THREATSPLOIT
ADVERSARY REPORT

JUNE

EDITION 46

BRISK INFOSEC
CYBER TRUST & ASSURANCE

www.briskinfosec.com

INTRODUCTION

“As cybersecurity leaders, we have to create our message of influence because security is a culture and you need the business to take place and be part of that security culture.” — Britney Hommertzheim

Britney is right, that's for sure. Cybersecurity has a culture, just like any other culture. This can only be done if companies and top executives know what's going on in the world. And it's our job to make you aware of this. So, what's been going on in the past month?

An attacker only needs to be able to send messages to a victim through Zoom chat over XMPP protocol. The end of the game. Yes, Zoom is what we're talking about. The most important parts of this month's report are how and why this happened, how it has changed things, and what can be done about it.

A group of cybercrooks made hundreds of rubber clones of fingerprints, whose images they copied along with name & Aadhar card from south of Haryana. This news has shocked all of us. How cybercrooks are exploiting others and vulnerable population.

Razor pay were unable to reconcile receipt of 7,38,36,192 against 831 transactions.Only to realise that a cyberfraudster is manupulating the authorisation process of payment gateway to authenticate 831 failed transaction. Razor pay attorney has filed the suit & police is looking for the fraidster. Razor pay is ISO 27001, SOC2, PCI DSS certified, yet, this happens. No one is safe oline, we can only harden the security layer.

These are the most important parts of this month's report. Aside from that, you should care about 23 other pieces of news. Another important story is that someone broke into Ferrari's subdomain to make fake NFTs. This month's news comes from many different fields. From the government, to health to airlines. We see that no one is safe online and that all industries are at risk.

To ensure that you get the most out of your read here, we've done all in our power to help you. Distribute this issue to anybody you think would benefit from it, whether they be coworkers, friends, or business partners. We wish you a safe and pleasurable month of online exploration.

CONTENTS

PARKER HANNIFIN REVEALS CYBER-ATTACK EXPOSED SENSITIVE EMPLOYEE DATA

The Fortune 500 engineering giant Parker Hannifin has revealed that its networks were breached and that the personal data of its employees and their dependents may have been compromised.The company shut down "certain systems" after discovering the problem.In the course of the investigation, Parker Hannifin's IT systems were discovered to have been accessed by an unauthorised third party.Among the personal information at risk are people's names, Social Security numbers, dates of birth, addresses, driver's licence numbers, passport numbers, bank account numbers, usernames and passwords, and health insurance plan member ID numbers and coverage dates, according to the insurance firm Parker Hannifin. Records included information on coverage dates, service dates and providers as well as information on claims and medical and clinical treatment for a small percentage of those enrolled in these plans.A complimentary two-year membership to an identity monitoring service is being offered to potential victims.Security of Parker's systems and data "is critical to Parker," said Parker Hannifin. The company is working to protect its systems and data against rapidly evolving threats to company information.

UKRAINIAN HACKER JAILED FOR SELLING ACCOUNT CREDENTIALS ON THE DARK WEB

A Ukrainian hacker has been sentenced to four years behind bars for selling stolen credentials online.Ukraine, was sentenced to time in federal prison for operating a botnet designed to brute-force attack servers.Botnets are slave networks made up of compromised computers and other devices. Operators can direct these networks to slam online services with traffic, known as distributed denial-of-service (DDoS) attacks.According to the DoJ filing, Ivanov-Tolpintsev’s botnet was used to “decrypt numerous computer login credentials simultaneously”. At its peak, roughly 2,000 machines were targeted and compromised each week.-The scheme was profitable – at least, until he was caught – and prosecutors estimate that the dark web store turned over a minimum of $82,648.Ivanov-Tolpintsev was tracked to Korczowa, Poland, and was arrested by local law enforcement on October 3, 2020. He was then extradited to the US and pleaded guilty to conspiring to traffic in unauthorized access devices and computer passwords.

RUTUBE HACK: RUSSIAN VIDEO PLATFORM DENIES LOSS OF SOURCE CODE FOLLOWING CYBER-ATTACK

RuTube, a Russian video streaming service, has denied the loss of its entire source code following this week's 'Victory Day' cyberattack that brought the site to a halt.RuTube, owned by Gazprom-Media and dubbed the "Russian YouTube," claims to have 25 million active monthly users.Positive Technologies, a security firm hired by the video platform, has been working to restore access, and the incident has been "localised.Majority of the main version's database, as well as 90% of the backup and cluster to restore it, have been severely affected. It is important to understand that video hosting is petabytes of archive data and hundreds of servers. The recovery will take longer than the engineers originally anticipated

Cyber Attack

75% of database and 90% of backup is severly affected

Entertainment Sector

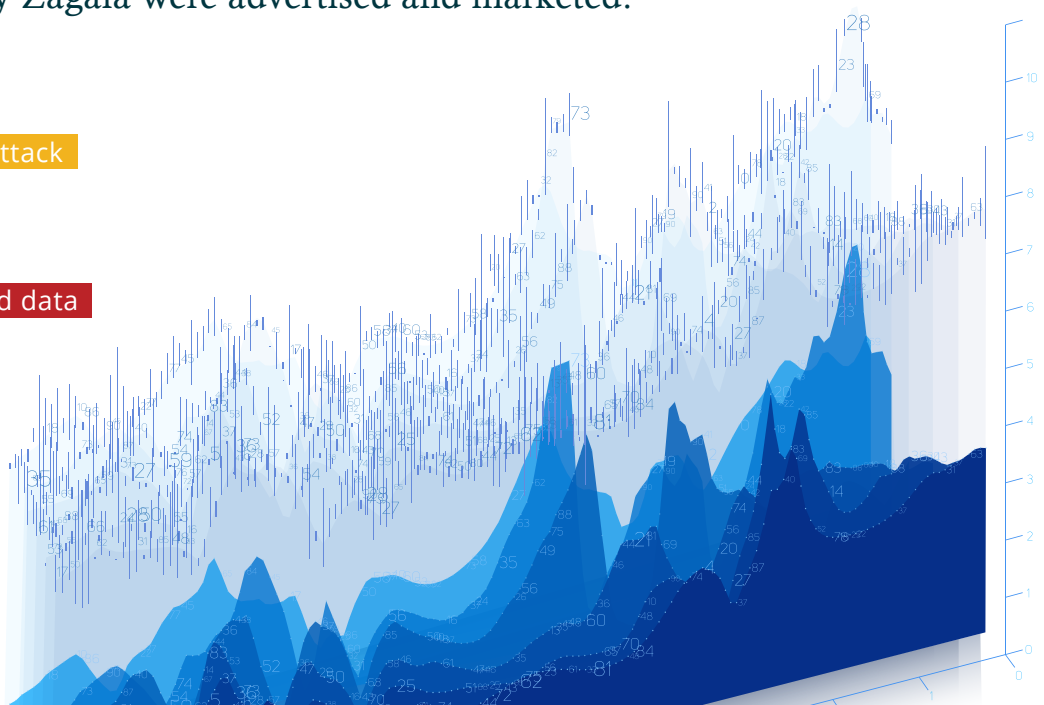
MEDICAL DOCTOR CHARGED WITH CREATING THE THANOS RANSOMWARE BUILDER

The Thanos ransomware builder was allegedly created by a former cardiologist turned malware developer.It is alleged that the untrained part-time programmer created a number of ransomware tools, malicious packages that encrypt files on a compromised system before demanding extortionate payments in exchange for a decryption key.Jigsaw v.2 was developed by Zagala before he created a more advanced private ransomware builder called Thanos.For example, a "data stealer" feature could allow attackers to steal files from infected computers using the Thanos platform, which could be used to create ransomware campaigns with custom ransom notes. He allegedly made money by selling his software to other cybercriminals and receiving payment in cryptocurrency or fiat currencies as part of the ransomware-as-a-service (Raas) scheme.In online forums frequented by cybercriminals, ransomware products allegedly offered by Zagala were advertised and marketed.

Ransomeware Attack

Stealing Files and data

Healthcare

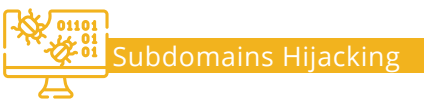


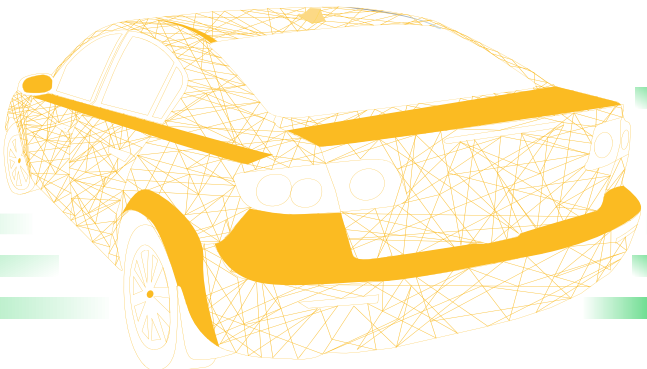
WORDPRESS SITES GETTING HACKED ´WITHIN SECONDS´ OF TLS CERTIFICATES BEING ISSUED

To take advantage of the typically short window of time before a content management system (CMS) is configured and therefore secured, attackers are taking advantage of WordPress' Certificate Transparency (CT) system.Web security standard CT monitors and audits TLS (aka SSL) certificates issued by certificate authorities (CAs) in order to verify the identity of a website's occupants.According to the standard, CAs must record all newly issued certificates on public logs right away so that rogue or misused certificates can be quickly discovered. After web administrators upload the WordPress files but before they can secure the site with a password, malicious hackers are using these log files to identify new domains and configure WordPress themselves.It is reported that a malicious file (/wp-includes/query.php) has appeared and that domains are being coerced into participating in DDoS attacks.

FERRARI SUBDOMAIN HIJACKED TO PUSH FAKE FERRARI NFT COLLECTION

"According to researchers, a subdomain belonging to Ferrari was hijacked yesterday and used to promote a scam promoting a fake Ferrari NFT collection.The fact that the luxury carmaker had previously announced plans to launch NFTs in partnership with Velas makes the scam particularly interesting.It appears that the hacked subdomain's Ethereum wallet had accumulated a few hundred dollars before it was shut down. Sam Curry, an ethical hacker and bug bounty hunter, reported seeing a Ferrari subdomain form.Ferrari is hosting a fake Non-Fungible Token (NFT) scam on its website.NFT, or Non-Fungible Token, is data that has been signed by a digital certificate to prove that it is unique and cannot be replicated on a cryptocurrency blockchain.Ferrari and Velas announced last year that they would be launching NFT products together, making this scam all the more convincing.The rapid adoption of NFTs by artists selling their digital art for cryptocurrency on well-known websites such as Rarible and OpenSea is largely responsible for the general public's interest in NFTs.Beeple, a digital artist, recently sold a piece of artwork for $69 million at Christie's auction. Fraud involving NFTs is a relatively new phenomenon, but it is already on the rise."



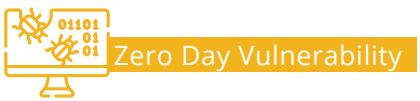


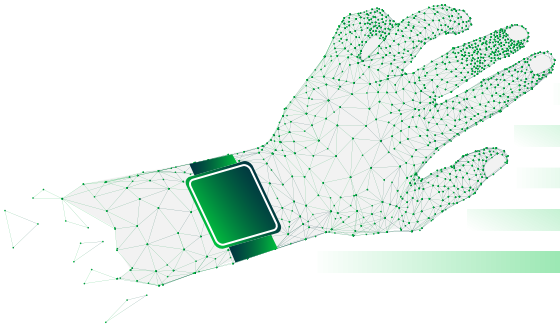
DATA BREACH AT US HEALTHCARE PROVIDER ARCARE IMPACTS 345,000 INDIVIDUALS

Healthcare provider ARcare has admitted to a data breach that could affect 345,000 people in Arkansas, Kentucky, and Mississippi.In a data breach alert published by ARcare, which provides discounted medical care in underserved communities via medical centres, pharmacies and school-based clinics, "ARcare experienced a data security incident that impacted its computer systems and caused a temporary disruption in services," reads a data breach alert published by ARcare. Names, Social Security numbers, driver's licence or state ID numbers, birth dates, financial account information, medical treatment, prescription, medical diagnosis or condition, and health insurance information were among the potentially exposed data.“ARcare is reviewing and updating existing data protection and security policies and procedures,” the alert states.Potentially impacted individuals are encouraged to "review account statements, explanations of benefits, and free credit reports for suspicious activity and errors"

APPLE EMERGENCY UPDATE FIXES ZERO-DAY USED TO HACK MACS, WATCHES

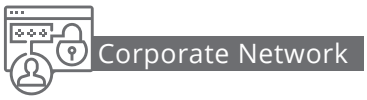
Apple released security updates to address a zero-day vulnerability threat actors can exploit on Macs and Apple Watches. Zero-days are software security flaws that haven't been patched.This type of vulnerability may have publicly available proof-of-concept exploits or be actively exploited before a patch isreleased.Using the AppleAVD (a kernel extension for audio and video decoding) flaw (CVE-2022-22675), apps can execute arbitrary code with kernel privileges.Apple fixed the bug with improved bounds checking in macOS Big Sur 11.6, watchOS 8.6, and tvOS 15.5.Apple Watch Series 3 or later, Macs running macOS Big Sur, Apple TV 4K, Apple TV 4K (2nd generation), and Apple TV HD are all affected.Apple disclosed reports of active exploitation in the wild but provided no additional details. That way, attackers won't be able to use the zero-day exploits in other attacks before Apple releases the security updates to as many Apple Watches and Macs as possible.This zero-day was probably only used in targeted attacks, but it's still important to install today's macOS and watchOS security updates to block attacks.





CRITICAL FLAW IN ZYXEL FIREWALLS GRANTS ACCESS TO CORPORATE NETWORKS (CVE-2022-30525)

"Several models of Zyxel firewalls have a critical vulnerability (CVE-2022-30525) and an exploitable Metasploit module. CVE-2022-30525 allows unauthenticated, remote attackers to inject OS commands via vulnerable firewalls' administrative HTTP interface (if exposed on the internet), allowing them to modify files and execute OS commands. With a reverse-engineered patch and a Metasploit module available, the 16,000+ vulnerable devices discovered by Shodan may be targeted in the coming weeks and months, possibly by initial access brokers.Administrators of affected devices should upgrade to V5.30 firmware as soon as possible.“This tends to only help active attackers, and leaves defenders in the dark about the true risk of newly discovered issues,” said Baines. "



FLUBOT SPREADS VIA SMS CAMPAIGNS TO TARGET FINNISH PEOPLE

Finland's National Cyber Security Center (NCSC-FI) warned of FluBot SMS and MMS attacks.NCSC-FI said this campaign sent thousands of malicious messages.Using voicemail links, missed call notifications, or alerts about incoming money from an unknown financial transaction to lure Android users.Likewise, iPhone users are redirected to premium subscription frauds and other scams. Apparently, attackers are not leaving any opportunity to make money after a successful infection.The links in these messages direct victims to a website hosting the FluBot APK, which they're urged to download and install. FluBot infects Android devices by overlaying phishing pages on banking and cryptocurrency apps.In order to steal regular login credentials, malware can access SMS data, make phone calls, and monitor incoming notifications.

SHAREPOINT RCE BUG RESURFACES THREE MONTHS AFTER BEING PATCHED BY MICROSOFT

A security researcher found a new way to exploit a recently patched deserialization bug in Microsoft SharePoint.The flaw uses SharePoint's site creation features to upload and run malicious files on the server.Many languages serialise and deserialize complex objects for servers and processes.An adversary can send malicious objects to the server if the deserialization process is insecure.StarLabs' Nguyn Tin Giang (Jang) discovered that certain SharePoint server configurations are vulnerable to deserialization attacks that lead to RC. By sending a render request for the uploaded file, the attacker will trigger the bug and execute the payload on the server.“A successful attack may give the attacker the ability to get code execution in the target server with privilege of running w3wp.exe process”

Insecure Deserialization

Remote Code Execution

Microsoft Company

CRITICAL FLAW IDENTIFIED IN F5 BIG-IP DEVICES

"BIG-IP networking devices contain a critical RCE, CVE-2022-1388.Attackers can bypass authentication and run commands on the device with elevated privileges via the BIG-IP iControl REST authentication component.The vulnerable devices are mostly used in enterprises and may allow attackers to access networks and spread to other devices.This vulnerability affects only the internet-facing device's management. Multiple researchers have created exploits for this F5 BIG-IP flaw. Researchers spent two days creating the exploit and expect attackers to find the root cause easily.This exploit allows threat actors to gain root access to devices. 2,500 internet-connected devices pose a risk to businesses. F5 has already released BIG-IP security updates that admins can apply for certain firmware versions. The devices running 11.x and 12.x firmware versions will not receive security updates. Further, the firm has released three mitigations (1, 2, 3) for those who cannot upgrade their BIG-IP devices."

F5-BIG IP Vulnerability

Internet facing device management is affected

Microsoft Company

NERBIAN RAT SPREADS VIA EMAILS IN ONGOING ATTACKS

Nerbian, a RAT, has been seen spreading via email.A technical report names the malware based on a named function in its code.The malware campaign impersonates WHO, according to Proofpoint.Hackers send COVID-19 to targets.It's written in Go and can avoid detection and analysis.Malicious emails contain RAR attachments with malicious Word macros.A bat file opens a 64-bit PowerShell dropper when opened in Office with content enabled. MoUso-Core[.]exe is Nerbian RAT's C:ProgramDataUSOSharedlocation download.Attackers use a Golang-based dropper named UpdateUAV[.]exe, packed in UPX to keep file sizes small.The RAT can be configured with only the required functions by its operators.It has an encrypted keylogger and a screen capturing tool for all major OS platforms.All C2 server communications use SSL.All data exchanges are encrypted to avoid in-transit network scanning tool inspection. Nerbian RAT is a complex malware that focuses on stealth with various checks and encrypted communications. At present, it is spread via low-volume email campaigns that could be changed in the future. Thus, deploy anti-phishing solutions and email gateways to stay protected.

HACKER STEALS ₹7.3 CRORE FROM PAYMENT GATEWAY COMPANY RAZORPAY IN BENGALURU

An estimated 7.3 crore rupees were stolen over the course of three months by tricking the payment gateway company into authenticating 831 rejected transactions. By manipulating a payment gateway company's authorization process to authenticate 831 failed transactions, a hacker stole a total of 7.3 crore over three months.Officials with Razorpay Software Private Limited discovered the fraud while auditing the transactions.

Reconciling 831 transactions with 738,362,192 receipts proved impossible.Razorpay Software Private Limited provides online payment services that allow Indian businesses to collect payments via credit card, debit card, net banking, and wallets. The police are trying to track down the hacker based on online transactions. An internal probe carried out by Razorpay Software Private Limited found that some person, or persons, had tampered, altered and manipulated the ‘authorisation and authentication process’. As a result, false ‘approvals’ were sent to Razorpay against the 831 failed transactions, resulting in a loss amounting to 7,38,36,192. The details of the 831 failed transactions, including the date, time, and IP address, were provided to the police by Razorpay Software Private Limited."Razorpay's payment gateway is at par with the industry standards on data security," a Razorpay spokesperson claimed in a statement.Unauthorized actors with malicious intent used the browser to tamper with authorization data on some merchant sites that were using an older version of Razorpay's integration because of gaps in their payment verification process.

The company is ISO 27k, PCI-DSS and SOC 2 compliant, it applies end-to-end transaction data security features, combined with strong authentication and authorization protocols to protect businesses from potential threats.Razorpay has proactively taken steps to mitigate the issue permanently and eliminate future occurrences. The company has already recovered part of the amount and is proactively working with the relevant authorities for the rest of the process."


Authorization Bypass


INR 7.3 Crores theft


Payment Gateway Company

FINGERPRINT CLONING GANG BUSTED IN HARYANA, 5 ARRESTED : POLICE

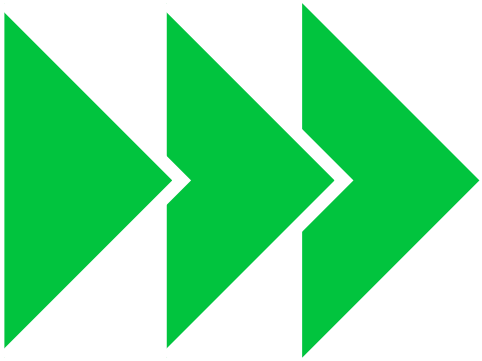
"On Monday, the Haryana Police announced that it had broken up a gang that allegedly used fingerprint cloning to steal money from bank accounts belonging to people who use the Aadhaar Enabled Payment System (AEPS).

According to a statement released by the Haryana Police, five members of the gang, including a woman, were arrested following raids on various locations in Delhi and Palwal on Monday. Other items found by the police include 11 debit cards from various banks, 270 SIM cards from various operators, fingerprint rubber stamp machine and 5 bottles of photo polymer. They also found one printer and a Laminator (out of which 10 copies used in online fraud) 220 fingerprint clones, 68 blank Aadhaar cards, 21 PAN cards, 64 passport-size photos, 5 Aadhaar cards, 1 pen drive, etc.There had been complaints in Palwal district from some people about money being withdrawn without any transactions, he said.An official report shows that from May 24 to June 2, 2021, the police have recorded 43 cases of online fraud. According to the spokesperson, fraudsters have attempted to obtain documents needed to commit fraud from registry office employees. A private individual in Palwal Tehsil who did registry document binding for the scammers was contacted and copies of the registry documents were obtained at a high cost after they had failed to do so. As a result, ""they used fingerprint clones to withdraw up to 10,000 in amounts from various prepaid wallets and committed online fraud worth crores of rupees,"" he stated.Investigation and disclosure statements have revealed that the gang has been implicated in all 43 cases. "


Sensitive Data Exposure


Personal Data Exposed


Banking Sector



SPICEJET FACES RANSOMWARE ATTACK : MORNING FLIGHTS IMPACTED

Systems of the budget carrier SpiceJet faced a ransomware attack on Tuesday night due to which morning flight departures were impacted. It further said that the situation has been rectified and flights are operating normally now. The airline confirmed the development in a tweet. SpiceJet tweeted, “Certain SpiceJet systems faced an attempted ransomware attack last night that impacted and slowed down morning flight departures today. Our IT team has contained and rectified the situation and flights are operating normally now.”The airline operates a fleet of 91 planes, 13 of which are Boeing 737 MAX models and the other 46 are older models.CMD Ajay Singh said in an email to his employees on the 17th anniversary of SpiceJet that the airline aims to begin offering broadband internet service onboard.We will continue to expand our network this year with new products and routes, according to Singh in an email obtained by PTI.Recently, SpiceClub, our wonderful loyalty programme, launched a co-branded credit card, and we hope to launch a broadband internet service onboard our aircraft soon." He added that SpiceJet’s route network will also be expanded to include unique destinations in India and around the world.

ZOOM PATCHES XMPP VULNERABILITY CHAIN THAT COULD LEAD TO REMOTE CODE EXECUTION

"Zoom users are advised to update their clients to version 5.10.0 to patch a number of holes found by Google Project Zero security researcher Ivan Fratric.""User interaction is not required for a successful attack. The only ability an attacker needs is to be able to send messages to the victim over Zoom chat over XMPP protocol,"" Fratric said in a bug tracker description of the chain.If a specially crafted message was sent, Fratric was able to trigger clients into connecting to a man-in-the-middle server that served up an old version of the Zoom client from mid-2019.The CVE-2022-22786 vulnerability that allowed for downgrading the client only impacted Windows users, while the other three issues -- CVE-2022-22784, CVE-2022-22785, and CVE-2022-22787 -- impacted Android, iOS, Linux, macOS, and Windows.Fratric discovered the vulnerabilities in February, with Zoom patching its server-side issues the same month, and releasing updated clients on April 24."

CRITICAL FLAWS IN JUPITER WORDPRESS PLUGIN

"The Jupiter Theme and JupiterX Core WordPress plugins have been found to have a number of security flaws, according to the researchers.Attackers can take control of compromised websites by exploiting a critical flaw in the system's privilege escalation mechanism, which has been publicly disclosed.An authenticated user or attacker can gain administrative privileges using the exposed plugins, which are tracked as CVE-2022-1654 and have a CVSS score of 9.9 (critical). The Jupiter Theme and JupiterX Core WordPress plugins have been found to have a number of security flaws, according to the researchers.Attackers can take control of compromised websites by exploiting a critical flaw in the system's privilege escalation mechanism, which has been publicly disclosed.An authenticated user or attacker can gain administrative privileges using the exposed plugins, which are tracked as CVE-2022-1654 and have a CVSS score of 9.9 (critical). Multiple critical vulnerabilities have been discovered in WordPress plugins recently, which are already being exploited. Further, one of these new vulnerabilities is critical, allowing any logged-in user to obtain administrator privileges. Thus, users are recommended to keep their machines up-to-date with the latest security patches."

MALICIOUS PYPI PACKAGE OPENS BACKDOORS ON WINDOWS, LINUX, AND MACS

Cobalt Strike beacons and backdoors are being dropped on Windows, Linux and macOS systems by a malicious Python package that has been discovered in the PyPI registry.You can use PyPI to share your work with the community and benefit from the contributions of others, by downloading functional libraries. PyPI was infected with a malicious package named 'pymafka' on May 17, 2022, according to threat actors.PyKafka, a popular Apache Kafka client with over 4 million downloads on the PyPI registry, shares a name with this project.There were only 325 downloads of the typo-squatted package before it was removed.In spite of that, it could still have a significant impact on those who are affected because it provides access to the developer's internal network. Sonatype discovered pymafka and reported it to PyPI, who removed it yesterday.

Nevertheless, developers who downloaded it will have to replace it immediately and check their systems for Cobalt Strike beacons and Linux backdoors.

Malware Attack | Internal Networks Compromised | Information Technology

NEW UNPATCHED BUG COULD LET ATTACKERS STEAL MONEY FROM PAYPAL USERS

Security researchers claim to have discovered a vulnerability in PayPal's money transfer service that allows attackers to trick victims into unknowingly completing attacker-directed transactions with a single click.When a user is tricked into clicking on seemingly innocent webpage elements like buttons in order to download malware, redirect to malicious websites, or reveal sensitive information, this technique is known as "UI redressing," or "clickjacking." This is typically achieved by displaying an invisible page or HTML element on top of the visible page, resulting in a scenario where users are fooled into thinking that they are clicking the legitimate page when they are in fact clicking the rogue element overlaid atop it."Thus, the attacker is 'hijacking' clicks meant for [the legitimate] page and routing them to another page, most likely owned by another application, domain, or both," security researcher h4x0r_dz wrote in a post documenting the findings.

In this case, an attacker could use an iframe to transfer funds from a victim's PayPal account to an attacker-controlled PayPal account with the click of a button.An even more worrying aspect of this hack is its potential impact on websites that use PayPal as a means of payment, allowing a malicious actor to deduct arbitrary amounts from the accounts of users. "There are online services that let you add balance using PayPal to your account," h4x0r_dz said. "I can use the same exploit and force the user to add money to my account, or I can exploit this bug and let the victim create/pay Netflix account for me!"

Payment Hijacking | Remote Code Execution | Payment Gateway Company

HIGH-SEVERITY BUG REPORTED IN GOOGLE'S OAUTH CLIENT LIBRARY FOR JAVA

Google last month addressed a high-severity flaw in its OAuth client library for Java that could be abused by a malicious actor with a compromised token to deploy arbitrary payloads.Tracked as CVE-2021-22573, the vulnerability is rated 8.7 out of 10 for severity and relates to an authentication bypass in the library that stems from an improper verification of the cryptographic signature."The vulnerability is that the IDToken verifier does not verify if the token is properly signed," an advisory for the flaw reads."Signature verification makes sure that the token's payload comes from a valid provider, not from someone else. An attacker can provide a compromised token with custom payload. The token will pass the validation on the client side."The open-source Java library, built on the Google HTTP Client Library for Java, makes it possible to obtain access tokens to any service on the web that supports the OAuth authorization standard.Google, in its README file for the project on GitHub, notes that the library is supported in maintenance mode and that it's only fixing necessary bugs, indicative of the severity of the vulnerability.Users of the google-oauth-java-client library are recommended to update to version 1.33.3, released on April 13, to mitigate any potential risk.

US CAR GIANT GENERAL MOTORS HIT BY CYBER-ATTACK EXPOSING CAR OWNERS' PERSONAL INFO

Last month's credential stuffing attack on General Motors (GM) exposed customer information and allowed hackers to redeem reward points for gift cards, the company said in a statement on Wednesday.As of April 11-29, 2022, GM said they had discovered the malicious login activity.Following up on the [DATE] email we sent to you, we want to let you know about an incident involving the identification of recent redemptions of your reward points that appear to be without your authorization.In a cyber-attack known as "credential stuffing," a hacker obtains credentials from a previous data breach on one service and uses them to try to log in to another unrelated service.When asked about a separate data breach notification, GM said, "Based on the investigation to date, there is no evidence that log-in information was obtained from General Motors."Unauthorized parties gained access to compromised customer login credentials from other non-GM sites, and then reused those credentials on the customer's GM account, according to the company. The personal information of affected customers includes first and last names, personal email addresses, home addresses, usernames and phone numbers for registered family members tied to the account, last known and saved favorite location information, currently subscribed OnStar package (if applicable), family members' avatars and photos (if uploaded), profile pictures and search and destination information.Information such as vehicle mileage, service history, emergency contact details and Wi-Fi hotspot settings are also at risk from hacking (including passwords).

People affected by this breach were advised to request credit reports from their banks and, if necessary, put a security freeze on their accounts.GM has also admitted that hackers were able to redeem customer reward points for gift cards in some cases.GM has an online platform that helps owners of Chevrolet, Buick, GMC, and Cadillac vehicles manage their bills and redeem reward points.GM also stated that it would be reimbursing rewards points to all of its customers.

Credential Stuffing | Personal Data Breach | Automobile Industry

142 MILLION MGM RESORTS RECORDS LEAKED ON TELEGRAM FOR FREE DOWNLOAD

Several databases belonging to the breach monitoring service DataViper were reportedly stolen by a hacker known as NightLion.MGM Resorts had a database with the personal information of 142 million customers in it.It was initially sold for $2,900 on seized Rainforums, but now reports reveal that the same database of 142 million records has been shared on Telegram and can be downloaded for free by the general public.The hotel and entertainment company MGM Resorts International is based in Las Vegas, Nevada.The company has hotels in both China and the United States.One should be aware that Telegram groups have recently become a source of data leaks.Some 21 million users of SuperVPN, GeckoVpn and ChatVpn have had their personal information leaked earlier this month on several Telegram groups.According to VPNMentor researchers, who discovered the data on 22 May 2022, four archives of files containing 8.7GB of data were found.The exact number of people affected by this leak is currently unknown, but estimates put the number at between 30 million and 40 million.

Sensitive Data Exposure | 142 Million customers sensitive data breach | Hotel and Entertainment Company

HACKERS CAN HACK YOUR ONLINE ACCOUNTS BEFORE YOU EVEN REGISTER THEM

Many popular websites like Instagram, LinkedIn, Zoom, WordPress, and Dropbox all had vulnerabilities that could be exploited by hackers before you even registered your account.At least 35 popular online services were found to be vulnerable to account pre-hijacking attacks, according to a study by Microsoft Security Response Center researcher Andrew Paverd and independent security researcher Avinash Sudhodanan. These attacks vary in type and severity, but they all stem from poor security practices on the side of the websites themselves.As some vulnerable websites run bug bounty programs, it is surprising and worrying to see that such elementary attacks are still possible against their users."The impact of account pre-hijacking attacks is the same as that of account hijacking. Depending on the nature of the target service, a successful attack could allow the attacker to read/modify sensitive information associated with the account (e.g., messages, billing statements, usage history, etc.) or perform actions using the victim's identity (e.g., send spoofed messages, make purchases using saved payment methods, etc.).

Hijacking Attack | Account Hijacking | Information Technology

WIDESPREAD SWAGGER-UI LIBRARY VULNERABILITY LEADS TO DOM XSS ATTACKS

Swagger-UI is vulnerable to account takeover because of a web security flaw. More than 60 incidents have been reported to impacted organisations.Several bug bounty programmes were alerted, including those run by PayPal, Shopify, Atlassian, Microsoft, GitLab, and Yahoo.In order to better understand and interact with APIs and their resources, SmartBear Software created the Swagger-UI open source suite.All browsers are supported, and the UI is generated automatically with support for Swagger 2.0 and OAS 3.0, making it completely independent. Swagger-UI is vulnerable to account takeover because of a web security flaw. More than 60 incidents have been reported to impacted organisations.Several bug bounty programmes were alerted, including those run by PayPal, Shopify, Atlassian, Microsoft, GitLab, and Yahoo.In order to better understand and interact with APIs and their resources, SmartBear Software created the Swagger-UI open source suite.All browsers are supported, and the UI is generated automatically with support for Swagger 2.0 and OAS 3.0, making it completely independent.

DOM Cross Site Scripting | Account Takeover | Information Technology

CORPORATE OFFICES

INDIA

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

USA

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

UK

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

BAHRAIN

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

contact@briskinfose.com | www.briskinfosec.com