THREATSPLOIT ADVERSARY REPORT

BRISK INFOSEC
CYBER TRUST & ASSURANCE

Edition 58

Introduction :

In the ever-evolving landscape of cybersecurity, staying informed about the latest threats is crucial. This summary highlights some of the significant attacks that occurred in June 2023, serving as a reminder of the importance of proactive measures and robust security practices. By understanding these incidents and their implications, readers can better protect themselves and their organizations from similar threats

1. 18-year-old charged with hacking 60,000 DraftKings betting accounts :

This attack emphasizes the need for strong authentication mechanisms and continuous monitoring to detect and prevent unauthorized access to user accounts.
Advise : Encourage users to enable multi-factor authentication and regularly review their account activity for any suspicious behavior.

2. LockBit 3.0 Leaks 600 GBs of Data Stolen From Indian Lender :

The breach highlights the critical importance of data encryption and secure storage practic es to prevent unauthorized access to sensitive information.
Advise : Implement robust encryption protocols and regularly test the security of data stor age systems to safeguard against data leaks.

3. Malicious VSCode Extensions: Password Theft and Remote Shell Exploits :

This attack underscores the significance of ensuring the integrity of software ecosystems and the need for careful evaluation of third-party extensions.
Advise : Only download extensions from trusted sources, regularly update software, and educate users about the risks of downloading unverified extensions.

In an increasingly interconnected world, cyber threats continue to pose significant risks to individuals and organizations. The attacks covered in this summary demonstrate the need for a proactive and comprehensive approach to cybersecurity. By implementing strong security measures, such as multi-factor authentication, data encryption, and regular software updates, individuals and organizations can enhance their resilience against evolving threats.

At Briskinfosec, we remain committed to providing cutting-edge solutions and guidance to our clients, empowering them to defend against cyber threats effectively. We encourage readers to stay informed, remain vigilant, and leverage the expertise of trusted cybersecurity professionals to protect their digital assets.

Once again, I extend my heartfelt appreciation to the Briskinfosec Threat Intelligence Team for their exceptional work and dedication to keeping our clients and the industry secure.

Together, we can create a safer digital landscape for everyone.

Best regards,
Briskinfosec Threat Intelligence Team.

Contents :

18-year-old charged with hacking 60,000 DraftKings betting accounts

"The Department of Justice revealed today that an 18-year-old man named Joseph Garrison from Wisconsin had been charged with hacking into the accounts of around 60,000 users of the DraftKings sports betting website. According to the complaint, the suspect used an extensive list of credentials from other breaches to hack into the accounts. He then sold the hijacked accounts, and the buyers stole approximately $600,000 from around 1,600 compromised accounts. Garrison and his co-conspirators devised a method allowing buyers of the stolen accounts to withdraw all funds, instructing them to add a new payment method to the hacked accounts, deposit a nominal sum of $5 through the newly added payment method to verify its validity, and subsequently withdraw all existing funds from the victims' accounts to a separate financial account under the attackers' control. bad actor(s) were able use login credentials obtained from a third-party source to gain access to certain user accounts. When the identified credential stuffing incident occurred in November 2022, DraftKings provided notice to customers in relevant jurisdictions and restored amounts for a limited number of users who may have had funds improperly withdrawn from their accounts."

Credential stuffing Attack

$600,000 Stolen

Sports Betting Company

LockBit 3.0 Leaks 600 GBs of Data Stolen From Indian Lender

The LockBit 3.0 ransomware group on Monday leaked 600 gigabytes of critical data stolen from Indian lender Fullerton India, two weeks after the group demanded a $3 million ransom from the company. Fullerton India said on April 24 that it had suffered a malware attack that forced it to temporarily operate offline as a precaution. The company said it had resumed customer services and worked with global cybersecurity experts to make its security environment more resilient. Fullerton India operates 699 branches across India that offer doorstep credit services to around 2.1 million customers. The company in 2022 had more than $2.5 billion worth of assets under management and employed over 13,000 people. Ritesh Bhatia, noted cybercrime researcher and the founder of V4WEB Cybersecurity, shared evidence with Information Security Media Group about the LockBit group releasing documents related to Fullerton India on the dark web. He said the data leak occurred as a result of Fullerton India refusing to engage with the ransomware group, leading to the group initiating triple-extortion tactics to force the company to pay. While double extortion involves ransomware actors encrypting a victim's data and exfiltrating it to place additional pressure on the victim to pay, a triple-extortion tactic involves hackers contacting the victim's clients, business partners, vendors and customers to make the breach public and force the victim to come to the negotiating table.

Ransomeware Attack

600 GB of Data Stolen

Retail Banking Company

Malicious VSCode Extensions : Password Theft and Remote Shell Exploits

Cybercriminals are starting to target Microsoft's VSCode Marketplace, uploading three malicious Visual Studio extensions that Windows developers downloaded 46,600 times. According to Check Point, whose analysts discovered the malicious extensions and reported them to Microsoft, the malware enabled the threat actors to steal credentials, system information, and establish a remote shell on the victim's machine. The extensions were discovered and reported on May 4, 2023, and they were subsequently removed from the VSCode marketplace on May 14, 2023. However, any software developers still using the malicious extensions must manually remove them from their systems and run a complete scan to detect any remnants of the infection. Check Point also found multiple suspicious extensions, which could not be characterized as malicious with certainty, but demonstrated unsafe behavior, such as fetching code from private repositories or downloading files.

File Upload

Information Disclosure

Information Technology

QR codes used in fake parking tickets, surveys to steal your money

As QR codes continue to be heavily used by legitimate organizations—from Super Bowl advertisements to enforcing parking fees and fines, scammers have crept in to abuse the very technology for their nefarious purposes.The 60-year old woman who has not been named, saw a sticker on the bubble tea shop's glass door encouraging visitors to scan a QR code and fill out a survey for a "free cup of milk tea."To an average person and even fairly technically savvy one, this alone may not raise red flags considering loyalty and rewards programs often tout such offers, and use QR codes to do so."Enticed by what seemed like a good deal, the 60-year-old scanned the QR code on the sticker and downloaded a third-party app onto her Android phone to complete the 'survey,'" reports Straits Times.+C2As she went to bed at night, her phone suddenly lit up. The bogus "survey" app she'd downloaded siphoned out $20,000 from her bank account."This scam is so insidious because scammers take over the victim's phone. And because victims lose control of their Internet banking account, they won't even know when their savings have been completely wiped out,.Of note is the fact that the particular malware app downloaded by the victim asks the user to grant access to the phone's microphone and camera, in addition to Android Accessibility Service, an Android functionality to assist users with special needs, that also lets an app control the phone screen.The scammer then passively monitors the victim's mobile banking app usage and notes down any login credentials entered by the user during the day."Besides website pop-up banners, which are most common, pasting bogus QR codes outside F&B establishments is another cunning way to hook victims as consumers may not be able to differentiate between legitimate and malicious QR codes."

Account Takeover

$20,000 Lost

Automotive Service & Collision Repair

Discord discloses data breach after support agent got hacked

Discord is notifying users of a data breach that occurred after the account of a third-party support agent was compromised. security breach exposed the agent's support ticket queue, which contained user email addresses, messages exchanged with Discord support, and any attachments sent as part of the tickets. Discord says it immediately addressed the breached support account by disabling it once the incident was discovered. "Due to the nature of the incident, it is possible that your email address, the contents of customer service messages and any attachments sent between you and Discord may have been exposed to a third party," Discord said in letters sent to affected users. They also worked with the customer service partner to implement effective measures to prevent similar incidents in the future. Additionally, the company claims on its website that the platform has 19 million active servers weekly.

Sensitive Data Exposure

Data Breach

VIP and instant messaging social platform

Toyota : Car location data of 2 million customers exposed for ten years

Toyota Motor Corporation disclosed a data breach on its cloud environment that exposed the car-location information of 2,150,000 customers for ten years, between November 6, 2013, and April 17, 2023. According to a security notice published in the company's Japanese newsroom, the data breach resulted from a database misconfiguration that allowed anyone to access its contents without a password. "It was discovered that part of the data that Toyota Motor Corporation entrusted to Toyota Connected Corporation to manage had been made public due to misconfiguration of the cloud environment,". This incident exposed the information of customers who used the company's T-Connect G-Link, G-Link Lite, or G-BOOK services. While there is no evidence that the data was misused, unauthorized users could have accessed the historical data and possibly the real-time location of 2.15 million Toyota cars. It is important to note that the exposed details do not constitute personally identifiable information, so it wouldn't be possible to use this data leak to track individuals unless the attacker knew the VIN (vehicle identification number) of their target's car.

A car's VIN, also known as chassis number, is easily accessible, so someone with enough motivation and physical access to a target's car could theoretically have exploited the decade-long data leak for location tracking.

Data Misconfiguration Attacak

2M CX Car Location Data Exposed

Motor Corporation Sector(Car)

T-Mobile discloses second data breach since the start of 2023

T-Mobile disclosed the second data breach of 2023 after discovering that attackers had access to the personal information of hundreds of customers for more than a month,Compared to previous data breaches reported by T-Mobile, the latest of which impacted 37 million people, this incident affected only 836 customers. Still, the amount of exposed information is highly extensive and exposes affected individuals to identity theft and phishing attacks. T-Mobile said the threat actors didn't gain access to call records or affected individuals' personal financial account info, but the exposed personally identifiable information contains more than enough data for identity theft. While the exposed information varied for each of the affected customers, it could include "full name, contact information, account number and associated phone numbers, T-Mobile account PIN, social security number, government ID, date of birth, balance due, internal codes that T-Mobile uses to service customer accounts (for example, rate plan and feature codes), and the number of lines."After detecting the security breach, T-Mobile proactively reset account PINs for impacted customers and now offers them two years of free credit monitoring and identity theft detection services through Transunion myTrueIdentity. A T-Mobile spokesperson was not immediately available for comment when contacted by BleepingComputer earlier today to ask for more details.

Sensitive Data Exposure

Data Breach

Telecommunications Company

Luxottica confirms 2021 data breach after info of 70M leaks online

Luxottica is the world's largest eyewear company, glasses, and prescription frames maker, and the owner of popular brands like Ray-Ban, Oakley, Chanel, Prada, Versace, Dolce and Gabbana, Burberry, Giorgio Armani, Michael Kors, and many other. The company also operates Eyemed, a vision insurance company in the US.Luxottica has confirmed one of its partners suffered a data breach in 2021 that exposed the personal information of 70 million customers after a database was posted this month for free on hacking forums. According to the seller, the database contained customers' personal information, such as email addresses, first and last names, addresses, and date of birth. The dump was offered for a private sale at the time on Breached, so it was not clear if the data was stolen in a new attack or during two attacks the company However, more recently, the database was leaked in its entirety for free on April 30th and May 12th, 2023, on different hacking forums, making the data far more accessible to threat actors. Andrea Draghetti, the leading researcher of the Italian cybersecurity firm D3Lab, analyzed the leaked data and confirmed to BleepingComputer that it contains 305 million lines, 74.4 million unique email addresses, and 2.6 million unique domain email addresses. To check if your information was exposed in this breach, you can visit the HIBP site and search for your email address on the main page, and the site will list all data breaches that your email address was exposed.

Sensitive Data Exposure

Data Breach

Eyewear Industry

LockBit Leaks 1.5TB of Data Stolen From Indonesia's BSI Bank

"The LockBit ransomware group on Tuesday published 1.5 terabytes of personal and financial information the group said it stole from Bank Syariah Indonesia after ransom negotiations broke down.The group said the records include the personal and financial information of about 15 million customers and employees of the country's largest Islamic bank.Bank Indonesia, the country's central bank, said on Thursday that under its supervision, BSI restored its real-time gross settlement, national clearing system, and Bank Indonesia Fast Payment services.

BSI President and CEO Hery Gunardi on May 11 said ATMs and bank branch services were again available and it was carrying out ""capacity building"" to restore core banking and critical channels. Gunardi said the disruptions occurred on May 8 due to BSI carrying out ""risk mitigation in the company's IT system by carrying out maintenance.""The bank found indications of a cyberattack and ""switched off several channels to ensure system security"" he said.LockBit responded that the bank had ""brazenly lied to their customers and partners, reporting some kind of 'technical work' being carried out at the bank"" when, in fact, its cyberattack had led to the disruptions.The screenshots reveal that the bank floated the possibility of paying $10 million to recover the stolen data. LockBit demanded $20 million before going silent.ndonesian Vice President Ma'ruf Amin said Monday that the BSI incident was a bad experience for the public, and he asked the bank to improve its technology to prevent further attacks. "

Sensitive data is being leaked from servers running Salesforce software

Servers running software sold by Salesforce are leaking sensitive data managed by government agencies, baAt least five separate sites run by the state of Vermont permitted access to sensitive data to anyone, Brian Krebs reported. The state's Pandemic Unemployment Assistance program was among those affected. It exposed applicants' full names, Social Security numbers, addresses, phone numbers, email addresses, and bank account numbers. Like the other organizations providing public access to private data, Vermont used Salesforce Community, a cloud-based software product designed to make it easy for organizations to quickly create websites.nks, and other organizations.Another affected Salesforce customer was Columbus, Ohio-based Huntington Bank. It recently acquired TCF Bank, which used Salesforce Community to process commercial loans. Data fields exposed included names, addresses, Social Security numbers, titles, federal IDs, IP addresses, average monthly payrolls, and loan amounts."The issue was that you are able to 'hack' the URL to see standard Salesforce pages - Account, Contact, User, etc.," Merrett wrote. "This would not really be an issue, except that the admin has not expected you to see the standard pages as they had not added the objects associated to the Aura community navigation and therefore had not created appropriate page layouts to hide fields that they did not want the user to see."In Salesforce parlance, Aura refers to reusable components in the user interface that can be applied to selected portions of a web page, from a single line of text to an entire app.

Android phones are vulnerable to fingerprint brute-force attacks

Researchers at Tencent Labs and Zhejiang University have presented a new attack called 'BrutePrint,' which brute-forces fingerprints on modern smartphones to bypass user authentication and take control of the device. Brute-force attacks rely on many trial-and-error attempts to crack a code, key, or password and gain unauthorized access to accounts, systems, or networks. The authors of the technical paper published on Arxiv.org also found that biometric data on the fingerprint sensors' Serial Peripheral Interface (SPI) were inadequately protected, allowing for a man-in-the-middle (MITM) attack to hijack fingerprint images. The authors of the technical paper published on Arxiv.org also found that biometric data on the fingerprint sensors' Serial Peripheral Interface (SPI) were inadequately protected, allowing for a man-in-the-middle (MITM) attack to hijack fingerprint images. BrutePrint and SPI MITM attacks were tested against ten popular smartphone models, achieving unlimited attempts on all Android and HarmonyOS (Huawei) devices and ten additional attempts on iOS devices.

Brute-Print Attack

Unauthorised Access to Accounts, Networks etc

Mobile Operating (Android) Sector

Dish Network likely paid ransom after recent ransomware attack

Dish Network, an American television provider, most likely paid a ransom after being hit by a ransomware attack in February based on the wording used in data breach notification letters sent to impacted employees. While it didn't directly confirm it paid, Dish implied as much by saying that it "received confirmation that the extracted data has been deleted." Ransomware gangs only delete data or provide a decryption key after a ransom is paid, meaning that is highly unlikely that Dish could receive confirmation that the stolen data was deleted without paying. Even if law enforcement was able to intercept the server hosting the data, there would be no way of knowing that a copy of the data was not also stored elsewhere by the threat actors without paying a ransom. The company also revealed in the notification letters that customer information was not compromised during the ransomware attack. However, Dish discovered that confidential records and sensitive information belonging to current and former employees (and their families) had been exposed during the breach. We have since determined that our customer databases were not accessed in this incident," the company revealed in data breach notification letters sent to affected individuals." The Company was unable to properly secure customer data, leaving it vulnerable to access by malicious third parties," states a class action complaint for violations of the federal securities law filed in the U.S. District Court of Colorado.

Ransomeware Attack

Information Compromised

Television Provider Sector

Crypto phishing service Inferno Drainer defrauds thousands of victims

"A cryptocurrency phishing and scam service called 'Inferno Drainer' has reportedly stolen over $5.9 million worth of crypto from 4,888 victims. According to a report by the Web3Anti-Scam firm 'Scam Sniffer,' the phishing service has created at least 689 fake websites since March 27, 2023.Most of the phishing sites came online after May 14, 2023, with the analysts reporting a spike in site-building activity around that time. The malicious websites created with Inferno Drainer target 229 popular brands, including Pepe, Bob, MetaMask, OpenSea, Collab.Land, LayerZero, and others.Scam Sniffer discovered the service after observing an Inferno Drainer member promoting the service on Telegram by posting a screenshot of a $103,000 theft demonstrating their capabilities. ""By querying the transaction hash obscured in the screenshot, we found this transaction in ScamSniffer's database and associated it with some known malicious addresses in our malicious address database,""Operators pay Inferno Drainer 20% of their proceeds, while the cut goes up to 30% for services that include the creation of phishing sites. However, due to high demand, the service will only offer phishing sites to ""good customers"" or clients who have proven their potential to generate much money.
Promotional post for the service"

Phishing Attack

$5.9M Crypto Stolen

Information Technology

EU slaps Meta with $1.3 billion fine for moving data to US servers

The Irish Data Protection Commission (DPC) has announced a $1.3 billion fine on Facebook after claiming that the company violated Article 46(1) of the GDPR (General Data Protection Regulation). More specifically, it was found that Facebook transferred data of EU-based users of the platform to the United States, where data protection regulations vary per state and have been deemed inadequate to protect the rights of EU data subjects. As a result of the infringement, the DPC imposed a record €1.2 billion fine ($1.3 billion) on Facebook's parent company, Meta Ireland, and requested that all data transfers that violate the GDPR be suspended within five months of the decision. Today, the Irish DPC imposes the $1.3 billion administrative fine reflecting EDPB's decision, punishing Meta with a penalty determined on EDPB's guidelines (20% to 100% of the maximum applicable), given the seriousness of the infringement. Meta criticizes EDPB's decision to ignore DPC's acknowledgment that the company had previously acted in good faith and also highlights the bad timing of these procedures, considering that the forthcoming Data Privacy Framework (DPF) is soon to be implemented, resolving the current legal conflicts.

Server Attack

$1.3Billion Fine

Social Media Platform(Facebook)

North Korean hackers breached major hospital in Seoul to steal data

The Korean National Police Agency (KNPA) warned that North Korean hackers had breached the network of one of the country's largest hospitals, Seoul National University Hospital (SNUH), to steal sensitive medical information and personal details. The police said the incident resulted in data exposure for 831,000 individuals, most of whom were patients. Also, 17,000 of the impacted people are current and former hospital employees.The KNPA press release cautioned that North Korean hackers might try to infiltrate information and communication networks across various industries. It emphasized the need for enhanced security measures and procedures, such as implementing security patches, managing system access, and encrypting sensitive data. North Korean hackers have been previously linked to hospital network intrusions aiming to steal sensitive data and extort a ransom payment from healthcare organizations. More specifically, the U.S. government has highlighted the Maui ransomware threat as such, warning the healthcare sector that they need to raise their defenses against the North Korean operation.

Sensitive Data Exposure

831000 Individuals Data Breach

Healthcare Industry

Zivame data breach : Personal info of thousands of Indian women customers up for sale online

India's popular intimate wear platform for women, Zivame has landed in a soup after the data of thousands of its women customers were put up for sale online. Zivame, a prominent e-commerce retailer known for offering a range of products in women's apparel, has fallen prey to a significant data breach. Threat actors have put the personal information of 1.5 million Zivame customers for sale. India Today Open Source Intelligence (OSINT) team spoke to one of the entities claiming to possess the alleged data and willing to sell it for $500 in cryptocurrencies.Zivame deals in online sale of women's clothing and the data on sale includes the personal information including name, email, phone number as well as the physical address of customers, who are mostly women.

Sensitive Data Exposure

Data Breach

Fashion Retail Sector

Food distribution giant Sysco warns of data breach after cyberattack

Sysco, a leading global food distribution company, has confirmed that its network was breached earlier this year by attackers who stole sensitive information, including business, customer, and employee data. In an internal memo sent to employees on May 3rd and seen by BleepingComputer, the company revealed that customer and supplier data in the U.S. and Canada, as well as personal information belonging to U.S. employees, may have been impacted in the incident. In total, the data breach affected 126,243 who had their names and other personal identifiers exposed together with Social Security Numbers, as revealed in a filing with the Maine Attorney General's OfficeSysco also confirmed the security breach in a 10-Q quarterly report filed with the U.S. Securities and Exchange Commission one week ago. The company believes the employees' data stolen from its systems during the breach is a combination of the following : personal information provided to Sysco for payroll purposes, including name, social security number, account numbers, or similar info.Sysco also hired a cybersecurity firm to help investigate the incident and notified federal law enforcement of the cyberattack.

Cyber Attack

Data Breach

Food Distribution Industry

Brightline data breach impacts 783K pediatric mental health patients

Pediatric mental health provider Brightline is warning patients that it suffered a data breach impacting 783,606 people after a ransomware gang stole data using a zero-day vulnerability in its Fortra GoAnywhere MFT secure file-sharing platform. Brightline is a mental and behavioral health provider offering virtual counseling for children, teenagers, and their families. In a new 'data security notice' displayed on the company's website, Brightline confirmed that data was stolen from its GoAnywhere MFT service that contained protected health information. These attacks were conducted by the Clop ransomware gang, who utilized a zero-day vulnerability tracked as CVE-2023-0669 to allegedly steal data from 130 companies. Brightline offers all impacted individuals two years of complimentary identity theft and credit monitoring services via Cyberscout.

Zero-Day Attack

Data Breach

Healthcare Industry

Airline exposes passenger info to others due to a 'technical error'

AirBaltic, Latvia's flag carrier has acknowledged that a 'technical error' exposed reservation details of some of its passengers to other airBaltic passengers. Passengers also reported receiving unexpected emails which addressed them by the name of another customer. The Riga-based airline, incorporated as AS Air Baltic Corporation operates flights to 80 destinations and is 97% government-owned. Although the air carrier says the leak impacts a small percentage of its customers and that no financial or payment data was exposed, the airline has yet to disclose the total number of impacted passengers. The airline also began emailing customers, informing them of a data leak that exposed their booking information to other passengers. "This email did not contain payment method or other financial details, or sensitive information. The protection of personal data is very important to us, thus we can guarantee that in the incident the personal information of the non-involved passengers is safe and the incident has been contained."Given the exposed data includes sensitive booking details such as the PNR/reservation number-knowledge of which could be used to modify an itinerary, some passengers expressed concern, urging the airline to issue them a new booking number." This has been done for passengers who contacted the airline individually and wanted it themselves," "The protection of personal data is very important to us, so we are thoroughly investigating this case and will contact all affected passengers within today. We guarantee that personal data of non-affected passengers is not compromised and the incident is currently contained. We apologize for any inconvenience caused."

Data Leaked

Passanger Information Leakage

Aerospace Industry

Illinois Data Breach Exposes Private Information of Medicaid, SNAP, and TANF Recipients

The Illinois Department of Healthcare and Family Services (HFS) and Department of Human Services (IDHS) have disclosed a data breach within the State of Illinois Application for Benefits Eligibility (ABE) system's Manage My Case (MMC) portal. The breach involved unauthorized accounts created in the ABE system, which accessed and linked to existing customer MMC accounts by using the customers' personal information, which was stolen from another source. The information accessed includes names, social security numbers, recipient identification numbers, addresses, phone numbers, and income information. The breach potentially affects individuals who have applied for or are receiving benefits through the ABE portal. The breach is a reminder of the importance of strong cybersecurity measures to protect personal information. The Departments' response to the breach will be closely watched, as the breach has the potential to impact a large number of individuals who rely on the State-funded benefits programs. The assistance line at 1-877-657-0006 will remain available until August 14, 2023. Potentially affected individuals can also contact consumer reporting agencies to place a free fraud alert or security freeze on their accounts or visit the Federal Trade Commission's website for more information.

Sensitive Data Exposure

Data Breach

Healthcare Industry

MSI Data Breach : Private Code Signing Keys Leaked on the Dark Web

The threat actors behind the ransomware attack on Taiwanese PC maker MSI last month have leaked the company's private code signing keys on their dark website. "Confirmed, Intel OEM private key leaked, causing an impact on the entire ecosystem,""It appears that Intel Boot Guard may not be effective on certain devices based on the 11th Tiger Lake, 12th Adler Lake, and 13th Raptor Lake."Present in the leaked data are firmware image signing keys associated with 57 PCs and private signing keys for Intel Boot Guard used on 116 MSI products. The Boot Guard keys from MSI are believed to impact several device vendors, including Intel, Lenovo and Supermicro. The leak of the Intel Boot Guard keys poses significant risks as it undermines a vital firmware integrity check and could allow threat actors to sign malicious updates and other payloads and deploy them on targeted systems without raising any red flags. This is not the first time UEFI firmware code has entered the public domain. In October 2022, Intel acknowledged the leak of Alder Lake BIOS source code by a third party, which also included the private signing key used for Boot Guard.

Ransomeware Attack

Private Code Signing Keys Leaked

Information Technology

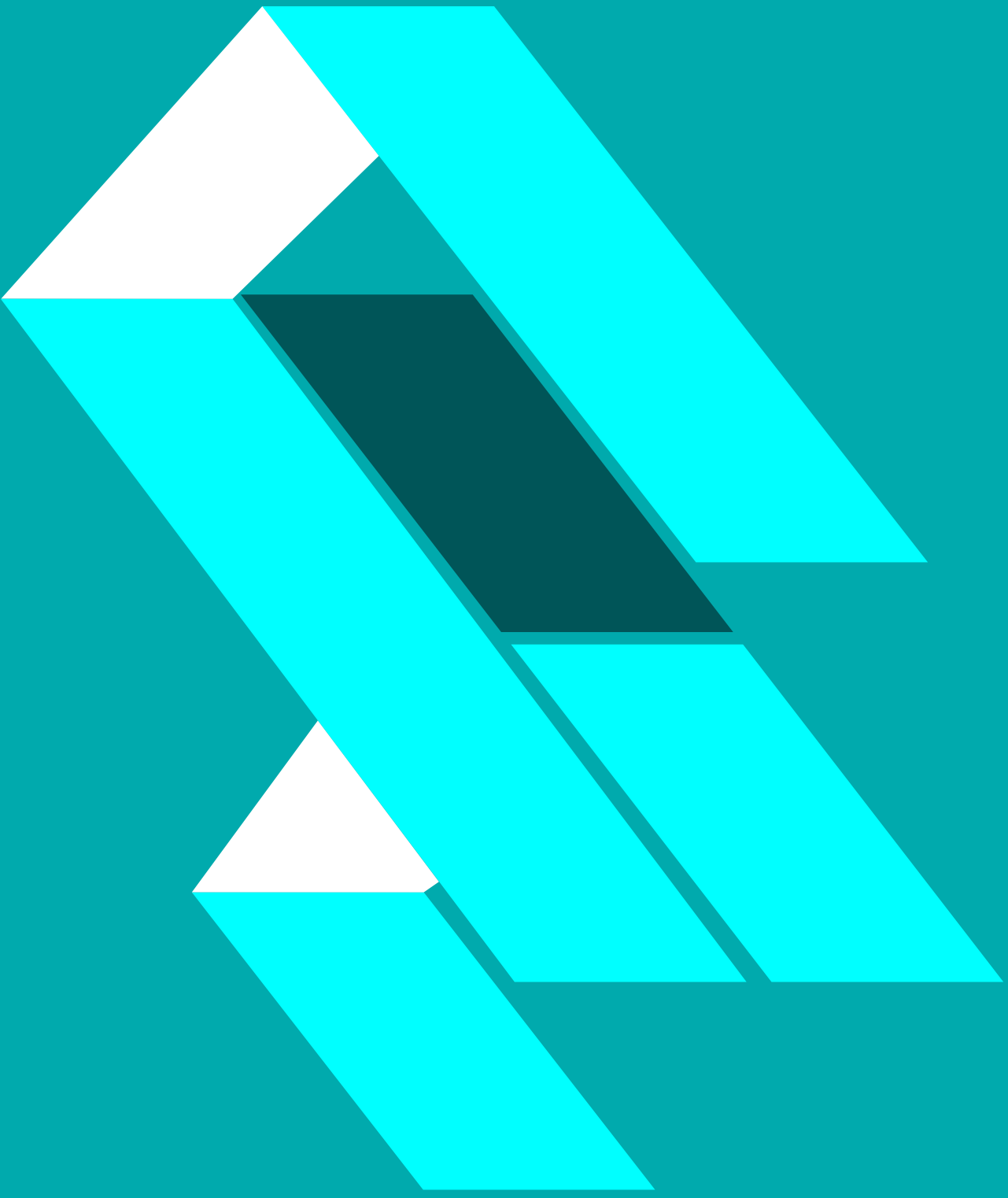
WhizComms data breach : About 50% of customers affected, notified on May 10

About 24,000 customers of broadband service provider WhizComms, or roughly half its customer base, had their personal information stolen by an external party in a data breach incident. The affected people received an e-mail on May 10 informing them that a third party had accessed the firm's Web server and downloaded scanned images of customers' personal information. Some scanned images of work permits and visa approval documents were also downloaded. But the spokesman stressed that customers' contact information and payment details had not been stolen. He said the firm had "investigated completely" and no other information had been compromised apart from what was found on the NRICs or work permits.While home addresses are among information available from the images of scanned NRICs, he said these could differ from the actual installation addresses for the broadband service, which had not been stolen by the third party. After WhizComms staff detected the breach while scanning the customer database, the service provider blocked any further third-party access and filed a police report, the spokesman added. He declined to elaborate further, citing ongoing investigations.

Sensitive Data Exposure

Data Breach

Broadband Service Provider



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