Threatsploit Adversary Report

Edition 53

Jan 2023

BRISK INFOSEC
CYBER TRUST & ASSURANCE

www.briskinfosec.com

Editorial

Dear Readers:

" One single vulnerability is all that an attacker needs"- Window Snyder, CSO Fastly, so true. To keep these vulnerabilities away;

We are here with the first issue of Threatsploit for the year 2023.

To be sure, we can't help but wonder what harm could come from someone gaining unauthorised access to your passport number. Nonetheless, believe us when we say that a lot of things can go wrong:

Theft of personal data, monetary fraud, fraudulent travel expenses, fraudulent job offers, and phishing attacks. The Global Pravasi Rishta webpage, run by the Indian government's foreign ministry, has recently made headlines.

The site's flaw was to blame for the incident. And getting at the information was a breeze. Based on our research, we can conclude that business owners routinely breach website security. They put almost no resources into website penetration testing. We are crossing our fingers that this information will give them the willies and push them toward investing in website security.

Last month, hackers made an attempt on AIIMS. This time, a hospital in Chennai was the target of an assault. Patients' information has apparently been stolen. According to reports, hackers have so far avoided India's health care sector. This is now, however, apparently on their radar screens. With access to patients' medical records, a hacker could commit a wide variety of fraudulent activities. To ensure patient safety, India's health care industry must prioritize cyber security.

There has been a recent outbreak of a new ransomware strain targeting Windows systems.It locks down numerous different file formats with an impenetrable layer of encryption. There has been a significant uptick in ransomware during the past year. Additionally, there are now cases where a new ransomware family is being produced.

Ever since Elon Musk took over, Twitter has been a topic of conversation.Due to a security flaw, the attacker gained access to the personal information of over 400 million Twitter users. Also, he's currently trying to sell it.

These are just some of the numerous noteworthy events that have occurred this month.

We hope you enjoy the report when you read it. And may this January be free of mishaps. If you need help, all it takes is a phone call to reach us.

Happy Reading !!! Wishing you a Happy New Year ahead from Briskinfosec Family

Contents

Indian foreign ministry's Global Pravasi Rishta portal leaks expat passport details

The Global Pravasi Rishta Portal, India's government platform for connecting with its overseas population, leaked sensitive data, including names and passport details. The platform exposed user names, surnames, country of residence, and email addresses in plaintext, as well as occupation status, phone and passport numbers. The leak was possible because of poor security measures, such as a lack of authentication methods. The Global Pravasi Rishta Portal is a platform with the goal of connecting 30 million Indian expats. The platform owner is the Ministry of External Affairs of India, the country's government body responsible for implementing foreign policy. The portal is meant as a tool for communication between the Ministry of External Affairs, Indian Missions, and the Indian diaspora. Pravasi Rishta means "expatriate relationships" in English. The Cybernews team has reached out to the Ministry of External Affairs to inform it of the leak. We did not receive a reply, but several days later the security issue had been fixed. The data was exposed via the website's edit function, where manipulating the URL allowed anyone to access the edit details of any user on the site. In other words, it takes only one registered user to access all of them, since changing the user ID in the URL leads to another user's account.

Broken Authentication

Sensitive Data Leakage

Government Sector

Hackers Selling Personal Data Of 150,000 Patients From TN Hospital On Dark Web

After a cyberattack on AIIMS knocked out its servers, a threat actor is selling medical records of patients of a Tamil Nadu-based multispecialty hospital. A report released by CloudSEK claims that patient data of Sree Saran Medical Centre in on sale by a threat actor. CloudSEK discovered a post that advertised the sale of sensitive data sourced from Three Cube IT Lab India - a Chennai-based provider of business and consulting services." We can term this incident as a Supply Chain Attack, since the IT Vendor of the Hospital, in this case Three Cube IT Lab, was targeted first. Using the access to the vendor's systems as initial foothold, the threat actor was able to exfiltrate Personally identifiable information (PII) and Protected Health Information (PHI) of their hospital clients," said Noel Varghese, Threat Analyst, CloudSEK. The seller shared a sample as proof for potential buyers, showing data records dated from the years 2007-2011. The data set of 150,000 records of patients' information includes their name, guardian name, date of birth, doctor's details, and address information.The data has been put on sale on popular cybercrime forums as well as on a Telegram channel that is frequented by threat actors. The database is on sale for $100 (Rs. 8,100), suggesting that multiple copies would be sold. For buyers seeking exclusive ownership, the price is $300 (Rs. 24,300). If the owner wants to resell the database, the price is set at $400 (Rs. 32,531).

Cyberattack

Sold Personal Data Of 150,000 Patients

Healthcare

New Ransomware Families Lead Attacks Against Windows Systems

"Fortinet's researchers recently came across three new ransomware families - Vohuk, ScareCrow, and AESRT (aka AERST). These typical ransomware families have been increasingly targeting Windows systems. Vohuk has been primarily targeting Germany and India.

1) It encrypts several file types and makes them completely unusable. It adds the .Vohuk extension to the encrypted files and replaces file icons with a red lock icon.
2) It replaces the desktop wallpaper with its own and leaves a distinctive mutex, which prevents different instances of Vohuk from running on the same system.
1) The ScareCrow ransomware encrypts files on victims' machines and adds the .CROW file extension to affected files. ScareCrow attacks are relatively widespread in Germany, India, Italy, the Philippines, Russia, and the U.S. The ransom note instructs victims to contact the attacker using one of the three Telegram channels provided.
2) ScareCrow carries some similarities with Conti, such as the use of the CHACHA algorithm to encrypt files and using the WMIC utility to delete volume shadow copies.
Researchers found one more new ransomware, dubbed AERST, that encrypts files on compromised machines and appends a AERST file extension to the affected files.
1) Instead of dropping a typical ransom note, it displays a popup window that includes the attacker's email address. It's too early to comment on whether Vohuk, ScareCrow, and AERST ransomware strains could evolve into a large-scale threat or remain as typical ransomware families with short lifespans. However, in such attacks, victims are surely at risk of losing valuable data, resulting in financial loss. Therefore, organizations need to stay ahead of the techniques used by threat actors and implement security best practices and controls."

Ransomeware Attack

Windows Systems are affected

Software Attack

Comcast Xfinity accounts hacked in widespread 2FA bypass attacks

Comcast Xfinity users claim rampant two-factor authentication-skipping hacks.These stolen accounts reset passwords for Coinbase and Gemini crypto exchanges. After regaining access, they realised they had been hacked and a disposable @yopmail.com email was added to their profile.Like Gmail, Xfinity lets customers set up a secondary email address for account notifications and password resets in case they lose access to their account. All Xfinity customers we spoke to have two-factor authentication activated, but the threat actors could still log in. "Bypassing 2FA, someone changed my password and account details. They created xxxxxxxx@yopmail.com" Reddit user Xfinity explained. After gaining access to the account and being requested to enter their 2FA code, the attackers allegedly employ a privately disseminated Xfinity site OTP bypass to fabricate valid 2FA verification requests.

The main Xfinity email will receive a warning that their information was updated, but since the password was changed, they cannot access it. They can reset passwords and change the secondary email to @yopmail.com once logged in. After gaining complete access to an Xfinity email account, the threat actors try to penetrate other consumer online services by confirming password reset requests to the compromised email account.

2FA Bypass Attack

Accounts Stolen

Telecommunications Company

Lastpass : Hackers stole customer vault data in cloud storage breach

"LastPass revealed today that attackers stole customer vault data after breaching its cloud storage earlier this year using information stolen during an August 2022 incident. This follows a previous update issued last month when the company's CEO, Karim Toubba, only said that the threat actor gained access to ""certain elements"" of customer information.Today, Toubba added that the cloud storage service is used by LastPass to store archived backups of production data.The attacker gained access to Lastpass' cloud storage using ""cloud storage access key and dual storage container decryption keys"" stolen from its developer environment.""The threat actor copied information from backup that contained basic customer account information and related metadata including company names, end-user names, billing addresses, email addresses, telephone numbers, and the IP addresses from which customers were accessing the LastPass service,"" Toubba said today.""The threat actor was also able to copy a backup of customer vault data from the encrypted storage container which is stored in a proprietary binary format that contains both unencrypted data, such as website URLs, as well as fully-encrypted sensitive fields such as website usernames and passwords, secure notes, and form-filled data.""According to Toubba, the master password is never known to LastPass, it is not stored on Lastpass' systems, and LastPass does not maintain it. Customers were also warned that the attackers might try to brute force their master passwords to gain access to the stolen encrypted vault data.
However, this would be very difficult and time-consuming if you've been following password best practices recommended by LastPass. If you do, ""it would take millions of years to guess your master password using generally-available password-cracking technology,"" Toubba added.""Your sensitive vault data, such as usernames and passwords, secure notes, attachments, and form-fill fields, remain safely encrypted based on LastPass' Zero Knowledge architecture."""

Data Breach

Stolen Customer Vault Data

Cloud Storage

Okta's source code stolen after GitHub repositories hacked

"Okta, a leading provider of authentication services and Identity and Access Management (IAM) solutions, says that its private GitHub repositories were hacked this month. Earlier this month, GitHub alerted Okta of suspicious access to Okta's code repositories, states the notification.""Upon investigation, we have concluded that such access was used to copy Okta code repositories,"" writes David Bradbury, the company's Chief Security Officer (CSO) in the email. Despite stealing Okta's source code, attackers did not gain unauthorized access to the Okta service or customer data, says the company. Okta's ""HIPAA, FedRAMP or DoD customers"" remain unaffected as the company ""does not rely on the confidentiality of its source code as a means to secure its services."" As such, no customer action is needed. At the time of writing our report, the incident appears to be relevant to Okta Workforce Identity Cloud (WIC) code repositories, but not Auth0 Customer Identity Cloud product, given the email wording. While ending its 'confidential' email that pledges a 'commitment to transparency,' Okta says it will publish a statement today on its blog."

Cyber Attack

Github Repositories

Identity and Access Management Company

Hacker claims to be selling Twitter data of 400 million users

A threat actor is selling public and private data from 400 million Twitter users gathered in 2021 via a now-fixed API vulnerability. Exclusive sales cost $200,000. Ryushi, a threat actor, is selling the alleged data dump on Breached, a hacking community that sells data breaches. A vulnerability allowed the threat actor to steal 400+ million Twitter users' data. They advised Elon Musk and Twitter to buy the data to avoid a huge GDPR fine. "Twitter or Elon Musk if you are reading this you are already risking a GDPR fine over 5.4m breach imaging the fine of 400m users breach source," Ryushi said on a forum." Your best alternative to avoid $276 million USD in GDPR breach fines like facebook (due to 533m people being scraped) is to buy this data solely." Forum post offering 400 million Twitter user info. The forum post provides example data for thirty-seven celebrities, politicians, journalists, corporations, and government institutions, including Alexandria Ocasio-Cortez, Donald Trump JR, Mark Cuba, Kevin O'Leary, and Piers Morgan.Later, 1,000 more Twitter profiles were released. Twitter user profiles include public and private data including email addresses, names, usernames, follower count, creation date, and phone numbers. Many leaked accounts lack phone numbers, but all include email addresses. Phone numbers and email addresses are private, but much of this data is public on Twitter.

Cyber Attack

400 Million Users Data Breach

Twitter Social Media Platform

Leading sports betting firm BetMGM discloses data breach

A threat actor obtained user data from BetMGM, a leading sports betting provider. The attackers collected names, contact info (including postal addresses, email addresses, and phone numbers), dates of birth, hashed Social Security numbers, account identifiers (such player IDs and screen names), and BetMGM transaction data from customers. "BetMGM's online activities were not compromised. BetMGM is working with police to improve security." The potential attackers are selling the betting firm's May hack victims' data online. "We breached BetMGM's casino database current as of Nov 2022," writes 'betmgm-hacked', who sold the stolen data on a hacker site yesterday. "BetMGM.com Casino Database Breach" claims 1,569,310 user records were taken from BetMGM. It also promises to feature BetMGM casino players from New Jersey and Pennsylvania and a "Master Casino" data set comprising customers from all states (all customer records include phone number, email, and address info, according to the threat actor). MGM Resorts International, an American hospitality and entertainment company, and Entain plc, one of the world's largest sports betting and gambling organisations, created BetMGM in 2018 in New Jersey.

xxxxxxxxxxx

Data Breach

Sports Betting Firm

MoneyMonger Campaign - All About Data Theft, Loan Extortions, and Blackmailing

"Hackers are using bad money lending apps to threaten and blackmail people into giving them a lot of money. Researchers at Zimperium recently found that a Flutter-obfuscated app and its variants were spreading malware as part of a new campaign called MoneyMonger (some sources have also named the malware as MoneyMonger). The people who are behind the MoneyMonger campaign are always making changes to the apps so that they can't be found. The bad apps use geo-targeting to find people in their area. One of the bad apps is aimed at people in India, and several other versions are aimed at people in Peru. The malicious apps are spread by people who pose a threat through multiple layers of social engineering. Hackers use malware to trick people into giving them access to private information on their devices. The information that was stolen includes contacts, messages, pictures taken with the camera, GPS location data, sound recordings, call logs, and storage data.

Attackers have been using social engineering and other tricks to get people to download infected apps for a long time. Before downloading an app from Google Play or a third-party source, users should read the reviews and know what information the app collects from their device. Hackers threaten their victims to give out information, call people from the contact list, or even use blackmail to get them to share photos that they have stolen. "

Social Engineering Attack

Data Theft

Android Market

Malware Disguised as YouTube Bot Steals Sensitive Data

"The recently found YouTube bot malware unfairly boosts the ranking of YouTube videos and steals sensitive information from the victim's systems. It is capable of downloading additional files from C2 servers which makes it an even bigger concern. Content creators are suggested to avoid the use of bots for video boosting.   Cyble researchers found that the YouTube bot malware is distributed as a 32-bit executable file compiled with .NET compiler. Four argument strings including the video ID, video duration, like, and comment, are required to run the executable file.Upon execution, the malware performs an AntiVM check to prevent malware detection and analysis by researchers in a virtual environment.Y ouTube bot launches the browser context with the parameters and uses YouTube Playwright function for automating tasks such as viewing, liking, and commenting on YouTube videos.

The function relies on Microsoft.Playwright package. The malware connects to a C2 server and receives commands to delete the scheduled task entry and terminate its own process, extract log files to the C2 server, download and execute other files, and start/stop viewing a YouTube video. In addition, it checks if the victim's system has the necessary dependencies, such as the Chrome browser and the Playwright package installed. If these dependencies are absent, it will download and install them when it receives the 'view' command."

Malware Attack

Sentive Information Stolen

Social Media Platform(Youtube)

Russians hacked JFK airport's taxi dispatch system for profit

Two U.S. citizens were detained for plotting with Russian hackers to hack the JFK taxi dispatch system to send certain taxis to the front of the queue for $10. The computer-controlled taxi dispatch system sends taxis from the airport's holding lot to pick up the next fare at the appropriate terminal. The dispatch system usually calls taxis after many hours in the lot. This technique ensures fairness for taxi drivers in a high-demand location. The DOJ claims the hackers used their illicit access to build a paid service that let JFK cabs skip the line and get delivered swiftly. Hackers demanded $10 in cash or mobile payment from taxi drivers. Promoters received free line-skipping waivers. Abayev and Leyman announced "Shop open" and "Shop closed" on private chat applications to the taxi drivers. "In order to skip the taxi queue, taxi drivers would communicate their taxi medallion numbers into the group chat threads, and a participant of the hacking scheme would then message the terminal that the taxi driver should proceed to to skip the taxi line and pick up a fare," the indictment states. The indictment alleges that Abayev and Leyman transmitted at least $100,000 to Russian hackers under the guise of "software development." Two counts of conspiracy to commit computer intrusion entail a 10-year prison penalty for both men.

Cyber Attack

Money Loss

Transportation Platform

GodFather Android malware targets 400 banks, crypto exchanges

"Godfather, an Android banking trojan, has targeted 16 countries to steal account information for over 400 online financial sites and cryptocurrency exchanges. When victims log in, the virus generates login screens overlaid on the banking and crypto exchange apps' login forms, deceiving them into entering their credentials on well-crafted HTML phishing pages. Group-IB analysts believe the Godfather trojan is the heir to Anubis, a banking trojan that lost popularity due to its inability to circumvent modern Android protections.Group-IB uncovered some malware in Google Play Store apps, however the primary distribution channels haven't been found, thus the initial infection mechanism is unknown. Godfather targeted 215 financial apps, most of them in the US (49), Turkey (31), Spain (30), Canada (22), France (20), Germany (19), and the UK (19). (17).

Besides banking apps, Godfather targets 110 bitcoin trading platforms and 94 cryptocurrency wallet apps. Godfather mimics Android's default security solution, Google Protect. Malware simulates device scanning. This scan seeks Accessibility Service access from a valid tool. The software receives all authorization to commit crimes after the victim consents. This includes SMS, notifications, screen recording, contacts, calls, writing to external storage, and device status.The Accessibility Service is also used to restrict users from deleting the trojan, exfiltrating Google Authenticator OTPs, processing commands, and stealing PIN and password fields.Instead of waiting for the target programme to start, the malware can send bogus notifications from installed apps to a phishing page. Turkish-targeted false overlays-Godfather steals a list of installed apps to accept C2 server injections (fake HTML login forms to steal credentials). "

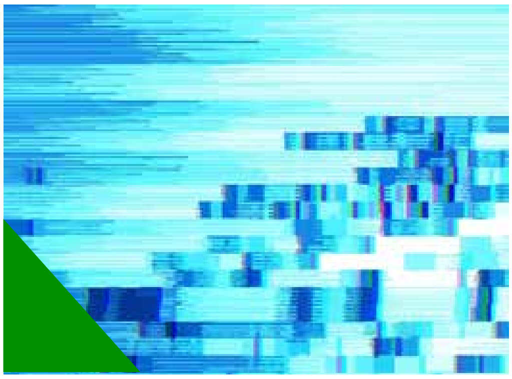
Malware Attack

Stolen Account Information

Banking Sites

Microsoft : KB5021233 causes blue screens with 0xc000021a errors

"Microsoft is investigating a known issue leading to Blue Screen of Death (BSOD) crashes with 0xc000021a errors after installing the Windows 10 KB5021233 cumulative update released. The company warned over the weekend that ""after installing KB5021233, some Windows devices might start up to an error (0xc000021a) with a blue screen.""This comes after a stream of users reports on Redmond's own community website [1, 2, 3] and Reddit [1, 2, 3], some of them reporting that the update reverted automatically or that they've been able to fix the issue after a system restore. The known issue is likely caused by a mismatch between the file versions of hidparse.sys in system32 and system32/drivers in the Windows folder, ""which might cause signature validation to fail when cleanup occurs.""The list of affected platforms includes only client Windows 10 versions, from Windows 10 20H2 to the latest release, Windows 10 22H2. Redmond added that it's already working on a fix to address this newly acknowledged issue but hasn't yet shared when it will be available."



Besides banking apps, Godfather targets 110 bitcoin trading platforms and 94 cryptocurrency wallet apps. Godfather mimics Android's default security solution, Google Protect. Malware simulates device scanning. This scan seeks Accessibility Service access from a valid tool. The software receives all authorization to commit crimes after the victim consents. This includes SMS, notifications, screen recording, contacts, calls, writing to external storage, and device status. The Accessibility Service is also used to restrict users from deleting the trojan, exfiltrating Google Authenticator OTPs, processing commands, and stealing PIN and password fields. Instead of waiting for the target programme to start, the malware can send bogus notifications from installed apps to a phishing page.Turkish-targeted false overlaysGodfather steals a list of installed apps to accept C2 server injections (fake HTML login forms to steal credentials)."

Cyber Attack

Errors

Information Technology(Microsoft)

Woman gets 66 months in prison for role in $3.3 million ID fraud op

"The Australian Federal Police (AFP) have announced today that a 24-year-old woman from Melbourne, arrested in 2019 for her role in large-scale, cyber-enabled identity theft crimes, was sentenced to five years and six months in prison. According to the AFT, she was part of an international crime syndicate engaged in ""large-scale and sophisticated cybercrimes,"" stealing at least $3.3 million and laundering another $2.5 million. In addition to these figures, the criminals attempted to steal $7.5 million from their victims. The AFP arrested the woman when she was 21 at the Melbourne Airport as part of an investigation codenamed ""Operation Birks,"" and executed search warrants in her residence. Further investigations aided by files found on seized devices revealed that the suspect was purchasing stolen identities of real individuals on the dark web, used fraudulently registered SIM cards, and spoofed email accounts to perform 'identity takeover.' The crooks then used these identities to open over 60 bank accounts across various Australian financial institutions and then stole money from the victims' superannuation (Australian pension program a company creates for the benefit of its employees) and stock trading accounts. After withdrawing the money from the fraudulent bank accounts, the woman sent them to a contact in Hong Kong who purchased assets that are more difficult to trace (e.g. luxury products) that were resold. Ultimately, portions of the laundered amounts were sent back to Australia in cryptocurrency, to minimize the chances of leaving a money trace."

Cyber Attack

$3.3 Million Stolen

Civil Service

Hackers leak personal info allegedly stolen from 5.7M Gemini users

"Gemini crypto exchange announced this week that customers were targeted in phishing campaigns after a threat actor collected their personal information from a third-party vendor. The notification comes after multiple posts on hacker forums seen by BleepingComputer offered to sell a database allegedly from Gemini containing phone numbers and email addresses of 5.7 million users. The Gemini product security team published a short notice that an unnamed third-party vendor suffered an ""incident"" that allowed an unauthorized actor to collect email addresses and incomplete phone numbers belonging to some Gemini customers. As a result of the breach, customers of the crypto exchange received phishing emails. The goal of the attacker has not been disclosed but such access to accounts and financial information is typically what threat actors are after.

The notification comes after multiple posts on a hacker forum offered to sell a database allegedly from Gemini containing phone numbers and email addresses of 5.7 million users. Yet another post under a different username (now banned on the forum) appeared in mid-November, offering databases from multiple crypto exchanges, including one from Gemini that supposedly had the same type of information for 5.7 million users. It appears that none of the attempts to monetize the database worked as yet another announcement appeared on a different forum offering the information for free. Gemini advises its customers to rely on strong authentication methods and recommends activating two-factor authentication (2FA) protection and/or the use of hardware security keys to access their accounts."

Phishing Attack

5.7M user Personal Information Leakage

Crypto Exchange Platform

Phishing attack uses Facebook posts to evade email security

"A new phishing campaign uses Facebook posts as part of its attack chain to trick users into giving away their account credentials and personally identifiable information (PII). The emails sent to targets pretend to be a copyright infringement issue on one of the recipient's Facebook posts, warning that their account will be deleted within 48 hours if no appeal is filed. The link to appeal the account deletion is an actual Facebook post on facebook.com, helping threat actors bypass email security solutions and ensure their phishing messages land in the target's inbox. The Facebook post pretends to be ""Page Support,"" using a Facebook logo to appear as if the company manages it.However, this post includes a link to an external phishing site named after Meta, Facebook's owner company, to slightly reduce the chances of victims realizing the scam. The phishing sites are crafted with care to make them appear like Facebook's actual copyright appeal page, containing a form where victims are requested to enter their full name, email address, phone number, and Facebook username. Upon submission of this data, the page also collects the victim's IP address and geolocation information and exfiltrates everything to a Telegram account under the threat actor's control. The threat actors might collect the extra information to bypass fingerprinting protections or security questions while taking over the victim's Facebook account. Whatever code the victim enters will result in an error, and if the 'Need another way to authenticate?' is clicked, the site redirects to the actual Facebook site. Trustwave's analysts also discovered that the threat actors use Google Analytics on their phishing pages to help them track the efficiency of their campaigns."

Phishing Attack

Account Credentials Stolen

Social Media Platform

Ukrainian govt networks breached via trojanized Windows 10 installers

"Ukrainian government entities were hacked in targeted attacks after their networks were first compromised via trojanized ISO files posing as legitimate Windows 10 installers. These malicious installers delivered malware capable of collecting data from compromised computers, deploying additional malicious tools, and exfiltrating stolen data to attacker-controlled servers.""The ISO was configured to disable the typical security telemetry a Windows computer would send to Microsoft and block automatic updates and license verification,"" said cybersecurity firm Mandiant which discovered the attacks."" There was no indication of a financial motivation for the intrusions, either through the theft of monetizable information or the deployment of ransomware or cryptominers.""While analyzing several infected devices on Ukrainian Government networks, Mandiant also spotted scheduled tasks set up in mid-July 2022 and designed to receive commands that would get executed via PowerShell.After the initial reconnaissance, the threat actors also deployed Stowaway, Beacon, and Sparepart backdoors that allowed them to maintain access to the compromised computers, execute commands, transfer files, and steal information, including credentials and keystrokes.""We assess that the threat actor distributed these installers publicly, and then used an embedded schedule task to determine whether the victim should have further payloads deployed,"" Mandiant added. While the malicious Windows 10 installers were not specifically targeting the Ukrainian government, the threat actors analyzed infected devices and performed further, more focused, attacks on those determined to belong to government entities."

Malware Attack (Trojan)

Network Breach

Government Sector

Social Blade confirms breach after hacker posts stolen user data

"Social media analytics platform Social Blade has confirmed they suffered a data breach after its database was breached and put up for sale on a hacking forum. Social Blade is an analytics platform that provides statistical graphs for YouTube, Twitter, Twitch, Daily Motion, Mixer, and Instagram accounts, allowing customers to see estimated earnings and projects. The company offers an API allowing customers to integrate the Social Blade data directly into their own platforms. ""On December 14th we were notified of a potential data breach whereby an individual had acquired exports our users database and were attempting to sell it on a hacker forum,"" reads a data breach notification sent to customers."" Samples were posted and we verified that they were indeed real. It appears this individual made use of of a vulnerability on our website to gain access to our database."" While Social Blade states that the user passwords were hashed using the bcrypt algorithm and cannot be easily deciphered, the company still suggests that all users reset their passwords. However, there won't be a platform-wide reset of credentials. The authorization tokens for Business users and connected social media accounts have also been cycled, preventing threat actors from continuing to use the ones listed in the stolen database."

Cyber Attack

Data Breach

Social Media Platform

FBI seized domains linked to 48 DDoS-for-hire service platforms

"The US Department of Justice has seized 48 Internet domains and charged six suspects for their involvement in running 'Booter' or 'Stresser' platforms that allow anyone to easily conduct distributed denial of service attacks. Booters are online platforms allowing threat actors to pay for distributed denial-of-service attacks on websites and Internet-connected devices. Essentially, they are ""booting"" the target off of the Internet. Stressers offer the same DDoS features but claim to be provided for legitimate testing of the reliability of web services and the servers behind them.""Some sites use the term ""stresser"" in an effort to suggest that the service could be used to test the resilience of one's own infrastructure; however, as described below, I believe this is a façade and that these services exist to conduct DDoS attacks on victim computers not controlled by the attacker, and without the authorization of the victim,"" reads an affidavit by FBI Special Agent Elliott Peterson out of the Alaska field office.

To use these services, threat actors register an account and deposit cryptocurrency, which is then used to pay for the services.While almost all booter/stresser sites require a subscriber to agree not to use the services to conduct attacks, many of these services are promoted on hacker forums and criminal marketplace. In many cases, the platforms' owners themselves promote deals and coupons on cybercrime sites or use affiliates who earn commissions for promoting the service."

DDOS Platform

48 Internet Domains seized

Service Platform

Ransomware attack at Louisiana hospital impacts 270,000 patients

"The Lake Charles Memorial Health System (LCMHS) is sending out notices of a data breach affecting almost 270,000 people who have received care at one of its medical centers. LCMHS' announcement clarifies that its electronic medical records were out of reach for the network intruders. LCMHS reported the incident to the secretary of the U.S. Department of Health and Human Services (HHS). The portal for healthcare-related breaches now reports that 269,752 individuals have been impacted by the incident. Hive has also published the files allegedly stolen after breaching LCMHS systems. The listed files include bills of materials, cards, contracts, medical info, papers, medical records, scans, residents, and more. BleepingComputer could not confirm if these files are authentic or not.

If you have received care on LCMHS in the past, it is recommended to stay vigilant for incoming communications asking you to give away personal information and payment data.Also, you should monitor your bank statements and report any suspicious transactions to your bank immediately."

Ransomeware Attack

270,000 patients Impacted

Healthcare

BTC.com lost $3 million worth of cryptocurrency in cyberattack

"BTC.com, one of the world's largest cryptocurrency mining pools, announced it was the victim of a cyberattack that resulted in the theft of approximately $3 million worth of crypto assets belonging to both customers and the company. According to its mining pool tracker, BTC.com is the seventh largest cryptocurrency mining pool, with 2.66% of the network's total hashrate.

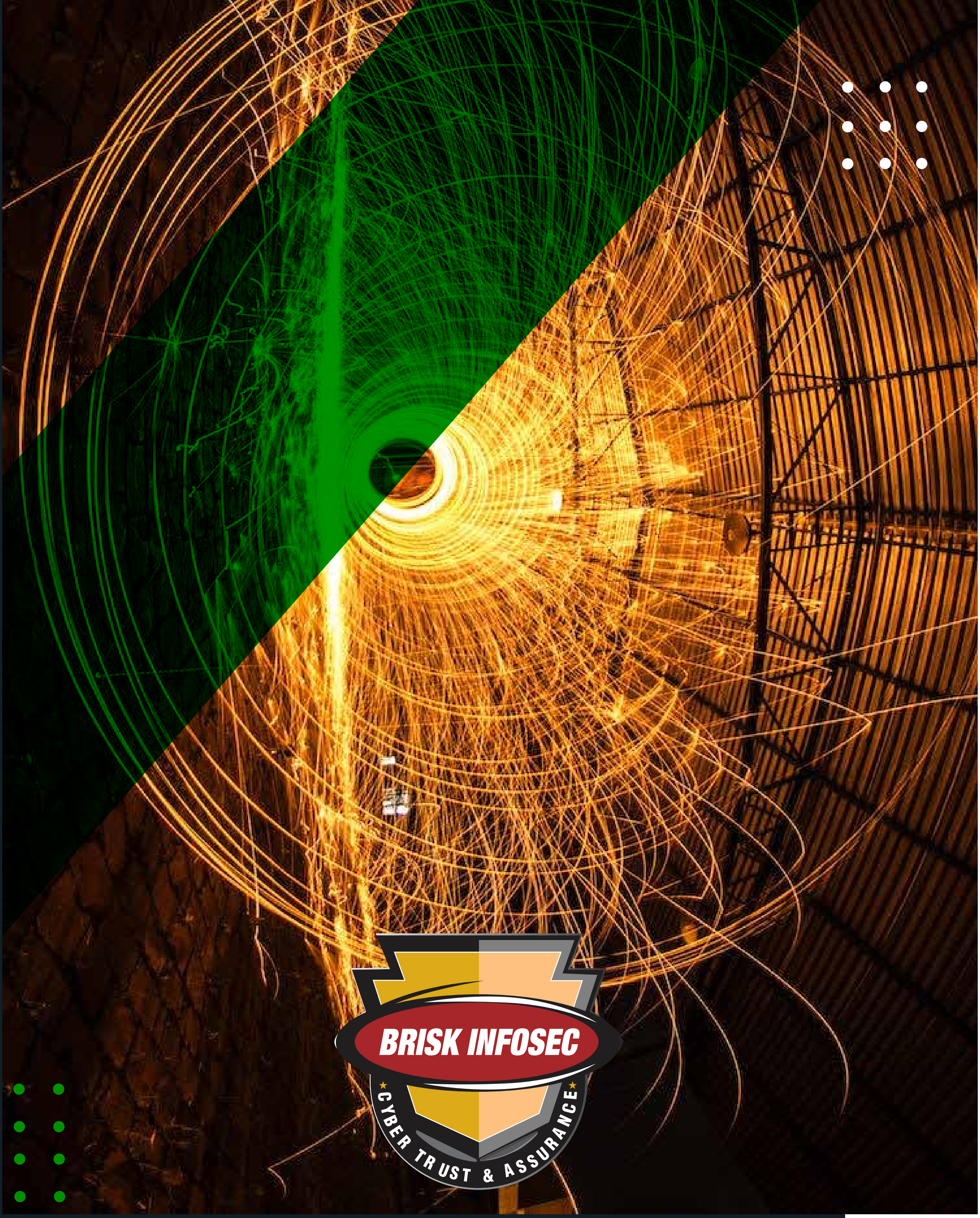
In a press release, BTC.com stated that around $700,000 worth of crypto owned by its clients and $2.3 million in digital assets owned by the company were stolen in the attack.""In the cyberattack, certain digital assets were stolen, including approximately US$700,000 in asset value owned by BTC.com's clients, and approximately US$2.3 million in asset value owned by the Company,"" BTC.com revealed. BTC.com added that it has taken measures to block similar attacks in the future and that its operations have not been affected. ""In the wake of discovering this cyberattack, the Company has implemented technology to better block and intercept hackers,"" the company added.

A BTC.com spokesperson was not immediately available for comment when contacted by BleepingComputer for more details regarding the cyberattack. There is currently no information on how the attackers could steal the cryptocurrency or if any data or personal information was stolen during the incident."

Cyber Attack

$3.3 Million Cryptocurrency Stolen

Cryptocurrency Mining Tool



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