpler than one might think." This is due to the fact that the Mikrotik RouterOS operating system does not provide any protection against password brute-force attacks and ships with a well-known default "admin" user, with its password being an empty string until October 2021, when administrators were prompted to update the blank passwords with the release of RouterOS 6.49. However, the security flaw was not patched until October 13, 2022, in RouterOS stable version 6.49.7, then on July 19, 2023, in RouterOS Long-term version 6.49.8.

Attack Type : Privilege Escalation

Cause of Issue : Vulnerability in MikroTik RouterOS

Domain Name : Networking and Telecommunications

DHL is examining the MOVEit hack as the number of victims exceeds 20 million

The United Kingdom subsidiary of shipping company DHL says it is investigating a data compromise linked to its usage of the MOVEit software, which has been exploited for over two months by a Russia-based ransomware organisation. DHL acknowledged to Recorded Future News that the vulnerability affecting MOVEit, a file-sharing service from Progress Software, affected one of its software vendors. "Upon learning of the incident, DHL immediately launched an investigation, working with relevant experts to understand the consequences," a spokeswoman said. "This investigation is ongoing, and we will continue to communicate with those affected when we have more information to share."

DHL is the latest large corporation to report a compromise connected to the Clop ransomware gang's use of the MOVEit flaw. Although Progress programme fixed the programme, fraudsters were still able to discover unpatched targets. Emsisoft researchers have been tracking the number of companies implicated, discovering that at least 383 organisations have been compromised, with the personal information of 20,421,414 people being leaked as a result.

Attack Type : Ransomware Attack

Cause of Issue : Vulnerability in MOVEit Software

Domain Name : Shipping and Logistics

A Bihar man and a juvenile were arrested by Delhi police for allegedly leaking CoWin Portal data

The Intelligence Fusion & Strategic Operations (IFSO) of the Delhi Police apprehended a guy in Bihar in connection with the alleged breach of data in the CoWIN site, the country's Covid-19 immunisation tracking tool. The individual is accused of leaking sensitive personal information on lawmakers, bureaucrats, and others on the social media network Telegram. The man's mother also worked as a healthcare worker in the state, according to the Delhi Police. According to investigators, the mother assisted her son in gathering data through the CoWIN portal. A juvenile was also apprehended in connection with the case, according to the Special Cell of the Delhi Police. Last week, news appeared about an alleged data breach involving beneficiaries registered on the CoWIN platform. A Telegram bot accessed the data, revealing information such as gender, DOB, Aadhar card, ID, passport numbers, mobile numbers, address, vaccination centre, and so on.

"Technical surveillance was used to identify the accused." He was apprehended near his home in Bihar. We believe he used his mother's assistance to break into the system. He built a bot and distributed it via Telegram. We know he wasn't selling the information to anyone specific. He attempted and succeeded in hacking the system. He uploaded all of the data online after realising he could. "We don't believe he had any other motives," a police officer added.

Attack Type : Data Breach

Cause of Issue : Data leak on social media network

Domain Name : Government Sector

Razer has been attacked by a potential data breach, with a hacker offering stolen data for S$135k in cryptocurrency

On Saturday (July 8), a merchant on a hackers' forum allegedly sold stolen data for US$100,000 (S$134,898) in cryptocurrency. In a tweet on Monday, the business stated that it is aware of a potential compromise and is investigating. The Straits Times investigated and discovered that the data being sold included the source code and back-end access logins for Razer's website and products. This contained folders branded zVault - a reference to Razer's digital wallet, which debuted in March 2017 and was replaced by Razer Gold in December 2018 - as well as those supposedly containing encryption keys and files related to the company's incentive system. ST also obtained a sample that included the claimed e-mail addresses of consumers having virtual credit in their Razer Gold accounts. The seller claimed to have 404,000 accounts, but this was not confirmed. On the hackers' forum, the seller stated that he would only sell the data to one buyer for $100,000 in Monero cryptocurrency.

Attack Type : Data Breach

Cause of Issue : Data breach where sensitive information

Domain Name : Technology and Gaming

BRISK INFOSEC

CYBER TRUST & ASSURANCE

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

+91 86086 34123
+044 4352 4537

contact@briskinfosec.com
www.briskinfosec.com