THREATSPLOIT ADVERSARY REPORT

BRISK INFOSEC
CYBER TRUST & ASSURANCE

www.briskinfosec.com

NOVEMBER
2022

Edition 51

Editorial

We hope that you had an absolute safe last month with zero to no incidents. So, here we are with this month's recap.

In this month's report, we see a lot of data leaks, delayed flights, sensitive information being released, and cryptoscam incidents. There have been a lot of healthcare data breaches lately. It's a bad time in the healthcare sector.

Financial fraudsters are preying on workers in order to steal their identification information. Emails are the most common method (96% of cases) in this type of attack, as well as the method of exit.

Imagine that you're minding your own business at the airport when you find that you must pay twice as much for the same flight. It's a scam like this that was discovered in Kolkata.

The iPhone and iPad don't appear to be safe from cyberattacks. CERTIN has found multiple vulnerabilities that need to be addressed. A lab in Australia was broken into, and the records of 223,000 people were stolen.

According to a recent report from non-profit Praja Foundation, cybercrimes in Mumbai increased by 112% from 2017 to 2021. From 1,361 cases in 2017 to 2,883 in 2021, there were 2,883 cases reported. Cheating, whether through loan apps, matrimonial frauds, or job scams, was the most popular last year with 1,154 cases. This is due to the increased use of phones and computers in transactions, which has led to normal crimes turning cyber.

It's not rare for an active Instagram user to get a request from someone who says they invest in crypto. And he said he would make you wealthy. He wants a couple hundred bucks. In the Indian state of Gujarat, this is happening right now.

Stay safe with this report, read it, discuss it & tell us what you think of this report & how it is helping you. We want to make sure that you are aware, updated & ready to tackle the bad actors. Ultimately, to know is to control & to control is to predict.

Contents

Ransomware attacks double since 2017, HR on hackers' targets : Verizon Data Breach Report

Verizon's 2018 Data Breach Investigations Report warns of ransomware attacks (DBIR). It's detected in 39% of malware-related data breaches, double last year's DBIR, and accounts for over 700 cases.There's more bad news : Verizon's analysis show that attacks are now moving into business critical systems, which encrypt file servers or databases, inflicting more damage and commanding bigger ransom requests. "Verizon's DBIR series and intelligent security solutions and services enable enterprises data-driven, real-world cyber-threat views. This 11th edition of the DBIR provides in-depth information and analysis on cybercrime, helping firms safeguard themselves "he said. Human weakness persists.Social attacks on employees continue.Financial pretexting and phishing account for 98% of social incidents and 93% of all breaches, with email being the main entrance method (96% of cases).Social attacks are three times more likely to breach a company than physical weaknesses, highlighting the need for cybersecurity education.Pretexting financesHR:Since the 2017 DBIR, 170 pretexting incidents were analysed (compared to just 61 incidents in the 2017 DBIR).88 cases targeted HR workers to gain personal data for fake tax returns.Phishing must be stopped.78% of people passed phishing tests last year, but 4% fail for each one campaign.A cybercriminal requires one victim to break into a company.

Ransomeware Attack

Data Breach

Information Technology

Cyber crooks target flyers, cancel tickets hours before flight take-off

Four travellers - three from one family and one travelling alone - have reported the strange cancellation of their flight tickets at the eleventh hour without their knowledge. The October 9 TOI reported on one passenger's ordeal. Both the airline and booking portal have denied any role in the cancellation.Kolkata is where the cancellations were made. IndiGo and MakeMyTrip did not respond to TOI's requests for comment. According to bank employee Abhishek Paul, who was travelling with wife Nidhi, daughter Aaditri, and two other families totaling seven people on another PNR, airline ground staff told him three tickets had been cancelled only when he produced the boarding passes at the check-in counter to get luggage tags." Two families and we went to Rishikesh. We had a separate PNR from the other seven. Three months ago, flights were booked. We web-checked in and downloaded boarding passes 48 hours before departure. The airline urged us to arrive early due to rush.Saturday at 3.30pm, we arrived at Terminal 2 for IndiGo flight 6E 2057 at 6.40pm. We learned about the cancellation when people on one PNR placed their luggage "Paul related.

TOI stated Saturday that former British Council director and current Future Hope CEO Sujata Sen had the same issue. Same flight for her. The airline personnel insisted the bookings were cancelled and said the IP address from where they were done was in Kolkata." I had to buy new flight tickets for three via Pune for Rs 51,000. Tickets cost Rs 26,000. Saturday night at 8.45pm, we were to arrive in Kolkata. We landed at 7am Sunday. A vacation gone wrong "He emphasised. Paul has spoken to Cyber PS cops and will submit over a written complaint at Lalbazar on Tuesday. Sujata Senhas written to the Cyber PS and sent a copy to the Kolkata Police joint CP (crime). Passengers have been in similar situations before. Narayan Banerjee, a senior executive of a tea processing equipment manufacturer, had a similar encounter in August 2022.

Cyber Attack

Tickets Loss

Airospace Industries

Cert-In warns of multiple iPhone, iPad vulnerabilities

"Multiple iOS and iPadOS vulnerabilities might allow a remote tracker to access private data, run arbitrary code, fake the interface address, or cause a denial of service. The cyber security watchdog said the vulnerability is exploited in the wild and customers should apply Apple Security patches.'CVE-2022-42827' affects Apple iOS 16.1, iOS versions before 16.0.3, and iPadOS versions before 16. iPhone 8 and after, iPad Pro Call models, iPad Air 3rd generation and later, iPad 5th generation and later, and iPad mini 5th generation and later are affected. As per the report, the severity rating of the vulnerability is high.The vulnerability exists due to inadequate security controls in the AppleMobileFileIntegrity component among a slew of other factors, it said. ""A remote attacker could exploit these vulnerabilities by persuading the victim to open a specially crafted file or application,"" the note said. ""Successful exploitation of these vulnerabilities could allow the attacker to gain access to sensitive information, execute arbitrary code, spoofing of the interface address, or denial of service conditions on the targeted system.""On the same day, the watchdog also reported multiple vulnerabilities in Apple Safari versions prior to 16.1. It said the vulnerabilities could allow an attacker to spoof URLs, disclose sensitive information or execute arbitrary code on the target system. As a solution, Cert-In said users should apply appropriate patches as mentioned by Apple. This vulnerability too was rated as one with a 'high' severity."

Security Misconfiguration

Allows access to sensitive information

Apple Technologies

Australian Clinical Labs says data of 223,000 people hacked

"Australian Clinical Labs said on Thursday its Medlab Pathology business suffered a data breach that affected health records and credit card information of about 223,000 patients and staff.This is the latest in a series of hacks to rock corporate Australia, after the country's biggest health insurer Medibank and No. 2 telco Optus were also hit by breaches that compromised the data of millions of customers. ACL said its affected data included more than 17,500 individual medical and health records, over 28,000 credit card numbers and individuals' names, as well as more than 128,600 Medicare numbers." "To date, there is no evidence of misuse of any of the information or any demand made of Medlab or ACL,"" it said, adding that the compromised Medlab server had been de-commissioned. ACL's broader systems and databases were unaffected, it added."

Cyber Attack | Personal Information Breach | Healthcare

Cybercrimes shoot up by 112% in Mumbai in five years

Cybercrimes in the city surged 112% in five years -from 1,361 cases in 2017 to 2,883 in 2021-according to a report released by non-profit Praja Foundation recently.Cheating cases, whether through loan apps, matrimonial frauds or job scams, topped the list of cybercrimes last year with 1,154 FIRs being lodged. Online frauds involving debit/-credit cards were next on the list-1,075 FIRs filed. According to the data, detection rate of cybercrimes was low at 16% in 2021. Experts pointed out that the number of FIRs being registered were very less compared to actual complaints."Mobile phones have become facilitators of cybercrime. Negligence in prosecution will make cybercriminals more arrogant," said cyber lawyer Prashant Mali. A large number of cybercrime victims make online complaints on the national portal (cybercrime.gov.in). This portal also has a mechanism to freeze the bank account of a culprit in case of a financial fraud. "But the portal largely forwards complaints to local police stations where not all complaints are converted into FIRs. Even the five dedicated cyber police stations set up in Mumbai deal with financial frauds of Rs 10 lakh and above," Mali said.In May 2022, a senior citizen from Jogeshwari had gone on a Kedarnath pilgrimage where he tried to book a chopper ride online and was duped of Rs 50,000. His son had made an online complaint. But Uttarakhand police advised him to approach Mumbai cops on his return home. The senior citizen went to Andheri police station on June 4 but he was not entertained. The FIR was lodged in October after he relentlessly pursued the issue with both Uttarakhand and Mumbai cops.

Cyber Attack | Sensitive Data Collection | Cyber Crime

Instagram accounts hacked, used in crypto scams

Foreign hackers have a new way to scam Instagram users, especially Gujarati influencers. Influencers and following are duped. They take over the compromised account and offer cryptocurrency investment perks and connections. Vadodara cybercrime detectives have received over 100 Instagram hacking allegations in 30 days." Gang sends victim a message and link promising a fee to promote a product or service. The user's account is hacked when they click the link.Hacker alters password and email, says ACP Hardik Makadia (cybercrime). Followers of the hacked Instagram influencer read bitcoin posts and invest in fraudulent schemes. Hackers highlight how the influencer got a lot of money through cryptocurrency investment to attract followers, said ACP Hardik Makadia (cybercrime). This scam has cost hundreds of Instagram followers money. "I get 3-4 calls daily from Instagram influencers whose accounts were hacked. Crypto scammers have started targeting Instagram users to deceive people, said Mayur Bhusawalkar, a computer expert helping victims regain their accounts. Once crypto scammers control an account, they message the victim's pals. "An Instagram friend asked for help recovering her account. When I clicked on the link, my account was hacked and I lost control of my Facebook and gmail," a young girl stated." The questionable links that promise money also ask influencers for personal information and an OTP to transmit to victims.Makadia said many individuals with many follows fall for it to make quick money.

Social Engineering Attack

Crypto Scams

Social Networking Platform

Data of 3 Million Advocate Aurora Health Patients Exposed via Malformed Pixel

Non-profit healthcare provider Advocate Aurora Health is informing 3 million individuals that a malformed tracking pixel has inadvertently exposed protected health information (PHI) to Facebook or Google.Advocate Aurora Health operates 26 hospitals and over 500 care sites with more than 75,000 employees.In a data breach notification on its website, the healthcare system informs patients that an incorrectly configured tracking pixel on MyChart, LiveWell, and some scheduling widgets exposed some of their information.The company says the pixel "sent patient information to third-party analytics vendors that provided us with the pixel technology, especially for users concurrently logged into Facebook or Google accounts."IP addresses, scheduled appointments, patient proximity to an Advocate Aurora Health location, provider data, type of appointment or procedure, MyChart communications (including names and medical record numbers), insurance details, and patient proxies could be exposed.

Advocate Aurora Health says it has no evidence Social Security numbers or credit/debit card details were exposed.The healthcare provider has disabled and/or removed pixels from its platforms and launched an internal investigation to learn what patient data was sent to its vendors.

Advocate Aurora Health has found no evidence that the exposed data has been misused, and the misconfiguration is unlikely to lead to identity theft or financial harm. Advocate Aurora Health says it's notifying all patients about the breach. The organisation told HHS that 3 million people were affected. Advocate Aurora Health is one of tens of US providers using malformed tracking pixels.

Cyber Attack Data Breach Healthcare Industry

Critical Flaws in Abode Home Security Kit Allow Hackers to Hijack, Disable Cameras

Abode Systems sells DIY security systems and cameras with motion sensors to detect intrusions.Apps or keyfobs can arm or disarm the system. The system can be controlled via a website or mobile app and integrated with Amazon Alexa, Apple Homekit, and Google Home. Cisco Talos researchers found vulnerabilities in the Iota all-in-one security kit. Attackers could change user passwords, change device configuration, inject arbitrary code, and shut down the system. Remotely controlling or disabling cameras is possible.

“The devices have format string injection vulnerabilities in various software functions that could cause memory corruption, information disclosure, and denial of service.A malicious XML payload could trigger these vulnerabilities, Cisco says. Home security kit has 14 critical OS command injection vulnerabilities (CVSS score of 10). Cisco's security researchers warn they could be exploited to run arbitrary commands as root.Format string injection, authentication bypass, and integer overflow are three other Abode Systems flaws. Nine of the vulnerabilities are high-severity format string injection flaws that can be exploited with specially-crafted HTTP requests, XCMDs, or configuration values.Authentication bypass, two command injection flaws, and a double-free bug are also high-severity vulnerabilities.Abode Systems patched all of Cisco's reported vulnerabilities in July. Iota 6.9X or 6.9Z should be updated immediately.

Remote Code Execution Root Previlages Takeover Information Security

SIM Swappers Sentenced to Prison for Hacking Accounts, Stealing Cryptocurrency

The two, Eric Meiggs, 24, of Brockton, and Declan Harrington, 22, of Beverly, employed SIM swapping, computer hacking, and other techniques as part of their nefarious activities, the US Department of Justice says. According to documents presented in court, the two targeted executives of cryptocurrency companies and individuals who had large amounts of cryptocurrency or who owned high-value OG (Original Gangster) social media accounts. Meiggs and Harrington conspired to take over OG accounts and steal their victim's cryptocurrency and other assets of value. One of the techniques they employed was SIM swapping, which consists of the attacker convincing the victim's mobile phone carrier to transfer the victim's number to a SIM card controlled by the attacker. This allows the cybercriminals to pose as the victim with social media account providers and initialize password reset procedures that involve sending reset links or authorization codes to the victim's phone number, which is now under the attacker's control. Next, the cybercriminals reset the account's login credentials and can then access the account. The two defendants targeted at least 10 victims in the US and allegedly stole roughly $330,000 in cryptocurrency from them. Meiggs allegedly took over two social media OG accounts. Meiggs and Harrington were sentenced to two years and one day in prison and two years and seven days in prison, respectively.

SIM Swapping Attack

$330,000 Cryptocurrency Stolen

Digital Curreency

Microsoft Confirms Data Breach, But Claims Numbers Are Exaggerated

Microsoft has confirmed that it inadvertently exposed information related to prospective customers, but claims that the company which reported the incident has exaggerated the numbers.Threat intelligence firm SOCRadar revealed on Wednesday that it has identified many misconfigured cloud storage systems, including six large buckets that stored information associated with 150,000 companies across 123 countries.Microsoft confirmed on Wednesday that a misconfigured endpoint exposed data, which the company said was related to "business transaction data corresponding to interactions between Microsoft and prospective customers". The tech giant said it quickly addressed the issue and notified impacted customers. "The business transaction data included names, email addresses, email content, company name, and phone numbers, and may have included attached files relating to business between a customer and Microsoft or an authorized Microsoft partner. The issue was caused by an unintentional misconfiguration on an endpoint that is not in use across the Microsoft ecosystem and was not the result of a security vulnerability," Microsoft explained. The tech giant has thanked SOCRadar, but it's not happy with the company's blog post, claiming that it greatly exaggerates the scope of the issue and the numbers involved. "Our in-depth investigation and analysis of the data set shows duplicate information, with multiple references to the same emails, projects, and users," Microsoft pointed out.

Security Misconfiguration

Business transaction data exposed

Information Security

FTC Targets Drizly and Its CEO Over Cybersecurity Failures That Led to Data Breach

"The FTC acted on the company's security failures that led to a data breach affecting over 2.5 million people, despite Drizly and Rellas being informed of security issues two years prior.-Because the company didn't implement strong data protections, the FTC now requires Drizzly to destroy unnecessary data and collect less customer information, and binds Rellas to specific data security requirements.Our proposed order against Drizly restricts what the company can keep and collect going forward and ensures the CEO faces consequences for the company's carelessness. FTC director Samuel Levine warned CEOs who skimp on security.Boston-based Drizly, acquired by Uber in 2021, operates an online store where adults can order alcohol for delivery.

The company collects customers' email, postal, phone, device, and location information. AWS hosts the data.Drizly and Rellas did not use multi-factor authentication, limit employee access to personal data, or develop adequate security policies, according to the FTC. The FTC's complaint alleges that the company and its CEO stored critical database information on an unsecured platform, did not monitor its network for security threats, and exposed customers to hacking and identity theft when stolen data was traded on dark web sites. The FTC is requiring Drizly to limit its data collection practises, destroy unnecessary data, and implement a comprehensive information security programme. The commission's order requires Rellas to implement security programmes at any company he moves to if it collects information from over 25,000 people and ""where he is a majority owner, CEO, or senior officer with information security responsibilities.""

Security Misconfiguration


Personal Information of 2.5 million users


Federal Trade Commission

Mirai Botnet Launched 2.5 Tbps DDoS Attack Against Minecraft Server

"The attack on Wynncraft used UDP and TCP floods.Web security company said it mitigated the attack, preventing game disruption.Microsoft saw an attack peak at 3.47 Tbps and another at 3.25 Tbps last year.Cloudflare saw a 26 million-request-per-second attack this year (RPS).The attack was notable because it used only 5,000 bots.Google saw the biggest attack ever, peaking at 46 million RPS.Cloudflare said the 2.5 Tbps attack lasted 2 minutes and the 26M rps attack lasted 15 seconds.

This requires automated, always-on solutions.Security teams are slow.By the time the security engineer checks PagerDuty on their phone, the attack is over.Cloudflare reported the massive Minecraft server attack in its Q3 2022 DDoS threat report.
Longer-lasting volumetric attacks and variants of the Mirai botnet have increased by 405% quarter-over-quarter (QoQ).

Cloudflare has seen more application-layer, network-layer, and ransom attacks than last year."

DDOS Attack

Server Data Leaked

Cloud Platform

Iran’s atomic energy agency confirms hack after stolen data leaked online

"The Iranian Atomic Energy Organization (AEOI) revealed that one of its subsidiary's email servers was hacked after 'Black Reward' published stolen data online. AEOI alleges an unnamed foreign entity stole daily correspondence and technical documents from the stolen site. The agency claims it quickly took preventive measures to limit the incident's effects and warned interested parties and officials of potential exploitation attempts. The hackers claim to have removed marketing and spam emails from the collection before publishing. Passports and visas of Iranian and Russian agency employees, power plant status and performance reports, contracts, and technical studies were leaked.

Threat actors pay tribute to Mehsa Amini, who died in Iran's ""moral"" police captivity.The tragedy sparked a month-long uprising against the theocratic administration, which responded with crackdowns and restrictions."

Cyber Attack

Data Leakage

Automic Energy Agency

Thousands of GitHub repositories deliver fake PoC exploits with malware

"Leiden Institute of Advanced Computer Science researchers uncovered thousands of GitHub projects with bogus PoC exploits for vulnerabilities, including malware. Researchers post PoC exploits on GitHub to help the security community validate vulnerability fixes or evaluate a flaw's effect and scope. According to a report from Leiden Institute of Advanced Computer Science, the chance of getting malware instead of a PoC is 10.3%, excluding proven fakes and prankware. The researchers analyzed a little over 47,300 repositories advertising an exploit for a vulnerability disclosed between 2017 and 2021 using the following three mechanisms :

IP address analysis : comparing the PoC's publisher IP to public blocklists and VT and AbuseIPDB.
Binary analysis : run VirusTotal checks on the provided executables and their hashes.
Hexadecimal and Base64 analysis : decode obfuscated files before performing binary and IP checks.

The binary analysis examined a set of 6,160 executables and revealed a total of 2,164 malicious samples hosted in 1,398 repositories. In total, 4,893 repositories out of the 47,313 tested were deemed malicious, with most of them concerning vulnerabilties from 2020."

Proxy Chain Attack

Code Execution

Code Hosting Platforms (Github)

Cuba ransomware affiliate targets Ukrainian govt agencies

Computer Emergency Response Team of Ukraine (CERT-UA) warns about .Cuba Ransomware assaults on key networks. CERT-UA noticed a new wave of phishing emails impersonating the Press Service of the General Staff of the Ukrainian Armed Forces on October 21. The link directs the recipient to a third-party website to download "aка 309.pdf," but a bogus notice says they need to upgrade their PDF reader first. The website prompts visitors to click "DOWNLOAD," which downloads a programme ("AcroRdrDCx642200120169 uk UA.exe") imitating an Acrobat Reader installer. Running this file instals and executes "rmtpak.dll," Cuba Ransomware's "ROMCOM RAT" virus. This malware lets threat actors steal data, fake processes, initiate reverse shells, and more." Considering the use of the RomCom backdoor and other properties of the connected files, we believe it is possible to associate the observed activity with the activity of Tropical Scorpius (Unit42) aka UNC2596 (Mandiant)," concluded CERT-UA.

Phishing Atack

Steal data, fake processes, initiate reverse shells

Automic Energy Agency

Indian Energy Company Tata Power's IT Infrastructure Hit By Cyber Attack

Tata Power Company Limited, India's largest integrated power company,The intrusion on IT infrastructure impacted "some of its IT systems," the company said in a filing with the National Stock Exchange (NSE) of India. It further said it has taken steps to retrieve and restore the affected machines, adding it put in place security guardrails for customer-facing portals to prevent unauthorized access.The Mumbai-based electric utility company, part of the Tata Group conglomerate, did not disclose any further details about the nature of the attack, or when it took place.

He network intrusions were said to have been aimed at "at least seven Indian State Load Despatch Centres (SLDCs) responsible for carrying out real-time operations for grid control and electricity dispatch within these respective states."

The attacks were attributed to an emerging threat cluster Recorded Future is tracking under the name Threat Activity Group 38 (TAG-38). The company further assessed that the targeting is intended to facilitate information gathering related to critical infrastructure assets or is likely a precursor for future activitie

Cyber Attack

It Inftastructure Affected

Integrated Power Company

Hyderabad Police bust 'Chinese investment fraud' of Rs 903 Cr

"Hyderabad city police arrested 10 persons, including a Chinese national, Wednesday in a Rs 903 crore Chinese investment fraud." "Hyderabad city police cyber crime wing has detected a Chinese investment fraud case," " said Hyderabad Police Commissioner C V Anand." "The modus operandi is to use authorised money changers, who are authorised by the RBI, to convert illegally gathered funds through investment apps into dollars and send them abroad." "A Hyderabad resident said he was scammed after investing Rs 1.6 lakh in an app. The complainant's money was deposited in a private company's bank account.

During interrogation, the account holder confessed he opened the bank account on the directions of a Chinese individual and handed him the user name and password, according to a police release. Another private company's bank account (established by a Delhi man) shared the previous firm's phone number. The Delhi man opened multiple bank accounts.

Two people who opened bank accounts got Rs 1.2 lakh each. The private company transferred money from 38 virtual bank accounts to two money changers.Cash is exchanged for rupees. Money changers and FX exchanges flouted RBI norms on money moving. Those who obtained US cash joined other fraudsters and transported it abroad via hawala, it claimed. The probe revealed a 903-crore hawala fraud, the release added. Police said two fraud suspects are in China. Anand said city police would communicate with ED and DRI due to the fraud's severity. "

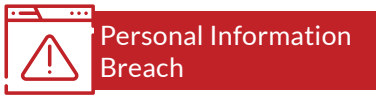
Money Scam

Cyber Crime

Alarm over fake ID-printing websites using customer data for cyber fraud

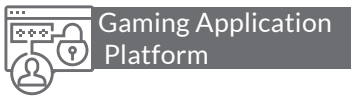
A cyber security firm reports a surge in data privacy breaches. Fake identity card-printing websites in Uttar Pradesh are stealing people's personal information. Many cases are reported from larger cities, especially the National Capital Region, says the police. According to research, many of these websites are in western Uttar Pradesh. According to a report by Bengaluru-based CloudSEK, these websites make physical identity cards like Aadhaar, PAN, driving licence, etc. and deliver them at affordable rates. Social engineering, identity theft, phishing, etc. use these data. "The domains impersonate Indian telecommunication providers, banks, payment wallets, courier services, etc. This includes Fino Payments Bank, DTDC, India Post, etc "study found.Popularize these domains with Google Ads, social media, and SEO. Victims are duped into sharing PII and OTPs on a KYC portal integrated with payment platforms.Such private data can be used for illegal financial transactions and SIM card issuance, the report said.

Superintendent of Police, Cyber Crime, Uttar Pradesh, Triveni Singh, told PTI that police are investigating impersonation complaints. Singh asked people to report online crimes at 1930 or cybercrime.gov.in. Fraudsters exploit people's preference for physical documents despite India's digital revolution, CloudSEK said. "This need explains why corner shops print IDs. Due to the pandemic, many people are using the internet to print IDs "addition-CloudSEK found many YouTube videos and channels with malicious domain links. It warned against clicking on suspicious links and ignoring e-mails from unknown sources.



Gaming app scam : Bitcoins worth ₹13Cr attached

"The Enforcement Directorate has attached Rs 13 crore worth of crypto currency Bitcoin of Aamir Khan of Kolkata from whose premises the agency had earlier this month recovered over Rs 17 crore in unaccounted cash. It was one of the highest recoveries of black money after the seizure of Rs 50 crore from the different premises linked to senior TMC leader and former former Bengal minister Partha Chatterjee. Investigating money trail against E-Nuggets, the mobile gaming app run by accused Aamir Khan, the ED has been on the trail of some high-profile people from Bengal linked to him after it was found that he was transferring part of the 'proceeds of crime' to overseas accounts by using crypto currency exchange Binance." "Investigation revealed that the accused was transferring part of the amount illegally earned through the gaming app (E-Nuggets) to overseas accounts by using crypto currency exchanges," " the ED said. in what can turn the case into a potentially bigger crime than that of an unaccounted cash stash found on an obscure figure."



Outsourcer Interserve fined £4.4m for failing to stop cyber-attack

Interserve was fined £4.4m after hackers stole the personal and financial information of 113,000 employees. Interserve was a "key supplier to the government with clients including the Ministry of Defense" when the attack occurred.Bank account details, NI numbers, ethnicity, sexual orientation, and religion were compromised. Interserve's system failed to intercept a phishing email an employee downloaded, and a subsequent anti-virus alert was not properly reviewed, according to the ICO. The attack compromised 283 systems and 16 accounts, removed Interserve's anti-virus system, and encrypted employee data.

The ICO stated Interserve used outdated software systems and protocols and lacked insufficient risk evaluations.John Edwards, the UK information commissioner, said the compromise left Interserve employees vulnerable to identity theft and financial crime."Leaving cyber-attackers open is never acceptable, especially when dealing with sensitive material."The largest cyber risk for businesses is internal complacency, not outside hackers.The ICO can fine up to £17.5m or 4% of yearly global revenue.If a company offers mitigating arguments, it can lessen a fine.After "careful examination" of Interserve's arguments, the ICO opted not to lessen its fourth-largest penalties.Edwards said the sanction was meant to make directors and chairmen examine CEOs' cyber preparedness.Advertisement-Edwards, who became ICO commissioner in January, said the agency had 80 active investigations and initiated 500 a year.

Phishing Attack

Personal Information of 113,000 Employees Stolen

Information Security

Twilio discloses another hack from June, blames voice phishing

"Cloud communications company Twilio disclosed a new data breach stemming from a June 2022 security incident where the same attackers behind the August hack accessed some customers' information. Twilio says this was a ""brief security incident"" on June 29. The attacker used social engineering to trick an employee into handing over their credentials in a voice phishing attack. The stolen credentials were then used ""to access customer contact information for a limited number of customers.""""The threat actor's access was identified and eradicated within 12 hours""209 customers - out of a total customer base of over 270,000 – and 93 Authy end users - out of approximately 75 million total users - had accounts that were impacted by the incident,"" Twilio said.

After concluding the incident investigation, Twilio also found no evidence that any of its customers' console account credentials, API keys, or authentication tokens were also accessed. While the company disclosed the incident on August 7, it now revealed the attackers maintained access to this environment for two more days.""The last observed unauthorized activity in our environment was on August 9, 2022,"" the company added."

Cyber Attack

Data Breach

Cloud Communication Company

Cybercriminals Used Two PoS Malware to Steal Details of Over 167,000 Credit Cards

Researchers reveal 80 ShadowPad C2 serversA threat actor used two point-of-sale (PoS) malware variants to collect 167,000 credit card details. According to Singapore-based cybersecurity company Group-IB, the stolen data dumps might be sold for $3.34 million on underground forums. While many assaults on e-commerce websites use JavaScript sniffers (web skimmers) to capture payment data, PoS malware is still a danger. Just last month, Kaspersky detailed additional strategies used by Prilex to steal money through fraudulent transactions. Treasure Hunter and its advanced sequel MajikPOS brute-force their way into PoS terminals or buy first access from initial access brokers, then harvest payment card information from the system's memory and transfer it to a remote server. Group-IB, which detected the two PoS malware's C2 servers, said 77,428 and 90,024 unique payment records were compromised between February and September 2022.The stolen cards were issued by banks in the U.S., Puerto Rico, Peru, Panama, the U.K., Canada, France, Poland, Norway, and Costa Rica. The scheme's perpetrators are unknown, and it's unclear if the stolen data has been sold. This can have serious ramifications if card-issuing institutions don't enforce proper safety systems, allowing bad actors to usecloned cards to steal money and make unauthorised transactions.

Cyber Attack

Stolen Details of Over 167,000 Credit Cards

Information Security

Microsoft Confirms Server Misconfiguration Led to 65,000+ Companies' Data Leak

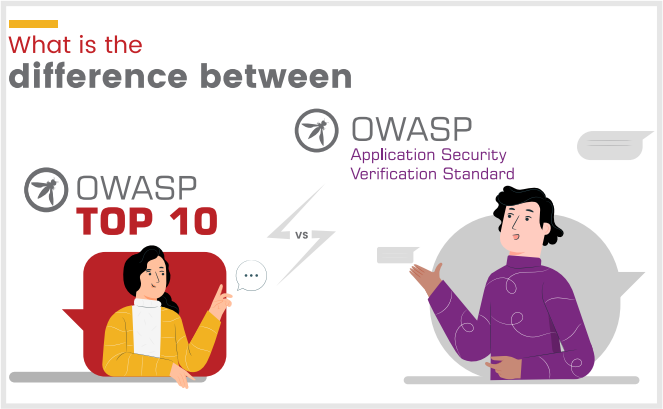
Microsoft revealed this week that it exposed customer data due to a security breach that left an endpoint publicly accessible without authentication. "This misconfiguration resulted in the potential for unauthenticated access to some business transaction data," Microsoft noted in an alert. Microsoft noted that the B2B leak was "triggered by an inadvertent misconfiguration on an endpoint" and not a security flaw. On September 24, 2022, cybersecurity startup SOCRadar discovered a misconfigured Azure Blob Storage, dubbed BlueBleed. Microsoft is alerting customers directly. The leak impacts more than 65,000 businesses in 111 countries, according to SOCRadar. The exposed data includes invoices, product orders, client documentation, and partner ecosystem details. Microsoft disputes the issue's scope, saying the data contained names, email addresses, email content, firm name, phone numbers, and attached files relevant to business "between a client and Microsoft or an authorised Microsoft partner. "Threat intel company "greatly overstated" the scale of the problem, it said, because the data set contained "duplicate information, with repeated references to the same emails, projects, and people."

Server Misconfiguration

65,000+ Companies Data Leak

Micrsoft Cimoay

Our recent blogs



Read More..

Read More..

Polls for the month

This month being Cybersecurity Awareness Month we polled some questions to know the awareness of our audience, partners, clients & customers

You too can quiz yourself and see your cybersecurity knowledge

"You get a text message from a vendor who asks you to click on a link to renew your password so that you can log in to its website"

What will be your reaction?
1. Reply to text to confirm
2. Call to confirm
3. Renew the password
4. Check if it's not a scam

Answer : 4

Which according to you is the biggest Cybersecurity threat?
1. Social Hacking
2. Ransomware
3. Wire transfer frauds
4.Unpatched Vulnerabilities

Answer : 1

Social engineering uses which aspects of human nature?
1.Trust manipulation
2.Desire to be helpful
3.Lack of understanding
4.All of the above

Answer : 4

What is the primary reason for cyber threats in your organization?
1. Lack of Security Awareness
2. Using Personal Device
3. Unrestricted Internet Access
4. All of the above

Answer : 4

What exciting happened last month?

We had an audio event where in we discussed about the difference between SSL and TLS . Please have a listen to this link to know more

We did a live for the Threatsploit of the last month, in case you missed it, here is the link

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