THREATSPLOIT

ADVERSARY REPORT

EDITION 54

BRISK INFOSEC

CYBER TRUST & ASSURANCE

www.briskinfosec.com

Feb 2K23

Editorial

Dear Readers:

“As we’ve come to realize, the idea that security starts and ends with the purchase of a prepackaged firewall is simply misguided.” – Art Wittmann

Though we all know that security starts not with the purchase of a prepackaged firewall, but with securing the network properly. Unfortunately, many people still believe that security begins and ends with the purchase of a prepackaged firewall. This belief is misguided.

Many people in India were upset after it was announced that a top ERP firm had leaked half a million Indian job seekers' data. Cybercriminals could now use this information to commit fraud and other crimes, and many of the people whose information was leaked were scared for their safety.

Some of the Indians who had their data exposed were angry that the ERP firm had not done more to protect it. They said that the firm should have done more to encrypt the data, and that they should have been notified about the breach sooner. Others were worried about how this incident might impact their ability to find jobs.

Regardless of the opinions of the people who were affected by the data leak, one thing was clear: this was a serious incident that could have negative impacts on many people.

The Indian railway catering and tourism Corporation (IRCTC) was hacked last week and 30 million passenger records were put up for sale on the dark web. The data breach is still ongoing and the hackers are still selling the data. The personal information of the passengers, such as their names, e-mails, and booking details, can be used by cybercriminals to engage in phishing scams, identity theft, and other forms of fraud.

The IRCTC has warned the passengers that their personal data could be stolen and put up for sale, and they urged them to be careful about clicking on links or opening attachments sent to them in emails that they don't know or trust. The IRCTC has also urged the passengers not to share their personal information online or contact the hackers for help.

This is a big issue for the IRCTC because it can have serious consequences for the affected individuals and the company itself. The personal information that was exposed can be used by cybercriminals to engage in phishing scams, identity theft, and other forms of fraud. This can lead to financial losses and other damage for the affected individuals.

The month of January is always a busy time for the news media. There are many stories to be reported, understood and digested. This year was no different.

One of the biggest stories of the month was the attack on businesses in all domains. From technology to healthcare, to finance, all sectors were hit.

While this story was happening, there were others unfolding too. Paypal got hacked. A famous french airline got breached. A famous compay's website got defaced.

While there are many more stories to be told, we hope that everyone has a happy and safe January ahead.

Contents

Top ERP Firm Exposing Half a Million Indian Job Seekers Data

"An Elasticsearch server belonging to a major international IT recruitment and software solution provider is currently exposing the personal data of more than half a million Indian candidates looking for jobs. However, the data is not limited to jobseeker as the server is also exposing the company's employees' data. Another important aspect of this data exposure is the fact that it also contains the company's client records from different companies, including Apple and Samsung. This was confirmed to Hackread.com by Anurag Sen, a prominent independent security researcher. What is worse, the server is still exposed and publicly accessible without any security authentication or password.Anurag's analysis of the server revealed that the exposed records contain personal data of over 575,000 individuals, while the size of the data is over 6.3GB and increasing with new data with each day passing. This data includes the following:email address,names,DOB etc,resume details,employee details etc."

Sensitive Data Exposure

Personal Data Breach

Information Technology

"Mailchimp says it was hacked — again"

Mailchimp claims it was hacked and revealed dozens of customers' info. The company was hacked twice in six months. Worse, this vulnerability is nearly identical to a previous event. In an unattributed blog post, the Intuit-owned firm stated its security team spotted an intruder on January 11 accessing one of its internal tools used by Mailchimp customer care and account administration. The company did not indicate how long the intruder was in its systems. Mailchimp says the hacker used social engineering to steal passwords from workers and contractors. The hacker exploited employee passwords to access 133 Mailchimp accounts, which the business notified of the breach. WooCommerce was targeted. WooCommerce informed consumers a day later that Mailchimp informed it that the breach may have revealed customers' names, store web URLs, and email addresses, but no passwords or other personal data was taken. WooCommerce uses Mailchimp to email customers. WooCommerce claims five million customers.

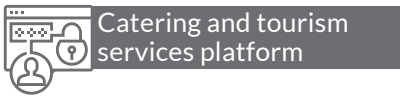
Social Engineering Attack

Data Breach

Email marketing and newsletter giant

IRCTC data breach : Names, e-mails, booking details of 30 million passengers put for sale by hackers

The Indian Railways is investigating an alleged data leak of the users of the Indian Railway Catering Tourism Corporation (IRCTC), the railways' ticketing-booking, catering and tourism services platform. "Railway Board had shared a possible data breach incident alert of CERTIn to IRCTC reporting a data breach pertaining to Indian Railways passengers. On analysis of sample data it is found that the sample data key pattern does not match with IRCTC history application programming interface (API). Suspected data breach is not from the IRCTC servers," a statement from the Railway Board said. "All IRCTC Business Partners have been asked to immediately examine whether there is any data leakage from their end and apprise the results along with corrective measures taken to IRCTC," the railway spokesperson said. It is to be noted that the ministry did not deny the report of the data leak, but said the breach did not occur at IRCTC servers. A hacker under the alias 'Shadowhacker' put up the data of 30 million IRCTC users for sale. The hacks information consists of names, email addresses, phone numbers, gender, city, states and language preference of the impacted IRCTC users. Other details include the passenger's name, phone number, train number, travel details, invoice PDF and other details required to book tickets on IRCTC.The report further said the authenticity of the hacked data seems legitimate. The sample data provided by the hacker was found to be legit when verified using PNR on IRCTC. The hacker is selling the data for USD 400, and the data and details of the vulnerability for USD 2000.



Zoho urges admins to patch severe ManageEngine bug immediately

"Business software provider Zoho has urged customers to patch a high-severity security flaw affecting multiple ManageEngine products. The bug, tracked as CVE-2022-47523, is an SQL injection vulnerability found in the company's Password Manager Pro secure vault, PAM360 privileged access management software, and Access Manager Plus privileged session management solution. Successful exploitation provides authenticated attackers with access to the backend database and allows them to execute custom queries to access database table entries. The company added that ""given the severity of this vulnerability, customers are strongly advised to upgrade to the latest build of PAM360, Password Manager Pro and Access Manager Plus immediately."

"Zoho says it fixed the issue last month by escaping special characters and adding proper validation. Zoho ManageEngine servers have been under constant targeting in recent years, with Desktop Central instances, for instance, getting hacked and access to breached organizations' networks sold on hacking forums.""The vulnerability could only be exploited by an authenticated user and the severity of the issue is 'High'. We have updated our advisory posts to reflect this information."""

SQL Injection Vulnerability

Access to Backend Database

Business software provider

HR management platform myrocket.co has exposed the personal information of hundreds of thousands of employees and millions of job candidates

Myrocket.co provides "end-to-end" recruitment and HR services for Indian organisations, and Cybernews found a publicly accessible database with 260GB of sensitive personal data. The leak affected approximately 200,000 employees and nine million job hopefuls. Researchers warn that data leaks can let threat actors launch targeted phishing attacks, fabricate identities, and deceive firms into paying. After being notified, the company addressed the misconfiguration issue. Unauthenticated databases were found. Security flaws exposed millions of confidential papers.Worryingly, threat actors could change wage amounts and bank account details. 435,000 payslips, 300 tax filings, 3,800 insurance payment papers, and 21,000 salary sheets from various HR platform users were found.

Employee names, taxpayer information, personal identification numbers, emails, phone numbers, bank details, parent names, dates of birth, salaries, payslips, employee roles, insurance and tax information, work contracts, addresses, and even photocopies of personal documents like driving licences or voter IDs were in the database. Researchers saw nine million job hopefuls' insecurely hashed emails, phone numbers, names, home addresses, andautomatically created resumes. The files contained plaintext hashed names and contact information. Researchers also uncovered 15 million job interview entries.

Security Misconfiguration

Sensitive Personal Data Leak

HR Management PLatform

Air France and KLM notify customers of account hacks

After a breach, Air France and KLM informed Flying Blue customers that their personal data was exposed. Flying Blue lets Air France, KLM, Transavia, Aircalin, Kenya Airways, and TAROM customers exchange loyalty points for rewards." Unauthorized activity on your account was detected by our security operations teams. We took immediate action to protect your data "notified customers."The attack was blocked in time and no miles were charged," KLM's official Twitter account told one affected customer. Names, emails, phone numbers, latest transactions, and Flying Blue information like miles balance may have been compromised. The breach alerts stated that customers' credit card and payment information was not compromised. Customers were also advised to change their passwords on the KLM and Air France websites after the breach locked their accounts "Air France and KLM apologise. We informed the competent authorities (Autoriteit Persoonsgegevens and Commission Nationale de l'Informatique et des Libertés) and affected customers of this event in accordance with procedures."

Cyber Attack

Personal Information Hacked

Airospace Industry

ODIN Intelligence website is defaced as hackers claim breach

On Sunday, ODIN Intelligence, a law enforcement technology company, had its website defaced. The apparent hack comes days after Wired reported that the company's SweepWizard app, which helps police manage and coordinate multi-agency raids, had a major security vulnerability that exposed police suspects' personal information and sensitive details of upcoming police operations to the public.Law enforcement agencies use SweepWizard and other ODIN apps. State and local law enforcement use its SONAR system to remotely manage registered sex offenders.The company is also controversial. Last year, ODIN was found marketing its facial recognition technology to identify homeless people in demeaning terms. The defacement's claim that "all data and backups have been shredded" suggests that the hackers attempted to erase ODIN's data. ODIN's Amazon Web Services keys were defaced. TechCrunch couldn't confirm that the keys belong to ODIN, but they match an instance on AWS' GovCloud, which stores sensitive police and law enforcement data.

Defacement Attack

Data Breach (Data and backups have been shredded)

Law Enforcement Departments

Android TV box on Amazon came pre-installed with malware

"A Canadian systems security consultant discovered that an Android TV box purchased from Amazon was pre-loaded with persistent, sophisticated malware baked into its firmware. The malware was discovered by Daniel Milisic, who created a script and instructions to help users nullify the payload and stop its communication with the C2 (command and control) server. The device in question is the T95 Android TV box with an AllWinner T616 processor, widely available through Amazon, AliExpress, and other big e-commerce platforms. It is unclear if this single device was affected or if all devices from this model or brand include the malicious component.

The T95 streaming device uses an Android 10-based ROM signed with test keys and the ADB (Android Debug Bridge) open over Ethernet and WiFi. Milisic says he initially bought this device to run the Pi-hole DNS sinkhole, which protects devices from unwanted content, advertisements, and malicious sites without installing software.While analyzing the DNS request in Pi-hole, Milisic discovered that the device was attempting to connect to several IP addresses associated with active malware. Milisic believes the malware installed on the device is a strain that resembles 'CopyCat,' a sophisticated Android malware first discovered by Check Point in 2017. This malware was previously seen in an adware campaign where it infected 14 million Android devices to make its operators over $1,500,000 in profits.However, as these devices are fairly inexpensive on Amazon, it may be wiser to discontinue using them if you can afford to do so."

Malware Attack

Devices Were Affected

E-Commerce-Platform

PayPal accounts breached in large-scale credential stuffing attack

PayPal is notifying thousands of users whose accounts were accessed by credential stuffing attacks that exposed personal data. Credential stuffing attacks use website data leaks to try username and password pairs to access an account. Credential stuffing targets password recyclers. The company detected and mitigated it and began an internal investigation to determine how the hackers got into the accounts. The company detected and mitigated it and began an internal investigation to determine how the hackers got into the accounts. The electronic payments platform claims there was no breach and no evidence that user credentials were stolen from them. PayPal reported 34,942 users affected by the data breach. Hackers had account holders' full names, birthdates, postal addresses, social security numbers, and individual tax identification numbers for two days.

PayPal accounts include transaction histories, connected credit or debit cards, and PayPal invoicing data. PayPal says it quickly blocked the intruders and reset the passwords of breached accounts.The notification also states that the attackers failed to use the breached PayPal accounts for transactions.The company strongly advises recipients to change other online account passwords to a unique and long string. A good password has at least 12 alphanumeric characters and symbols. PayPal recommends activating two-factor authentication (2FA) from the "Account Settings" menu to prevent unauthorised access even with a valid username and password.

Credential Stuffing Attack | Accounts Breached | Electronic Payment Platform

GoTo says hackers stole customers' backups and encryption key

GoTo (formerly LogMeIn) is warning customers that threat actors breached its development environment in November 2022 and stole encrypted customer data backups and an encryption key.GoTo offers cloud-based remote working, collaboration, communication, IT management, and technical support.The company reported a security breach on its development environment and LastPass' cloud storage service. The internal investigation shows that GoTo's customers were affected by the incident. A reader shared GoTo's security incident notification with BleepingComputer, stating that the attack affected Central and Pro product tier backups in a third-party cloud storage facility.

GoTo resets Central and Pro passwords for affected customers and migrates accounts to its enhanced Identity Management Platform. This platform's security controls make account takeover harder.GoTo has updated the incident to say it is contacting affected customers directly to provide more information and recommendations for account security. Customers were informed that a threat actor stole encrypted Central and Pro backups from a third-party cloud storage facility. GoTo will notify customers of any significant findings from its investigation.

Cryprographic Failure | Customers Backup Stolen | Cloud-Based Platform

A Major App Flaw Exposed the Data of Millions of Indian Students

For over a year, a security flaw in an app operated by India's Education Ministry exposed the personally identifying information of millions of students and teachers.The data was saved by the Digital Infrastructure for Knowledge Sharing app, also known as Diksha, a public education app that was launched in 2017. Diksha became a primary tool for allowing students to access materials and coursework from home during the height of the Covid-19 pandemic, when the government was forced to close schools across the country.The unsecured server's files contained the full names, phone numbers, and email addresses of over 1 million teachers. The teachers worked for hundreds of thousands of schools in every state in India, according to data in the files verified by WIRED. Another file contained data on nearly 600,000 students. While the students' email addresses and phone numbers were partially hidden, the data included their full names as well as information about where they went to school, when they enrolled in a course through the app, and how much of the course they completed.

Hosted Unsecure Server

PII of 1 Million Teacher and Students Data Breach

Education Sector

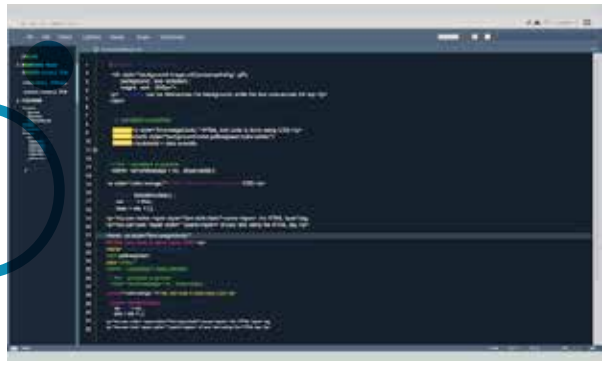
Yandex denies hack, blames source code leak on former employee

"A Yandex source code repository allegedly stolen by a former employee of the Russian technology company has been leaked as a Torrent on a popular hacking forum. The leaker posted a magnet link that they claim are 'Yandex git sources' consisting of 44.7 GB of files stolen from the company. These code repositories allegedly contain all of the company's source code besides anti-spam rules. Software engineer Arseniy Shestakov analyzed the leaked Yandex Git repository and said it contains technical data and code about the following products : Yandex search engine and indexing bot, Yandex Maps, Alice (AI assistant), Yandex Taxi, Yandex Direct (ads service), Yandex Mail, Yandex Disk (cloud storage service),Yandex Market, Yandex Travel (travel booking platform),Yandex360 (workspaces service),Yandex Cloud, Yandex Pay (payment processing service),Yandex Metrika (internet analytics), Shestakov also shared a directory listing of the leaked files on GitHub for those who want to see what source code was stolen. There are at least some API keys, but they are likely only been used for testing deployment only,"" said Shestakov about the leaked data."

Sensitive Data Exposure

Source Code

Multinational technology company



Ransomware gang steals data from KFC, Taco Bell, and Pizza Hut brand owner

Yum! Brands, the owner of Pizza Hut and KFC, has confirmed that data was stolen during a recent ransomware attack. The company has not disclosed the extent of the data breach or the type of information that was taken. Personal information of some customers may have been compromised. The company is working with law enforcement and cybersecurity experts to investigate the incident. It is recommended for affected customers to monitor their financial statements for any suspicious activity. The impacted restaurants in the United Kingdom have returned to"Although data was taken from the company's network and an investigation is ongoing, at this stage, there is no evidence that customer databases were stolen," reads the Yum! Brands announcement. In an 8-K form filed with the Securities and Exchange Commission (SEC), Yum! Brands assured investors the ransomware attack would cause no notable negative financial impact.

"While this incident caused temporary disruption, the company is aware of no other restaurant disruptions and does not expect this event to have a material adverse impact on its business, operations or financial results," mentions the firm's SEC report. normal operations and are not expected to face any other problems relevant to the cyberattack.

Ransomeware Attack

Data Stolen

Fast food restaurant chain Industry

Riot Games Says Source Code Stolen in Ransomware Attack

Riot Games, the developer of the popular video game "League of Legends," has reported a ransomware attack where their source code was stolen. They have not confirmed if they paid the ransom or if the stolen code has been leaked. Riot is working with law enforcement and cybersecurity firms to investigate the breach and prevent further incidents. The company has advised its users to be cautious of any suspicious activity and not to click on unknown links. The game developer also revealed that it received a ransom demand, but noted that it has no intention to pay the attackers. The company has promised to publish a detailed report of the incident.According to Motherboard, the attackers wrote in the ransom note that they were able to steal the anti-cheat source code and game code for League of Legends and for the usermode anti-cheat Packman. The attackers are demanding $10 million in return for not sharing the code publicly.

Ransomeware Attack

Source Code Stolen

Gaming Industry

JD Sports says hackers stole data of 10 million customers

JD Sports, a UK-based sportswear retailer, JD Sports says it detected the unauthorized access immediately and responded quickly to secure the breached server, preventing subsequent access attempts. It has confirmed that data of 10 million customers was stolen in a cyber attack. The stolen information includes names, addresses, and email addresses, but not payment information. The company is working with law enforcement and cybersecurity experts to investigate JD Sports says it does not store full payment card details for online orders, so complete financial information cannot have been compromised. The same applies to account passwords, which the firm says it has no reason to believe were accessed. the incident and has advised customers to be vigilant against potential fraud. JD Sports has also stated that they will be offering identity protection services to affected customers.

Cyber Attack

10 Million CX Data Stolen

Sportswear Retailer

Ukraine links data-wiping attack on news agency to Russian hackers

A malicious software attack against Ukraine's national news agency (Ukrinform) has been connected to Sandworm Russian military hackers by the country's computer emergency response team (CERT-UA). Athough the threat was quickly contained, according to the Ukrainian State Service for Special Communications and Information Protection (SSSCIP)."Ukrinform was able to keep running as a result. In the present, CERT-UA experts are supporting infrastructure recovery efforts and carrying out the event investigation." CERT-U says the cyberattack was likely carried out by the Sandworm group based on the threat actors' tactics, which was previously linked to the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU). The attackers launched the CaddyWiper malware on the news agency's systems using a Windows group policy (GPO), showing that they had breached the target's network beforehand. Still, they failed to impact the news agency's operations."Russians have been trying to cut off Ukrainians from the information on the current situation and the course of the war since the early days of the full-scale invasion."They have shut off Ukrainian TV, the Internet and mobile communication in the territories, temporarily controlled by the enemy, and they have been striking TV and radio transmitting towers in multiple cities of Ukraine with their missiles. They have waged cyberattacks on Ukrainian media."

Data-Wiping Attack

Ukrainian TV, the Internet and mobile communication was shut down

Government Sector

Latvia confirms phishing attack on Ministry of Defense, linking it to Russian hacking group

The Russian cyber-espionage group known as Gamaredon may have been behind a phishing attack on Latvia's Ministry of Defense last week, Hackers sent malicious emails to several employees of the ministry, pretending to be Ukrainian government officials. The attempted cyberattack was unsuccessful, the ministry added. The company obtained it from VirusTotal, a Google-owned service that analyzes suspicious files, where one of the targeted users may have downloaded it to verify its sender, according to Sekoia threat intelligence researcher Felix Aime.Researchers attributed this phishing campaign to Gamaredon because the hackers used the same domain (admou[.]org) as previous cyberattacks, Aime said. According to the Latvian computer emergency response team, CERT-LV, the attack was "unusual" because the Russian hackers communicated with researchers in the final stages of the attack when they learned they were being investigated. Ukrainian cybersecurity officials described Gamaredon's attacks as intrusive and audacious, and said the group's main purpose was "to conduct targeted cyberintelligence operations."

Phishing Attack

Cyber Intelligence Operations

Government Sector

Ransomware attack on Indianapolis Housing Agency leaks sensitive info on 200,000 residents

The Indianapolis Housing Agency is notifying more than 200,000 people that their information, including Social Security numbers and more, was leaked during a ransomware attack. The federally-funded agency is responsible for providing housing to low-income tenants across Indianapolis. It did not respond to requests for comment in October when the attack was revealed but reported the incident to the Maine Attorney General's office last week, explaining that 212,910 people were affected. The agency submitted two separate versions of the breach notification letter – one for adults affected and one for children who had information leaked in the incident. Victims are being provided with 12 months of IDX identity protection services that includes identity theft recovery services and a $1,000,000 insurance reimbursement policy. The agency said IDX "will help resolve issues if your child's identity is compromised."The newspaper noted that in total, about 25,000 people rely on the agency for a variety of services and it also runs several public housing buildings. mployees of the agency were forced to send checks out manually and were locked out of email systems for days.

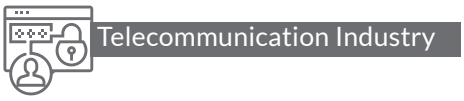
Ransomeware Attack

Sensitive Data Exposed

Housing Agency

Charter Communications says vendor breach exposed some customer data

Telecommunications company Charter Communications said one of its third-party vendors suffered from a security breach after data from the company showed up on a hacking forum. A forum user posted information allegedly stolen from the company that included names, account numbers, addresses and more for about 550,000 customers. “We are aware of the post and following our security protocol in response. The initial evidence suggests that one of our third-party vendors had a security breach,” a spokesperson said. “At this time, we do not believe that any customer proprietary network information or customer financial data was included.”The spokesperson did not respond to follow-up questions about what third-party vendor was hacked, when the hack occurred or when affected customers will be notified. Charter Communications is the second largest cable operator in the U.S. and fifth largest telephone provider – with more than 32 million customers in 41 states. n a 40-page proposal document, the FCC explained that there have been multiple breaches affecting the country’s largest telecommunications companies : Verizon, T-Mobile and AT&T.“The law requires carriers to protect sensitive consumer information but, given the increase in frequency, sophistication, and scale of data leaks, we must update our rules to protect consumers and strengthen reporting requirements,” Rosenworcel said.



Cyberattack confirmed as cause for phone and IT problems at British music school

A school in Guildford, southwest of London, has confirmed that a cyberattack is responsible for knocking out its phone lines and impacting the school’s IT systems. Guildford County School, a specialist music academy with over 1,000 students, first announced IT issues on Twitter on January 19. At the time its headteacher Steve Smith said the incident would “not impact upon learning.”n a statement sent to Surrey Live on Thursday, the school’s parent organization Learning Partners Academy Trust — comprising 12 state schools — confirmed that a cyberattack was responsible for the outages.

“Guildford County School detected a cyber-intrusion into its network on January 19 which affected the school IT systems, The school remains open to all students and the delivery of lessons continues, drawing upon the significant skill and experience of all staff members,” the spokesperson said. It comes amid a spate of ransomware attacks on education establishments in Britain — many conducted by the Vice Society ransomware group to extort victims by stealing sensitive data and threatening to release it unless a ransom is paid.

According to the Guildford County School spokesperson, there is “a robust backup regime in place, [and the school] is being supported by a professional team and has taken immediate remedial action to limit data loss.”

Cyber Attack | IT System Impacted | Educational Sector (Music School/Academy)

Los Angeles Unified School District confirms SSNs leaked in September ransomware attack

"The Los Angeles Unified School District (LAUSD) sent out breach notification letters to an unknown number of contractors in recent days notifying them that sensitive information – including Social Security numbers – was leaked during a wide-ranging cyberattack last year. Those affected include current and former contractors and subcontractors who had provided the district with personal information in connection with Facilities Services Division projects. The ransomware attack on LAUSD drew national headlines and widespread attention from the White House, FBI and Cybersecurity and Infrastructure Security Agency after it was revealed on the morning of September 6 – right as the school year was beginning. The ransomware attack on LAUSD drew national headlines and widespread attention from the White House, FBI and Cybersecurity and Infrastructure Security Agency after it was revealed on the morning of September 6 – right as the school year was beginning.

LAUSD is the second-largest school district in the country and last year served an estimated 574,570 students across early education, elementary, secondary, and adult education classes, according to the district’s data. It operates more than 1,400 schools and educational centers, while employing more than 73,000 people. The hackers claimed they stole 500 GB of data, sharing several samples of W-9 forms and contracts from the leak. Researchers said the data included SSNs, contracts, invoices, passports and more. Since the attack on LAUSD, hackers using the Vice Society ransomware have targeted dozens of colleges, universities and grade schools across the world, ranging from Elmbrook School District in Wisconsin to Cincinnati State College, Linn-Mar School District in Iowa, and Grand Valley State University in Michigan."

Ransomeware Attack | Sensitive Information Leakage | Education Sector

CORPORATE OFFICE

Briskinfosec Technology and Consulting Pvt ltd,
No : 21, 2nd Floor, Krishnama Road,
Nungambakkam, Chennai - 600034, India.
+91 86086 34123 | 044 4352 4537

contact@briskinfosec.com | www.briskinfosec.com