THREATSPLOIT ADVERSARY REPORT

BRISK INFOSEC
CYBER TRUST & ASSURANCE

www.briskinfosec.com

Edition 49
SEPTEMBER

Editorial

"Hello, Mr. XYZ,

This is your city's Electricity Board's message. You have been billed for Rs XXX. Please pay it by the deadline of XX-XX-XXX. The payment link is provided below. After that, we would be forced to disconnect your connection."

What would you do if you received a message like this? You may pay, correct? We all require electricity. The inhabitants of Bengaluru, India's IT powerhouse, did the same thing. Then they realize it was all a sham. We are all vulnerable to such social engineering attacks. As a result, it is preferable that we are well informed about what is going on around us.

Such horrifying next-door incidents are featured in this month's Threatsploit Report for August 2022.

We all use Fast Tag and recharge it. However, a 34-year-old banker contacted a phoney number and was fooled out of INR 7 lacs. Yes, I am sure she was aware, but the fraudsters took advantage of her at the time.

Rotary International is one of the world's largest humanitarian organizations, assisting millions of people. Many wealthy people donate to charity through Rotary. What would happen if these people's data was leaked? And it happened exactly last month. The manner in which such massive data was leaked is still under investigation.

A Mumbai-based company was defrauded by a man impersonating a scrap supplier. He then cheated the corporation out of INR 1 crore. This is known as an MITM (Man in the middle attack.

Healthcare data breaches are on the rise on a global scale. As each record of health care data costs hundreds of dollars. Attacks against airlines have escalated as the tourism business has become more accessible.
The Israeli air force was purportedly infiltrated, and an air siren was allegedly activated by Iranian hackers. For its solutions and security, Israel is considered as the best in the cyber world.

A thorough reading of the report will familiarize you with what is going on in the world. After all, knowledge is power, and it is the only way we can defend ourselves. Happy online safety month! Keep yourself safe.

Contents

Healthcare provider Novant issues data breach warning after site tracking pixels sent patients’ information to Meta servers

Novant Health, a US healthcare provider, is warning patients of a potential data breach resulting from an incorrect configuration of an online tracking tool from the company behind Facebook.the tracking pixel in question was “configured incorrectly and may have allowed certain private information to be transmitted to Meta” from the Novant Health website and patient portal, the company said.In a recent privacy statement, Novant Health said that it removed the pixel as soon as it discovered that it had the capability to transmit information to Meta.

Upon further investigation, the healthcare provider said that, depending on a user’s activity within the Novant Health website and MyChart portal, the leaked data could include email address, phone number, computer IP address, and healthcare appointment information.The company said it has mailed letters to “some patients” following the discovery of the pixel misconfiguration. According to local press reports, more than 1.3 million individuals have been notified.Patients at Novant’s New Hanover Regional Medical Center are not impacted. The incident, however, may affect other individuals who aren’t registered Novant Health patients but received a Covid-19 vaccine at a Novant facility.“Based on our investigation, we do not have any evidence that this information was acted on by Meta or any other third party,” Novant said.

Data Breach

Personal Information Exposed

Healthcare

CompleteFTP path traversal flaw allowed attackers to delete server files

File transfer program CompleteFTP had a security flaw that allowed unauthenticated attackers to delete any files they wanted on vulnerable installations.CompleteFTP is an exclusive FTP and SFTP server for Windows that was created by EnterpriseDT of Australia and is compatible with FTPS, SFTP, and HTTPS.The HttpFile class has a vulnerability that allows for arbitrary code execution due to improper validation of a user-supplied path before using it in file operations, as discovered by security researcher rgod. “This vulnerability allows remote attackers to delete arbitrary files on affected installations of EnterpriseDT CompleteFTP server,” “An attacker can leverage this vulnerability to delete files in the context of SYSTEM.”

Cyber Attack

Delete Server Files

Information Technology

Rotary India members receive message offering data of other members, hacking plaint filed

This month, the private software company responsible for data security went to the police with a written complaint, prompting the Kasarwadavli police in Thane to file a First Information Report (FIR) on August 12.The website of the Rotary India club was hacked, and the perpetrators notified the club's members that their personal information was for sale for Rs 20,000. The complainant told the police that many influential Indians are members of Rotary India and that his company has been providing data protection services to the organization since 2014.The complainant was contacted by a club member in Gujarat who claimed he had received a hacker's email.The email was riddled with typos and read, "Data of 1,00,000 Members of Rotsry India for sale at Rs.19,999/-only."Information includes contact details for Membars, such as name, cell phone number, and email address.Business Identification Numbers : Birth Dates, Wedding Dates, Addresses, Email IDs, etc.

Offer valid for a limited time only!Some time later, a few more people got the same WhatsApp message from a couple of mysterious phone numbers.The complainant stated he attempted to contact the hacker via email and both phone numbers provided but received no response.The complainant went to the police after receiving a flurry of complaints that led him to suspect that his software had been hacked in order to leak the data.When asked for their thoughts on the situation, the Kasarwadavli police department remained silent.An individual who answered the phone number listed for Rotary India on their website said a senior member of the organization would call back, but no response had been received as of the time this story was filed.

Cyber Attack

Personal Information Exposed

Software Company

"BharatPay data breach: Personal data, transaction details of 37,000 users leaked .."

"BharatPay's backend database was leaked on a cybercrime forum on August 13, according to XVigil, the threat intelligence arm of CloudSEK. This database contained customers' personal information, bank balance, and transaction data from February 2018 through August 2022.BharatPay has over 50,000 retail locations across 11 states, as stated on the official company website.The company additionally provides prepaid cards, which can be issued to customers through the company's partner system.Transaction data and API keys of online bill payment facilitators like Pathway Recharge (for utility bill payments and DTH recharges) and Mr. Robotics were also discovered to have been leaked by researchers. Not only was customer data compromised, but so was that of SMS providers.Callback response logs, for example, may reveal sensitive information such as the phone number, transaction ID, and bank balance amount of the transacting entity."

Phishing Attack

Transaction details of 37,000 users leaked

Digital Finance Service

Business company cheated of Rs 1 crore in man-in-the-middle..

Three collaborators in a man-in-the-middle (MITM) cyber attack cheated a corporation of Rs 1 crore, according to the south region cyber police station.The main accused constructed a phony email ID similar to a reputable construction and technology company and sent an email to their client acting as the company, asking for Rs 1 crore."One day, the complaint company (client), which deals with buying scrap, received an email from the'seller company' saying it should deposit Rs 1 crore to two additional accounts that supposedly belonged to the seller company," claimed a senior executive.Since both organizations mostly communicated electronically, the buyer transferred the money.In a previous case, they transferred Rs 4 crore and bought scrap.After exchanging money, the purchase company contacted the seller company about the scrap."The seller said it didn't get paid.The buyer company was astonished to learn that the two accounts didn't belong to the sale company.ACP Ramchandra Lotlikar lead the investigation.The cyber team of SPI Devraj Borse, PSI Shweta Dhok, and PC Madhukar Lohar found that Rs 50 lakh was transferred to an individual, Bhumeshwar Sharma's bank account and other Rs 50 lakh was transferred to a company, Ashok Enerprises' account in Jaipur.Police froze Rs 39 lakh from a Jaipur company's account.

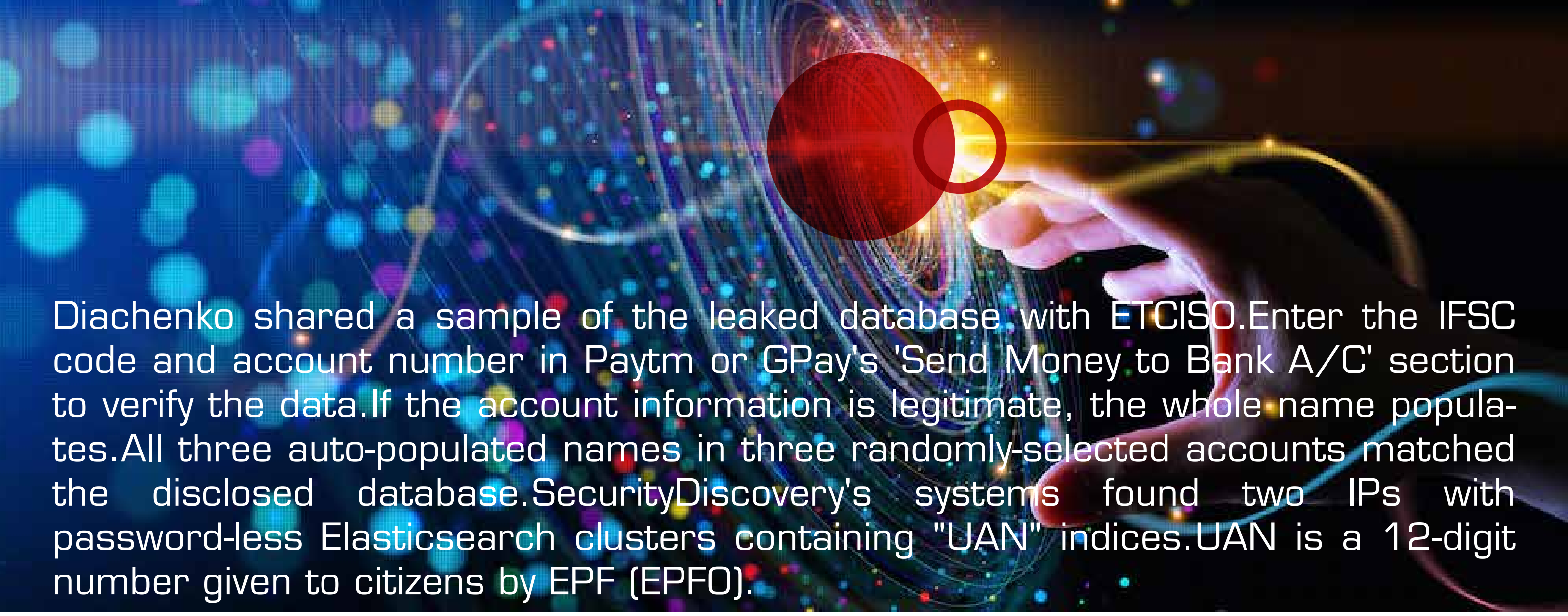
Man-In-The-Middle-Attack

Money Loss

Private Sector

Over 280M records comprising UANs, bank account numbers, incomes, and PFs leaked online

Ukrainian cybersecurity researcher and founder of SecurityDiscovery.com, Volodymyr "Bob" Diachenko, during a routine search for public exposures on the internet, found two IPs containing massive amounts of highly sensitive data belonging to Indian citizens.Volodymyr "Bob" Diachenko, founder of SecurityDiscovery.com, uncovered two IPs with sensitive Indian data during a normal scan.One IP had 280,472,941 records, the other 8,390,524.The hacked data contained names and addresses, Universal Account Numbers (UANs), bank account numbers with IFSC codes, Aadhaar card numbers, employment details, income slabs, marital status, and guardians' names and personal information.



Diachenko shared a sample of the leaked database with ETCISO.Enter the IFSC code and account number in Paytm or GPay's 'Send Money to Bank A/C' section to verify the data.If the account information is legitimate, the whole name populates.All three auto-populated names in three randomly-selected accounts matched the disclosed database.SecurityDiscovery's systems found two IPs with password-less Elasticsearch clusters containing "UAN" indices.UAN is a 12-digit number given to citizens by EPF (EPFO).

Sensitive Data Exposure

280 Million Record Data Breach

Government Sector

FasTag fraud: Victim calls fake customer care number, lakhs vanish from bank account

A Mumbai banker lost Rs 4.5 lakh after falling victim to hacking when recharging her FasTag online.Police have filed a report and are looking for the offender.The woman's brother told her to recharge her FasTag, an NHAI sticker for automated toll deduction.The victim searched online for a FasTag customer service number.Unaware, she called the number and was given help recharging her card.The fraudster provided her a recharge link to click. When the victim clicked the link, an app labeled 'Customer Support' was instantly downloaded, according to TOI. The bogus customer service rep urged her to log into mobile banking on her bank's app. She received a notification saying the FasTag recharge was successful. The victim later noticed many bank transactions. 6.99 lakh rupees were deducted. Her mobile banking had four payees.Upon realizing the fraud, the woman raced to the North Region Cyber Officers Station in the city, where police stopped Rs 2.45 lakh in transactions with the bank's cooperation.She lost 4.54 lakh rupees.People should utilize trustworthy apps and websites to recharge toll stickers instead than searching online.

Phishing Attack

MoneyTheft

Government Sector

Textile Company Sferra Discloses Data Breach

Sferra designs and sells Italian-made premium linens, including sheets, table linens, beds, and home accessories. Sferra discovered the breach on April 24, although the threat actor had access to its servers for two weeks.Names, addresses, birth dates, passport data, driver's license data, Social Security numbers, financial account information, medical and/or health insurance data, electronic/digital signatures, and account credentials were compromised.-The compromised data appears to be mostly Sferra employees'.The corporation hasn't said how many were affected.Sferra said the occurrence didn't affect its e-commerce platforms or data.Unknown if ransomware group attacked.It's unclear if this was an attack conducted by a ransomware gang. SecurityWeek has checked the leak websites of major groups, but has not found any mention of Sferra.

Sensitive Data Exposure

Personal Information Disclosure

Textile Industry

Hackers Stole Crypto from Bitcoin ATMs by Exploiting Zero-Day Vulnerability

"Bitcoin ATM manufacturer General Bytes confirmed a cyberattack exploited a flaw in its software to steal users' cryptocurrency.""The attacker was able to create an admin user remotely via CAS administrative interface via a URL call,"" the company said last week.""CAS software has had this vulnerability since 2020-12-08""It's unclear how many servers were breached or how much cryptocurrency was stolen.-CAS is a self-hosted product from General Bytes that allows companies to manage Bitcoin ATMs from a central location via a web browser.""The attacker modified two-way machines' crypto settings with his wallet settings and 'invalid payment address',"" it said.Two-way ATMs sent customers' coins to an attacker's wallet.

The attack aimed to change settings so that all funds were transferred to an adversary's digital wallet address.The company stressed that it had conducted" "multiple security audits" " since 2020 and that this shortcoming was never identified. The attack occurred three days after it announced a" "Help Ukraine" " feature on its ATMs."

Zero Day Attack

Cryptocurrency Stolen

Bitcoin Atm Manufacturere

Ransomware Gang Leaks Data Allegedly Stolen From Greek Gas Supplier

Desfa, a Depa subsidiary founded in 2007, operates Greece's natural gas transmission and distribution networks. The company announced a cyberattack that affected some systems and leaked data.Desfa deactivated IT services to contain the incident and is gradually restoring them."We've ensured and continued safe and reliable operation of the NNGS. Desfa supplies natural gas to all entry and exit points safely and adequately, the company said.Ragnar Locker's operators boasted on their Tor website about hacking Desfa and stealing sensitive data the day before.In March, the FBI warned that Ragnar Locker had compromised 52 entities across 10 critical infrastructure sectors and was changing obfuscation techniques to avoid detection and prevention.Cybercriminals previously targeted Remote Desktop Protocol (RDP) connections for intrusion and then deployed a custom virtual machine to perform malicious activities unhindered.

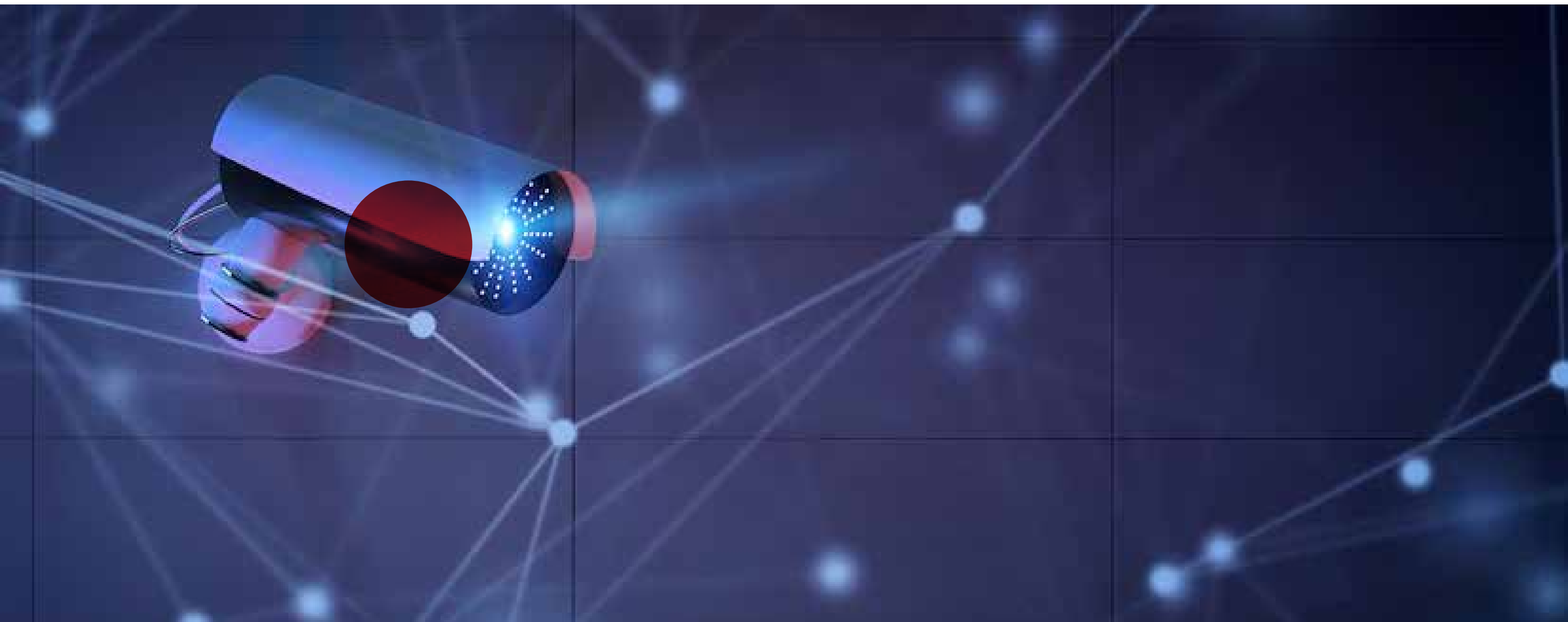
Cyber Attack

360 GB of Data Loss

Government Sector

Over 80,000 exploitable Hikvision cameras exposed online

Over 80,000 Hikvision cameras are vulnerable to a command injection flaw exploitable via specially crafted web server messages.Hikvision patched CVE-2021-36260 with firmware.TENS OF THOUSANDS OF SYSTEMS USED BY 2,300 ORGANIZATIONS IN 100 COUNTRIES HAVE NOT APPLIED THE SECURITY UPDATE, ACCORDING Russian-speaking hacking forums sell network entrance points using exploitable Hikvision cameras, CYFIRMA says.



The cybersecurity firm found 80,000 internet-facing Hikvision web servers vulnerable.Vietnam, the UK, Ukraine, Thailand, South Africa, France, the Netherlands, and Romania all have more than 2,000 vulnerable endpoints.Multiple threat actors are exploiting the flaw, so there is no clear pattern yet. CYFIRMA highlights the cases of Chinese hacking groups APT41 and APT10 and Russian cyberespionage groups."Cybercriminals from countries that don't have cordial relations with other nations could use vulnerable Hikvision camera products to launch geopolitically motivated cyber warfare," explains CYFIRMA in the whitepaper. "From an External Threat Landscape Management (ETLM) analogy, cybercriminals from countries that may not have a cordial relation with other nations could use the vulnerable Hikvision camera products to launch a geopolitically motivated cyber warfare," explains CYFIRMA in the whitepaper.

Command Injection Attack

360 GB of Data Loss

Private Sector

Microsoft Employees Exposed Own Company’s Internal Logins

Multiple people who appear to be Microsoft employees exposed sensitive login credentials to the company's infrastructure on GitHub. Microsoft confirmed the data exposure when contacted by Motherboard., according to a cybersecurity research firm that found the exposed credentials. Accidental source code and credential leakages are part of a company's attack surface, and they're becoming harder to identify.This is a very challenging issue for most companies today, Mossab Hussein, chief security officer at spiderSilk, told Motherboard in an online chat. Three of the seven login credentials were still active when spiderSilk discovered them, with one uploaded just days ago.One of the exposed and active GitHub profiles references the Azure DevOps code repository.In an apparently unrelated hack in March, attackers gained access to an Azure DevOps account and published a large amount of Microsoft source code, including for Bing and Cortana.We haven't seen any evidence that sensitive data was accessed or the credentials were misused. We'll continue to investigate and prevent accidental credential sharing.

Sensitive Data Exposure

Reputational Damage

Microsoft Company

Twilio hack exposed Signal phone numbers of 1,900 users

Twilio's data breach at the beginning of the month exposed 1,900 Signal users' phone numbers.Twilio's data breach at the beginning of the month exposed 1,900 Signal users' phone numbers.-Twilio, which provides phone number verification for Signal, was hacked last week.Hackers accessed Twilio employee accounts by sending them text messages with malicious links, exposing 125 customers' data.-The Twilio attacker could have registered 1,900 Signal users' phone numbers to another device.Signal's investigation found that the hacker's access to Twilio's customer support console revealed the SMS verification code for registering with the service.The encrypted messaging service says the attacker "explicitly searched" for three phone numbers.One user reported reregistering their account.Signal assures users that their message history is safe because there is no copy on the service's servers.Signal PIN protected contact lists and profile information during the Twilio breach.

Sensitive Data Exposure

1900 people mobile numbers exposed

Cloud Communcation Company

Over 9,000 VNC servers exposed online without a password

"At least 9,000 exposed VNC (virtual network computing) endpoints allow threat actors easy access to internal networks.

VNC (virtual network computing) is a platform-independent system that lets users monitor and adjust remote computers over a network.If these endpoints aren't properly password-protected, often due to negligence, error, or convenience, they can be used by unauthorized users, including threat actors.Cyble found over 9,000 internet-facing VNC instances with no password.China and Sweden have the most exposed VNCs, followed by the US, Spain, and Brazil.

During the investigation, researchers found multiple HMI, SCADA, and workstations connected via VNC and exposed over the internet, according to Cyble.Cyble used cyber-intelligence tools to monitor VNC's default port 5900 for attacks.the default port for VNC. Cyble found that there were over six million requests over one month. Most attempts to access VNC servers originated from the Netherlands, Russia, and the United State"

Sensitive Data Exposure

9,000 VNC servers exposed publically

Private Sector

Simple IDOR vulnerability in Reddit allowed mischief-makers to perform mod actions

A vulnerability in Reddit allowed attackers to perform moderator actions or elevate regular users to mod status without the appropriate permissions.The flaw could have allowed for all kinds of mischief, as Reddit mods are privileged to perform actions such as pin or remove posts, ban other users, and edit subreddit information.As detailed in a recent HackerOne report, a bug hunter with the handle 'high_ping_ninja' found that Reddit failed to check if the user was a moderator of a particular subreddit when they attempted to access the mod logs via GraphQL."You can change the parameter subredditName to any target subreddit name which is public or restricted and get access to mod logs of that subreddit," they explained.The insecure direct object reference (IDOR) bug was reported on August 3 and fixed on the same day."I increased severity to high based on our program policy," a member of the Reddit triage team said in the disclosure notes.The researcher was awarded a $5,000 bug bounty for the find.

Insecure Direct Object Reference

Unauthorised actions by users

Social Networking

PlatformQ Exposes Personal Info of Nearly 100,000 US Healthcare Workers

"VPNOverview discovered a data breach that could have affected 100,000 doctors, nurses, and other healthcare professionals at major U.S. hospitals.PlatformQ, a ""leading provider of digital engagement solutions"" for healthcare and education, published a database backup in a misconfigured AWS S3 bucket.Our security team believes Zarex marketing data leaked.

VPNOverview's security team found personal data in a backup database and thousands of files.Our research shows that the information relates to Zarex, a generic drug used to treat and prevent stomach ulcers.10-digit NPIs are often used on Medicare or Medicaid forms to identify medical professionals and providers.

The identifiers can also be used to search public government databases for more detailed information on medical professionals, such as mailing addresses and practice addresses.Email addresses like @gmail.com, @yahoo.com, and @verizon.com indicate they're personal.The data above identifies US hospital doctors, nurses, and other healthcare workers.255 hospitals were affected, but here are some of the major ones. "

Security Misconfiguration

Personal Information of 100,000 workers

Healthcare

Anonymous Source Leaks 4TB of Cellebrite Data After Cyberattack

An anonymous source has leaked around 4TB of proprietary data belonging to Israeli digital intelligence firm, Cellebrite. The affected products are the company's flagship product, Cellebrite Mobilogy, and the Cellebrite Team Foundation server. Cellebrite provides digital data collection, analysis, and management services. Its services are quite similar to the infamous NSO Group behind Pegasus spyware. Cellebrite's tools are used by companies, enterprises, and federal/state/local law enforcement authorities. Cellebrite Universal Forensic Extraction Device is among the key products from Cellebrite used by law enforcement agencies, and it shared its code with the impacted product Cellebrite Mobilogy. Team Foundation Server offers a platform for collaborative working and has now been replaced with Azure DevOps Server, which is used for sharing code, tracking work, and shipping software. Another attack targeted against backup files for the Cellebrite Team Foundation Server resulted in the leaking of 430 GB of data. Reportedly, around 3.6TB of data was compromised and leaked from Cellebrite Mobilogy. This product is used for device diagnostics, content backup, transfer, and restoration. The source behind this data leak is not yet identified. And no cybercriminal or hacker group has claimed its responsibility. The hacking technique is also not disclosed as yet.

Cyber Attack

4TB Data Leakage

Digital Intelligence Platform

T-Mobile store owner in the US made millions by unlocking cellphones with stolen credentials

"A former US T-Mobile store owner made $25 million by using stolen credentials to unlock ""hundreds of thousands of cellphones.""According to the US Department of Justice, Argishti Khudaverdyan, stole T-Mobile employee credentials to illegally ""unlock"" and ""unblock"" cellphones.Khudaverdyan illegally unlocked cellphones for years and made $25 million.

He and others stole more than 50 T-Mobile employee credentials across the US and unblocked hundreds of thousands of cellphones, the Justice Department said.Khudaverdyan fraudulently unlocked and unblocked T-Mobile, Sprint, AT&T, and other carriers' phones from August 2014 to June 2019.T-Mobile store owner made millions unlocking phones with stolen credentials.Khudaverdyan ran a multi-year scheme that illegally unlocked and unlocked cellphones, generating $25 million in criminal proceeds.The 6-part video series will capture Indian SaaS leaders' vision and future potential.

Removing the unlock allowed T-Mobile customers to stop using T-services, Mobile's depriving the company of revenue from service contracts and equipment instalment plans.Khudaverdyan advertised his fake unlocking services through brokers, email, and unlocks247.com.He claimed his fake T-Mobile unlocks were ""official.Khudaverdyan faces two years for aggravated identity theft and up to 165 years for wire fraud, money laundering, and unauthorised computer access. "

Credentials Theft Attack

Credentials Loss

T-Mobile Company

Thousands of Solana wallets drained in multimillion-dollar exploit

"Solana, a popular blockchain known for fast transactions, has been hacked, with funds drained from ""hot"" wallets.

Solana's Status Twitter account said an unknown actor emptied 8,000 wallets.So far, $8 million has been lost.

The attack, which only affects ""hot"" wallets that are always connected to the internet, is not limited to Solana.

Justin Barlow, a Solana Ventures investor, also lost USDC.Crypto analyst @0xfoobar confirmed that ""the attacker is stealing both native tokens (SOL) and SPL tokens (USDC) from inactive wallets""Initial reports said Solflare users were affected, but the company told TechCrunch they are not.Solana advised users to switch to hardware or ""cold"" wallets for drained wallets.Magic Eden, a non-fungible token (NFT) marketplace, asked users to revoke permissions for any suspicious links in their Phantom wallets. "

Supply Chain Attack

Private Key Compromise

Private Sector

Karakurt threatens leak of data stolen from Texas hospital

"Texas-based Methodist McKinney Hospital has been threatened by the Karakurt hacking group to have information regarding data stolen from its servers,Karakurt hackers have claimed exfiltrating 360GB of files from Methodist McKinney, as well as two of its surgical centers, including patient cards, prescription scans, invoices, accounting, contracts, and financial documents.Cybersecurity experts have praised Methodist McKinney's decision not to pay the ransom demanded by Karakurt." "I think it was absolutely the right call. Had the hospital paid, it had no guarantees that the data would have been deleted," " said Emsisoft Threat Analyst Brett Callow. However, the incident should prompt healthcare providers to strengthen their defenses, with data breaches already having impacted more than 50 hospitals across the U.S. so far this year. ""They absolutely need to do more. Most attacks like this are preventable; they occur because of security weaknesses," " said cybersecurity expert Andrew Sternke."

Security Misconfiguration

360 GB Medical Data Theft

Healthcare

More than 3200 Apps Found Exposing Twitter API Keys

"Researchers found 3,207 mobile apps exposing Twitter API keys, which can be used to take over accounts.

These apps leaked consumer keys and API keys.230 of these apps leaked all four Twitter authentication credentials.

Keys and tokens serve as usernames and passwords for apps and API users.The app can log into Twitter, create tweets, send direct messages, delete tweets, access account settings, follow other accounts, remove followers, and change the profile picture.Abusing Twitter accounts with stolen API keys is nothing new.API key rotation helps developers reduce leak risks.Hard-coded API keys can also be reviewed.Developers should never store keys in a mobile app where threat actors can find them to avoid leaks."

Account Takeover Attack

Secret Key Exposure

Social Networking

Beaware of Electricity Bill Scams! BESCOM cautions consumers

"Nowadays, consumers are receiving fraudulent messages or phone calls that claim to be from the Bangalore Electricity Supply Company Limited (BESCOM) saying that the power supply to their houses will be disconnected owing to payment failure.People who responded to their messages or calls have lost their money and later, register complaints with the cyber crime police. Following such incidents, BESCOM cautioned the consumers not to fall prey to these fraudsters.Generally, the Bengaluru electricity board notifies about power cuts in various areas on its official website—bescom.co.in. It also said that the city might witness some power outages due to some pending works in several areas of Bengaluru on Sunday and Monday,The electricity board has multiple large-scale projects that have been delayed due to the monsoon showers, which uprooted many trees and electric poles, increasing the number of tasks for BESCOM."

Social Engineering Attack

Money Theft

Government Sector

Lamoille Health Partners Experiences Ransomware Attack Leading to Data Breach Involving Patient Information

"Lamoille Health Partners reported a data breach on August 11, 2022, after a ransomware attack.Lamoille Health says the breach exposed patient names, addresses, birth dates, Social Security numbers, health insurance information, and medical treatment information.Lamoille Health Partners sent data breach letters to all affected parties after confirming the breach.An unauthorised party accessed Lamoille Health's network between June 12 and 13, 2022, according to the company's investigation.On June 24, 2022, it was determined that hackers may have accessed personal documents.

Lamoille Health Partners sent breach letters to all affected individuals on August 11, 2022.Lamoille Health Partners may have compromised Social Security numbers and PHI.PHI is any identifying information about a patient's health or how they pay for healthcare.MRI or CT scan results, insurance claims, or a patient's medical history are examples of protected health information.Healthcare-related information is only protected if it contains identifiers.An identifier is extra patient data. "

Ransomeware Attack

Data Breach

Healthcare

Newly Launched Akasa Airlines Faces Data Breach : Leaks Passenger Information Online

Akasa Air, India's newest airline that began operations less than a month ago, disclosed on Sunday that it has suffered a data breach resulting in unauthorised access to user information.Akasa Airlines apologised for the data breach and stated that the incident was self-reported to the relevant authority, the Indian Computer Emergency Response Team (CERT-In).According to the airline's records, "no hacking attempt was carried out intentionally."However, Akasa airlines has warned users to be wary of possible phishing attempts.Learn more about the airlines' response to the data breach issue by continuing to read.The official Twitter account of Aksa Airlines announced on August 28 that a significant update to its website had been made.

Regarding the data breach reported on August 25, a website update stated, "As a result, some Akasa Air registered user information, including names, gender, e-mail addresses, and phone numbers, may have been viewed by unauthorised parties."We can confirm that, aside from the above, no other travel-related information, travel records, or payment information was compromised."As soon as the data breach was discovered, Akasa Airline immediately halted the unauthorised access by shutting down all relevant system components.According to Akasa Air's Co-Founder and Chief Information Officer Anand Srinivasan, the information was shared proactively with customers who could have been affected.It was impossible to immediately determine the incident's particulars.Regarding the significance of security, Srinivasan stated that at Akasa airlines, system security and the protection of customer data are of the utmost importance.While extensive protocols are in place to prevent incidents of this nature, we have taken additional steps to ensure the security of all our systems.As additional statements continued to pour in, Akasa Airlines also asserted that system security and the protection of customer data are of the utmost importance.Additionally, the airline sincerely apologised to the passengers for any inconveniences caused by the data breach.

Sensitive Data Exposure   Data Breach   Aerospace

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