BRISK INFOSEC

CYBER TRUST & ASSURANCE

THREATSPLOIT ADVERSARY REPORT

Edition 59

www.briskinfosec.com

INTRODUCTION :

The month of June was a challenging one for the security community. We saw a number of high-profile attacks and data breaches, which highlight the ever-evolving threat landscape.

One of the most notable attacks was the ChatGPT data breach, in which over 100,000 stolen account credentials were being sold on the dark web. This breach exposed the personal information of many ChatGPT users, including usernames, passwords, email addresses, and IP addresses. The breach occurred in June, but we are releasing our report in July to give our readers time to take steps to protect themselves.

Another notable attack was the data breach affecting pilots at American Airlines and Southwest Airlines. The breach affected the personal information of about 41,000 pilots, including names, addresses, and Social Security numbers. The breach also occurred in June, and we are releasing our report in July to give our readers time to take steps to protect themselves.

These are just two examples of the many cyber attacks that occurred in June 2023. It is important to be aware of these attacks so that you can take steps to protect yourself and your data.

As CEO of Threatsploit, I want to assure our readers that we are committed to providing the best possible security solutions. We are constantly monitoring the threat landscape and working to develop new tools and techniques to protect our customers.

We also want to remind our readers that they can play a role in protecting themselves from cyber attacks. By following some simple security best practices, you can help to keep your data safe.

Here are a few tips:

- Use strong passwords and change them regularly.
- Be careful about what information you share online.
- Be suspicious of emails and links from unknown senders.
- Keep your software up to date.
- Use a firewall and antivirus software.

By following these tips, you can help to protect yourself from cyber attacks.

also want to take this opportunity to thank our readers for their continued trust in Threatsploit. We are committed to keeping you safe."

In addition to the tips mentioned above, I would also like to recommend that you:

- Be aware of the latest phishing scams.
- Enable two-factor authentication on your accounts.
- Use a password manager to keep track of your passwords.
- Back up your data regularly.

By following these tips, you can help to protect yourself from cyber attacks and keep your data safe.

Best regards,
Briskinfosec Threat Intelligence Team.

CONTENTS :

OVER 100,000 STOLEN CHATGPT ACCOUNT CREDENTIALS ARE BEING SOLD ON THE DARK WEB

"Between June 2022 and May 2023, over 101,100 compromised OpenAI ChatGPT account credentials were discovered on illegal dark web marketplaces, with India alone accounting for 12,632 stolen credentials.

The credentials were discovered in information stealer logs for sale on the cybercrime underground, according to Group-IB in a report shared with The Hacker News.The amount of public records including compromised ChatGPT accounts peaked at 26,802 in May 2023, according to the Singapore-based business. ""Over the past year, the Asia-Pacific region has seen the highest concentration of ChatGPT credentials for sale.""Further investigation found that the notorious Raccoon info stealer (78,348) was responsible for the majority of logs including ChatGPT accounts, followed by Vidar (12,984) and RedLine (6,773).Because of their capacity to steal passwords, cookies, credit cards, and other information from browsers and cryptocurrency wallet extensions, information stealers have grown in popularity among hackers.

""Logs containing compromised information harvested by info stealers are actively traded on dark web marketplaces,"" according to Group-IB. ""Additional information about logs available on such markets includes lists of domains found in the log as well as information about the IP address of the compromised host.""

They have not only lowered the bar for cybercrime, but also serve as a conduit for launching follow-on attacks utilising the syphoned credentials. They are often offered on a subscription-based payment plan. ""Many enterprises are integrating ChatGPT into their operational flow,"" said Dmitry Shestakov, Group-IB's head of threat intelligence."

DATA BREACHES AFFECTING PILOTS ARE DISCLOSED BYAMERICAN AIRLINES AND SOUTHWEST AIRLINES

On Friday, two of the world's major airlines, American Airlines and Southwest Airlines, announced data breaches caused by a compromise of Pilot Credentials, a third-party vendor that maintains various airlines' pilot applications and recruitment websites.On May 3, both airlines were notified of the Pilot Credentials incident, which was limited to the third-party vendor's systems and had no impact or compromise on the airlines' own networks or systems.On April 30, an unauthorised person got access to Pilot Credentials' systems and stole papers comprising information submitted by specific applicants throughout the pilot and cadet hiring processes.According to breach notices submitted with Maine's Office of the Attorney General on Friday, American Airlines reported 5745 pilots and candidates were compromised, while Southwest reported 3009. Although there was no evidence that the pilots' personal information was intentionally targeted or misused for fraudulent or identity theft reasons, the airlines will now drive all pilot and cadet candidates to self-managed internal websites.

Following a July 2022 phishing attempt that compromised a number of employee email accounts, American Airlines announced another data breach in September 2022 that impacted approximately 1,708 American Airlines customers and team employees.Personal information exposed in the July 2022 breach could have included workers' and customers' names, dates of birth, mailing addresses, phone numbers, email addresses, driver's licence numbers, passport numbers, and/or some medical information, as stated at the time. A further examination revealed that the attackers utilised the hacked employees' accounts to send more phishing emails.

Data breach

Third-party vendor security compromise

Airlines Sector

AFTER BEING HACKED TO STEAL CREDIT CARDS, IOTTIE ADMITS A DATA BREACH

iOttie, a manufacturer of automobile mounts and mobile accessories, has warned that its website has been infiltrated for over two months in order to steal online buyers' credit cards and personal information.According to a fresh data breach warning made yesterday, iOttie discovered on June 13th that its online store was infiltrated with malicious scripts between April 12th, 2023 and June 2nd."We believe criminal e-skimming took place between April 12, 2023, and June 2, 2023." "However, the malicious code was removed on June 2, 2023, during a WordPress/plugin update," says the iOttie data breach notification.iOttie has not disclosed how many customers were affected, but has stated that names, personal information, and payment information, including financial account numbers, credit and debit card numbers, security codes, access codes, passwords, and PINs, could have been taken.This is a MageCart assault, in which threat actors breach online retailers and inject harmful JavaScript into checkout pages. When a customer enters their credit card information, the script grabs it and sends it to the threat actors.This data is subsequently utilised to commit financial fraud, identity theft, or is sold on dark web marketplaces to other threat actors. Because of the sensitive information that could be revealed in this assault, all iOttie customers who purchased a product between April 12th and June 2nd should keep an eye on their credit card transactions and bank accounts for any suspicious activity.As iOttie disclosed that the malicious code was removed with a plugin update, the hackers likely breached the site using a vulnerability in one of its WordPress plugins.

MageCart

MageCart JavaScript Injection Attack

Online shopping

HACKERS POST I2VPN ADMIN PASSWORDS ON TELEGRAM

The hackers allegedly got access to i2VPN's primary admin dashboard, where they obtained sensitive information on hundreds of thousands of subscribers. The intrusion was detected after SafetyDetectives' cybersecurity team noticed that hackers had posted what looked to be critical information from i2VPN on Telegram. The exposed material included the admin's email address and password, as well as screenshots of the dashboard displaying data centres and users' subscription details, according to facts published by SafetyDetective with Hackread.com. Although the hackers did not immediately expose user data, the hacked admin panel credentials may have given the hackers access to a large amount of personal information and data centres.If the allegations are genuine, the leaked data could reveal sensitive information such as user IDs, account names, registered email addresses, and subscription-related information such as payment methods and expiry dates.This breach has far-reaching consequences. Hackers with access to such data could use it for a variety of harmful objectives, including spying on users' actions and committing fraud.As the investigation into this breach proceeds, i2VPN must act quickly to remedy the security flaws and strengthen its system in order to prevent such instances in the future. Users should be attentive and keep up to speed on any official announcements or notifications from i2VPN regarding the compromise and recommended security measures.

RATEFORCE, A US AUTO INSURANCE PRICE COMPARISON SITE, HAS LEAKED A MASSIVE AMOUNT OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

A significant data breach has been revealed, exposing over 250,000 documents holding the personal and sensitive information of thousands of Americans. An insecure database containing scans and photos of numerous documents, including vehicle registrations, driver's licences, insurance cards, vehicle titles, and state Medicaid health coverage cards, was used in the breach, which lasted at least two weeks. Jeremiah Fowler, a security researcher, found the problem when he came across the unsecured database. Further examination indicated that USA Underwriters was the principal insurer linked with all of the policies included in the database. Concerned about the seriousness of the data breach, the researcher sent an email to USA Underwriters with a responsible disclosure notification. Despite several tries, however, the researcher received no response.

The database comprised 96,175 folders containing 255,756 records, totaling 93.93 GB in size. Insurance policy cards, driver's licences (front and back), and, in certain cases, extra documents such as auto loan information, state registrations, Medicaid or health insurance cards, utility bills, and letters from banks indicating current accounts were kept in these folders. Furthermore, the breach exposed customer and applicant names, home addresses, phone numbers, driver's licence numbers, VINs, and insurance policy details.

Sales records containing auto dealer information, such as EIN tax identification numbers, were also compromised, with some records containing customers' social security numbers in plain text.

Database Exposure | Inadequate Security Measures | Insurance Domain

ADMINISTRATORS ON DISCORD MALICIOUS BOOKMARKS HACKED

A number of cryptocurrency-focused Discord communities have been hijacked in the last month after their administrators were duped into running malicious Javascript code disguised as a Web browser bookmark. According to victim testimonials, several of the attacks started with an interview request from someone acting as a reporter for an online crypto-focused news organisation. Those that take the bait are emailed a link to what looks to be the official Discord server of the crypto news site, where they must complete a verification process to prove their identity.The bookmark, on the other hand, is a cunning snippet of Javascript that stealthily captures the user's Discord token and transfers it to the scammer's website. The attacker then loads the stolen token into their own browser session and posts a notice on the targeted Discord about an exclusive "airdrop," "NFT mint event," or some other potential money generating opportunity for Discord users (typically late at night after the admins are asleep). Unsuspecting Discord users follow the link supplied by the compromised administrator account and are requested to connect their crypto wallet to the scammer's site, where it requests unlimited spend approvals on their tokens and then empties the balance of any valued accounts. Meanwhile, everyone who discovers the fraud and reacts in the hijacked Discord channel is banned, and their messages are wiped by the compromised admin account.In the above scam, a sort of bookmark called a "bookmarklet" is used to store Javascript code as a clickable link in the bookmarks bar at the top of one's browser. While bookmarklets might be useful and harmless, malicious Javascript run by the user in the browser is particularly harmful. So, unless it was your idea in the first place, please avoid adding (or dragging) any bookmarks or bookmarklets to your browser.

Bookmarks Hijacking | Social Engineering | Comuunication Domain

TOYOTA DISCOVERS MORE MISCONFIGURED SERVERS THAT ARE LEAKING CONSUMER INFORMATION

Toyota Motor Corporation has identified two more misconfigured cloud services that have been leaking personal information from automobile owners for over seven years. This discovery came after the Japanese automaker performed an extensive investigation into all cloud environments administered by Toyota Connected Corporation following the discovery of a misconfigured server that exposed the location data of over 2 million consumers for ten years. The database, which should have been restricted to dealers and service providers, was made public, revealing the Name, Address, Phone Number, Email Address, Customer identification number, Vehicle registration number, VIN (Vehicle Identification Number). The second cloud instance was accessible between February 9th, 2015 and May 12th, 2023, and held less sensitive data linked to car navigation systems.

This data includes roughly 260,000 clients in Japan's in-car device ID (navigation terminal), map data updates, and data creation dates (no vehicle location data). According to Toyota, data entries were automatically removed from the cloud environment after a certain period of time, thus there was only a limited quantity of data exposed at any given time.

Misconfiguration of servers

Misconfigured Cloud Settings

Automobile Industry

A RETAILER'S DATABASE ERROR EXPOSES OVER A MILLION CUSTOMER RECORDS

According to WebsitePlanet, a database configuration issue at a popular automobile retailer exposed 1TB of records, including consumers' personal information. Jeremiah Fowler, a security researcher, reported the incident to the web-builder site after tracing the records to the Philadelphia-based company SimpleTire. According to the online tyre merchant, it has a network of over 10,000 installers and over 3000 independent supply sources. Despite sending SimpleTire "multiple email notices" to appropriately publicise his results, Fowler said the non-password secured database remained publicly accessible to anyone with an internet connection for more than three weeks before being locked down. It is unknown how long the database has been publicly accessible prior to Fowler's discovery. If hackers gained access to the unprotected database, the researcher warned of the possibility of further social engineering assaults.

Database Exposure

Unsecured Database Configuration

Automobile Industry

A NEW HACKER FORUM HAS EXPOSED THE PERSONAL INFORMATION OF 478,000 RAIDFORUMS MEMBERS

"The information for the infamous RaidForums hacker forums has been published online, giving threat actors and security experts insight into the forum's users. RaidForums was a well-known and infamous hacking and data leak site that was known for hosting, leaking, and selling data obtained from compromised organisations.Threat actors that frequented the forum would steal client information by hacking into websites or accessing vulnerable database servers. The threat actors subsequently attempted to sell the data to other threat actors for use in their campaigns, such as phishing attacks, cryptocurrency scams, or malware distribution. In many situations, if the stolen data was not sold or if some time had passed, it would be leaked for free on RaidForums in order to acquire a reputation among the community. A forum called 'Exposed' was started earlier this month to fill the hole left by the closure of Breached, and it has swiftly gained popularity.

The RaidForums member database was hacked today by one of the site's administrators, 'Impotent,' exposing a wealth of information to other threat actors, researchers, and, potentially, law enforcement. The exposed data, according to BleepingComputer, comprises of a single SQL file for the'mybb_users' database used by RaidForums' forum software to hold registration information. This table provides registration information for 478,870 RaidForums members, including usernames, email addresses, hashed passwords, registration dates, and other forum software-related information.The stolen table contains member information for anyone who registered between March 20, 2015 and September 24, 2020, when the database was most likely dumped. According to Impotent, certain RaidForums members have been removed from the database, and it is unknown when and why the dump was made in the first place."

Data breach

Internal Compromise

Internet forum

VPN SERVICE FOR FREE SUPERVPN MAKES 360 MILLION USER RECORDS PUBLIC

Security researcher Jeremiah Fowler identified a massive data leak in a non-password-protected database associated with a popular free VPN provider in a recent cybersecurity incident. The exposed database was 133 GB in size and contained 360,308,817 records. These records contained sensitive data such as user email addresses, originating IP addresses, geolocation data, and server usage logs. The breach also revealed secret keys, Unique App User ID numbers, and UUID numbers, which can be used to identify further important information. The database also contained phone or device models, operating systems, internet connection kinds, and VPN programme versions. The leak also included refund requests and paid account information. This spike in services, however, has resulted in an alarming amount of VPN apps that are untrustworthy and fail to provide the desired level of anonymity and protection. This creates a negative user experience since a lack of sufficient security standards puts their information at danger of being leaked in the event of a data breach. According to VPNmentor's assessment, the majority of entries in the exposed database were related with SuperVPN, a free VPN programme available on both the Apple and Google app stores.

Database Exposure

Misconfigured Database Settings

VPN Attack

AFTER A SECURITY AUDIT, NEW MOVEIT TRANSFER SEVERE ISSUES WERE DISCOVERED; REPAIR NOW

Progress Software today issued a warning to customers about newly discovered significant SQL injection vulnerabilities in its MOVEit Transfer managed file transfer (MFT) service, which might let attackers to steal information from customers' databases. Following extensive code checks began by Progress on May 31, when it patched a hole used as a zero-day by the Clop ransomware gang in data theft attacks, these security issues (together tracked as CVE-2023-35036) were found with the assistance of cybersecurity firm Huntress. They affect all versions of MOVEit Transfer and allow unauthenticated attackers to compromise Internet-exposed servers in order to change or extract client information. All MOVEit Cloud clusters, according to the company, have already been patched against these new vulnerabilities to safeguard them from potential attack attempts.

In a statement delivered to Bleepingomputer over the weekend, the Clop ransomware gang claimed responsibility for targeting the CVE-2023-34362 MOVEit Transfer zero-day, which led to a series of data-theft assaults that purportedly damaged "hundreds of companies." These exploits included the December 2020 zero-day breach of Accellion FTA servers, the 2021 SolarWinds Serv-U Managed File Transfer attacks, and the January 2023 widespread exploitation of a GoAnywhere MFT zero-day.

SQL injection

Managed file transfer (MFT) service

Software Sector

A PROBLEM IN MICROSOFT TEAMS ALLOWS MALWARE TO BE DELIVERED FROM EXTERNAL ACCOUNTS

Despite the application's limits on files from external sources, security researchers have discovered an easy way to distribute malware to an organisation using Microsoft Teams. Microsoft Teams, which has 280 million monthly active users, has been used by organisations as a communication and collaboration platform as part of the Microsoft 365 cloud-based services. Given the product's popularity across numerous organisations, Max Corbridge and Tom Ellson of UK-based security services firm Jumpsec dug around and uncovered a technique to deploy malware via Microsoft Teams using an account outside the target organisation. The attack works with Microsoft Teams in its default configuration, which allows communication with Microsoft Teams accounts outside the enterprise, sometimes known as "external tenants." Corbridge adds in a paper that while this communication bridge would suffice for social engineering and phishing assaults, the way they discovered is more effective because it allows harmful payloads to be delivered directly to a target inbox.

This exploit circumvents existing security safeguards and anti-phishing training recommendations, allowing attackers to infect any organisation utilising Microsoft Teams in its default configuration. Furthermore, if the attacker establishes a domain similar to the target organisations on Microsoft 365, their mails may be disguised as coming from someone within the organisation rather than an external tenant, increasing the possibility that the target will download the file.

Malware attack

Configuration vulnerability in Microsoft Teams

Microsoft Teams

MORE THAN 300,000 FORTINET FIREWALLS ARE EXPOSED TO THE CRITICAL FORTIOS RCE FLAW

Hundreds of thousands of FortiGate firewalls are vulnerable to a severe security flaw known as CVE-2023-27997, despite Fortinet issuing an update to address the issue. The vulnerability is a remote code execution vulnerability with a severity score of 9.8 out of 10 caused by a heap-based buffer overflow in FortiOS, the operating system that connects all Fortinet networking components in order to integrate them into the vendor's Security Fabric platform.CVE-2023-27997 is exploitable, allowing an unauthenticated attacker to remotely execute code on susceptible devices via the SSL VPN interface exposed on the internet. In a mid-June report, the vendor cautioned that the flaw may have been used in attacks.According to Bishop Fox researchers, this suggests that around 335,900 of the FortiGate firewalls reachable over the web are vulnerable to attacks, a figure that is substantially higher than the 250,000 recent estimate based on other, less accurate queries.Bishop Fox built an exploit to show how CVE-2023-27997 may be used to remotely execute code on susceptible devices. The exploit "smashes the heap, connects back to an attacker-controlled server, downloads a BusyBox binary, and opens an interactive shell."

Remote Code Execution

Buffer overflow vulnerability

Fortinet FortiGate firewalls

DATA LEAK FROM COWIN! TELEGRAM MAKES PUBLIC AADHAAR AND PAN CARD INFORMATION SHARED ON THE COVID VACCINATION PORTAL

On Monday, claims of a large data breach surfaced, prompting the government to promise an investigation. The alleged hack affected all Indian residents who had entered their information to the CoWIN immunisation platform, including high-profile political leaders. According to reports, the hacked material is now available on the social media site Telegram and may be accessed by any user. According to the article, when a cellphone number registered with the CoWIN portal is input, the Telegram bot reveals the number of the ID card used for vaccination, as well as the gender, birth year, and name of the vaccination centre, as well as his or her doses. The Aadhaar card, voter ID, and PAN card numbers of Indian individuals are now available to everyone on Telegram as a result of this major data leak. The developers of the Telegram bot that released sensitive information from the hacked Co-WIN database have been removed in the most recent version.

The bot's developers took the action after Manorama broke the story. Officials told the Hindustan Times, Livemint's sister publication, that anytime such a report is published, a comprehensive audit is performed to ensure database access.

Data breach

Data leak, inadequate security

Vaccination domain

IN A NEW PROXYJACKING CAMPAIGN, CYBERCRIMINALS ARE HIJACKING VULNERABLE SSH SERVERS

A financially motivated attack is actively targeting vulnerable SSH servers in order to entrap them in a proxy network. "This is an active campaign in which the attacker leverages SSH for remote access, running malicious scripts that stealthily enlist victim servers into a peer-to-peer (P2P) proxy network, such as Peer2Profit or Honeygain," Akamai researcher Allen West wrote in a paper published on Thursday. Unlike cryptojacking, which uses a compromised system's resources to illicitly generate bitcoin, proxyjacking allows threat actors to use the victim's idle bandwidth to secretly run various services as a P2P node. This has two advantages: It not only allows the attacker to monetize the extra bandwidth with a substantially reduced resource load than would be required to carry out cryptojacking, but it also lowers the chances of detection.

Proxyjacking

Vulnerability in SSH servers

SSH server

THE FREE AKIRA RANSOMWARE DECRYPTOR AIDS IN THE RECOVERY OF YOUR FILES

Avast has produced a free decryptor for the Akira ransomware that can assist victims in recovering their data without having to pay the thieves any money. Akira first debuted in March 2023, quickly accruing victims as it targeted organisations globally in a wide range of areas. Akira operators began using a Linux variation of their encryptor to attack VMware ESXi virtual machines in June 2023, increasing the group's exposure to encryption attacks. Unfortunately, now that a decryptor is available, the Akira ransomware organisation will most likely pore through their code to locate and repair the hole in their encryption, preventing future victims from recovering files for free.

Ransomeware

Vulnerability in security measures

Avast

MILITARY SATELLITE ACCESS IS BEING SOLD FOR $15,000 ON A RUSSIAN HACKER FORUM

"A hacker active on a Russian-language hacker site advertised access to a military satellite operated by Maxar Technologies for sale. The Colorado-based space technology firm specialises in the production of communication, Earth observation, radar, and on-orbit servicing satellites. According to the hacker's assertion, potential purchasers might acquire access to vital information about the US military and strategic posture.

Although the legitimacy of these claims is unknown, the hacker's offer to use Escrow—a trustworthy third-party payment service-adds credence to the offer The consequences of such a breach are severe, as military satellites play an important role in surveillance, communication, and strategic operations. Unauthorised access to these systems may jeopardise national security and pose a major threat."

Data Breach

Potential security breach

Space technology and intelligence

AN ABANDONED S3 BUCKET IS USED IN A NEW SUPPLY CHAIN ATTACK TO DISTRIBUTE MALICIOUS BINARIES

It has emerged that threat actors might grab control of expired Amazon S3 buckets to serve malicious binaries without modifying the modules themselves in a new type of software supply chain attack aimed at open source projects. "Malicious binaries steal user IDs, passwords, local machine environment variables, and local host name, then exfiltrates the stolen data to the hijacked bucket," Checkmarx researcher Guy Nachshon explained. The attack was originally noticed in the instance of a npm package called bignum, which relied on an Amazon S3 bucket to download pre-built binary versions of an addon called node-pre-gyp during installation until version 0.13.0. According to a GitHub advisory published on May 24, 2023, "these binaries were published on a now-expired S3 bucket that has since been claimed by a malicious third party that is now serving binaries containing malware that exfiltrates data from the user's computer.

According to a reverse engineering of the malware sample, it is capable of stealing user credentials and environment details and sending them to the same hijacked bucket. Checkmarx stated that it discovered several packages that were using abandoned S3 buckets, putting them vulnerable to the novel attack vector. If anything, the development shows that threat actors are continually looking for new ways to contaminate the software supply chain.

Supply chain attack

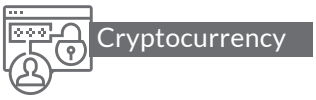
Expired S3 buckets

AWS S3 service

KUCOIN'S TWITTER ACCOUNT WAS HACKED IN ORDER TO PROMOTE A CRYPTOCURRENCY HOAX

KuCoin's Twitter account was compromised, allowing attackers to promote a bogus giveaway fraud that resulted in the theft of more than $22.6K in cryptocurrency. The cryptocurrency exchange and trading platform has vowed to fully compensate victims for all verifiable damages caused by the theft of its official Twitter account. Furthermore, it ensures that all of the platform's users' assets are completely protected. Despite the fact that the account was only hijacked for 45 minutes, the crypto exchange claims it was enough time for its followers to send 22 Bitcoin and Ethereum transactions, allowing the hackers to steal $22,600. According to several KuCoin users on social media, the scammers built up a convincing campaign comparable to the platform's normal promotional events, making it easier for them to be duped. The fraudulent giveaway was hosted on "kucoinevent[.]com," which claimed to be airdropping 5,000 Bitcoin and 10,000 Ethereum to commemorate the exchange's 10 millionth user.

The phoney giveaway urged all users to participate by contributing any amount and receiving double in return, saying that anybody, including those without a KuCoin account, was entitled to participate. As is customary in this type of bogus marketing, the scammers uploaded bogus user comments supporting the legitimacy of the giveaway and attempting to persuade visitors who may have misgivings. Users who have been affected by this issue are recommended to contact KuCoin's support team at "support@kucoin.com" and to disregard any advice or recommendations received through other methods.



THE LANTUM S3 BUCKET LEAK IS A RECIPE FOR DISASTER FOR THOUSANDS OF UK CLINICIANS

A UK organisation for freelance doctors may have exposed personal information about 3,200 people via insecure S3 buckets, which one expert believes might be used to conduct ID theft attacks or blackmail. According to experts, Lantum, an online locum medical agency, has left the storage available on its old backend system, Network Locum. Cybernews found the Amazon AWS S3 bucket, which could have exposed 98,000 files pertaining to thousands of people. The security analysis firm analyses various cloud blob storage to determine the possibility of misconfiguration. It detected the Lantum S3 bucket while doing so, which was accessible and indexed on several IoT search engines. According to the experts, any hostile actor may have discovered the repository of personal data from 2014 to 2016.

Lantum has been invited to comment by the Register. A spokeswoman for Lantum told doctors' news site Pulse, "While this data may have been accessible to unauthorised individuals, there is currently no indication that data has been accessed and no reason to suspect that this is the case." "We are, however, treating this as a potential data breach and will continue to communicate with any individuals who may be affected if our investigations reveal additional information."

Data Breach | Insecure S3 bucket configuration | Medical Agency

PFLEGIA, A GERMAN RECRUITER, HAS LEAKED CRITICAL JOB SEEKER INFORMATION

Pflegia is a German job board that recruits healthcare professionals for hospitals, nursing homes, outpatient services, and critical care. We've contacted Pflegia to inform them of the problem. While the corporation did not respond, the exposed server was swiftly shut down.He revealed Hundreds of thousands of files containing sensitive information were stored in an AWS bucket. The majority of the files were user-submitted resumes with information such as Complete names, the dates of birth, Employment history, Household addresses, Phone numbers, Email address.

Data Breach | Misconfiguration | Recruitment Platform

VULNERABILITIES IN THE HONDA ECOMMERCE PLATFORM EXPOSED CUSTOMER AND DEALER DATA

A researcher has revealed the specifics of critical flaws uncovered in a Honda ecommerce platform used for equipment sales. An attacker could have gained access to customer and dealer information by exploiting the weaknesses. The security flaws and data leakage were identified earlier this year by Eaton Zveare, a US-based researcher who notified Honda of his findings in mid-March. The vendor instantly addressed the issues and congratulated the white hat hacker for his efforts, but did not compensate him because it does not have a bug bounty programme. Honda stated that it found no evidence of deliberate exploitation. The researcher uncovered a password reset API vulnerability in an admin panel, which enabled him to reset the password of a Honda-created test account. While this only granted him access to the test account, he uncovered an insecure direct object references (IDOR) vulnerability that let him to access all of the dealers' data by simply altering the value of an ID in the admin panel's URL.

With access to over 21,000 client orders, highly targeted phishing operations might be developed to deceive customers into submitting even more important data or to attempt to install malware on their devices. Another option would have been to "check for new Honda orders every day and send phishing emails to customers disguised as 'Register your new Honda product' or 'You mistyped your credit card number, click here to correct it'," the researcher wrote in a blog post about the possible consequences.

Vulnerability Exploitation

API Vulnerability

Ecommerce Platform

THE ZELLIS DATA HACK HAD AN IMPACT ON BRITISH AIRWAYS, THE BBC, AND BOOTS

The personal data of employees at the BBC and British Airways has been compromised and revealed as a result of a cyber attack on the payroll provider Zellis. "A cyber security attack targeting file transfer company MOVEit is believed to have impacted Zellis, a payroll company based in the United Kingdom, with British Airways among the firms impacted." "We have been informed that we are one of the companies impacted by Zellis' cybersecurity incident, which occurred via one of their third-party suppliers called MOVEit," British Airways said in a statement. "Zellis provides payroll support services to hundreds of businesses in the UK, including ours... We have alerted colleagues whose personal information has been compromised in order to provide assistance and guidance."An unauthenticated attacker could use the SQL injection vulnerability to obtain unauthorised access to MOVEit Transfer's database. "A SQL injection vulnerability in the MOVEit Transfer web application has been discovered, which could allow an unauthenticated attacker to gain unauthorised access to MOVEit Transfer's database." according to the company's recommendation. "Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database in addition to executing SQL statements that alter or delete database elements."Aer Lingus, another affected company, revealed that "some of our current and former employee data" had been exposed.

SQL Injection

Web Application

Airlines Sector

SCRUBS & BEYOND EXPOSES 400GB OF USER PII AND CREDIT CARD DATA IN PLAIN TEXT

Scrubs & Beyond, a popular online store specialising in healthcare uniforms and accessories, has suffered a catastrophic data exposure breach, exposing personally identifiable information and sensitive financial data of its customers to the public. The leaked server, which contains a wealth of personal information such as full names, email addresses, mobile numbers, physical addresses, and even internal credentials, is publicly accessible and can be downloaded by anyone who knows how to use tools such as Shodan—an open-source intelligence (OSINT) tool commonly referred to as an Internet of Things (IoT) search engine. On May 16, 2023, the database was made public. Researchers discovered the exposure on May 25, 2023, and the data has stayed public since then.

The server currently houses over 100,000 client records totaling 400 GB in size. With each new piece of information, the database size and consumer base grow. Since the server is up and running and there has been no response from the organisation, the likelihood of data misuse and abuse is significant if it falls into the hands of a third party with malicious intent. While the data can be used to commit identity theft-related fraud, hackers can hold the company's server or data hostage and then release it on cybercrime forums if their demands are not satisfied.

Data Breach

Unauthorized Access

E-commerce Sector

OVER $35 MILLION IN CRYPTOCURRENCY IS STOLEN AS A RESULT OF ATOMIC WALLET BREACHES

The makers of Atomic Wallet are looking into accusations of large-scale cryptocurrency theft from customers' wallets, with over $35 million in cryptocurrencies allegedly stolen. Atomic Wallet is a mobile and desktop cryptocurrency wallet that allows users to store a variety of coins. The wallet is available for a variety of platforms, including Windows, Android, iOS, macOS, and Linux. Users of Atomic Wallet began reporting cryptocurrency theft from their Atomic Wallet wallets on Twitter and the developer's Telegram channel on Saturday morning. Victims are also invited to enter this information, as well as other details, on a Google Docs form established to examine the occurrence. While some customers indicate that their cryptocurrency was stolen following a recent software update, others report [1, 2, 3, 4] that they never updated and their cryptocurrency was still stolen. It is unclear how the compromise occurred at this moment, but users are encouraged to move their crypto assets to other wallets until the developers examine the security incident. Atomic Wallet was approached by BleepingComputer with inquiries about the hack, but no comment was immediately available.

Wallet Breached

Software Breached

Cryptocurrency Sector

CORPORATE OFFICE

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