THREATSPLOIT ADVERSARY REPORT

BRISK INFOSEC

CYBER TRUST & ASSURANCE

www.briskinfosec.com

Edition 50

OCTOBER 2022

Editorial

"The web is not written with a pencil, but with a pen. Think before you post ". Yes, it does. It leaves a footprint that bad people can use to their advantage and scan networks. Welcome to the Threatsploit report for the month of October. Let me tell you what you can expect. Let's start,

Optus, which is owned by Singapore Telecommunications Ltd, said last week that one of the biggest data breaches in Australia exposed the personal information of up to 10 million customers, or about 40% of the country's population. Names, addresses, driver's license numbers, and passport numbers are all part of this. This could leave them vulnerable to phishing scams.This could make people more vulnerable to a phishing attack.

Second, Uber, the most wellknown city transportation company in the world, said it had been hacked. This was big news because the bad guy stole the credential and used an MFA fatigue attack to get into the system and mess with it. Uber did everything that had to be done and has set the record straight about how safe the data is.

Third, the email account of an employee at the American airline has been used to steal information. The information has been stolen. Airlines and other wellknown companies are still on the hackers' radar every month.

Fourth, hackers still want to get their hands on health care data. This time, they broke into New York's ambulance service system. Health care information is sold on the dark web for many hundreds of dollars. Healthcare problems still exist.

Last but not least, the appordering customers of Starbuck Singapore were hacked to get their information. This was found out when the information was verified on the dark web. These are just a few of the other news stories that were chosen for this month's therats-ploit. We ask you to read these stories and share them with your coworkers, friends, and family. Because making people aware is the only way to win the war against bad people. I hope you have a safe month online.

Contents

Uber links breach to Lapsus$ group, blames contractor for hack

Uber thinks that the hacker who caused the breach last week is part of the Lapsus$ extortion group, which is known for hacking Microsoft, Cisco, NVIDIA, Samsung, and Okta.The company also said that the attacker used the stolen credentials of an Uber EXT contractor in an MFA fatigue attack where the contractor was flooded with two-factor authentication (2FA) login requests until one of them was accepted. "From there, the attacker accessed several other employee accounts which ultimately gave the attacker elevated permissions to a number of tools, including G-Suite and Slack," Uber explained in an update to the original statement."The attacker then posted a message to a company-wide Slack channel, which many of you saw, and reconfigured Uber's OpenDNS to display a graphic image to employees on some internal sites."

The company added that it found no evidence that the threat actor could access production systems that store sensitive user information, including personal and financial data (e.g., credit card numbers, user bank account info, personal health data, or trip history).Uber says our codebase and have not found that the attacker made any changes. We also have not found that the attacker accessed any customer or user data stored by our cloud providers (e.g. AWS S3)." Unfortunately, the intrusion resulted in some confidential information being accessed, including some of Uber's invoices from an internal tool used by the company's finance team and HackerOne vulnerability reports. "However, any bug reports the attacker was able to access have been remediated," the company said. HackerOne has since disabled the Uber bug bounty program, thus cutting off access to the disclosed Uber vulnerabilities.

MFA fatigue attack

Account Takeover

Transportation Mobility

Revolut hack exposes data of 50,000 users, fuels new phishing wave

Revolut has suffered a cyberattack that gave an unauthorized third party access to personal information of tens of thousands of clients.Revolut is a financial technology company that has seen a rapid growth, now offering banking, money management, and investment services to customers all over the world.According to the breach disclosure to the State Data Protection Inspectorate in Lithuania, where Revolut has a banking license, 50,150 customers have been impacted.Based on the information from Revolut, the agency said that the number of affected customers in the European Economic Area is 20,687, and just 379 Lithuanian citizens are potentially impacted by this incident.

Details on how the threat actor gained access to the database have not been disclosed but it appears that the attacker relied on social engineering. However, in a message to an affected customer, Revolut says that the type of compromised personal data varies for different customers. Card details, PINs, or passwords were not accessed. Revolut emphasizes that the intruder did not gain access to users' funds. "Our customers' money is safe - as it has always been. All customers can continue to use their cards and accounts as normal," the company spokesperson said.

Cyber Attack

Data Leakage of 50000 users

Financial Technology

American Airlines discloses data breach after employee email compromise

"Attackers broke into an unknown number of employee email accounts and got access to sensitive personal information, which American Airlines has told its customers about.""We found out in July 2022 that an unauthorised person had hacked into the email accounts of a small number of American Airlines employees,"" the airline told customers who were affected.""When we found out about the incident, we locked down the affected email accounts and hired a third-party cybersecurity forensic firm to find out what happened and how big it was.""Personal information like names, dates of birth, mailing addresses, phone numbers, email addresses, driver's licence numbers, passport numbers, and/or certain medical information may have been exposed during the attack and could have been viewed by the threat actors.The airline said it would give customers who had their identities stolen a free two-year membership to Experian's IdentityWorks service to help them find and fix the problem.The company hasn't said how many customers were affected or how many email accounts were broken into."

Phishing Atack

Data Breach

Aerospace

Russian Sandworm hackers pose as Ukrainian telcos to drop malware

Sandworm, a Russian government-backed hacking group, has been seen posing as telecommunication providers in order to send malware to Ukrainian organisations.The US government says that Sandworm is part of the Russian GRU foreign military intelligence service, which is a threat actor backed by the government.The APT hacking group is thought to have been behind a number of attacks this year, including one on Ukrainian energy infrastructure and the use of a persistent botnet called "Cyclops Blink.Even though Sandworm has made a lot of changes to its C2 infrastructure, it has done so slowly, so historical data from CERT-UA reports let Recorded Future strongly link current operations to the threat actor.The attack starts by getting people to visit the domains, usually by sending them emails from the domains that make it look like the sender is a Ukrainian phone company.These sites are written in Ukrainian, and they have information about military operations, government notices, reports, etc.Notably, HTML smuggling is used by a number of Russian government-backed hacking groups, such as APT29.The image file's payload is Warzone RAT, a virus that was made in 2018 and became very popular in 2019.It replaces the DarkCrystal RAT that Sandworm used in previous months.It's possible that the Russian hackers want to make it harder for security analysts to track and figure out who did what by using malware that is easy to find and hoping that their tracks will get "lost in the noise."The WarZone RAT malware is old, but it still has powerful features like a UAC bypass, a hidden remote desktop, cookie and password stealing, a live keylogger, file operations, a reverse proxy, a remote shell (CMD), and process management.

Phishing Atack

#VALUE!

Government Sector

GTA 6 source code and videos leaked after Rockstar Games hack

A hacker broke into Rockstar Games' Slack server and Confluence wiki and leaked gameplay videos and source code for Grand Theft Auto 6.Threat actor named "teapotuberhacker" posted a link to a RAR archive with 90 stolen videos. This was the first time that the videos and source code were made public.The videos look like they were made by game developers testing things like camera angles, NPC tracking, and locations in Vice City.Some of the videos also have voiced conversations between the main character and other non-playable characters.The hacker says he has stolen "GTA 5 and 6 source code and assets, and a GTA 6 testing build," but he is trying to get money from Rockstar Games to keep more information from getting out.

But the threat actor says they will take offers over $10,000 for the GTA V source code and assets, but they are not selling the GTA 6 source code right now.Since then, the leaked videos have been posted on YouTube and Twitter, and Rockstar Games has sent DMCA infringement notices and requests to take down the videos.A copyright claim from Take 2 Interactive, the company that owns Rockstar Games, says, "This video is no longer available due to a copyright claim by Take 2 Interactive."These requests to take down the videos make it more likely that they are real.

Cyber Attack

Data Theft

Gaming Sector

New York ambulance service discloses data breach after ransomware attack

Empress EMS, which is based in New York and provides emergency response and ambulance services, said that a data breach exposed customer information. After looking into what happened, it was found that the intruder got into Empress EMS's systems on May 26, 2022. About a month and a half later, on July 13, a day before the encryption was put in place, the hackers removed "a small subset of files."

The disclosure from Empress EMS says, "Some of these files had patient names, dates of service, insurance information, and in some cases, Social Security numbers." "Empress EMS is sending letters to those who were affected and offering credit monitoring services to those who qualify," the company said. The details of the attack show that it was a standard double-extortion ransomware attack, in which hackers steal files, encrypt systems, and then threaten to publish the data if the victim doesn't pay a ransom. The ransomware gang has removed the related entry from their website, but we were able to confirm that Hive published the data by looking at historical dark web data from cyber-intelligence firm KELA. Cole & Van Note, an American law firm that helps consumers, said today that they will look into the incident to see if the people who were affected can file a lawsuit or get money back.

Double-Extortion Ransomware Attack

Personal Data Breach

Healthcare

Hacker sells stolen Starbucks data of 219,000 Singapore customers

The Starbucks branch in Singapore, which is part of the well-known American coffeehouse chain, has admitted that it had a data breach that affected more than 219,000 of its customers.On September 10, a threat actor on a popular hacking forum offered to sell a database with sensitive information about 219,675 Starbucks customers. This was the first sign that they had been broken into.The owner of the hacking forum, who goes by the name "pompompurin," joined the discussion to back the validity of the stolen data. He said that the samples provided show that the data is real.Customers who have used the Starbucks mobile app to place orders or the chain's online store to buy items from one of its 125 shops in Singapore are the only ones affected by this breach.

The Starbucks branch in Singapore, which is part of the well-known American coffeehouse chain, has admitted that it had a data breach that affected more than 219,000 of its customers.On September 10, a threat actor on a popular hacking forum offered to sell a database with sensitive information about 219,675 Starbucks customers. This was the first sign that they had been broken into.The owner of the hacking forum, who goes by the name "pompompurin," joined the discussion to back the validity of the stolen data. He said that the samples provided show that the data is real.Customers who have used the Starbucks mobile app to place orders or the chain's online store to buy items from one of its 125 shops in Singapore are the only ones affected by this breach.

Sensitive Data Exposure

219,675 Customer
Sensitive Data Breach

Retail Coffee
& Snacks Store Industry

Hive ransomware claims cyberattack on Bell Canada subsidiary

"The Hive ransomware group took credit for an attack on the systems of Bell Technical Solutions, which is a division of Bell Canada (BTS). BTS is a separate branch of Bell that has more than 4,500 employees and focuses on installing Bell services for homes and small businesses in Ontario and Québec. The website for BTS, which is usually found at bellsolutionstech.ca, is currently inaccessible." "The unauthorised party accessed information that may have included the name, address, and phone number of residential and small business customers in Ontario and Québec who booked a technician visit." " Bell Technical Solutions took immediate steps to secure affected systems, and we want to reassure you that no database containing customer information like credit and debit card numbers, banking or other financial data was accessed during the incident.

After this happened, the Bell subsidiary warned its customers that they could be the target of phishing attacks and told them to keep an eye on their accounts for any strange activity." "We will tell directly anyone whose private information may have been viewed. Bell Technical Solutions is separate from Bell and uses its own IT system, so other Bell customers and Bell subsidiaries were not affected, the company said. "

Cyber Attack

Sensitive Data Exposed

Telecommunication
Company

Akamai stopped new record-breaking DDoS attack in Europe

A new distributed denial-of-service (DDoS) attack that took place on Monday, September 12, has broken the previous record that Akamai recorded recently in July.DDoS attacks are cyberattacks that flood servers with fake requests and garbage traffic, rendering them unavailable to legitimate visitors and customers. The cybersecurity and cloud services company Akamai reports that the recent attack appears to originate from the same threat actor, meaning that the operators are in the process of empowering their swarm further. On September 12, these attacks culminated at unprecedented levels when the "garbage" traffic sent to the target network peaked at 704.8 Mpps, roughly 7% higher than the July attack. Apart from the volume of the attack, the threat actors also expanded their targeting, which was previously rather narrow, focusing on the company's primary data center.This time, the threat actors spread their firepower to six data center locations in Europe and North America.Additionally, Akamai detected and blocked 201 cumulative attacks, compared to 75 in July, and recorded traffic sources from 1813 IPs, compared to 512 previously. "The attackers' command and control system had no delay in activating the multidestination attack, which escalated in 60 seconds from 100 to 1,813 IPs active per minute," comments Akamai in the report. This expansion in the targeting scope aims at hitting resources that are not prioritized as critical and thus inadequately protected but whose downtime will still cause trouble to the firm. The particular company, however, had taken precautions due to the July attack and had secured all their 12 datacenters, resulting in 99.8% of the malicious traffic being pre-mitigated.

DDOS Attack

Data Theft

Cybersecurity & Cloud Services Company

Microsoft Edge's News Feed ads abused for tech support scams

As part of an ongoing malvertising campaign, ads are being put into the Microsoft Edge News Feed to send potential victims to websites that try to trick them into paying for fake tech support.According to Statcounter's Global Stats, Microsoft Edge is the default web browser on computers that run the Windows operating system, and it has a 4.3% market share around the world.They are also adding several malicious ads to the Edge News Feed timeline. These ads are linked to more than a dozen domains, and at least one of them (tissatweb.us) has been known to host a browser lock in the past.The threat actors use the Taboola ad network to load a Base64-encoded JavaScript script that is meant to filter out people who might fall for their scams and send them to their scam landing pages.Malwarebytes explained, "The goal of this script is to only show the malicious redirection to potential victims. Bots, VPNs, and geolocations that are not of interest are shown a harmless page related to the ad instead."Malwarebytes didn't say what would happen if you called the scammers' phone number, but in most cases, they would lock your computer or tell you that your device is infected and you need to buy a support licence.In either case, once the scammers connect to your computer to help you, they will try to get you to pay for an expensive tech support contract that does nothing for you.

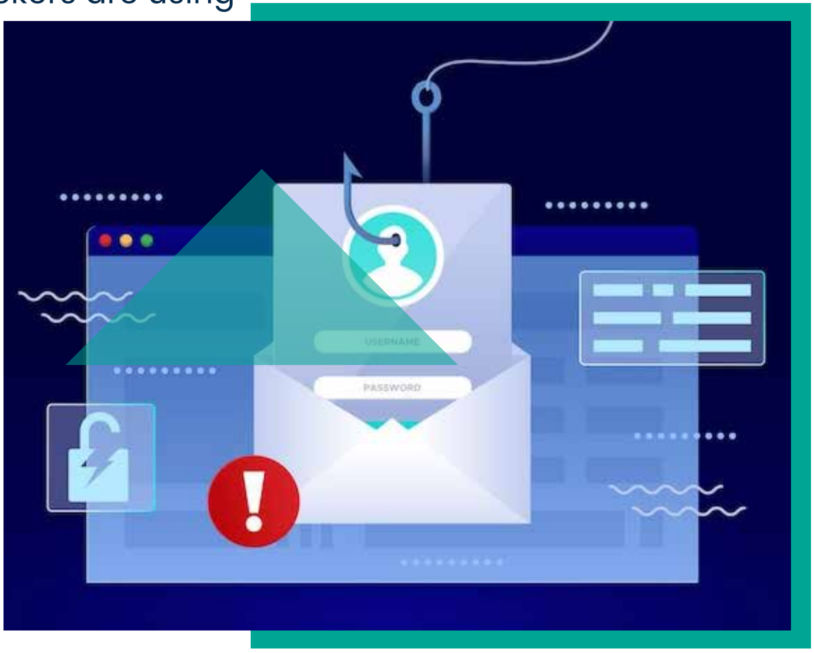
URL Redirection

Can lead to Victim Scams

IT Sector

FBI : Hackers steal millions from healthcare payment processors

The Federal Bureau of Investigation (FBI) has issued an alert about hackers targeting healthcare payment processors to route payments to bank accounts controlled by the attacker.This year alone, threat actors have stolen more than $4.6 million from healthcare companies after gaining access to customer accounts and changing payment details. Cybercriminals are combining multiple tactics to obtain login credentials of employees at payment processors in the healthcare industry and to modify payment instructions. The FBI says that it received multiple reports where hackers are using publicly available personal details and social engineering to impersonate victims with access to healthcare portals, websites, and payment information. Phishing and spoofing support centers are additional methods that help hackers achieve their goal of gaining access to entities that process and distribute healthcare payments. FBI's alert today notes that this specific threat actor activity includes sending phishing emails to financial departments of healthcare payment processors.They are also modifying Exchange Servers' configuration and setting up custom rules for targeted accounts, likely to receive a copy of the victim's messages.



Parameter Tampering

$4.6 Million Theft

Healthcare

Death of Queen Elizabeth II exploited to steal Microsoft credentials

Threat actors are using the death of Queen Elizabeth II in phishing attacks to get their targets to visit sites that steal their Microsoft account credentials. The attackers also try to get their victims' multi-factor authentication (MFA) codes so they can take over their Microsoft accounts." Messages that said they were from Microsoft invited people to a "artificial technology hub" in her honour," the Threat Insight team at Proofpoint said today. In the campaign seen by Proofpoint, the phishing actors pretend to be "the Microsoft team" and try to get the recipients to add their memo to an online memory board " in memory of Her Majesty Queen Elizabeth II."

After clicking on a button in the phishing email, the target is taken to a phishing landing page where they are asked to enter their Microsoft credentials. "Messages had links to a URL that went to a page that collected Microsoft email credentials, including MFA," said Proofpoint. The attackers use a new reverse-proxy Phishing-as-a-Service (PaaS) platform called EvilProxy, which is advertised on clearnet and dark web hacking forums. This platform lets low-skill threat actors steal authentication tokens to get around MFA. The National Cyber Security Centre of the United Kingdom warned on Tuesday that cybercriminals are more likely to use the Queen's death to make money through phishing and other scams.

Phishing Atack

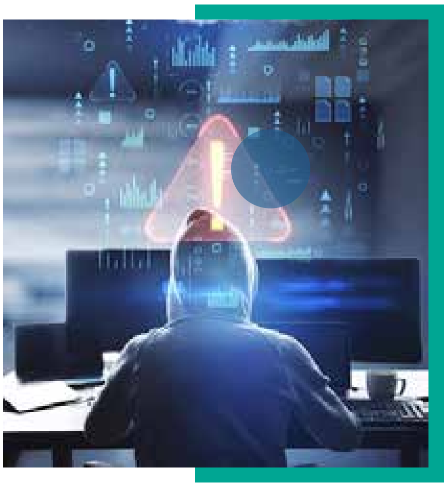
Microsoft Credentials Stolen

#VALUE!

Iranian hackers lurked in Albania's govt network for 14 months

"The Federal Bureau of Investigation (FBI) and the Computer Security and Information Analysis Center (CISA) said that one of the Iranian threat groups that attacked the Albanian government's network in July and caused damage was hiding in its systems for about 14 months." "An FBI investigation shows that Iranian state cyber actors first got into the victim's network about 14 months before launching the destructive cyber attack, which included a ransomware-style file encryptor and disc wiping malware," " the two agencies said in a joint advisory released today." "The actors had constant access to the network for about a year, going in and out of it to read and send e-mails." "The attackers were part of a threat group called" "HomeLand Justice," " which the FBI says is backed by Iran. They attacked the Government of Albania 14 months after the initial breach, shutting down multiple websites and services. This month, hackers working for the Iranian government launched a new set of cyberattacks against the Government of Albania. They used similar tactics and methods to the ones they used in July.

The joint advisory gives more technical information about the bad things HomeLand Justice did inside Albania's government network. For example, it used a hacked Microsoft Exchange account to find and steal a lot of credentials and data. Following the July attack, Albanian Prime Minister Edi Rama said the entire staff of the Embassy of Iran was asked to leave the country within 24 hours. The U.S. government also blamed Iran for attacking Albania in July and said the country would be held accountable for threatening the security of a NATO ally.In July 2021, U.S. President Biden warned that cyber-attacks that lead to severe security breaches could also lead to a ""real shooting war."""



Cyber Attack

Credntials & Data Theft

Government Sector

LockBit ransomware builder leaked online by "angry developer"

"A dissatisfied developer leaked LockBit's newest encryptor function Object() { [native code] }. LockBit ransomware released LockBit Black 3.0 in June after two months of testing. New anti-analysis features, a bug reward programme, and extortion tactics promised to ""Make Ransomware Great Again.""Two persons (or maybe the same person) leaked LockBit 3.0 on Twitter.

A newly registered Twitter user named 'Ali Qushji' claims their team penetrated LockBits servers and identified a LockBit 3.0 ransomware encryptor. Regardless of how the private ransomware function Object() { [native code] } was released, this is a serious blow to LockBit and the enterprise, which will see more threat actors adopting it to launch attacks.The disclosed LockBit 3.0 builder allows anyone to quickly develop executables for their own operation, including an encryptor, decryptor,and specialised tools to start the decryptor.

The builder has four files : an encryption key generator, a builder, a customizable configuration file, and a batch file to create everything.config.json' can be used to personalise an encryptor's ransom letter, configuration parameters, processes and services to terminate, and command and control server to deliver data to.By customising the configuration file, a threat actor can link the ransom letter to their own infrastructure. When the batch file is run, the builder creates all the ransomware files.This isn't the first time a ransomware function Object() { [native code] } or source code leaked online, leading to greater attacks by other threat actors. "

Cyber Attack

LockBit 3.0 Ransomware Encryptor Leaked

Information Security

Credential stuffing accounts for 34% of all login attempts

In some countries, credential stuffing assaults outpaced legal login attempts in the first quarter of 2022.This type of attack exploits "password recycling," or using the same login name and password on various sites.Once credentials are leaked or brute-forced from one site, threat actors use a credential stuffing assault to access users' accounts on other sites.Okta reported approximately 10 billion credential stuffing occurrences in the first 90 days of 2022.This statistic reflects 34% of overall authentication traffic, meaning one-third of attempts are fake.Because most of these attacks use a "burst" technique, trying many credentials quickly, afflicted platforms see abrupt load increases of up to tenfold.Recently, 200,000 North Face online shop accounts were compromised by a credential stuffing assault.Online platforms should use fingerprinting checks, proactive credential checking, proxy discovery systems, and "shadow-ban" questionable accounts to prevent credential stuffing attacks.Multi-factor authentication and strong passwords protect online accounts from most attackers.

Credential Stuffing Attack

200,000 Accounts Compromised

E-Commerce Platform

Microsoft Exchange servers hacked via OAuth apps for phishing

"Microsoft says a threat actor used credential stuffing to gain access to cloud tenants hosting Microsoft Exchange servers and deploy malicious OAuth apps and send phishing emails. The Microsoft 365 Defender Research Team found that the threat actor used insecure administrator accounts to acquire first access to high-risk accounts without MFA." Unauthorized cloud access allowed the actor to develop a malicious OAuth application that introduced a malicious inbound connection to the email server. Attacker used inbound connector and transport rules to transmit phishing emails through compromised Exchange servers. As a defence evasion strategy, threat actors erased the malicious inbound connector and all spam transport rules.

Amazon SES and Mail Chimp are used to deliver bulk marketing emails. Throughout the attack, the attacker used a network of single-tenant apps.Redmond shut down all apps linked to this network, delivered alerts, and recommended remediation to all affected consumers. Microsoft said this threat actor ran phishing attempts for years. The attacker also sent large amounts of spam emails quickly by connecting to mail servers from rogue IP addresses or sending directly from legitimate cloud-based bulk email infrastructure. Microsoft said the actor used bogus sweepstakes spam emails to lure recipients into submitting credit card data and signing up for recurring subscriptions."

Credential Stuffing Attack

Microsoft Servers Hacked

Information Security

Hackers stealing GitHub accounts using fake CircleCI notifications

GitHub warns about a phishing campaign that began on September 16 and impersonates CircleCI.The false messages say the user terms and privacy policy have changed and recipients must sign into their GitHub account to accept the changes and continue using the services. Threat actors want to steal GitHub credentials and 2FA codes through reverse proxies.Multi-factor authentication (MFA) hardware keys protect accounts from this attack."While GitHub itself wasn't touched, the campaign affected several victim organisations," GitHub said Wednesday. CircleCI placed a message on its forums to increase awareness of the malicious effort, emphasising that the platform would never ask users for passwords to read terms of service modifications. Phishing domains mirror official CircleCI domains (circleci.com). Threat actors produce personal access tokens (PATs), authorise OAuth apps, and sometimes add SSH keys to accounts to remain after a password reset. GitHub reports almost rapid exfiltration from private repositories. They employ VPN or proxy services to evade detection.If the hijacked account has organisation management permissions, hackers create additional user accounts for persistence.

Phishing Atack

Github Accounts Compromised

CircleCI integration and delivery platform

Unpatched 15-year old Python bug allows code execution in 350k projects

"A 15-year-old Python vulnerability that affects 350,000 open-source repositories can lead to code execution. The vulnerability is in the Python tarfile package, in code that uses tarfile.extract() or tarfile.extractall (). It's a path traversal flaw that lets attackers overwrite files. Researchers at Trellix uncovered the vulnerability in thousands of open and closed source programmes. Researchers scanned 257 repositories expected to have susceptible code and manually verified 175 of them.

This showed 61% were vulnerable. An automatic assessment on the remaining repositories boosted the number of affected projects to 65%, indicating a broad problem. However, the limited sample set provided as a baseline for estimating all afflicted GitHub repositories. Using the 61% vulnerability rate manually validated by Trellix, there are more than 350,000 susceptible repositories, many of them used by machine learning technologies (e.g. GitHub Copilot) that help developers complete a project faster. In addition to highlighting the vulnerability and its implications, Trellix provided patches for 11,000 projects. A fork of the affected repository will have the fixes. Later, they'll be included as pull requests. Because of the quantity of affected repositories, researchers expect more than 70,000 projects to be fixed in the following several weeks. To reach 100%, merge requests must be accepted by maintainers."

Remote Code Execution

350,000 Projects Leads to code execution

Github Repositories

LinkedIn Smart Links abused in evasive email phishing attacks

"Phishers utilise LinkedIn's Smart Link function to bypass email security and send users to phishing pages that steal payment information. LinkedIn Sales Navigator and Enterprise members can send up to 15 documents using a single trackable link.

Smart Link generates data about who saw shared content and for how long. Using Smart Link, phishing actors can evade email security safeguards and obtain data about their campaigns' efficacy, allowing them to refine their lures. The phishing email sent to targets purports to be from Slovenská pota, Slovakia's state-owned postal service, and requests payment for a pending parcel dispatch. Using email header trickery, the address appears authentic to the receiver, but if studied closely, the sender is ""sis.sk@augenlabs.com,"" unrelated to the post office.

The embedded ""confirm"" button has a LinkedIn Smart Link URL with alphanumeric variables to redirect to a phishing page.

Threat actors utilise the redirection capability in Smart Links to bypass security checks.The shipping cost on the landing page isn't excessive, set to €2.99, but the phishers want the target's credit card number, holder's name, expiration date, and CVV. Visitors who enter their information and click ""submit"" will be sent to a final SMS code confirmation page to add validity. While this continuing campaign targets Slovakians, broader phishing criminals may soon abuse LinkedIn Smart Link. "

URL Redirection

Stealing Payment Information

Business Platform

Hive ransomware claims attack on New York Racing Association

The Hive ransomware operation claimed responsibility for an attack on the New York Racing Association (NYRA), which earlier announced that a cyber breach on June 30, 2022, compromised member data.NYRA operates Aqueduct, Belmont, and Saratoga racetracks. According to security breach notices issued late last month and released with authorities last week, threat actors may have exfiltrated member information including : The data breach notices contain information on how to enrol in Experian's 24-month identity protection programme, which NYRA pays for. No modifications have been made to the calendar, and race betting continues as usual. The association's website remains inaccessible, indicating that the attack hasn't been fully mitigated.

Ransomeware Attack

Data Compromise

Sports Industry

Hackers breach software vendor for Magento supply-chain attacks

"Hackers have injected malware in multiple extensions from FishPig, a vendor of Magento-WordPress integrations that count over 200,000 downloads.Magento is a popular open-source eCommerce platform used for building electronic shops, supporting the sale of tens of billions USD worth of goods annually..Hackers injected malicious code into License.php, a file that validates licenses in premium FishPig plugins, which downloads a Linux binary (""lic.bin"") from FishPig's servers (""license.fishpig.co.uk"").

Security researchers at Sansec, a company offering eCommerce malware and vulnerability detection services, have confirmed the compromise of 'FishPig Magento Security Suite' and 'FishPig WordPress Multisite'. They say that other paid extensions from the vendor are likely compromised, too. Free extensions hosted on GitHub appear to be clean, though. The binary is Rekoobe, a remote access trojan (RAT) that has been seen in the past being dropped by the 'Syslogk' Linux rootkit.

When launching from memory, Rekoobe loads its configuration, removes all malicious files, and assumes the name of a system service to make its discovery more difficult. Eventually, Rekoobe lies dormant and waits for commands from a Latvia-based command and control (C2) server that Sans researchers located at 46.183.217.2. Sansec didn't see any action taking place, suggesting that the threat actors behind the breach were likely planning to sell access to the compromised eCommerce stores."

Supply Chain Attack

Security Suite Compromised

eCommerce Platform

Cisco confirms Yanluowang ransomware leaked stolen company data

Cisco has confirmed that the data that the Yanluowang ransomware group released was taken from the company's network in May during a cyberattack. In an update, the company says that the leak doesn't change the first conclusion that the incident won't hurt the business. Yanluowang ransomware got into Cisco's network after hackers broke into a VPN account belonging to an employee. The company says that non-sensitive files from the employee's Box folder were among the files that were stolen, and the attack was stopped before the Yanluowang ransomware could start encrypting systems. They stole thousands of files with a total size of 55GB. The cache contained classified documents, technical schematics, and source code, among other things. The hacker, however, did not show any proof. They only showed a screenshot that showed access to what looks like a system for development.Media could not check if this claim was true. When asked for a comment, Cisco said that it was impossible for the hackers to have taken any source code or gotten to it.

Ransomeware Attack

Company Data Stolen

Information Security

InterContinental Hotels Group cyberattack disrupts booking systems

InterContinental Hotels Group PLC, also known as IHG Hotels & Resorts, is a leading hospitality company. It says that its IT systems have been down since yesterday because someone broke into its network. IHG is a British multinational company that runs 6,028 hotels in more than 100 countries and is planning to build more than 1,800 more. Its brands include InterContinental, Regent, Six Senses, Crowne Plaza, Holiday Inn, and many others in the luxury, premium, and essential hotel categories. "InterContinental Hotels Group PLC (IHG or the Company) reports that parts of the Company's technology systems have been hacked." "IHG's booking channels and other applications have been severely disrupted since yesterday, and this is still going on.

"The global hotel group has hired outside experts to look into what happened and is also telling the right government agencies. Even though the company didn't say anything about what kind of attack it was, it did say that it is working to fix the systems that were affected.

Cyber Attack

Disrupted Booking System

Hospitality Company

Microsoft found TikTok Android flaw that let hackers hijack accounts

Microsoft found and reported a high severity flaw in the TikTok Android app in February that allowed attackers to "quickly and quietly" take over accounts with one click by tricking targets into clicking a specially crafted malicious link."Attackers could have leveraged the vulnerability to hijack an account without users' awareness if a targeted user simply clicked a specially crafted link," Microsoft 365 Defender Research Team's Dimitrios Valsamaras said."Attackers could have then accessed and modified users' TikTok profiles and sensitive information, such as by publicizing private videos, sending messages, and uploading videos on behalf of users."Clicking the link exposed more than 70 JavaScript methods that could be abused by an attacker with the help of an exploit designed to hijack the TikTok app's WebView.Using the exposed methods, threat actors could access or modify TikTok users' private information or perform authenticated HTTP requests."A WebView Hijacking vulnerability was found on the TikTok Android application via an un-validated deeplink on an un-sanitized parameter. This could have resulted in account hijacking through a JavaScript interface," the HackerOne report further explains.

Account Hijacking

Senstive Videos, Images Disclosed

Social Media Platform

Australia plans privacy rule changes after Optus cyber attack

Australia plans changes to its privacy rules so that banks can be alerted faster following cyber attacks at companies, Prime Minister Anthony Albanese said on Monday, after hackers targeted Australia's second-largest telecommunications firm.

Optus, owned by Singapore Telecommunications Ltd, last week revealed databases containing home addresses, drivers licences and passport numbers of up to 10 million customers - about 40% of Australia's population - were compromised in one of the biggest data breaches in the country.

Calling it "a massive breach" and "a huge wake-up call" for the corporate sector, Albanese said there were some state actors and criminal organisations who want to access people's data. The federal government is planning reforms that would require businesses to alert banks in the event customer data is compromised so that lenders can then monitor affected accounts for suspicious activity, Australian media reported.

Australia has been looking to beef up its cyber defence and in 2020 pledged to spend A$1.66 billion ($1.1 billion) over the decade to fortify network infrastructure of companies and households.

Cyber Attack

10 Million Users
Sensitive Data Breach

Telecommunications Company

“ Engagement with the Experts ”

Arul @ NCDRC event

We are pleased to announce that Arulselvar Thomas & Jaya Ram Kumar Pothi attended the National Council for Defending Rights of Children (NCDRC) convention in Coimbatore on August 26 and 27. It was exciting to watch them perform. Giving speeches that truly matter.

Jayram @ NCDRC event

We have always associated with organizations with the likes of NCDRC.This helps us understand teh trends that our domain is into & challenges that they are facing,. In turn, it helps us to educate our end clients.

Abhishek @ SRM event

If a picture is worth 1000 words. Then, a video is worth a million words ....!

Abhishek Kokate our Client Advisor had an amazing time at SRM University Ramapuram Campus. He educated the students on Cybersafety. It was important to create awareness among the young minds.

Here is a glimpse of the session.

BRISK INFOSEC

CYBER TRUST & ASSURANCE

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