Threatsploit Adversary Report

Dec - 2022

Edition 52

www.briskinfosec.com

Editorial

75 million investor Demat accounts are managed by Mumbai-based CDSL. After NDSL, CDSL is India's second-largest depository. And, what if this repository stands hacked?

There are limitless possibilities for what a hacker can do with such data. The point is why wait till this happens? Why, not take massive action? And, for that, you must be aware of what happened last month in the world of Cybersecurity.

Trains are usually run by the loco pilot or the driver. And, how can these get affected by hackers? Well, that is a thing of the past. In Denmark, Cyberattacks delayed trains. The event reveals how an attack on a third-party IT service provider can cause physical interruption. Many other nations have similar incidents.

After the physical infrastructure, now it's time for cloud attacks. Dropbox is a well-known name with 700 million users. Hackers grabbed 130 code repositories using employee phishing credentials. Phishing attacks can bypass any security measure.

Since June 2021, the FBI claims the Hive ransomware gang has extorted $100 million from 1,000 companies. FBI said Hive organization will distribute new ransomware payloads on networks of non-paying victims. Most companies will try to clean their systems & get going. But the new payload worsens this further.

Ransomware groups have strategies such as attacks on the non-paying victim. You cannot ignore them anymore; you need to pay. These incidents are moving towards a more organized, strategized, and well-planned system.

One more ransomware, Drinik impersonates the Income Tax Department of India to steal income tax credentials from 18 Indian banks. It tricks victims into giving their entire name, Aadhar number, PAN number, and financial information to receive a quick tax refund. Ransomware is plaguing developed and developing nations. From government to private, all are on their radar.

Malware infiltrated India's largest securities depository, CDSL. The securities depository reported malware on "a couple of its internal machines." This is a shocking case, as so much financial data is available on these systems. Close to 75 million users' data is at stake.

On the whole, ransomware, and malware have peaked. Attacks are getting much more organized & sophisticated. Phishing & social engineering remains the biggest hook to get victims.

We wish you a safe & secure month. We are sure you do not want to miss any of these incidents. As these make you ready for any untoward incident.

Happy Reading!

Contents

AIIMS Delhi services hit due to ransomware attack on server

The server for National Informatics Centre's Hospital being used at AIIMS, New Delhi was down due to which outpatient and inpatient digital hospital services including, smart lab, billing, report generation, appointment system etc, have been affected," the institute said on Wednesday. "All these services are running on manual mode currently." The institute has sought support from the Indian Computer Emergency Response Team, or CERT-IN, to restore digital services. CERT-IN is the nodal agency within the Union Ministry of Electronics and Information Technology that deals with cyber security threats. In October, AIIMS Delhi announced that its operations will be paperless from January 1, 2023. TSeveral hospital staff tweeted after the server stopped working and patients were standing in queues and complaining about the delay. Some of them tweeted that they were not able to generate barcode to send samples, and were not able to see imaging reports. A hospital staff claimed that the work which was just a click away took more time as everything was being done manually. "All basic details of the patients are being written manually. In fact reports and being sent manually, which takes a lot of time," said a hospital staff, adding that it was a chaos in the institute on Wednesday. he head of the institute, M Srinivas, had issued an office memorandum in this regard to all heads of departments, chiefs of centres and nodal officers in this regard. On November 18, the institute had also said that all payments would go completely digital from April 1, 2023.

Ransomeware Attack

Server Hit

Healthcare

Cyberattack Causes Trains to Stop in Denmarkv

Trains stopped in Denmark on Saturday as a result of a cyberattack. The incident shows how an attack on a third-party IT service provider could result in significant disruption in the physical world. According to Danish broadcaster DR, all DSB trains stopped Saturday morning and couldn't move for several hours. This may sound like the work of a sophisticated threat actor targeting operational technology (OT) systems, but it was actually a security incident at Supeo, a Danish company that provides enterprise asset management solutions to railway companies, transportation infrastructure operators, and public passenger authorities. Supeo may have been hacked. A DSB representative told Reuters it was a "economic crime" without providing details. Supeo shut down its systems after a hacking attack, disrupting trains. This broke train driver software. Train drivers use Supeo's smartphone app to access operational information including speed limits and railroad operations.

When the subcontractor shut down its servers, the application stopped working and train drivers had to stop. Recent targets include Belarus, Italy, the UK, Israel, and Iran. Modern train systems are vulnerable to hackers, but these recent hacks targeted websites, ticketing, and other IT systems. The Transportation Security Administration (TSA) recently issued a mandate to improve railroad cybersecurity.

Cyber Attack

Train Stoppage

Transportation (Train) Domain

Dropbox discloses breach after hacker stole 130 GitHub repositories

"Dropbox announced a security issue after threat actors stole 130 code repositories using employee phishingcredentials."

"The code and data included a few thousand Dropbox employees, current and past customers, sales leads, and vendors (Dropbox has more than 700 million registered users)." "The successful breach was the result of a phishing assault on many Dropbox workers utilising emails imitating the CircleCI continuous integration and delivery platform and referring them to a phishing landing page asking for their GitHub account and password. Employees were requested to " "use their hardware authentication key to pass an OTP" " on the same phishing page.After gaining Dropbox credentials, attackers accessed one of its GitHub groups and stole 130 code repositories." "These repositories featured Dropbox-modified third-party libraries, prototypes, and security tools and configuration files," " the company said.Dropbox said attackers never accessed customer accounts, passwords, or payment information, and its key products and infrastructure were not compromised. "

Phishing Attack

130 GB github repositories stolen

File Hosting Service

Hackers steal $300,000 in DraftKings credential stuffing attack

DraftKings will reimburse clients who lost up to $200,000 in a credential stuffing hack.All stolen accounts seem to have had an initial $5 deposit, followed by attackers changing the password, enabling 2FA on a different phone number, then withdrawing as much as possible from related bank accounts. Some victims complained on social media that they couldn't reach anyone at DraftKings while attackers drained their bank accounts." We think that these consumers' login information was hacked on other websites and subsequently utilised to access their DraftKings accounts," said DraftKings President and Cofounder Paul Liberman 12 hours later." We have no proof that DraftKings' systems were compromised. We've discovered less than $300,000 in affected client funds and will reimburse them." DraftKings urged consumers not to use the same password for several online services and not to share their credentials with third-party sites like betting trackers and betting apps. DraftKings customers who haven't been touched by this credential-stuffing scam should turn on 2FA and erase any banking details to block fraudulent withdrawal requests. The attackers will also utilise the stolen information in future identity theft operations to make illicit purchases or transfer money from associated bank accounts to accounts under their control.

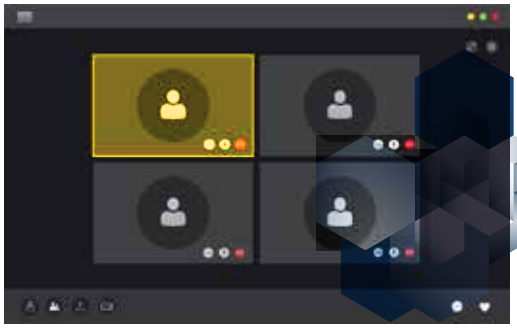
Credential Stuffing Attack

$300000 Stolen

Sports Betting Company

Attackers bypass Coinbase and MetaMask 2FA via TeamViewer, fake support chat

"A phishing campaign is stealing cryptocurrency from Coinbase, MetaMask, Crypto.com, and KuCoin by bypassing multi-factor authentication. Threat actors utilise Microsoft Azure Web Apps to host phishing sites and entice victims to them with fake transaction confirmation requests or suspicious activity alerts. When targets visit the phishing site, a scammer controls a 'customer support' chat window and guides them through a multi-step scamming procedure. The attackers attempt the entered credentials on the legitimate website, which sends a 2FA code to the victim, who inputs it on the phishing site.- Threat actors try to utilise the 2FA code to log into the victim's account before the timer expires. MetaMask phishing targets recovery phrases, not credentials or 2FA codes. Whether a 2FA code works or not, scammers start on-screen chat help, say researchers. Displaying a bogus error message that the account has been suspended due to suspicious behaviour prompts the visitor to contact support. In this support chat, threat actors keep the victim around in case they require different credentials, recovery phrases, or 2FA codes. For successfully breached accounts, the victim may still need to confirm fund transfers while fraudsters empty their wallets.



For accounts they can't hack through support chat, threat actors use a different approach to authenticate their device for the cryptocurrency platform. "

Phishing Attack | Account Breach | Cryptocurrency Platform

Ducktail hackers now use WhatsApp to phish for Facebook Ad accounts

"Ducktail has stolen $600,000 in advertising credits from Facebook Business accounts.The gang has used malware to acquire Facebook-related information and hijack company accounts to run victim-paid adverts. Ducktail, believed to be the product of a Vietnam-based threat actor, was first detected this year targeting Facebook business account users with high-level access.

The threat actor would transmit info-stealing malware through LinkedIn, tricking the target into launching a malicious file with a name associated to brands, products, and product planning. The threat actor contacted some of its newest victims using WhatsApp to trick them into accepting and executing malicious payloads that steal critical information or give the attacker access to a Facebook business account." "The spyware can steal the victim's Facebook Business account.It tries to give the threat actor's emails high-level business access " "Ducktail targets administrators and finance editors since they control settings, permissions, tools, and financial facts (business credit card info, transactions, invoices, and account payment methods). Ducktail malware can steal Facebook session cookies from Google Chrome, Microsoft Edge, Brave, and Firefox.

Using the session cookie, it interacts with multiple Facebook endpoints from the victim's machine and collects information (access tokens, two-factor authentication codes, user agents, IP address, geolocation) that allows the threat actor to impersonate the victim from other systems. "

Malware Attack | $600,000 Loss | Social Media Platform

Pro-Russian hacktivists take down EU Parliament site in DDoS attack

The website of the European Parliament has been taken down following a DDoS (Distributed Denial of Service) attack claimed by Anonymous Russia, part of the pro-Russian hacktivist group Killnet. European Parliament President confirmed the incident saying that the Parliament's "IT experts are pushing back against it & protecting our systems." The Director General for Communication and Spokesperson of the European Parliament, Jaume Dauch, also stated after the website went down that the outage was caused by an ongoing DDoS attack.Pro-Kremlin hacktivist groups have targeted European and U.S. websites since Russia invaded Ukraine. For instance, Killnet recently claimed large-scale distributed denial-of-service (DDoS) attacks targeting the websites of several major U.S. airports last month. Notable examples of airport websites taken down following their attack include the Los Angeles International Airport (LAX), which was intermittently offline, and the Hartsfield-Jackson Atlanta International Airport (ATL), a large U.S. air traffic hub. One week before, they attacked multiple U.S. government websites in Colorado, Kentucky, and Mississippi, with moderate success, managing to knock some of them offline for a short time. Killnet also claimed to have taken down CISA's Protected Critical Infrastructure Information Management System website after its attacks on the U.S. Treasury in early October were thwarted before having a real effect on the agency's infrastructure. Earlier this month, the FBI said that DDoS attacks coordinated by pro-Russian hacktivists have a minor impact on their targets because they're attacking public-facing infrastructure like websites instead of the actual services, leading to limited disruption.

Russian cybergangs stole over 50 million passwords this year

"At least 34 Russian-speaking cybercrime gangs have obtained 50,350,000 account passwords from over 896,000 infections.

Most victims are in the U.S., Germany, India, Brazil, and Indonesia, but 111 nations were targeted, according to Group-IB.

In 2022, information-stealing malware reached historic levels, involving low-skilled hackers looking to make a profit.

Group-IB alleges low-level scammers supporting info-stealer deployment are ""victim callers"" in ""Classiscam"" phishing campaigns.""The flood of workers into the popular scam Classiscam, which at its peak included over a thousand criminal groups and hundreds of thousands of bogus websites, has led to criminals battling for resources and looking for new ways to earn profits,"" says Group-IB. There are 34 active cybercrime gangs on Telegram, each with 200 members23 groups use Redline, 8 use Raccoon, and 3 use unique malware.SEKOIA also warned this week that another info-stealer termed 'Aurora' has been accepted by seven key threat organisations. Telegram helps cybergangs organise campaigns and maintain a working structure for data-stealing.

Private Telegram channels offer operators support and technical guidance, can serve as data exfiltration points, hold critical announcements, and operate as bug-reporting portals. They also have bots that can manufacture custom malware 24/7 for clients.

The organisations still follow hierarchical regulations, with ""administrators"" selling info-stealing software to ""employees"" for a few hundred dollars per month. Workers drive traffic to malware-dropping sites utilising YouTube videos, BlackSEO, SEO poisoning, laced torrent files, and fraudulent social media posts. Users can limit info-stealer infection by avoiding sketchy downloads, scanning downloaded executables with antivirus software, and keeping their system updated. "

Cyber Attacks

50,350,000 Account Passwords Stolen

Information Technology

Backdoored Chrome extension installed by 200,000 Roblox players

More than 200,000 users of the Chrome browser extension 'SearchBlox' installed a backdoor that can steal Roblox credentials and Rolimons assets. There are two 'SearchBlox' results on Chrome. These extensions claim to "search Roblox servers for a player... blazingly fast," yet both contain a backdoor. Roblox community users suspected SearchBlox included malware early Wednesday. Unofficial Roblox news and community account RTC tweeted, "SearchBlox has been compromised / backdoored. If you have it, your account may be at risk." "Change your passwords and credentials to secure your account."For the first extension (blddohgncmehcepnokognejaaahehncd) downloaded by almost 200,000 users, the backdoor is on line 3 of the 'content.js' file : As if the URL structure 'image.png/image.txt' itself wasn't already interesting, the page contains HTML code that pretends to display an image using the '<img>' tag, but instead loads obfuscated JavaScript that is further encoded as HTML character entities (using the '&' and '#' symbols):The code when decoded yields obfuscated code which further appears to be exfiltrating Roblox credentials to another domain: releasethen.site. The code also appears to survey a player's profile on Rolimons.com, a Roblox trading platform. This detail becomes relevant given today's account suspensions on the platform, as explained in the following section.

Malware Attack

Webstore Compromised

Trading Platform

Android file manager apps infect thousands with Sharkbot malware

Malicious Android apps serving as file managers infected users with the Sharkbot financial trojan.The apps fetch the malicious payload from a remote location after installation to avoid detection on Google Play.As file managers, trojan programmes are less likely to arouse suspicions when asking Sharkbot malware access. Sharkbot steals online bank accounts by showing fraudulent login forms in banking apps.When a user tries to log in to their bank using one of these bogus forms, the credentials are taken. Malware appears on the Play Store under many guises or in trojan apps. Bitdefender revealed new Android malware apps posing as file managers to Google.They're all gone from Google Play. The malicious app demands dangerous rights like reading/writing external storage, installing new packages, accessing account details, removing packages (to remove traces), etc.

In file management apps, these rights are typical and anticipated, thus users are less inclined to be cautious. As threat actors spread these apps straight from Google Play, maintain Play Protect activated to remove harmful apps as they are found.

Malware Attack

Fake File Manager

Android Platform

Chinese hackers use Google Drive to drop malware on govt networks

State-backed Chinese hackers launched a spearphishing campaign to deliver custom malware stored in Google Drive to government, research, and academic organizations worldwide. According to Trend Micro researchers, the threat group targeted mostly organizations in Australia, Japan, Taiwan, Myanmar, and the Philippines. The Chinese hackers used Google accounts to send their targets email messages with lures that tricked them into downloading custom malware from Google Drive links. In a report today, Trend Micro researchers say that the hackers used messages with geopolitical subjects and that most of them (84%) targeted government/legal organizations. To bypass security mechanisms, the embedded link points to a Google Drive or Dropbox folder, both legitimate platforms with good reputation that are typically less suspicious. These links lead to downloading compressed files (RAR, ZIP, JAR) with custom malware strains such as ToneShell, ToneIns, and PubLoad. Although the hackers used various malware loading routines, the process typically involved DLL side-loading after the victim launched an executable present in the archives. A decoy document is displayed in the foreground to minimize suspicions.

Spearphishing Attack

Google Drive Affected

Government Sector

Hive ransomware extorted $100M from over 1,300 victims

The FBI says the Hive ransomware gang has extorted $100 million from over 1,000 firms since June 2021. FBI said Hive group will release new ransomware payloads on networks of non-paying victims. "As of November 2022, Hive ransomware criminals have attacked over 1,300 firms globally," the FBI said.Hive actors have reinfected victim organisations that repaired their network without paying a ransom. The list of victims includes firms from a wide range of industries and critical infrastructure sectors, such as government facilities, communications, and IT, with a focus on HPH entities. Today's warning shares IOCs and TTPs uncovered by the FBI while investigating Hive ransomware outbreaks. While the three government agencies supporting the alert do not recommend paying the ransoms, victims are asked to report Hive assaults to their local FBI field office or to CISA at report@cisa.gov regardless of whether they pay the ransom. This will assist law enforcement track ransomware activity, prevent attacks, or punish offenders accountable. We found indications that HIVE used Conti's initial assault accesses and pen-testers.

Hive Ransomeware Attack

Extorted $100 Million

Information Technology

Updated RapperBot malware targets game servers in DDoS attacks

"Mirai-based botnet 'RapperBot' has re-emerged via a new effort that infects IoT devices for DDoS assaults against game servers. Fortinet researchers detected the malware last August when it propagated through SSH brute-force. The newest variant employs Telnet self-propagation, like the original Mirai infection. The current campaign's motivation is clearer because the latest DoS instructions target online game servers. The virus now brute-forces devices using a hardcoded list of weak credentials, whereas before it got a list from the C2. This allows less sophisticated IoT malware to avoid testing all credentials.

To optimise brute forcing, the malware compares the server prompt upon connection to a hardcoded list of strings to identify the possible device and then only tries the known credentials for that device. RapperBot's prior DoS capabilities were so generic that researchers suspected its owners were interested in early access. Using HTTP DoS, the malware seems to target game servers."

DDOS Attack

IOT Devices Infected

Server Attack

Whoosh confirms data breach after hackers sell 7.2M user records

Whoosh, a Russian scooter-sharing business, confirmed a data breach after hackers sold 7.2 million client records on a hacking site. Whoosh operates approximately 75,000 scooters in 40 Russian cities. On Friday, a threat actor began selling the stolen data on a hacking forum. It allegedly contains free promotion codes and partial user ID and payment card data. The corporation revealed the cyberattack in Russian media earlier this month but said its IT experts thwarted it. Whoosh confirms a data leak in a statement to RIA Novosti and says it is working with law enforcement to stop the leak.

A Whoosh spokeswoman said the disclosure didn't affect account access, transaction information, or trip details. "Our security procedures prevent third parties from accessing cardholder data." Auser posted a database containing 7.2 millionWhoosh customers' email addresses, phone numbers, and first names. The database had partial payment card details for 1,900,000 users. The merchant said the stolen data included 3,000,000 promo codes for free Whoosh scooter rentals. According to the SatoshiDisk platform used for the transaction, no one has yet purchased the database.

Cyber Attack

7.2 Million Users Data Breach

Mobility Service Platform

India’s securities depository CDSL says malware compromised its network

CDSL, India's largest securities depository, says malware infected its systems. The securities depository reported malware on "a couple of its internal machines" As a precaution, the company withdrew itself from the capital market, the document said. CSDL says it's still investigating and has "no reason to suspect confidential information or investor data was compromised" CDSL hasn't released malware specifics. The company's website was down when written. The corporation wouldn't disclose if they're connected. Banali Banerjee, an agency official, said CDSL declined to address other queries, including if it retains logs that would show what data was exfiltrated from its network.

The spokeswoman said, "We're seeking resolutions." Banali Banerjee, an agency official, said CDSL declined to address other queries, including if it retains logs that would show what data was exfiltrated from its network. The spokeswoman said, "We're seeking resolutions." Mumbai-based CDSL claims to maintain and serve 75 million investor trading accounts, dubbed demat accounts.BSE, Standard Chartered Bank, and Life Insurance Corporation are major stockholders. CDSL was founded in 1999 and is India's second-largest depository after NDSL, the oldest.CDSL permits keeping securities electronically and streamlines stock exchange deal settlements. The corporation reported the event to authorities and is working with cyber security advisers to examine the impact.

Interpol Seized $130 Million from Cybercriminals in Global "HAECHI-III" Crackdown Operation

"In a global crackdown on cyber-enabled financial crimes and money laundering, Interpol seized $130 million in virtual assets Thursday. HAECHI-III, an international police operation, arrested 975 people and closed over 1,600 cases between June 28 and November 23, 2022. Two South Korean fugitives were accused of embezzling €28 million from 2,000 victims in a Ponzi scam.

A call centre scam in India impersonated Interpol and Europol personnel to defraud Austrian victims. New Delhi and Noida hosted call centres. Illegal activities notified victims that their ""identities were stolen and narcotics crimes were committed in their names,"" pushing them to send money. The victims had to transfer their assets/money to a trust account via bank transfers, crypto wallets, gift card numbers, or voucher codes to clear their names ""the Indian CBI revealed last month. The investigation targeted voice phishing, romance scams, sextortion, investment fraud, and unlawful online gambling-related money laundering, according to law enforcement. Authorities found romance frauds, sextortion, and encrypted chat apps pushing fake crypto wallet schemes. Operation HAECHI-III comes exactly a year after Interpol announced the arrests of over 1,000 cybercriminals and the recovery of $27 million in HAECHI-II. "

Hackers Target Indian Military with Spyware Loaded in Dating and Communication Apps

"Spyware targeting Indian military personnel is active. The spyware campaign has been active since January and found in dating and instant messaging apps. Cyble and 360 Core Security Lab have recently spotted the PJobRAT spyware and reported that the spyware samples are disguised as Android dating apps.Researchers found that this variation is masquerading as Trendbanter, a dating app for non-resident Indians, and Signal. The attackers spread numerous spyware using third-party app shops, fraudulent URLs, and SMS. It mimics WhatsApp or other legal apps to hide in the app list. It doesn't even match the app store icon. The experts that noticed the newest operation did not link it to any of the hacker groups now.However, the exact nature of the targets suggest at China- or Pakistan-based actors.PJobRAT steals.pdf,.doc,.docx,.xls,.xlsx,.ppt, and.pptx files.

It uploads SMS, music, video, image, and address books.Additionally, it uploads a list of installed programmes, WiFi/GPS information, geographic location, external storage files, phone number, WhatsApp contacts/messages, and recording via the mic or camera. Recent studies indicate that this spyware's perpetrators are not skilled because their private servers keeping exfiltrated data are publicly accessible. It remains active and dangerous to naive users. "

Malware Attack

Servers are Affected

Indian Military Sector

5.4 million Twitter users' stolen data leaked online - more shared privately

A hacker forum shared over 5.4 million Twitter user records with non-public information acquired using an API vulnerability resolved in January. Another enormous, potentially more significant data dump of millions of Twitter records was disclosed by a security researcher, showing how widely threat actors misused this problem. Scraped public data and private phone numbers and email addresses make up the data.Last July, a threat actor sold the private data of approximately 5.4 million Twitter users on a hacking community for $30,000. Most of the data was public, such as Twitter IDs, names, login names, localities, and verified status, but it also included sensitive information like phone numbers and email addresses. Threat actors might then scrape public information about the account to establish a user record with both private and public information using this ID. The 5.4 million data for sale included 1.4 million Twitter profiles for suspended users obtained via a different API, bringing the total to over 7 million Twitter profiles with private information.

Pompompurin stated that this second data dump was not sold and simply shared with a few persons. These records include a private email address or phone number and public scraped data, such as the account's Twitter ID, name, screen name, verified status, location, URL, description, follower count, account creation date, friends count, likes count, statuses count, and profile image URLs.

Cyber Attack

Data Breach

Social Media Platform (Twitter)

Drinik Malware Now Targets 18 Indian Banks

"A new upgraded variant of Drinik Android trojan is targeting 18 Indian banks and stealing personal and bank account information from the victims. Drinik is impersonating the Income Tax Department of India and targeting potential victims across 18 Indian banks to steal their income tax credentials. The latest variant of the malware, found in August, is being distributed as an APK file (iAssist.apk) that is integrated into the iAssist app for Android. It lures victims to claim an instant tax refund, tricking them into submitting personal details such as full name, Aadhar number, PAN number, and financial information. The phishing scam is targeting 18 Indian banks, including the State Bank of India by abusing Accessibility Service. This way, it obtains the necessary permissions to perform several tasks on the compromised systems. The latest malware is capable of screen recording and keylogging to harvest credentials. It abuses CallScreeningService to manage incoming calls.

The discovery of the new two active Drinik variants this year indicates that its operators have enhanced the framework to launch more attacks in near future. Users are recommended to always avoid downloading apps or APKs from untrusted sources and enable multi-factor authentication."

APT36 Targets Indian Government Employees with Limepad

APT36 (Transparent Tribe) adds additional tools and TTPs to its arsenal.It used CrimsonRAT, ObliqueRAT, and proprietary malware in 2022. It launched a Limepad-based data exfiltration campaign recently. Zscaler experts say the Pakistan-linked adversary targets Indian government officials. Transparent Tribe threat actors utilise Google ads for malvertising to spread Kavach trojanized two-factor authentication solutions. They control third-party application shops and utilise them to lead unsuspecting users to attacker-registered domains holding the latest backdoored Indian government-related software.

APT-36 has created multiple domains mimicking Indian government entity sites for credential harvesting and phishing. These domains mimic Kavach NIC (National Informatics Center) or other government login pages. Unless accessed from an Indian IP address, it redirects victims to trustworthy sites. Limepad is still under development, but its primary features suggest it could become the malware of choice for long-term victim network access.Its consistent malvertising, credential harvesting, and phishing attacks suggest a higher purpose.

Ransomware gang targets Belgian municipality, hits police instead

The Ragnar Locker ransomware gang has published stolen data from what they thought was the municipality of Zwijndrecht, but turned out to be stolen from Zwijndrecht police, a local police unit in Antwerp, Belgium. The leaked data reportedly exposed thousands of car number plates, fines, crime report files, personnel details, investigation reports, and more. This data could jeopardise law enforcement investigations and reveal victims of crimes or abuse. Zwijndrecht police replied to local media coverage on Facebook by downplaying the event and stating the hackers only accessed the police's administrative data. The authorities said the threat actors could only access administrative network data, hurting staff.Chief of police at Zwijndrecht, Marc Snels, told the VRT news network that the data leak resulted from human error, and they are now contacting all exposed individuals to inform them about the incident. "Data was not leaked.

This network mostly comprises personal datafrom our employees, such as personnel lists and party images "Snels told local media. Moreover, the leaked files contain footage from traffic cameras, exposing the whereabouts of individuals at specific dates and times. "It should be a wakeup call for local police and how they manage citizens' data, and perhaps it will start improvements on that front." The prosecutor initiated a criminal process on the hacking event, but the data protection office has not opened an inquiry.

Ransomeware Attack

Data Breach

Government Sector (Munsipalty)

Urlscan.io API unwittingly leaks sensitive URLs, data

Researchers warned about business software misconfigurations leaking sensitive data on urlscan.io.Urlscan.io analyses websites. URL submissions generate domains, IPs, DOM information, cookies, and screenshots. The developers say the engine lets "anyone easily and confidently assess unknown and potentially dangerous websites". Urlscan.io provides an API to integrate checks into third-party solutions for enterprise and open source customers. Positive Security discovered that urlscan.io dorks, password reset URLs, setup pages, Telegram bots, DocuSign signing requests, meeting invitations, package tracking links, and PayPal bills might be included. Positive Security contacted several exposed email accounts, but only one responded-an organisation that emailed an employee a DocuSign link to their job contract and then investigated. Positive Security investigated historic urlscan.io data and found misconfigured clients that might be misused by scraping the system for email addresses and sending them unique links to see if they appeared on urlscan. Misconfigured clients can change passwords for various web services and utilise the leaked link to take over accounts.

Security Misconfiguration

Sensitive Data Leakage

Information Technology

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