EDITION 55
MARCH
2023

THREATSPLOIT ADVERSARY REPORT

BRISK INFOSEC
CYBER TRUST & ASSURANCE

EDITORIAL

Dear readers,

Welcome to the latest edition of Threatsploit, where we provide you with an overview of the most significant cybersecurity threats and trends from the past month. In March 2023, we saw a continuation of the trend towards more sophisticated and targeted attacks, as well as an increase in the use of data breaches.

One of the most significant threats in March was the emergence of a new cyber espionage campaign dubbed 'No Pineapple!' has been attributed to the North Korean Lazarus hacking group, allowing the threat actors to stealthily steal 100GB of data from the victim without causing any destruction.

Another trend we observed in March was an increase in data breaches. Cybercriminals are increasingly targeting organizations. Recent attack on a book shop in Canada. Also, attack on high profile Pepsi bottling plant in the USA.

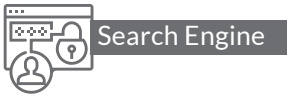
Besides these new threats, we also saw continued use of well-established attack vectors such as phishing and social engineering. Cybercriminals are becoming more sophisticated in their approach to these attacks, making them more difficult to detect and defend against. It is essential for individuals and organizations to remain vigilant and educate themselves on best practices for avoiding these types of attacks.

As always, the best defense against these and other cybersecurity threats is to maintain up-to-date security software, employ strong passwords, and remain vigilant for signs of suspicious activity. By staying informed and taking appropriate precautions, we can work together to protect ourselves and our data from cybercriminals.

CONTENTS

TRUTHFINDER, INSTANT CHECKMATE CONFIRM DATA BREACH AFFECTING 20M CUSTOMERS

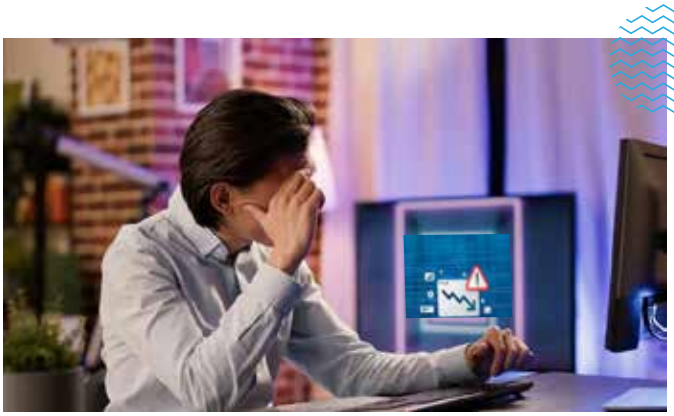
PeopleConnect, the owners of the TruthFinder and Instant Checkmate background check services, confirmed they suffered a data breach after hackers leaked a 2019 backup database containing the info of millions of customers. TruthFinder and Instant Checkmate are subscription-based services allowing customers to perform background checks on other people. When conducting background checks, the sites will use publicly scraped data, federal, state, and court records, criminal records, social media, and other sources. In 2020, PubRec, LLC (owners of TruthFinder and Instant Checkmate) merged with PeopleConnect Holdings, Inc. (the owners of Classmates and Intellius), creating a massive portfolio of services specialized in finding information about people. On January 21st, a member of the Breached hacking and data breach forum leaked the data for allegedly 20.22 million TruthFinder and Instant Checkmate customers who used the services up to April 16th, 2019. The stolen data was shared as two 2.9 GB CSV files containing only customer information before the backup was created on April 16th, 2019. The exposed TruthFinder and Instant Checkmate customer information includes email addresses, hashed passwords, first and last names, and phone numbers.



JD SPORTS SAYS HACKERS STOLE DATA OF 10 MILLION CUSTOMERS

"UK sports apparel chain JD Sports is warning customers of a data breach after a server was hacked that contained online order information for 10 million customers. In data breach notices shared by affected customers, the company warns that the ""attack"" exposed customer information for orders placed between November 2018 and October 2020. JD Sports says it detected the unauthorized access immediately and responded quickly to secure the breached server, preventing subsequent access attempts. However, the hackers were able to steal the data for approximately 10 million unique customers, which consisted of the following information:Full name, Billing details, Delivery address, Email address, Phone number, Order details, Four final digits of the payment card.

This data could be used to launch phishing or social engineering attacks against exposed individuals." "We are proactively contacting affected customers so that we can advise them to be vigilant to the risk of fraud and phishing attacks,"" reads the incident report."



"This includes being on the lookout for any suspicious or unusual communications purporting to be from JD Sports or any of our group brands. ""JD Sports says it does not store full payment card details for online orders, so complete financial information cannot have been compromised. The same applies to account passwords, which the firm says it has no reason to believe were accessed."

Phishing Attacks

10 Million Customers Data Breach

Sports-fashion retail company

NORTH KOREAN HACKERS STOLE RESEARCH DATA IN TWO-MONTH-LONG BREACH

A new cyber espionage campaign dubbed 'No Pineapple!' has been attributed to the North Korean Lazarus hacking group, allowing the threat actors to stealthily steal 100GB of data from the victim without causing any destruction. The campaign lasted between August and November 2022, targeting organizations in medical research, healthcare, chemical engineering, energy, defense, and a leading research university. The operation was discovered by Finnish cybersecurity firm with Secure, whose analysts were called to investigate a potential ransomware incident on one of its customers. However, thanks to an operational mistake by Lazarus, they were able to link the campaign to the North Korean APT. The Lazarus hackers compromised the victim's network on August 22nd, 2022, by leveraging the CVE-2022-27925 (remote code execution) and CVE-2022-37042 (authentication bypass) Zimbra vulnerabilities to drop a webshell on the target's mail server. This RCE flaw was patched in May 2022, but the authentication bypass took Zimbra until August 12th to release a security update. By that time, it was already under active exploitation by threat actors. After successfully breaching the network, the hackers deployed the tunneling tools 'Plink and '3Proxy' to create reverse tunnels back to the threat actors' infrastructure, allowing the threat actors to bypass the firewall.

Remote Code Execution

100GB Data Theft

Research University

ARNOLD CLARK CUSTOMER DATA STOLEN IN ATTACK CLAIMED BY PLAY RANSOMWARE

Arnold Clark, self-described as Europe's largest independent car retailer, is notifying some customers that their personal information was stolen in a December 23 cyberattack claimed by the Play ransomware group. The company said in emails sent to affected clients on that the stolen data includes ID information and banking details. "During this incident, it appears that some personal data stored in our network may have been stolen, including names, contact details, dates of birth, vehicle details, ID documents (such as passports and driver's licenses), National Insurance numbers (in limited cases) and bank account details," the car retailer said. "Upon advice from our cyber security team, we understand the some personal data has been extracted by the hackers who carried out the cyber attack."

Arnold Clark says its security team and external consultants are still investigating the incident to establish the extent and the nature of the information that was exfiltrated from its systems.The company's systems were disconnected from the Internet on the morning of December 24 to cut the attackers' access to the network.Since then, Arnold Clark has been working on restoring the compromised systems and says it will rebuild its "network in a new segregated environment."

Ransomware Attack

Custemers Personal Information

Automobiles Industry

DRUG DISTRIBUTOR AMERISOURCEBERGEN CONFIRMS SECURITY BREACH

Pharmaceutical distributor AmerisourceBergen confirmed that hackers compromised the IT system of one of its subsidiaries after threat actors began leaking allegedly stolen data. AmerisourceBergen is a pharmaceutical product distributor, medical business consultant, and patient services provider. The company is a giant in the healthcare industry, employing 42,000 people and operating multiple distribution centers in the United States, Canada, and the UK, with 150 offices worldwide. As first reported by security researcher Dominic Alvieri, the Lorenz ransomware gang ended a lengthy period of silence by listing AmerisourceBergen and their allegedly stolen data on its extortion site. AmerisourceBergen confirmed the attack to BleepingComputer, stating that the intrusion was contained and they are investigating whether the incident has resulted in the compromise of sensitive data.

The complete statement from AmerisourceBergen is shared below:"AmerisourceBergen's internal investigation quickly identified that a subsidiary's IT system was compromised. We immediately engaged the appropriate teams to limit the intrusion, contained the disruption and took precautionary measures to ensure all systems were and are now clear of any intrusions." "This was an isolated incident and we are in the process of investigating to determine whether any sensitive data was compromised. We take our responsibility to protect data very seriously and continue to secure and strengthen our networks to prevent any future issues." - AmerisourceBergen. The Lorenz ransomware group has posted all files allegedly stolen from AmerisourceBergen and MWI Animal Health, presumably the subsidiary that was breached.

Ransomware Attack

Data Breach

Farmasutical Industry

RESEARCHER BREACHES TOYOTA SUPPLIER PORTAL WITH INFO ON 14,000 PARTNERS

Toyota's Global Supplier Preparation Information Management System (GSPIMS) was breached by a security researcher who responsibly reported the issue to the company. GSPIMS is the car manufacturer's web application that allows employees and suppliers to remotely log in and manage the firm's global supply chain. The security researcher, who publishes under the pseudonym EatonWorks, discovered a "backdoor" in Toyota's system that allowed anyone to access an existing user account as long as they knew their email. In a test intrusion, the researcher found that he could freely access thousands of confidential documents, internal projects, supplier information, and more. The issues were responsibly disclosed to Toyota on November 3, 2022, and the Japanese car maker confirmed they had been fixed by November 23, 2022EatonWorks published a detailed writeup about the discoveries today after 90 days disclosure process had passed. Toyota did not compensate the researcher for responsibly disclosing the discovered vulnerabilities. Toyota's GSPIMS app is built on the Angular JavaScript framework and used specific routes and functions to determine which users can access which pages.The researcher found that by modifying the JavaScript for these functions so that they returned "true" values, he could unlock access to the app.

Security Misconfiguration

Breach data for 14,000 users

Information Management System

A10 NETWORKS CONFIRMS DATA BREACH AFTER PLAY RANSOMWARE ATTACK

The California-based networking hardware manufacturer 'A10 Networks' has confirmed to BleepingComputer that the Play ransomware gang briefly gained access to its IT infrastructure and compromised data.A10 Networks specializes in the manufacturing of software and hardware application delivery controllers (ADC), identity management solutions, and bandwidth management appliances, while it also offers firewall and DDoS threat intelligence and mitigation services. Its customers include Twitter, LinkedIn, Samsung, Uber, NTT Communications, Sony Pictures, Windows Azure, Xbox, Yahoo, Alibaba, China Mobile, Comcast, Deutsche Telekom, Softbank, GE Healthcare, GoDaddy, and Huffington Post.

In an 8-K filing submitted earlier this week, the company says the security incident occurred on January 23, 2023, and lasted for a few hours before its IT team managed to stop the intrusion and contain the damage. The company's investigation determined that the threat actors managed to gain access to shared drives, deployed malware, and 'compromised' data related to human resources, finance, and legal functions. Despite the successful network intrusion, the firm says the security incident has not impacted any of its products or solutions and cannot have affected its customers. “Working with outside experts, the Company has contained the attack within its network and has notified the appropriate law enforcement authorities of the incident,” reads the 8-K filing. “The Company currently does not expect this incident to have a material impact on its operations.”

Remote Code Execution

Access to IT infrastructure and compromised data

Manufacturing of application delivery controller

CALIFORNIA MEDICAL GROUP DATA BREACH IMPACTS 3.3 MILLION PATIENTS

Multiple medical groups in the Heritage Provider Network in California have suffered a ransomware attack, exposing sensitive patient information to cybercriminals. The medical groups impacted by the cyberattack are Regal Medical Group, Lakeside Medical Organization, ADOC Medical Group, and Greater Covina Medical. The entities collectively issued a notice of data breach at the start of the month and shared a sample letter with the California Attorney General's office earlier this week. Today, the healthcare organization reported on the U.S. Department of Health and Human Services breach portal that the data of 3,300,638 patients was exposed in the attack.

Based on the review of the logs, the investigation determined that the following data had been compromised:Full name, Social Security Number (SSN), Date of birth, Address, Medical diagnosis and treatment, Laboratory test results, Prescription data, Radiology reports, Health plan member number, Phone number. Ransomware actors steal this data to create further leverage when extorting healthcare organizations, taking advantage of the highly sensitive nature of medical data. Regal's notice encloses instructions on enrolling for one year of free credit monitoring via Norton LifeLock."Regal understands the importance of safeguarding your personal information and takes that responsibility very seriously," reads the notice."We will do all we can to assist any individuals whose personal information may have been compromised and help them work through the process."

Ransomware Attack

3.3 Million Patients Data Breach

Medical Industry

LARGEST CANADIAN BOOKSTORE INDIGO SHUTS DOWN SITE AFTER CYBERATTACK

Indigo Books & Music, the largest bookstore chain in Canada, has been struck by a cyberattack yesterday, causing the company to make the website unavailable to customers and to only accept cash payments. The exact nature of the incident remains unclear but Indigo is not ruling out that hackers may have stolen customer data. On Wednesday, Indigo announced that "technical issues" were preventing access to the website and customers at physical stores could pay only by cash. Additionally, the company announced that gift card transactions were not possible and that there may be delays with online orders. A few hours later, Indigo disclosed that its computer systems were the target of a cyberattack and it was in the process of investigating the incident with the help of third-party experts. The company has not disclosed the type of cybersecurity incident it is currently dealing with but said that it is trying to determine if the intruders managed to gain access to and/or steal customer data. As Indigo said that it is working to restore the systems, another possibility would be a ransomware attack, which typically results in a data breach as hackers steal data and threaten to publish it unless the victim pays the ransom. Cybercriminals are often targeting big brands, and with an annual revenue of more than CAD $1 billion, Indigo fits the bill. The company's operations include selling books, magazines, toys, beauty and wellness products, and even "items on everything baby" and electronics such as smart home devices.Indigo has thousands of employees, 86 superstores under the banners Chapters and Indigo, and 123 small format stores.

Ransomware Attack

Customer Data Stolen

Books Music & Cafe Website

FLAGSTAR BANK HIT BY DATA BREACH EXPOSING CUSTOMER, EMPLOYEE DATA

US bank and mortgage lender Flagstar has disclosed a data breach after the Clop ransomware gang hacked their Accellion file transfer server in January. In December, threat actors affiliated with the Clop ransomware gang began exploiting vulnerabilities in Accellion FTA servers used by organizations to share sensitive files with people outside of their organization. "Accellion, a vendor that Flagstar uses for its file sharing platform, informed Flagstar on January 22, 2021, that the platform had a vulnerability that was exploited by an unauthorized party. After Accellion informed us of the incident, Flagstar permanently discontinued use of this file sharing platform.

"Unfortunately, we have learned that the unauthorized party was able to access some of Flagstar's information on the Accellion platform and that we are one of numerous Accellion clients who were impacted," Accellion warned in the security advisory. When we contacted Flagstar Bank on Friday with questions about the data breach, the bank directed us to their already published advisory. However, Bleeping Computer has learned that Flagstar was breached not by the original December zero-day vulnerability, which they had patched, but for a new vulnerability utilized by threat actors in January.

Security Misconfiguration | Sensitive Documents Breached | Banking Sector

PEPSI BOTTLING VENTURES SUFFERS DATA BREACH AFTER MALWARE ATTACK

Pepsi Bottling Ventures LLC suffered a data breach caused by a network intrusion that resulted in the installation of information-stealing malware and the extraction of data from its IT systems.-Pepsi Bottling Ventures is the largest bottler of Pepsi-Cola beverages in the United States, responsible for manufacturing, selling, and distributing popular consumer brands. It operates 18 bottling facilities across North and South Carolina, Virginia, Maryland, and Delaware.In a sample security incident notice filed with Montana's Attorney General office, the company explains that the breach occurred on December 23, 2022.

But it wasn't until January 10th 2023, or 18 days later that it was discovered, with remediation taking even longer."We took prompt action to contain the incident and secure our systems. While we are continuing to monitor our systems for unauthorized activity, the last known date of unauthorized IT system access was January 19, 2023."

Based on the results of Pepsi's internal investigation so far, the following information has been impacted:Full name,Home address,Financial account information (including passwords, PINs, and access numbers),State and Federal government-issued ID numbers and driver's license numbers,ID cards,Social Security Numbers (SSNs),Passport information,Digital signatures,Information related to benefits and employment (health insurance claims and medical history).In response to this incident, the company has implemented additional network security measures, reset all company passwords, and informed the law enforcement authorities.At this time, the review of potentially affected records and systems is still underway, while all affected systems have been suspended from the firm's regular operations.The recipients of the breach notices are being offered a one-year free-of-charge identity monitoring service through Kroll to help them prevent identity theft that may occur as a result of the stolen data.

Malware Attack | Company Credentials Taken | Cooldrinks Industry

WEEE! GROCERY SERVICE CONFIRMS DATA BREACH, 1.1 MILLION AFFECTED

The Weee! Asian and Hispanic food delivery service suffered a data breach exposing the personal information of 1.1 million customers. Weee! claims to be the largest Asian and Hispanic grocery store in North America, delivering food across 48 states in the USA via warehouses spread throughout the country. According to the forum post, "In February 2023, a database of 11 million customers belonging to the Sayweee was stolen by hackers."The leaked database contains Weee! customers' first and last names, email addresses, phone numbers, device type (iOS/PC/Android), order notes, and other data the delivery platform uses. After contacting Weee! about the breach, the company confirmed to BleepingComputer that customer information was stolen in the data breach."

We recently became aware of a data breach that has affected some customer information," reads the complete statement from Weee!. "We can confirm that no customer payment data was exposed as Weee!, does not retain any customer payment information in our databases. For customers that placed an order between July 12, 2021 and July 12, 2022, information such as name, address, email addresses, phone number, order number and order comments may have been impacted.""We have notified all customers of the issue and will be notifiying all impacted customers individually if their information was exposed."While the threat actor stated the leak contains 11 million customers, Troy Hunt of the Have I Been Pwned data breach notification service told BleepingComputer that the leaked data only includes 1.1 million unique email addresses. The additional records are likely caused by the same customer placing multiple orders. To check if your information was exposed in this breach, you can search for your email address on Have I Been Pwned later today after the data is added.Once the data is added to Have I Been Pwned, existing members of the notification service will automatically be notified of the data breach via email.

Security Misconfiguration

1.1 Million Customer Data

Ecommerce

INDIAN SOCIAL MEDIA APP SLICK EXPOSED CHILDRENS' USER DATA

Emerging Indian social media app Slick left an internal database containing users' personal information, including data of school-going children, publicly exposed to the internet for months. Bengaluru-based Slick launched in November 2022 by former Unacademy executive Archit Nanda after pivoting from crypto and closing his earlier startup CoinMint. His latest venture, Slick, is available on both Android and iOS and works similarly to Gas, a compliments-based app that is popular in the United States. The app also allows school and college students to talk with and about their friends anonymously. Due to a misconfiguration, anyone familiar with the database's IP address could access the database, which contained entries of more than 153,000 users at the time it was secured. TechCrunch also found that the database could be accessed by an easy-to-guess subdomain on Slick's main website.

The researcher also informed India's computer emergency response team, known as CERT-In, the country's lead agency for handling cybersecurity issues. Nanda confirmed to TechCrunch that Slick fixed the exposure. It's not known if anyone other than Sen found the database before it was secured. Slick attracted many younger users in India shortly after debuting last year. Earlier this month, Nanda took to Twitter to announce that the app crossed 100,000 downloads.

Sensitive Data Exposure

Childrens User Data Exposed

Social Media Apps

INDIAN TICKETING PLATFORM RAILYATRI HACKED 31 MILLION IMPACTED

RailYatri, a popular Indian train ticket booking platform, has suffered a massive data breach that has exposed the personal information of over 31 million (31,062,673) users/travellers. The 12 GB worth of leaked data includes email addresses, full names, genders, phone numbers, locations and 37,000 invoices which could put millions of users at risk of identity theft, phishing attacks, and other cyber crimes.

Hackread.com can confirm that the database has been leaked on Breachforums, a hacker and cybercrime forum that surfaced as an alternative to the popular and now-seized Raidforums.the company claimed that it was merely test data. At that time, the server contained over 700,000 logs with over 37 million entries in total including internal production logs. Hackread.com advises all users to change their passwords and enable two-factor authentication on their accounts as a precautionary measure.

They have also advised users to monitor their bank accounts and credit card statements for any suspicious activity. This breach serves as a stark reminder of the increasing frequency and severity of cyber attacks, particularly in the wake of the COVID-19 pandemic, which has forced millions of people to rely on online platforms for their daily needs. It highlights the need for companies to prioritize cybersecurity measures and take all necessary steps to protect their customers' personal information.

Data Breach

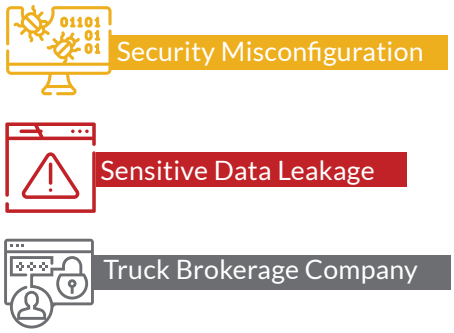
31 Million Users Personal Data

Train Ticket Booking Platform

INDIA'S LARGEST TRUCK BROKERAGE COMPANY LEAKING 140GB OF DATA

India's largest truck brokerage and freight delivery company, FR8, is facing a serious data leak problem. According to the IT security researcher Anurag Sen working with Italian cyber security firm FlashStart, the organization has exposed more than 140 gigabytes of data, which is available to the public without any password or security authentication. According to Hackread.com, the leaked data includes sensitive information such as customer records, invoices, and payment details across India. Not only that, but it also contains other personal information, such as names, addresses, and contact numbers of both customers and employees.

FR8 claims to be "India's largest truck transport service company," currently operating in over 60 cities across the country. Anurag discovered the server on Shodan while searching for misconfigured cloud databases on January 30th, 2023. The researchers informed FR8 about the leak, but they did not receive any response. Their only contact email address available to the public is bouncing back all emails. With a population of over 1.4 billion people, India is a lucrative place for businesses to invest and for cybercriminals to target. The more investment there is, the more widespread and vulnerable the IT infrastructure becomes. As we know, misconfigured or unsecured databases have become a major privacy threat to companies and unsuspecting users. Researchers identified over 10,000 unsecured databases that exposed more than 10 billion (10,463,315,645) records to public access without any security authentication.



CHARTER COMMUNICATIONS SAYS VENDOR BREACH EXPOSED SOME CUSTOMER DATA

Telecommunications company Charter Communications said one of its third-party vendors suffered from a security breach after data from the company showed up on a hacking forum. The spokesperson did not respond to follow-up questions about what third-party vendor was hacked, when the hack occurred or when affected customers will be notified. Charter Communications is the second largest cable operator in the U.S. and fifth largest telephone provider – with more than 32 million customers in 41 states. On Friday, it reported nearly $14 billion in revenue for the last quarter of 2022. The hacker post says the database includes a range of information on repairs and sales. The breach comes just two weeks after the Federal Communications Commission voted unanimously to investigate potential changes to the breach notification rules for telecommunications companies. In a 40-page proposal document, the FCC explained that there have been multiple breaches affecting the country's largest telecommunications companies: Verizon, T-Mobile and AT&T.

"The law requires carriers to protect sensitive consumer information but, given the increase in frequency, sophistication, and scale of data leaks, we must update our rules to protect consumers and strengthen reporting requirements," Rosenworcel said. "This new proceeding will take a much-needed, fresh look at our data breach reporting rules to better protect consumers, increase security, and reduce the impact of future breaches."

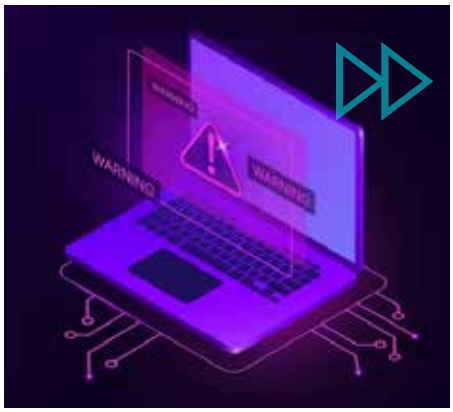
Security Breached

Data Breach

Telecommunications company

HACKERS RAN AMOK ACROSS GODADDY FOR THREE YEARS

"Internet domain registrar GoDaddy recently announced that it has experienced a cyberattack on its infrastructure, which is believed to be part of a larger series of incidents. The company has provided details of these attacks in its annual report, known as Form 10-K, which is a formal requirement for listed entities in the U.S.experts detected that an unauthorized third party had gained access to the company's cPanel hosting servers and installed malware. This resulted in random customer websites being intermittently redirected to malicious sites.URL redirection is a legitimate aspect of HTTP and is commonly utilized for various purposes. To make matters worse, if attackers only initiate malicious redirects sporadically, it can be difficult to detect the subterfuge. This appears to be what happened to GoDaddy. GoDaddy took almost three months to disclose the breach, and there's little information available. If you have visited a GoDaddy-hosted site since December 2022, there are no IOCs to look for. While the company refers to the breach as recent, its 10-K filing suggests it could have been ongoing for longer."



Cyber Attack

Data Breach

Internet Domain Registrar and Web Hosting Company

SENSITIVE US MILITARY EMAILS SPILL ONLINE

A government cloud email server was connected to the internet without a password. The exposed server was hosted on Microsoft's Azure government cloud for Department of Defense customers, which uses servers that are physically separated from other commercial customers and as such can be used to share sensitive but unclassified government data. The exposed server was part of an internal mailbox system storing about three terabytes of internal military emails, many pertaining to U.S. Special Operations Command, or USSOCOM, the U.S. military unit tasked with conducting special military operations. But a misconfiguration left the server without a password, allowing anyone on the internet access to the sensitive mailbox data inside using only a web browser, just by knowing its IP address.

The server was packed with internal military email messages, dating back years, some of which contained sensitive personnel information. One of the exposed files included a completed SF-86 questionnaire, which are filled out by federal employees seeking a security clearance and contain highly sensitive personal and health information for vetting individuals before they are cleared to handle classified information. These personnel questionnaires contain a significant amount of background information on security clearance holders valuable to foreign adversaries.

Cyber Attack

Three Terabytes of Internal Military Emails Exposed

Government Sector

HACKERS STEAL ACTIVISION GAMES AND EMPLOYEE DATA

The cybersecurity and malware research group vx-underground published screenshots of data purportedly stolen from Activision, including the schedule of planned content to be released for the popular first-person shooter Call of Duty.On Monday, games blog Insider Gaming said it confirmed a data breach after obtaining "the entirety" of the stolen data, which was not published by vx-underground.According to the site, hackers stole employee information such as "full names, emails, phone numbers, salaries, places of work, addresses, and more."TechCrunch has not been able to confirm the legitimacy of the published data or the details of the breach. Activision spokesperson Joseph Christinat sent the following statement: "The security of our data is paramount, and we have comprehensive information security protocols in place to ensure its confidentiality. Following a thorough investigation, we determined that no sensitive employee data, game code, or player data was accessed."

Cyber Attack

Employee Data Stolen

Gaming Sector

RUSSIAN STATE TV WEBSITE GOES DOWN DURING PUTIN SPEECH

Russian state media websites broadcasting President Vladimir Putin's address to the country's two houses of parliaments on Tuesday suffered an outage during his speech. Reuters journalists in multiple locations were unable to access the All-Russia State Television and Radio Broadcasting Company (VGTRK) website or the Smotrim live-streaming platform for periods during the speech. A message on the VGTRK website said that "technical works were being carried out" while the Smotrim website was not loading. Shortly before the speech started, state TV channels had broadcast a segment on the technical preparations that go into broadcasting the speech, saying the live stream would be carried across all major Russian TV channels. The state-run RIA Novosti news agency said the outage was the result of a distributed denial of service (DDoS) attack. Reuters was unable to independently verify the reason for the outages.

Denial Of Service

Television and Radio Broadcasting Company

Network Outage During Speech

QR CODE GENERATOR MY QR CODE LEAKS USERS' LOGIN DATA AND ADDRESSES

MyQRcode, a popular Sofia, Bulgaria-based QR code generator website, is leaking the personal data of its users. The security breach or data leak has resulted in the leakage of over 128 GB of data, including the personal information of 66,000 customers. The leak was caused by misconfiguration, making the server publicly accessible to the public without any security authentication or password. What's worse, it was also noted that the data was being actively updated with new records each day, indicating that the leak was still ongoing on further investigation with CloudDefenseAI, it was discovered that new records were being actively added to the data each day. For instance, at the time of writing, the total number of impacted customers was 65,000 however at the time of publishing this article, the number increased to 67,000.

This leak can have serious consequences for the affected customers. Cybercriminals and scammers can potentially use the leaked data to carry out identity theft, phishing attacks, or physical crimes since the addresses of users are part of the leak. Here, it is worth noting that the server has been misconfigured since February 4th, 2023. MyQRcode was informed about the leak last week, but the company has not responded or released a statement on the matter. It is also unclear how long the server has been left unprotected, or if it has been accessed by a third party with malicious intent. In the meantime, Hackread.com can advise customers who have used MyQRcode to generate QR codes to be vigilant about any suspicious activity on their accounts and to monitor their personal information closely. It is also recommended that they change their passwords and enable two-factor authentication wherever possible.

Security Misconfiguration


Personal Data Breach


QR Code Manufacturing

GERMAN AIRPORT WEBSITES DOWN IN POSSIBLE HACKER ATTACK

Several German airports had their websites disrupted on Thursday, with experts investigating a possible online attack. The problems come a day after a major IT failure at Germany's national carrier Lufthansa left thousands of passengers stranded at Frankfurt airport. "Once again, airports fell victim to large-scale DDoS attacks," Ralph Beisel. chief executive of the ADV airport association, said in a statement." According to the information we have so far, other systems are not affected," she said, adding it was not clear whether the situation will spread to other locations. Nüremberg Airport in northern Bavaria said its site had been receiving so many requests that it collapsed. German news magazine Spiegel's website reported that the problems could have been caused by a DDos attack, in which hackers direct heavy internet traffic at targeted servers in a relatively unsophisticated effort to take them offline. There were no reported effects on air traffic. There was travel chaos at Frankfurt Airport — one of Europe's biggest airports — on Wednesday after cable damage at a construction site caused a computer system failure, with more than 200 flights canceled. The websites of German airports were among multiple targets believed to have been brought down last month by the pro-Russian hacking group Killnet.

DDOS Attack

Airport Websites Down

Aerospace Industry

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