AUGUST
2022

THREATSPLOIT ADVERSARY REPORT

Edition 48

www.briskinfosec.com

INTRODUCTION

Can a traditional battle between two armies be transformed into a war between its citizens? Do you know there's a phoney version of WhatsApp circulating the internet that sends malicious links to your phone? Well, these are only a couple of the twenty or so things you should be aware of "Hackers must get it right once, and we must get it right every time." This is a well-known slogan in the field of cyber security. We must get it right each and every time. So, in order to be prepared, we must be aware of what is going on around us. We need to know how it impacts us and what treatment options we have. Not to worry, this month's Threatsploit report is here. This has been a month of ransomware, with hackers encrypting data and demanding a ransom, for example, a new red alert. Small restaurant chains, when not secure, can sometimes undermine what can go wrong. Credit card information from US-based restaurant chains was sold on the dark web. This news shatters the façade of "We are small, thus we are safe."

Ukraine The conflict with Russia is far from over. However, misinformation campaigns are on the rise. Ukraine's radio stations were hacked and taken over. Then, fraudulent messages about their President's illness were broadcast. It was eventually discovered to be false. A doctored video of Ukraine's President's talking head also surfaced a few months ago. Hacking allows hackers to gain access to any system that runs on information.

Outdated, incorrectly set firewalls and anti-virus software can cost you a flood. The Goan government is also a victim of this. They were hacked, and data relating to flood control was stolen. Because Goa floods during the monsoon, it can be fatal.

SEBI is a quasi-governmental organization, and we all expect them to keep information secure. They have valuable financial knowledge because they regulate stock markets and securities. A couple of their employees were phished, and their email addresses were exploited to send emails to unknown senders.

Nobody is secure. Nations, corporations, states, and restaurants Because they all share a common pain point: information. We hope that this reading will help you understand what is going on. It will also assist you in hardening your security procedures.

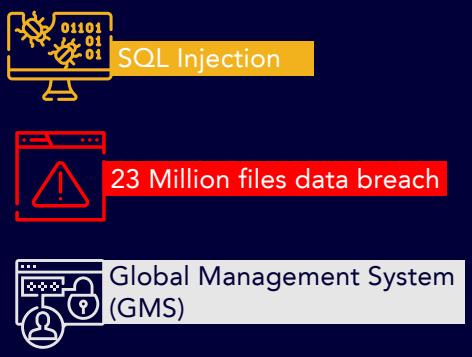
Happy reading, and have a safe internet month!
Let us strengthen our defenses

CONTENTS

SONICWALL : PATCH CRITICAL SQL INJECTION BUG IMMEDIATELY

“SonicWall has published a security advisory today to warn of a critical SQL injection flaw impacting the GMS (Global Management System) and Analytics On-Prem products.""SonicWall PSIRT strongly suggests that organizations using the Analytics On-Prem version outlined below should upgrade to the respective patched version immediately,""The flaw, tracked as CVE-2022-22280, allows SQL injection due to improper neutralization of special elements used in an SQL Command.Considering the widespread deployment of SonicWall GMS and Analytics, which are used for central management, rapid deployment, real-time reporting, and data insight, the attack surface is significant and typically on critical organizations”.

“The recommended action to resolve this vulnerability is to upgrade to GMS 9.3.1-SP2-Hotfix-2 or later and Analytics 2.5.0.3-Hotfix-1 or later. Any version number below these is vulnerable to CVE-2022-22280. Additionally, SonicWall recommends the incorporation of a Web Application Firewall (WAF), which should be adequate for blocking SQL injection attacks even on unpatched deployments”.



UKRAINIAN RADIO STATIONS HACKED TO BROADCAST FAKE NEWS ABOUT ZELENSKYY'S HEALTH

It appears that the latest cyberattack victim has been TAVR Media, a Ukrainian radio station, which was hit with a fake message claiming that President Volodymyr Zelenskyy was seriously ill.In an update, the State Service of Special Communications and Information Protection of Ukraine (SSSCIP) stated that "cybercriminals spread information that President of Ukraine, Volodymyr Zelenskyy, is allegedly in intensive care and his duties are performed by Verkhovna Rada Chairman Ruslan Stefanchuk."

the Kyiv-based holding company oversees nine major radio stations, including Hit FM, Radio ROKS, KISS FM, Radio RELAX, Melody FM, Nashe Radio, Radio JAZZ, Classic Radio, and Radio Bayraktar. In n a separate post on Facebook, TAVR Media disclosed its servers and networks were targeted in a cyberattack and it's working to resolve the issue. The company also emphasized that "no information about the health problems of the President of Ukraine Volodymyr Zelenskyy is true.

"The false reports, which were broadcasted between 12 and 2 p.m., also prompted Zelenskyy to take to Instagram, stating, "I have never felt as healthy as I do now."The provenance of the intrusion remains unknown as yet, although several threat actors have capitalized on the ongoing conflict between Russia and Ukraine to carry out a barrage of cyberattacks, with hacking groups taking sides.In a related development, the Computer Emergency Response Team of Ukraine (CERT-UA) also warned of macro-laden PowerPoint documents being used to deploy Agent Tesla malware targeting state organizations of the country.

BRITISH ARMY'S YOUTUBE AND TWITTER ACCOUNTS WERE HACKED TO PROMOTE CRYPTO SCAMS

Both the British Army's YouTube and Twitter accounts were hacked and used to promote cryptocurrency scams, the UK Ministry of Defence confirmed on Sunday. It's unclear when exactly hackers took over the two accounts, but they both appear to be back to normal now.Hackers hijacked the British Army's Twitter page, swapping out the organization's profile picture, bio, and cover photo to make it seem like it was associated with The Possessed NFT collection.

The account sent out various retweets for NFT giveaways, and its pinned tweet linked users to a fake NFT minting website.Bad actors also stripped the British Army's YouTube channel, deleting all its videos, as well as changing its name and profile picture to resemble the legit investment firm Ark Invest. Hackers replaced the British Army's videos with a series of old livestreams featuring former Twitter CEO Jack Dorsey and Tesla CEO Elon Musk.

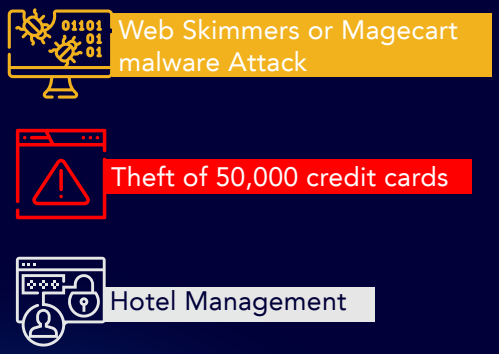
As Web3 Is Going Just Great blogger Molly White points out, the scammers who took over the British Army's accounts carried out their scheme with some of the same tactics used in the recent past. In March, hackers took over the Twitter account belonging to MKLeo, one of the world's top Super Smash Bros.

Ultimate players, and used it to peddle phony NFTs made to look like they were associated with The Possessed. Just two months after that incident, scammers managed to steal $1.3 million using the same Ark Invest livestreams that were repurposed for this hack.

Twitter spokesperson Rocio Vives told The Verge that the British Army's account Twitter "has since been locked and secured," and that "account holders have now regained access and the account is back up and running."

HACKERS STEAL 50,000 CREDIT CARDS FROM 300 U.S. RESTAURANTS

Payment card details from customers of more than 300 restaurants have been stolen in two web-skimming campaigns targeting three online ordering platforms.Web-skimmers, or Magecart malware, are typically JavaScript code that collects credit card data when online shoppers type it on the checkout page.Recently, Recorded Future's threat detection tools identified two Magecart campaigns injecting malicious code into the online ordering portals of MenuDrive, Harbortouch, and InTouchPOS.As a result, 50,000 payment cards were stolen and have already been offered for sale on various marketplaces on the dark web.On both platforms, the web skimmer was injected into the restaurant's web pages and its assigned subdomain on the online payment service's platform.



The malware deployed for MenuDrive used two scripts, one for snatching the payment card data and another for collecting the cardholder's name, email address, and phone number, achieved by attaching to the 'onmousedown' event and "responding to clicks of multiple buttons during the account creation and checkout process."In this case, the skimmer doesn't steal the details from the site but instead overlays a fake payment form on valid targets that are ready for the checkout process using a credit card.

RAINING BITCOIN : FAKE NVIDIA GIVEAWAY

The fraudsters created a fake website supposedly dedicated to Nvidia's 30th anniversary, and announced a large bitcoin giveaway there. On the splash screen of the fake website visitors see the company logo (albeit purple, not the usual green) and the name of its CEO, Jensen Huang. Visitors are asked here to "select a category" to take part in the "event". In fact, there's nothing to choose from: under the invitation there's only a single big button with the words "Bitcoin giveaway".After clicking the button, the user is taken to a page with detailed information about the mythical giveaway. At first glance the page looks convincing : there's a photo of the CEO and additional menu sections, all nicely designed. But instead of the Nvidia logo there's a Bitcoin icon, plus numerous grammatical errors in the text - something a serious company wouldn't permit.

Here, purportedly on behalf of Mr. Huang and Nvidia, the cybercriminals announce a giveaway of 50,000 BTC (worth more than a billion US dollars at the time of writing). One of the main conditions for taking part is that users themselves must first make a contribution, like buying a lottery ticket.

The scammers promise that the participant will immediately get double their money back, not to mention the prospect of winning the 50,000 BTC.- The address of the cryptowallet to which they should make a transfer is given in the instructions for participants. And at the very bottom of the page is an online broadcast of the “winnings” paid out by the organizers.

Phishing Attack

Accounts Compromised

Information Technologies

NEW REDALERT RANSOMWARE TARGETS WINDOWS, LINUX VMWARE ESXI SERVERS

A new ransomware operation called RedAlert, or N13V, encrypts both Windows and Linux VMWare ESXi servers in attacks on corporate networks.The Linux encryptor is created to target VMware ESXi servers, with command-line options that allow the threat actors to shut down any running virtual machines before encrypting files.

When encrypting files, the ransomware utilizes the NTRUEncrypt public-key encryption algorithm, which support various 'Parameter Sets' that offer different levels of security.An interesting feature of RedAlert/N13V is the '-x' command-line option that performs 'asymmetric cryptography performance testing' using these different NTRUEncrypt parameter sets.

However, it is unclear if there is a way to force a particular parameter set when encrypting and/or if the ransomware will select a more efficient one.When encrypting files, the ransomware will only target files associated with VMware ESXi virtual machines, including log files, swap files, virtual disks, and memory files

Redalert Ransomeware Attack

Windows, Linux VMWare ESXi Servers Compromise

Information Technologies

WHATSAPP WARNS USERS : FAKE VERSIONS OF WHATSAPP ARE TRYING TO STEAL YOUR PERSONAL INFO

WhatsApp has issued a stern warning to users and is asking them to be aware of the fake versions of the messaging app. The instant messaging app's CEO, Will Cathcart, is requesting people on Twitter to not use the modified version of WhatsApp as users could end up in big trouble.

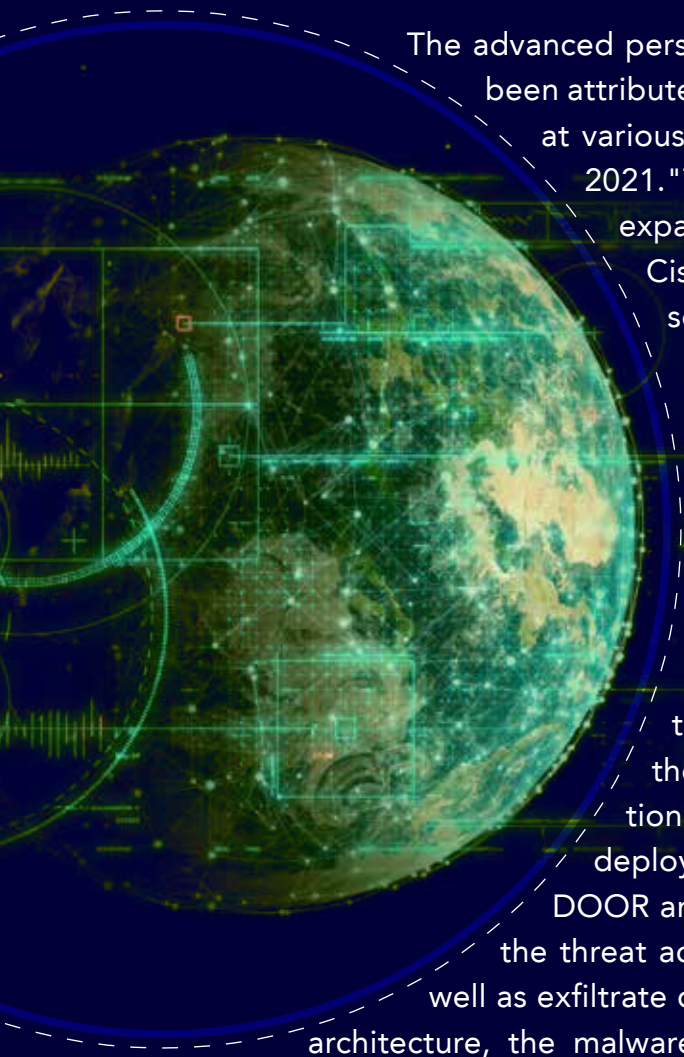
WhatsApp is one of the most popular messaging apps all over the world, which makes it easier for scammers to trick users through different techniques.The security research team of the company found some malicious apps that claim to offer services similar to WhatsApp.

While the modified or fake versions of WhatsApp can offer features similar to WhatsApp, do keep in mind that they don't offer the end-to-end encryption feature that you get with the original version of the messaging app. This helps protect your chats and personal data, so no one can access your details, not even WhatsApp.The new fake version of WhatsApp is not visible on Play Store, but users who try to download the apps from unofficial sources should be cautious before installing them on their phone.

Cathcart pointed out that apps like "Hey WhatsApp" from a developer called "HeyMods" are dangerous and people should avoid downloading them. The team discovered that these apps promise to offer some new features to users, but that is just a scam to steal personal information stored on people's phones.

People are advised to download the official version of WhatsApp via the company's website or through trusted app stores like Google Play Store."We'll of course continue our efforts to detect and block these kinds of apps going forward. We're also taking enforcement action against HeyMods to stop future harm, and will further explore legal options to hold HeyMods and others like them accountable.

PAKISTANI HACKERS TARGETING INDIAN STUDENTS IN LATEST MALWARE CAMPAIGN



The advanced persistent threat (APT) group known as Transparent Tribe has been attributed to a new ongoing phishing campaign targeting students at various educational institutions in India at least since December 2021."This new campaign also suggests that the APT is actively expanding its network of victims to include civilian users," Cisco Talos said in a report shared with The Hacker News.Also tracked under the monikers APT36, Operation C-Major, PROJECTM, Mythic Leopard, the Transparent Tribe actor is suspected to be of Pakistani origin and is known to strike government entities and think tanks in India and Afghanistan with custom malware such as CrimsonRAT, ObliqueRAT, and CapraRAT.But the targeting of educational institutions and students, first observed by India-based K7 Labs in May 2022, indicates a deviation from the adversary's typical focus.Attack chains documented by the cybersecurity firm involve delivering a maldoc to the targets either as an attachment or a link to a remote location via a spear-phishing email, ultimately leading to the deployment of CrimsonRAT.CrimsonRAT, also known as SEEDOOR and Scarimson, functions as the staple implant of choice for the threat actor to establish long-term access into victim networks as well as exfiltrate data of interest to a remote server.Courtesy of its modular architecture, the malware allows the attackers to remotely control the infected machine, steal browser credentials, record keystrokes, capture screenshots, and execute arbitrary commands.

Spear Phishing Attack

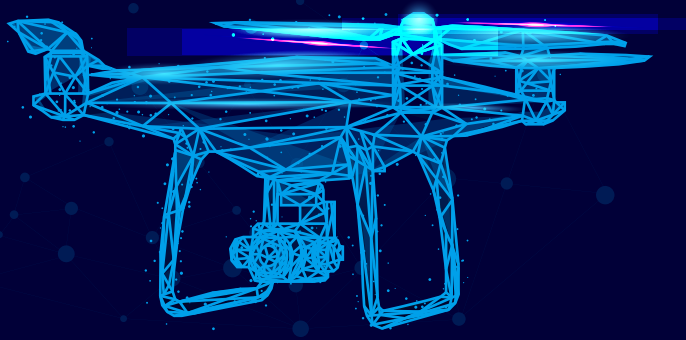
Remote Code Execution

Government Sector

FLAWS IN THE EXPRESSLRS PROTOCOL ALLOW THE TAKEOVER OF DRONES

Researchers warn of vulnerabilities that affect the protocol for radio-controlled (RC) drones, named ExpressLRS, which can be exploited to take over unmanned vehicles. “ExpressLRS uses a ‘binding phrase’, built into the firmware at compile time to bind a transmitter to a receiver. ExpressLRS states that the binding phrase is not for security, it is anti-collision.” reads a bulletin published by NccGroup. “Due to weaknesses related to the binding phase, it is possible to extract part of the identifier shared between the receiver and transmitter. A combination of analysis and brute force can be utilised to determine the remaining portion of the identifier. Once the full identifier is discovered, it is then possible to use an attacker’s transmitter to control the craft containing the receiver with no knowledge of the binding phrase.

This is possible entirely in software using standard ExpressLRS compatible hardware."The phrase used by the ExpressLRS protocol is encrypted using the hashing algorithm MD5 which is known to be cryptographically broken. The experts observed that the "sync packets" that are exchanged between transmitter and receiver at regular intervals for synchronizing purposes leak a major part of the binding phrase's unique identifier (UID).



An attacker can determine the remaining part via brute-force attacks or by observing packets over the air without brute-forcing the sequences.The advisory recommends avoiding sending the UID over the control link. The data used to generate the FHSS sequence should not be sent over the air. It also recommends to improve the random number generator by using a more secure algorithm or adjusting the existing algorithm to work around repeated sequences.

Bruteforce Attack

UAV (Drones) Takeover

Automotive Sector

HACKERS TARGET WRD'S FLOOD MONITORING SYSTEM

Goa police registered a FIR against an unknown person after the flood monitoring system of the water resource department (WRD) came under a ransomware cyber-attack and hackers demanded bitcoin cryptocurrency to decrypt the data.PI Rahul Parab said that they have asked the representatives of the Hyderabad-based software developer ASTRA Microwave Products Ltd to join the investigation to trace the accused.WRD executive engineer Sunil Karmarkar said that the attack was carried out on June 21 between 12AM and 2 AM.

The WRD has a flood monitoring system at 15 locations on major rivers in Goa to monitor water levels in rivers as a part of disaster management in order to have a control on flood eventualities. Karmarkar said that the data of the flood monitoring system, automated rain and weather gauges gets stored in the server located at the data center at Porvorim."The server has been under cyberattack of ransomware. Under the attack, all the files are encrypted with eking extension and cannot be accessed.

In a popup and stored file, the attackers are demanding bitcoin cryptocurrency for the decryption of the data," he said He also said that as a consequence, data could not be observed or downloaded from the server, especially the data related to battery voltages of different stations, data packets related to 12 stations could not be transferred to the WIMS server, SMS and email reports could not be obtained and old data could not be be backed up.

Ransomeware Attack

Flood Monitoring System Compromised

Water Resource Department

DISNEYLAND'S INSTAGRAM AND FACEBOOK ACCOUNTS HACKED TO SHOW RACIST CONTENT

"Disneyland's Facebook and Instagram accounts were taken over on Thursday by a self-proclaimed "super hacker" who posted a series of racist and homophobic posts.Operating under the name "David Do," the threat actor claimed he was seeking "revenge" on Disneyland employees after some of them had allegedly insulted him.The hacker also published posts claiming to have "invented" COVID-19 and suggested he was working on a new "COVID20" virus.Overall, the culprit made four posts on Disneyland's Instagram account before 5 am PT, according to a post on the Disneyland blog."The hacker also tagged several other Instagram accounts, but it is unknown if they are friends and will help lead police to the hacker,"

Disneyland

Further, he encouraged social media users to follow his private Instagram account @chi11estpanda. The posts received thousands of comments of shock and outrage from Disney's 8.4 million followers. The Disneyland Facebook and Instagram accounts were temporarily taken down shortly after the posts went live and were brought back online after the team removed the posts. The park's other social media pages appeared to be unaffected.

A version of the hacker's posts with profanity and slurs censored is available at the bottom of the Disneyland blog post.The incident comes almost a year after three Disney theme park employees were arrested in Florida as part of an operation to catch sexual predators who target children via the internet."

Compromised Credentials

Disneyland's FB & Insta Accounts takeover

Social Media

MUMBAI: ELEVEN SEBI STAFF'S EMAIL ACCOUNTS HACKED

A cyber security officer with Securities Exchange Board of India (SEBI) complained to Bandra-Kurla Complex (BKC) police about official email accounts of 11 staffers being hacked and emails being sent from them to unknown entities.

" He said the hacker sent out emails to Gourav Kapoor, with whom he was not acquainted, besides others on May 23. The officer went to SEBI's disaster recovery site, where he found 11 official email accounts of SEBI staff had been hacked on May 23. Thirty-four emails had been sent from these accounts".

Police registered an FIR on Friday under provisions of IPC and Information Technology Act. The cyber security officer said a colleague from SEBI approached him on May 24 and told him someone had unauthorisedly accessed his official account.

"It was a small incident. No sensitive data was lost. Mitigation measures were immediately taken, including informing CERT-IN as per SOP and strengthening required security configuration of the system, etc. Root cause was diagnosed and fixed," said a SEBI spokesperson."

Phishing Attack

11 Official Email Accounts Compromised

Information Technologies

WORDPRESS PLUGIN SECURITY AUDIT UNEARTHS DOZENS OF VULNERABILITIES IMPACTING 60,000 WEBSITES

A researcher at security firm Cyllective has unearthed vulnerabilities in dozens of WordPress plugins, affecting tens of thousands of installations.Dave Miller, who leads Cyllective's penetration testing team, says they started out testing randomly selected plugins, quickly finding an unauthenticated SQL injection vulnerability.They also found a series of local file inclusion and remote code execution (RCE) vulnerabilities.

However, as these issues were found in severely outdated plugins, the team decided to concentrate its efforts on those that have received updates in the last two years - around 5,000 plugins in total.

Looking particularly for unauthenticated SQL injection vulnerabilities, the researcher used a system of tags to identify plugins showing interaction with the WordPress database; string interpolation in SQL-like strings; security measures relating to sanitization attempts; and exposure of unauthenticated endpoints.And after three months' research, says Miller, the result was a total of 35 vulnerabilities, all of which could have been exploited by unauthenticated attackers, affecting around 60,500 instances running the affected WordPress plugins."Although the vast majority of the vulnerabilities I reported were unauthenticated SQL injection vulnerabilities, which would have enabled an attacker to dump the entire WordPress database contents, these were not the most devastating ones,."

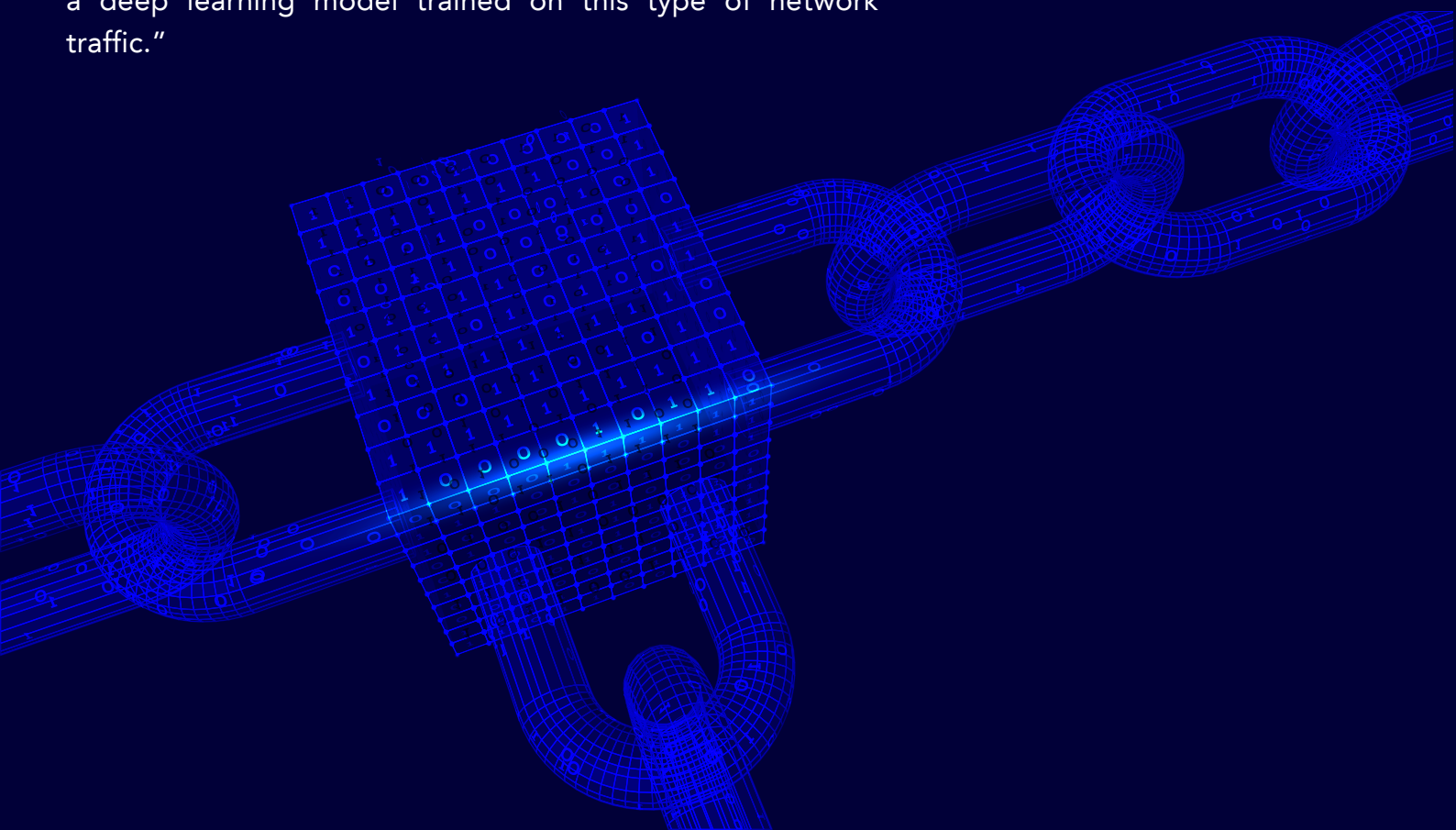
LDAP ACCOUNT MANAGER BUG POSES UNAUTHENTICATED REMOTE CODE EXECUTION RISK

An unauthenticated arbitrary object instantiation vulnerability in LDAP Account Manager (LAM) has been discovered during an internal penetration test.LAM is a PHP web application for managing entries such as users, groups, or DHCP settings in LDAP directories via a web frontend, and is one of the alternatives to FreeIPA. It's included in Debian repositories.But a vulnerability discovered by researcher Arseniy Sharoglazov could allow an attacker to create arbitrary objects and achieve remote code execution (RCE) in one request, and without any out-of-band connections.The technique depends on exploiting the construction new $a($b), with the variable $a standing for the class name that the object will be created for, and the variable $b denoting the first argument to be passed to the object's constructor."When you code in any programming language, you can use good or bad programming practices. The usage of the construction new $a($b), which instantiates arbitrary objects, is a bad practice, if $a and $b come from a non-controlled input," While the technique requires the Imagick extension, he says, this is usually present in larger websites, including the LAM system itself.Sharoglazov says that similar arbitrary object instantiation vulnerabilities have been around for quite some time, but aren't usually reported as such.

"For example, you might read about an SSRF in a commercial software. If you knew the PoC, you would see that it's actually an arbitrary object instantiation with the usage of the SoapClient class, for instance. But for the public it will be just SSRF," he says."Or you might read about an SQL injection. But it's actually an arbitrary object instantiation exploited via a user-defined class which has an SQL injection. This technique, which I found and described, shows how to exploit an arbitrary object instantiation directly to RCE."

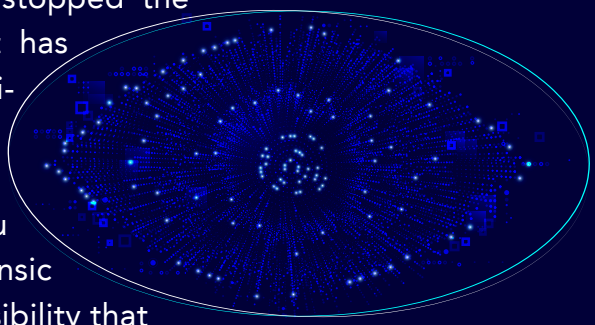
ADVERSARIAL ATTACKS CAN CAUSE DNS AMPLIFICATION, FOOL NETWORK DEFENSE SYSTEMS, MACHINE LEARNING STUDY FINDS

The study (PDF) focuses on DNS amplification, a kind of denial-of-service attack in which the attacker spoofs the victim's IP address and sends multiple name lookup requests to a DNS server.The server will then send all the responses to the victim. Since a DNS request is much smaller than the response, it results in an amplification attack where the victim is flooded with bogus traffic."We decided to study deep learning in DNS amplification due to the increasing popularity of machine learning-based intrusion detection systems," Jared Mathews, the lead author of the paper, ."DNS amplification is one of the more popular and destructive forms of DoS attacks so we wanted to explore the viability and resilience of a deep learning model trained on this type of network traffic."

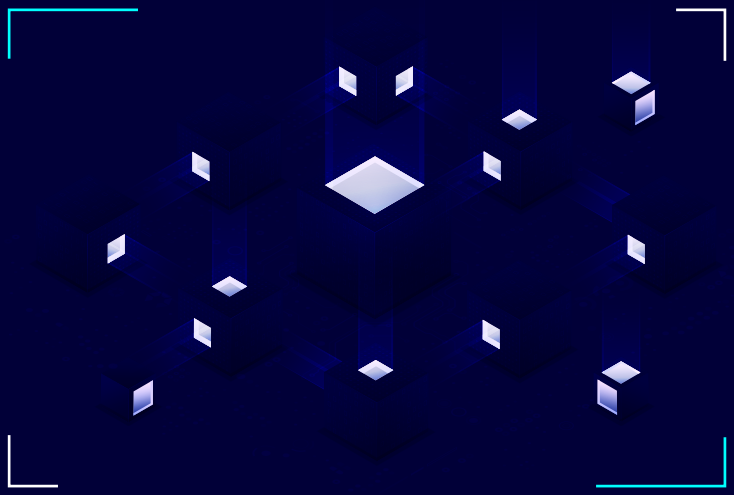


US EYE CLINIC SUFFERS DATA BREACH IMPACTING 92,000 PATIENTS

A healthcare clinic based in Missouri has informed US regulators of a data breach incident affecting more than 90,000 individuals.According to HIPAA, 92,361 individuals were impacted by the breach.-Mattax Neu Prater, which provides surgical and non-surgical care, said that the "third -party data security incident" may have resulted in unauthorized access to the sensitive personal information of some patients.he incident concerns electronic medical records platform myCare Integrity, which is owned by the practice performance company Eye Care Leaders.After discovering the suspicious activity, Eye Care Leaders said its incident response team immediately stopped the unauthorized access and began investigating."This incident has affected eye care practices across the country, and is not specific to Mattax Neu Prater."This data security incident occurred entirely within Eye Care Leaders' network environment, and there were no other remedial actions available to Mattax Neu Prater."The center added: "However, a lack of available forensic evidence prevented Eye Care Leaders from ruling out the possibility that some protected health information and personally identifiable information may have been exposed to the bad actor."Mattax Neu Prater said it does not have any evidence of identity theft as a result of the incident, but has informed anyone who might be impacted via postal mail.



FANTASY PREMIER LEAGUE FOOTBALL APP INTRODUCES 2FA TO TACKLE ACCOUNT TAKEOVER HACKS



The English Premier League has introduced two-factor authentication (2FA) controls to its official Fantasy Premier League game (FPL), offering football fans the option to secure their accounts.The debut of 2FA for the 2022/23 season follows a wave of account hijacking attack allegations over the last two seasons. Miscreants were said to have made multiple player 'transfers' from compromised accounts, leaving victims with weaker fantasy football teams while simultaneously racking up penalty points.

Victims struggled to make up lost ground and for many, their whole season was ruined. The as-yet unidentified attackers, whose potential motives could range from mischief to sabotage, were also in the habit of changing hacked victims' team names.The FPL game had more than nine million players last season, but the wave of hack attacks seemed to have disproportionately targeted the most successful teams - those ranked in the top 100,000 of players.

The FPL game had more than nine million players last season, but the wave of hack attacks seemed to have disproportionately targeted the most successful teams - those ranked in the top 100,000 of players."There is no indication or evidence of a security breach on the accounts of these individuals via fantasy.premierleague.com or the Premier League mobile app," it said at the time.In response to the ongoing issue, the Premier League initially went for the half measure of tweaking how the game worked so that managers were prevented from making more than 20 transfers in a single game week, except in cases where a free hit chip was in play.

Account Hijacking Attack


Compromised Account


Sports

MARRIOTT CONFIRMS LATEST DATA BREACH, POSSIBLY EXPOSING INFORMATION ON HOTEL GUESTS, EMPLOYEES

"Marriott International confirmed Tuesday that unknown criminal hackers broke into its computer networks and then attempted to extort the company, marking the latest in a string of successful cyberattacks against one of the world's biggest hotel chains.

The incident, first reported early Tuesday by databreaches.net, allegedly occurred roughly a month ago and was the work of a group claiming to be "an international group working for about five years," according to the site.A Marriott spokesperson told CyberScoop that the company" is aware of a threat actor who used social engineering to trick one associate at a single Marriott hotel into providing access to the associate's computer. The group claiming responsibility for the attack told Databreaches.net - a news site that focuses on data breaches and cyberattacks - that it stole roughly 20 gigabytes of data, which included credit card information and confidential information about guests and workers from an employee at the BWI Airport Marriott in Baltimore.

The attackers "emailed numerous employees" at Marriott about the breach, the site reported, and had been in at least limited communications with Marriott.Marriott told CyberScoop that most of the stolen information was "non-sensitive internal business files regarding the operation of the property." The company told Databreaches.net that the it would be notifying 300-400 people and regulators, as required, a figure the Marriott spokesperson confirmed late Tuesday to CyberScoop.CyberScoop could not independently verify information about the stolen material or about the attackers claiming responsibility. "

Social Engineering Attack


20 GB Data Breach

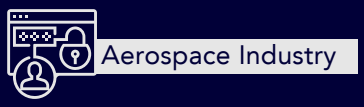

Hotel Management

CLOUD MISCONFIG EXPOSES 3TB OF SENSITIVE AIRPORT DATA IN AMAZON S3 BUCKET : 'LIVES AT STAKE'

A misconfigured Amazon S3 bucket resulted in 3TB of airport data (more than 1.5 million files) being publicly accessible, open, and without an authentication requirement for access, highlighting the dangers of unsecured cloud infrastructure within the travel sector.

The exposed information, uncovered by Skyhigh Security, includes employee personal identification information (PII) and other sensitive company data affecting at least four airports in Colombia and Peru.

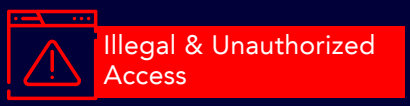
The PII ranged from photos of airline employees and national ID cards - which could present a serious threat if leveraged by terrorist groups or criminal organizations - to information about planes, fuel lines, and GPS map coordinates."Airport security protects the lives of travelers and airport staff," the report explains. "As such, this breach is extremely dangerous with potentially devastating consequences should the bucket's content end up in the wrong hands."As travel picks up dramatically following restrictions during the pandemic, Fortune Business Insights found that the global smart airport market size is set to be driven by the rising preference of the masses for air travel.

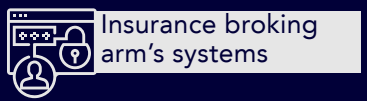


POLICYBAZAAR'S IT SYSTEMS BREACHED

Policybazaar's parent company PB Fintech on Sunday informed stock exchanges of a breach in its insurance broking arm's systems. The online insurance distributor said that the vulnerabilities have been fixed and a thorough audit of the systems is being initiated. "The matter is currently being reviewed by the information security team along with external advisers. While we are in the process of undertaking a detailed review, As on date, our review has found that no significant customer data was exposed," it said in a filing. According to Policybazaar, certain vulnerabilities were identified as a part of Policybazaar Insurance Brokers IT systems and the same were subject of illegal and unauthorised access. "In this regard, Policybazaar has reached out to the appropriate authorities and is taking due recourse according to law," the company said.

Until recently there were no public disclosure norms for data breaches. Recently, Indian Computer Emergency Response Team (CERT-In) issued guidelines on reporting of cyber incidents. In terms of the guidelines, entities have to report such an incident within six hours of such incidents or such incidents being brought to applicable entities."





HACKER SELLING TWITTER ACCOUNT DATA OF 5.4 MILLION USERS FOR $30K

"Twitter has suffered a data breach after threat actors used a vulnerability to build a database of phone numbers and email addresses belonging to 5.4 million accounts, with the data now up for sale on a hacker forum for $30,000. Yesterday, a threat actor known as 'devil' said on a stolen data market that the database contains info about various accounts, including celebrities, companies, and random users.""The vulnerability allows any party without any authentication to obtain a twitter ID (which is almost equal to getting the username of an account) of any user by submitting a phone number/email even though the user has prohibitted this action in the privacy settings,"" reads the vulnerability disclosure by security researcher 'zhirinovskiy.'"

"The bug exists due to the proccess of authorization used in the Android Client of Twitter, specifically in the procces of checking the duplication of a Twitter account.""The hacker told us that you could feed email addresses and phone numbers to the vulnerability to determine if it is associated with a Twitter account and retrieve that account's ID.Since we could only verify a small number of users listed in the scraped data, it is impossible to say if all 5.4 million accounts being sold are valid.Even though most of the data being sold is publicly available, threat actors can use the email addresses and phone numbers in targeted phishing attacks.Therefore, all Twitter users should be vigilant when receiving emails from Twitter, especially if they ask you to enter login credentials, which users should only be done on Twitter.com."

Phishing Attack


Data Breach of 5.4 Million accounts


Twitter Social Media

NEW WINE, OLD BOTTLE : ABUSED QUICKBOOKS SITE SENDS PHONE SCAM EMAILS

INKY data analysts recently detected a new variant of the tried-and-true phone scam. This time, the perps abused QuickBooks, an accounting software package used primarily by small business and mid-market customers who lack in-house expertise in finance and accounting. QuickBooks is a core offering of Intuit, which fields a range of digital financial products.All versions of QuickBooks have the ability to send invoices, and in this case, the bad guys turned this capability into an attack vector for a low-tech phone scam. In the past year, phone scams have been on the rise as phishers respond to the increasing sophistication of anti-phishing defenses : defenders go high, phishers go low. A simple mechanism is a phone number that the phishers want the mark to call. When they do, an operative will try to extract valuable information from them. These attacks were highly effective at evading detection because they were identical to non-fraudulent QuickBooks notifications, even when examining the emails' raw HTML files closely. All notifications originated from authentic Intuit IP addresses, passed email authentication (SPF and DKIM) tests for intuit[.]com, and only contained high-reputation intuit[.]-com URLs.In these scams, a recipient was presented with an invoice or order confirmation indicating that their credit card had already been charged and that if they wished to dispute the charge, they should contact the phone number in the email. Once a victim called, a scammer attempted to extract information (login credentials, credit card info, other personally identifiable information) or directed them to a spoofed site to extract it.

Phone Scan Email Attack


Personal Information Compromise


Social Media

DATA BREACH AT PFC USA IMPACTS PATIENTS OF 650 HEALTHCARE PROVIDERS

Just ahead of the 4th of July weekend, accounts receivable management firm Professional Finance Company (PFC USA) started sending out data breach notification letters to patients of over 650 healthcare providers across the country. The information that might have been accessed by the attackers includes names, addresses, birth dates, accounts receivable balance and payments information, Social Security numbers, and health insurance and medical treatment information. PFC did not say how many individuals were potentially impacted in the data breach, but it did share a list of impacted healthcare providers, which contains a total of 657 entries.

The ransomware attack on PFC appears to be part of a trend where cybercriminals are not targeting healthcare providers directly, but turn on their partner organizations instead. The data of more than 2.2 individuals was likely compromised in a cyberattack at eye care management software solutions provider Eye Care Leaders, and patient care guidelines provider MCG Health announced last month that the data of 1.1 million individuals was compromised.

VERIFIED TWITTER ACCOUNTS HACKED TO SEND FAKE SUSPENSION NOTICES

Threat actors are hacking verified Twitter accounts to send fake but well-written suspension messages that attempt to steal other verified users' credentials. Twitter verifies accounts if they are considered notable influencers, celebrities, politicians, journalists, activists, and government and private organizations. To receive the verified 'blue badge,' Twitter users must apply for verification and submit supporting documentation to show why their account is 'notable.' As it is not easy to gain a blue badge, threats of suspension can lead to people reacting without thinking, making them prime targets for threat actors who value these types of accounts for their own scams. These scams are not only being sent to verified users but they are being sent by verified users whose accounts were hacked, likely through similar phishing scams. It is also common to see users, including verified users, post to Twitter that they fell for a phishing attack, even when some of the victims are involved in cybersecurity. Threat actors continue to evolve their tactics to make their attacks look legitimate, and by targeting verified users, they add a sense of urgency that may cause people to overlook suspicious signs. Therefore, if you receive a message directing you to a site where they ask for your credentials, always take your time analyzing it for strange domain names, unusual typos, and bad grammar. To be safe, only log in with your Twitter credentials on twitter.com and never on any other site.

MORE THAN 4,000 INDIVIDUALS' MEDICAL DATA LEFT EXPOSED FOR 16 YEARS

"The private health information of more than 4,000 patients was left exposed for 16 years by a US medical transplant center. Virginia Commonwealth University Health System (VCU) announced that sensitive data belonging to both transplant donors and recipients was available to view by others on a patient portal since 2006. The healthcare provider said that 4,441 people were affected in the breach, which concerned data, including names, Social Security numbers, lab results, medical record numbers, and/or dates of birth. This information "may have been viewable" to transplant recipients, donors, and/or their representatives when they logged into the recipient's and/or donor's patient portal, VCU said. VCU has not yet released any details about how the privacy incident occurred, but said that there was no evidence that any information has been misused.

Rana said : "From the limited information out on this, it seems to be a typical case of design issue or misconfiguration, where a patient (donor or recipient) can access someone else's data without actively exploiting any weakness in the system."Patient portal is a critical part of any healthcare system, so it is surprising to see this flaw was undetected for that long. The good part is that it seems any patient has to have a valid account (donor or recipient) to be part of this incident which contains the incident in some sense." They added : "These days many health care systems are designed in way where sensitive information like SSN, DOB or other PII/PHI is either not shared at all or at least masked on the screen by default, also viewing them needs an additional step-up authentication."

CORPORATE OFFICES

Briskinfosec
No:21, 2nd Floor, Krishnama Road,
Nungambakkam, Chennai - 600034.
+91 86086 34123 | 044 4352 4537

INDIA

3839 McKinney Ave,
Ste 155 - 4920,
Dalls TX 75204.
+1 (214) 571 - 6261

USA

Imperial House 2A,
Heigham Road, Eastham,
London E6 2JG.
+44 (745) 388 4040

UK

Urbansoft, Manama Center, Entrance One,
Building No.58, No.316, Government Road,
Manama Area, Kingdom of Bahrain.
+973 777 87226

BAHRAIN

contact@briskinfose.com | www.briskinfosec.com