EDITION - 25
2'ND ANNIVERSARY

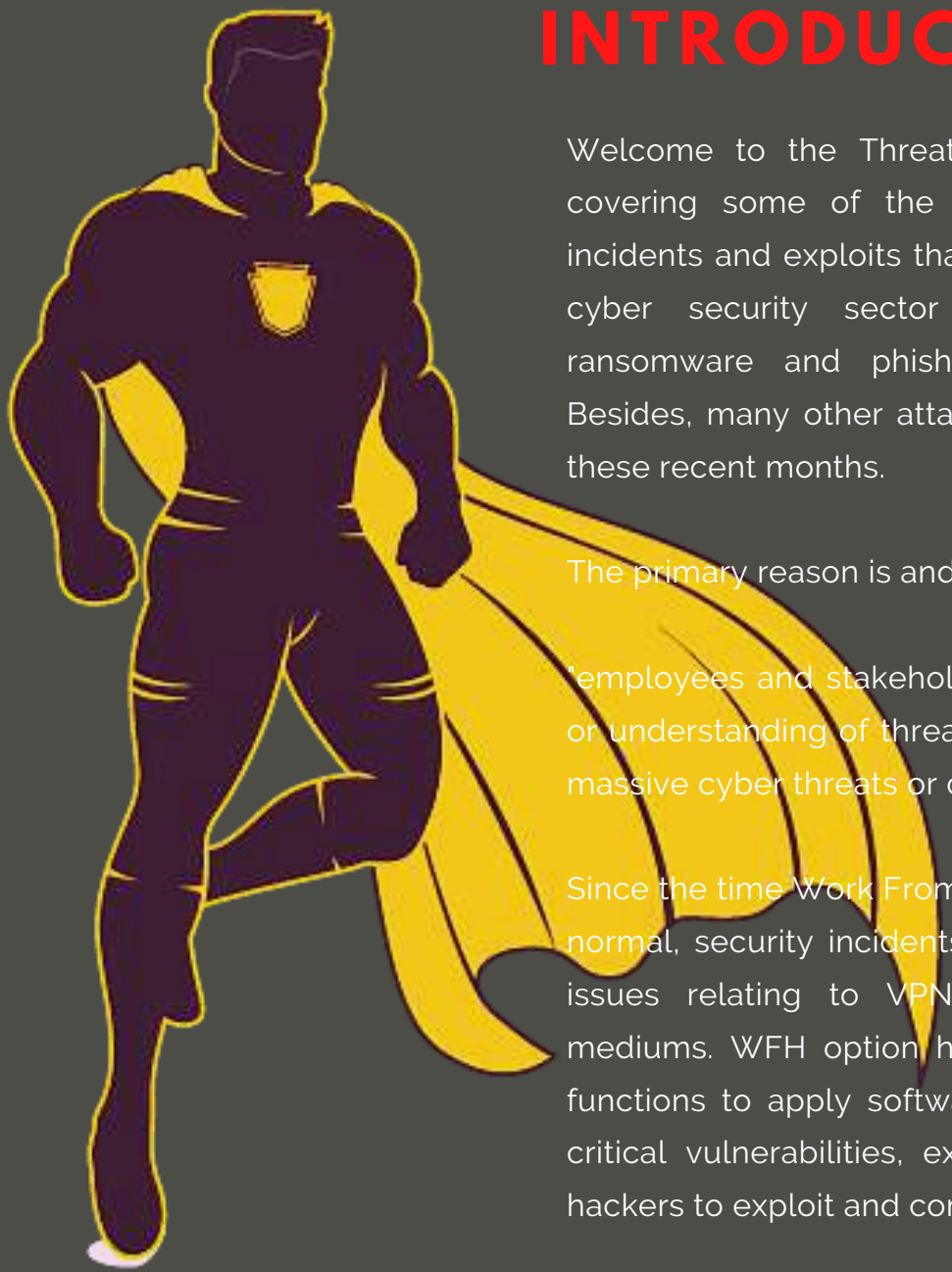
SEPTEMBER 2020

THREATSPLOIT ADVERSARY REPORT

PREPARED BY
Briskinfosec Technology

www.briskinfosec.com

THREATSPLOIT CELEBRATING 2'ND ANNIVERSARY EDITION 25



INTRODUCTION

Welcome to the Threatsploit report of September 2020 covering some of the important cyber security events, incidents and exploits that occurred this month. This month, cyber security sector witnessed a massive rise in ransomware and phishing attacks across geographies. Besides, many other attack types were seen spiking during these recent months.

The primary reason is and has always been the same….

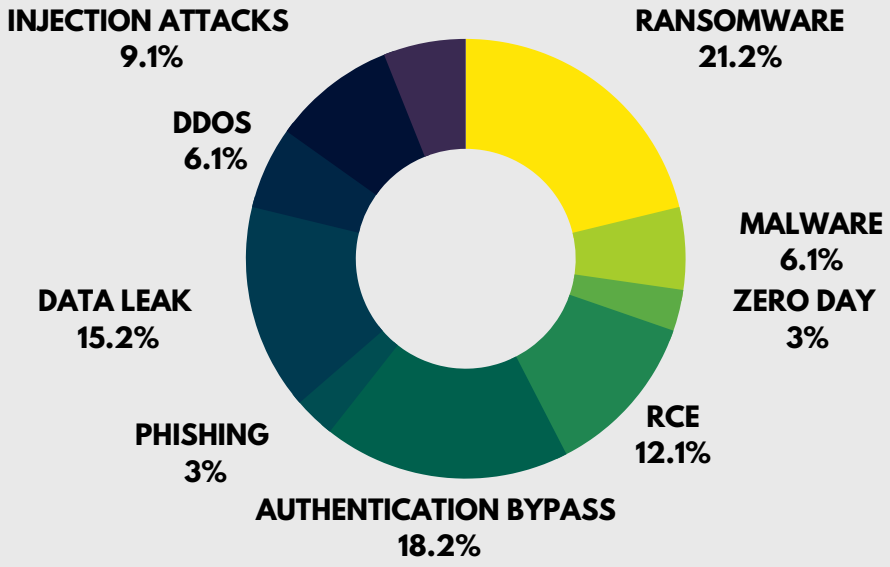
"employees and stakeholders have limited or no perception or understanding of threats and misplaced understanding of massive cyber threats or consequences".

Since the time Work From Home (WFH) has become the new normal, security incidents has peaked with more and more issues relating to VPNs and other remote connecting mediums. WFH option has further limited the ability of IT functions to apply software patches for both old and new critical vulnerabilities, exposing the information assets for hackers to exploit and compromise.

Let us walk you through some of the important security incidents that happened in the month of September 2020.

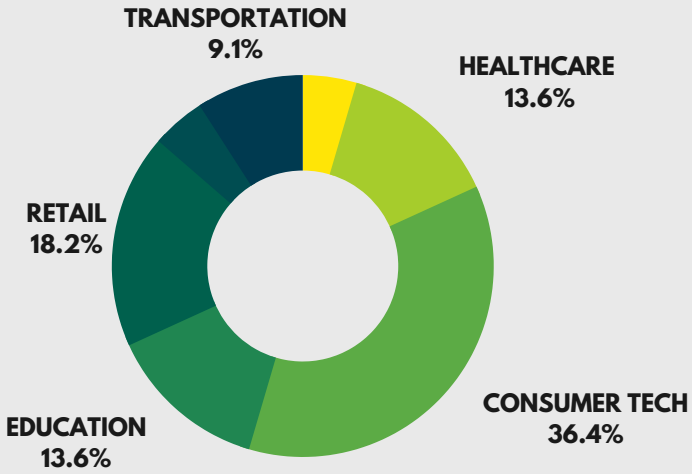
TYPES OF ATTACK VECTORS

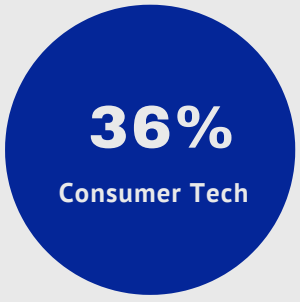
Below pie-chart indicates the percentage of nefarious cyber attacks that broke the security mechanisms of distinct organizations.



SECTORS AFFECTED BY ATTACKS

This chart shows the percentage of Industry sectors that are victim to the cyber threats. It is evident that the Consumer Technology has been hit the most.





Cyberattacks target every sector. But, a majority of them seemed to be impacting consumer technology sector (30%). To prevent any attack, organisations need the best of cyber security partners. Needless to say, Cybersecurity as a function is assuming very high importance like the Operations, Sales, Finance or Human Resources.

CONSUMER TECH

- Google Researcher Reported 3 Flaws in Apache Web Server Software
- Microsoft Issues Emergency Security Updates for Windows 8.1 and Server 2012 R2
- Critical Jenkins Server Vulnerability Could Leak Sensitive Information
- Flaws in Samsung Phones Exposed Android Users to Remote Attacks
- A New vBulletin Zero-Day RCE Vulnerability
- TeamViewer Flaw Could Let Hackers Steal System Password Remotely
- Apple Touch ID Flaw Could Let Attackers Hijack iCloud Accounts
- A Google Drive 'Feature' Could Let Attackers Trick You Into Installing Malware
- A mysterious group has hijacked Tor exit nodes to perform SSL stripping attacks
- Hacker leaks passwords for 900+ enterprise VPN servers
- Malicious npm package caught trying to steal sensitive Discord and browser files
- Experts Reported Security Bug in IBM's Db2 Data Management Software
- Critical Flaws Affect Citrix Endpoint Management (XenMobile Servers)
- Google Chrome Bug Could Let Hackers Bypass CSP Protection; Update Web Browsers
- Intel, ARM, IBM, AMD Processors Vulnerable to New Side-Channel Attacks
- Hackers Exploit Autodesk Flaw in Recent Cyberespionage Attack

EDUCATION

- Myerscough College hit by cyber attack
- University of Utah pays $457,000 to ransomware gang
- Ponca City Schools Gives Update On Ransomware Attack
- SANS Institute Phishing Attack Leads to Theft of 28,000 Records
- NCC Group admits its training data was leaked online after folders full of CREST pentest certification exam notes posted to GitHub
- Michigan State University discloses credit card theft incident

GOVERNMENT

- Thousands of Canadian Government accounts hacked

RETAIL

- Eight Million Freepik Users Suffer Data Compromise
- Warehouse management software biz SnapFulfil hit by ransomware
- security bug that can be abused to bypass PIN codes for Visa contactless payments.

HEALTHCARE

- Ransomware Attack Impacts Medical Debt Collections Firm R1 RCM
- Data Breach at Illinois Healthcare System

TRANSPORTATION

- Ransomware attack hits TFI's Canadian courier divisions
- Travel Site Exposed 37 Million Records Before Meow Attack
- Canadian delivery company Canpar Express suffered a ransomware attack
- World's largest cruise line operator discloses ransomware attack

BANKING AND FINANCE

- Experian South Africa discloses data breach impacting 24 million customers
- New Zealand Stock Exchange suffers day four disruption following DDoS attacks

CONSUMER TECH

Google Researcher Reported 3 Flaws in Apache Web Server Software

Apache recently fixed multiple vulnerabilities (CVE-2020-9490, CVE-2020-11984, CVE-2020-11993) in its web server software that could have potentially led to the execution of arbitrary code and, in specific scenarios, even could allow attackers to cause a crash and denial of service. Hence, it's essential that the patches are applied to vulnerable systems immediately after appropriate testing.

ATTACK TYPE
Arbitary code execution

CAUSE OF ISSUE
Security flaw

TYPE OF LOSS
Reputation/Data

Microsoft Issues Emergency Security Updates for Windows 8.1 and Server 2012 R2

ATTACK TYPE
Privilege escalaction

CAUSE OF ISSUE
Lack of maintenance

TYPE OF LOSS
Reputation

Microsoft has issued an emergency out-of-band software update for Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2 systems to patch two new disclosed vulnerabilities tracked as CVE-2020-1530 and CVE-2020-1537, both residing in the Remote Access Service (RAS) in a way it manages memory and file operations and could let remote attackers gain elevated privileges after successful exploitation. A patch has been released a week after and users are urged to apply it.

Critical Jenkins Server Vulnerability Could Leak Sensitive Information

A flaw in Jenkins server named CVE-2019-17638 with a critical rating of 9.4 could cause memory corruption and disclosure of significant information issues. It's recommended that Jenkins users update their software to the latest version to mitigate the buffer corruption flaw.

ATTACK TYPE
Memory corruption

CAUSE OF ISSUE
Security flaw

TYPE OF LOSS
Reputation/Data

Flaws in Samsung Phones Exposed Android Users to Remote Attacks

ATTACK TYPE
Remote attack

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

Security vulnerabilities are discovered in 'Find My Mobile' an Android app that comes pre-installed on most Samsung smartphones—that could have allowed remote attackers to track victims' real-time location, monitor phone calls, and messages, and even delete data stored on the phone. To stay safe, users are asked to uninstall this app ASAP.

CONSUMER TECH

A New vBulletin Zero-Day RCE Vulnerability

A severe zero day vulnerability traced as CVE-2019-16759 was re-identified to be active despite applying a path for it dating back to September 2019 in vBulletin software. It was found to be exploitable again as a security researcher named Austin proved that the prior applied patch was insufficient to jeopardize the exploitation. Hence, he urged for a stronger patch to be applied to fix it once and for all.

ATTACK TYPE
Zero day

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

TeamViewer Flaw Could Let Hackers Steal System Password Remotely

ATTACK TYPE
Remote attack

CAUSE OF ISSUE
Security flaw

TYPE OF LOSS
Reputation/Data

A severe vulnerability has been identified in Team viewer (CVE 2020-13699), which, if exploited, could let remote attackers steal your system password and eventually compromise it. What's more worrisome is that the attack can be executed almost automatically without requiring much interaction of the victims and just by convincing them to visit a malicious web page once. Hence, users are urged to update to latest version.

Apple Touch ID Flaw Could Let Attackers Hijack iCloud Accounts

A sever flaw resided in Apple's implementation of TouchID (or FaceID) biometric feature that authenticated users to log in to websites on Safari, specifically those that use Apple ID logins. It was also possible to abuse those domains to verify a client ID without authentication. The company has been notified on this and they are looking to fix this ASAP.

ATTACK TYPE
Authentication bypass

CAUSE OF ISSUE
Security flaw

TYPE OF LOSS
Reputation/Data

A Google Drive 'Feature' Could Let Attackers Trick You Into Installing Malware

ATTACK TYPE
Malware

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

An unpatched security weakness in Google Drive could be exploited by malware attackers to distribute malicious files disguised as legitimate documents or images, enabling bad actors to perform spear-phishing attacks comparatively with a high success rate. Needless to say, the issue leaves the door open for highly effective spear-phishing campaigns that take advantage of the widespread prevalence of cloud services such as Google Drive to distribute malware.

CONSUMER TECH

A mysterious group has hijacked Tor exit nodes to perform SSL stripping attacks

A mysterious threat actor has been adding servers to the Tor network in order to perform SSL stripping attacks on users accessing cryptocurrency-related sites through the Tor Browser. The group managed 380 malicious Tor exit relays at its peak, before the Tor team made the first of three interventions to cull this network. The issue has been observed and steps to mitigate the same are taken.

ATTACK TYPE
SSL Stripping

CAUSE OF ISSUE
Lack of maintainces

TYPE OF LOSS
Reputation/Data

Hacker leaks passwords for 900+ enterprise VPN servers

ATTACK TYPE
Data leak

CAUSE OF ISSUE
Poor security patch

TYPE OF LOSS
Reputation/Data

An anonymous hacker has published today a list of plaintext usernames and passwords, along with IP addresses for more than 900 Pulse Secure VPN enterprise servers. All the Pulse Secure VPN servers included in the list were running a firmware version vulnerable to the CVE-2019-11510 vulnerability which was exploited. Companies have to patch their Pulse Secure VPNs and change passwords with the utmost urgency as a precautionary.

Malicious npm package caught trying to steal sensitive Discord and browser files

The npm security team has removed a malicious JavaScript library from the npm portal named fallguys that provides interface to Fall guys: ultimate knockout game for designing to steal sensitive files from an infected users' browser and Discord application. The malicious package appears to have been performed reconnaissance, gathering data on victims. However, the npm security team advises that developers remove the malicious package from their projects.

ATTACK TYPE
Malicious Javascript

CAUSE OF ISSUE
Poor security pratice

TYPE OF LOSS
Reputation/Data

Intel, ARM, IBM, AMD Processors Vulnerable to New Side-Channel Attacks

ATTACK TYPE
Side channel

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

Microarchitectural attacks were actually caused by speculative dereferencing of user-space registers in the kernel, which not just impacts the most recent Intel CPUs with the latest hardware mitigations, but also several modern processors from ARM, IBM, and AMD. The "address-translation attack allows unprivileged applications to fetch arbitrary kernel addresses into the cache.

Experts Reported Security Bug in IBM's Db2 Data Management Software

A memory vulnerability in IBM's Db2 family named CVE-2020-4414 allows bad actors to perform unauthorized actions. By sending a specially crafted request, an attacker could exploit this vulnerability to obtain sensitive information or cause a DoS. The main cause is the fact that developers of IBM forget to put memory protection features. It's recommended that Db2 users update their software to the latest version to mitigate the risk.

ATTACK TYPE
DOS

CAUSE OF ISSUE
Memory vulnerability

TYPE OF LOSS
Reputation/Data

Critical Flaws Affect Citrix Endpoint Management (XenMobile Servers)

ATTACK TYPE
Privilege escalation

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
None

Citrix today released patches for 5 new security vulnerabilities affecting its Citrix Endpoint Management (CEM), also known as XenMobile, a product made for securing end users mobile devices remotely. If these aren't patched, then the hacker could gain admin privileges. Hence, users are required to apply the patches ASAP which if not, could result in severe consequences.

Google Chrome Bug Could Let Hackers Bypass CSP Protection; Update Web Browsers

A zero-day flaw tracked as CVE-2020-6519 in Chromium-based web browsers for Windows, Mac and Android that could have allowed attackers to entirely bypass Content Security Policy (CSP) rules since Chrome 73. As a result, users are urged to update their chrome version without further delay.

ATTACK TYPE
Bypass CSP protection

CAUSE OF ISSUE
Security flaw

TYPE OF LOSS
Reputation/Data

Hackers Exploit Autodesk Flaw in Recent Cyberespionage Attack

ATTACK TYPE
Unauthorized access

CAUSE OF ISSUE
Security flaw

TYPE OF LOSS
Reputation/Data

Threat actors exploited a vulnerability in the popular 3D computer graphics Autodesk software in order to launch a recent cyber-espionage attack against an international architectural and video production company. The hallmark of the attack is its use of a malicious plugin for Autodesk 3ds Max. Another key takeaway of the campaign is that it appears to have been launched by APT hacker group.

EDUCATION

Myerscough College hit by cyber attack

Myerscough College, in Billsborrow, Lancashire, said it meant staff had to email each student individually with their grades as the college was severely affected by a DoS attack and the server wouldn't be back online. Online enrolment was also affected following the attack. Due to this, the college has owed an apology to all students.

ATTACK TYPE
DOS

CAUSE OF ISSUE
Lack of maintaince

TYPE OF LOSS
Reputation/Data

University of Utah pays $457,000 to ransomware gang

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of maintainces

TYPE OF LOSS
Financial/Data

The University of Utah revealed today that it paid a ransomware gang $457,059 in order to avoid having hackers leak student information online. The university said its staff restored from backups; however, the ransomware gang threatened to release student-related data online, which, in turn, made university management re-think their approach towards not paying the attackers and out of fear, they did.

Ponca City Schools Gives Update On Ransomware Attack

Ponca City Public Schools is working with the Federal Bureau of Investigation after being hit by a ransomware attack over the weekend. The backup files on an external server. They are working to restore those files but admit it could take weeks. The district wants to stress that no student, personnel, or financial information was compromised in the attack since the effected files impacted were encrypted, not stolen.

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of awarness

TYPE OF LOSS
Reputation/Data

SANS Institute Phishing Attack Leads to Theft of 28,000 Records

ATTACK TYPE
Phishing

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

The SANS Institute has revealed that hundreds of emails from an internal account were forwarded to an unknown third party, compromising exposing nearly 30,000 records of PII (Personal Identifiable Information) through 513 emails that were forwarded to the external address. The sent malicious emails included files that contained some subset of email, first name, last name, work title, company name, industry, address, and country of residence. However, SANS quickly stopped any further release of information from the account.

NCC Group admits its training data was leaked online after folders full of CREST pentest certification exam notes posted to GitHub

ATTACK TYPE
Data leak

CAUSE OF ISSUE
Poor security pratices

TYPE OF LOSS
Reputation/Data

British infosec biz NCC Group has admitted to The Register that its internal training materials were leaked on GitHub – after folders purporting to help people pass the CREST pentest certification exams appeared in a couple of repositories inadvertently. However, they've been asked to be removed and work is put in to contain and fix this ASAP.

EDUCATION

Michigan State University discloses credit card theft incident

ATTACK TYPE
Skimming

CAUSE OF ISSUE
Website vulnerability

TYPE OF LOSS
Reputation/Data

Michigan State University (MSU) today disclosed that attackers were able to steal credit card and personal information from roughly 2,600 users of its shop.msu.edu online store through online skimming attacks. The attackers were able to inject malicious scripts designed to harvest and exfiltrate customers' payment cards after exploiting a now-addressed website vulnerability.

Thousands of Canadian Government accounts hacked

ATTACK TYPE
Credential stuffing

CAUSE OF ISSUE
Lack of awarness

TYPE OF LOSS
Reputation/Data

Thousands of user accounts for online government services in Canada were recently hacked during cyberattacks, Canadian authorities have announced due to credential stuffing attacks. These attacks, which used passwords and usernames collected from previous hacks of accounts worldwide, took advantage of the fact that many people reuse passwords and usernames across multiple accounts.

GOVERNMENT

RETAIL

Eight Million Freepik Users Suffer Data Compromise

ATTACK TYPE
Sql injection

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

Freepik, a popular platform for designers offering free graphic resources has announced that it has suffered a massive data breach affecting users on Freepik.com and Flaticon.com. According to the statement, Freepik has revealed that a hacker managed to exploit an SQL vulnerability stealing 8.3 million records from both platforms collectively. The data stolen in the breach includes email addresses and password hashes.

RETAIL

Warehouse management software biz SnapFulfil hit by ransomware

A UK cloud-based warehouse management software provider was struck by ransomware earlier this week. Emails from SnapFulfil, a trading name of Synergy Logistics, sent to its customers on how the attack targeted the company's services, disrupting warehouse operations for at least one of its customers. They've been cautioned to be aware of this incident and ensured to contain this ASAP.

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of awarness

TYPE OF LOSS
Reputation/Data

security bug that can be abused to bypass PIN codes for Visa contactless payments.

ATTACK TYPE
Bypass pin codes

CAUSE OF ISSUE
Security bug

TYPE OF LOSS
Reputation/Data

A team of academics from Switzerland has discovered a security bug that can be abused to bypass PIN codes for Visa contactless payments. This means that if criminals are ever in possession of a stolen Visa contactless card, they can use it to pay for expensive products, above the contactless transaction limit, and without needing to enter the card's PIN code. Users are cautioned to stay away from any luring messages.

HEALTHCARE

Data Breach at Illinois Healthcare System

Illinois healthcare system FHN has notified patients of a data breach. FHN stated: "The investigation was unable to determine whether the unauthorized person actually viewed any emails or attachments in the accounts. Out of an abundance of caution, we reviewed the emails and attachments contained in the email accounts to identify patient information that may have been accessible to the unauthorized person in which some sensitive info were mishandled. Efforts are being made to fix the same ASAP.

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

Ransomware Attack Impacts Medical Debt Collections Firm R1 RCM

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Poor security pratices

TYPE OF LOSS
Reputation/Data

R1 RCM, one of the largest US medical debt collections firms, recently took down its systems in response to a ransomware attack; an email hack, ransomware, malware, and COVID-19 patient data complete this week's breach roundup. The ransomware name as per reports point to the variant known as Defray that was 1st detected in 2017 that was also seen targeting the healthcare and education sectors.

TRANSPORTATION

Ransomware attack hits TFI's Canadian courier divisions

A ransomware attack hit TFI International's (NYSE:TFII) four Canadian courier divisions on Thursday, two days after the transportation and logistics company raised millions of dollars in a share offering. A ransomware attack hit TFI International's (NYSE:TFII) four Canadian courier divisions on Thursday, two days after the transportation and logistics company raised millions of dollars in a share offering.

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Unauthorized access

TYPE OF LOSS
Reputation/Data

Travel Site Exposed 37 Million Records Before Meow Attack

ATTACK TYPE
Data exposed

CAUSE OF ISSUE
Poor security practice

TYPE OF LOSS
Reputation/Data

An elasticsearch server was left unprotected in rail yatri (a travel app) that exposed 43 million travellers information in the wild. The attack had been launched by the notorious pseudo named 'meow' attacker who successfully exploited the elastic search server. Further, around 1 TB of data has been deleted and many user's data were exposed in the wild. This is reported to the concerned people and steps are taken to reduce this ASAP.

Canadian delivery company Canpar Express suffered a ransomware attack

Canadian delivery company Canpar Express experienced a ransomware attack Wednesday, and the company is investigating as customers complain about deliveries on hold. The company's website is now inaccessible. Out of an abundance of caution, we want to make our clients aware of the incident, should you be experiencing any issues... said the company.

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

World's largest cruise line operator discloses ransomware attack

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation

Carnival Corporation, the world's largest cruise ship operator, has disclosed today a security breach, admitting to suffering a ransomware attack over the weekend. The hackers accessed and encrypted a portion of one brand's information technology systems, and that the intruders also downloaded files from the company's network. The reason for this is currently unknown and an official investigation is underway to sort it out.

New Zealand Stock Exchange suffers day four disruption following DDoS attacks

ATTACK TYPE
DDOS

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

The New Zealand Stock Exchange (NZX) is still suffering from the aftermath of distributed denial of service (DDoS) attacks that hit the exchange. The exchange's website is currently offline. The NZX and Spark were hopeful markets would resume normal operations and the required work is being put to fix the same.

Experian South Africa discloses data breach impacting 24 million customers

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Poor security pratices

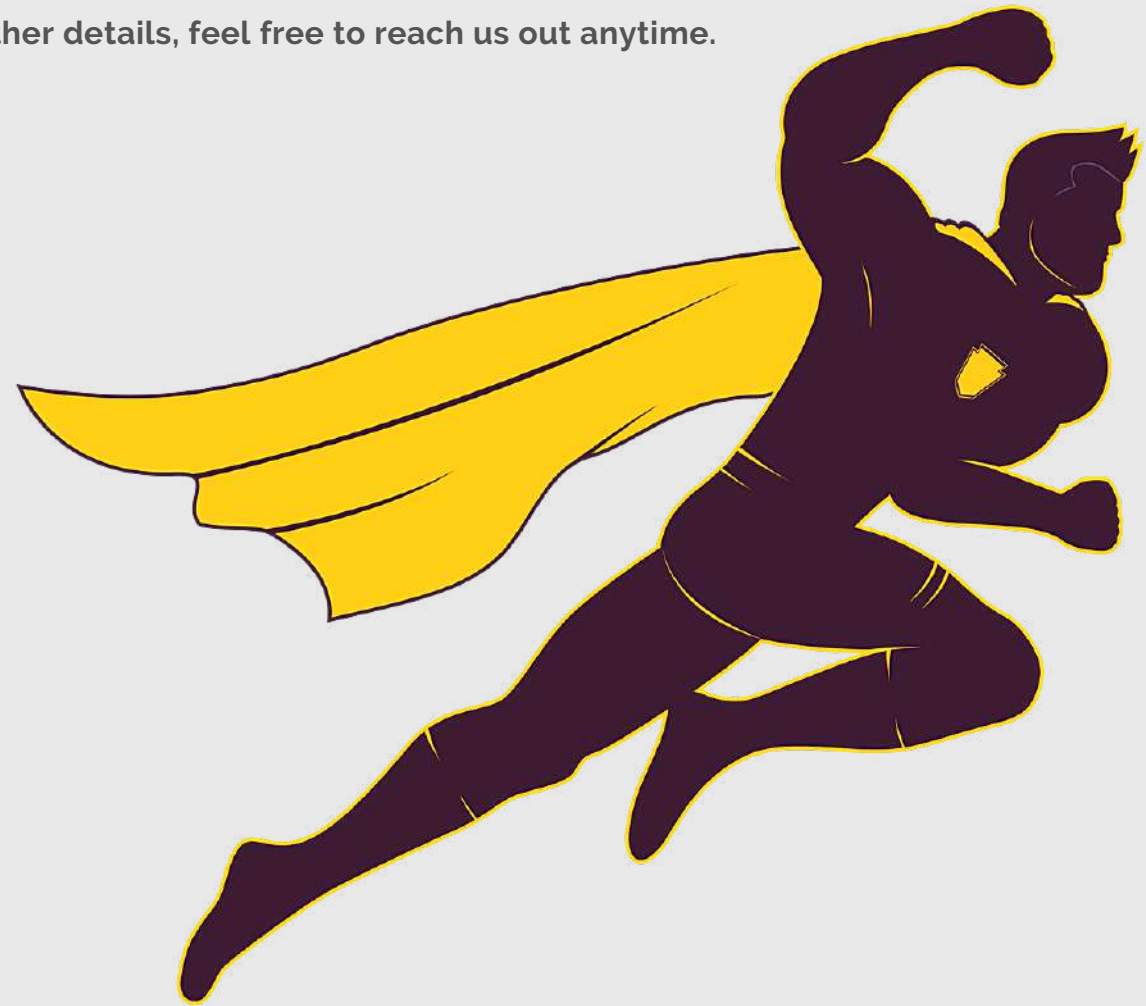
TYPE OF LOSS
Reputation/Data

The South African branch of consumer credit reporting agency Experian disclosed a data breach on Wednesday. The credit agency admitted to handing over the personal details of its South African customers to a fraudster posing as a client. The breach impacted 24 million South Africans and 793,749 local businesses. Efforts are taken to contain this mayhem ASAP.

CONCLUSION

All the attacks mentioned above - their types, the financial and reputational impacts they have caused to organizations, the loopholes that paved way for such attacks invariably causing disaster to organizations - are just like drop in an ocean. There are more unreported than that meets the eye. Even for COVID-19 vaccines are being tested globally at various stages to bring down its intensity alleviating in time as anti-vaccines are being introduced and COVID itself lost its. But, with regards to cyber threats, there is no “one-shot cure-all” type of remediation and moreover, these attack vectors show absolutely zerosymptoms of declining over time but are on the rise.The Director of CERT-IN has declared that ever sinceWork From Home began, there has been whopping 4300% increase in cyber threats, caused by phishing click baits disguising as COVID-19 protection.

Millions of organizations and individuals have clicked those links and have fallen victims to these baits of hackers. The most obvious reason being ‘lack of awareness’.Well, as the saying goes, "Prevention is better than Cure" - be it COVID-19 or Cyber threats.Briskinfosec is ready to help you in your journey to protect your information infrastructure and the assets. For further details, feel free to reach us out anytime.



REFERENCES

- https://www.dailystuff.org/2020/08/20/experts-reported-security-bug-in-ibms-db2-data-management-software/
- https://thehackernews.com/2020/08/apache-webserver-security.html
- https://portswigger.net/daily-swig/play-framework-vulnerability-could-lead-to-csrf-protection-bypass
- https://thehackernews.com/2020/08/windows-update-download.html
- https://www.infosecurity-magazine.com/news/data-breach-at-illinois-healthcare/
- https://digit.fyi/private-data-stolen-from-british-dental-association-in-latest-cyberbreach/#:~:text=The%20British%20Dental%20Association%20(BDA,of%20its%20members%20at%20risk.&text=Chief%20executive%20of%20the%20BDA,hackers%20had%20accessed%20our%20systems.
- https://https://threatpost.com/hackers-exploit-autodesk-flaw-in-recent-cyberespionage-attack/158669/thehackernews.com/2020/08/samsung-find-my-phone-hacking.html
- https://threatpost.com/citrix-warns-of-critical-flaws-in-xenmobile-server/158293/
- https://thehackernews.com/2020/08/citrix-endpoint-management.html
- https://www.malwaredevil.com/2020/08/11/google-chrome-bug-could-let-hackers-bypass-csp-protection-update-web-browsers-2/
- https://www.zdnet.com/article/security-researcher-publishes-details-and-exploit-code-for-a-vbulletin-zero-day/
- https://thehackernews.com/2020/08/teamviewer-password-hacking.html
- https://thehackernews.com/2020/08/apple-touchid-sign-in.html
- https://thehackernews.com/2020/08/foreshadow-processor-vulnerability.html
- https://www.freightwaves.com/news/breaking-news-tfi-ransomware-attack-hits-canadian-courier-divisions
- https://www.zdnet.com/article/experian-south-africa-discloses-data-breach-impacting-24-million-customers/
- https://www.infosecurity-magazine.com/news/travel-site-exposed-37m-records/?&web_view=true
- https://www.hackread.com/freepik-flaticon-data-breach-million-of-users-affected/?web_view=true
- https://montreal.ctvnews.ca/customers-complain-of-delays-after-ransomware-attack-on-delivery-company-canpar-express-1.5074228#:~:text=MONTREAL%20%2D%2D%20Canadian%20delivery%20company,only%20notice%20on%20the%20site.
- https://www.bbc.com/news/uk-england-lancashire-53822246#:~:text=A%20higher%20education%20college%20suffered,student%20individually%20with%20their%20grades.
- https://www.zdnet.com/article/university-of-utah-pays-457000-to-ransomware-gang/?&web_view=true
- https://www.warehouseautomation.ca/news-notes-1/2020/8/20/warehouse-management-software-company-snapfulfil-hit-by-ransomware
- https://www.theregister.com/2020/08/20/snapfulfil_ransomware_attack/?&web_view=true
- https://www.newson6.com/story/5f3bbf338382de1054305d50/ponca-city-schools-gives-update-on-ransomware-attack#:~:text=Ponca%20City%20Public%20Schools%20is,the%20ransomware%20attack%20on%20Saturday.
- https://www.zdnet.com/article/worlds-largest-cruise-line-operator-discloses-ransomware-attack/?&web_view=true
- https://www.securitymagazine.com/articles/93102-thousands-of-canadian-government-accounts-hacked
- https://www.thehindu.com/news/international/thousands-of-canadian-government-accounts-hacked/article32369557.ece
- https://healthitsecurity.com/news/ransomware-attack-impacts-medical-debt-collections-firm-r1-rcm
- https://www.infosecurity-magazine.com/news/sans-phishing-attack/?&web_view=true
- https://www.theregister.com/2020/08/11/ncc_group_crest_cheat_sheets/?&web_view=true
- https://thehackernews.com/2020/08/google-drive-file-versions.html
- https://www.bleepingcomputer.com/news/security/michigan-state-university-discloses-credit-card-theft-incident/?&web_view=true
- https://www.zdnet.com/article/a-mysterious-group-has-hijacked-tor-exit-nodes-to-perform-ssl-stripping-attacks/?&web_view=true
- https://www.zdnet.com/article/hacker-leaks-passwords-for-900-enterprise-vpn-servers/?&web_view=true
- https://newsd.in/pakistan-website-hacked-indian-hackers-write-ramlalla-hum-aaege-mandir-karachi-lahore-me-banaege/
- https://www.zdnet.com/article/malicious-npm-package-caught-trying-to-steal-sensitive-discord-and-browser-files/
- https://www.zdnet.com/article/academics-bypass-pins-for-visa-contactless-payments/
- https://www.bbc.com/news/53918580#:~:text=The%20New%20Zealand%20stock%20exchange,attack%20from%20abroad%2C%20on%20Tuesday.&text=Trading%20halted%20briefly%20for%20a,the%20end%20of%20the%20day.
- https://portswigger.net/daily-swig/canadian-government-services-forced-offline-after-credential-stuffing-attacks


Blog
CLICK HERE


Analyzing
Circumstances
Data
Case Study
Researcher
Knowledge
Criteria
CLICK HERE

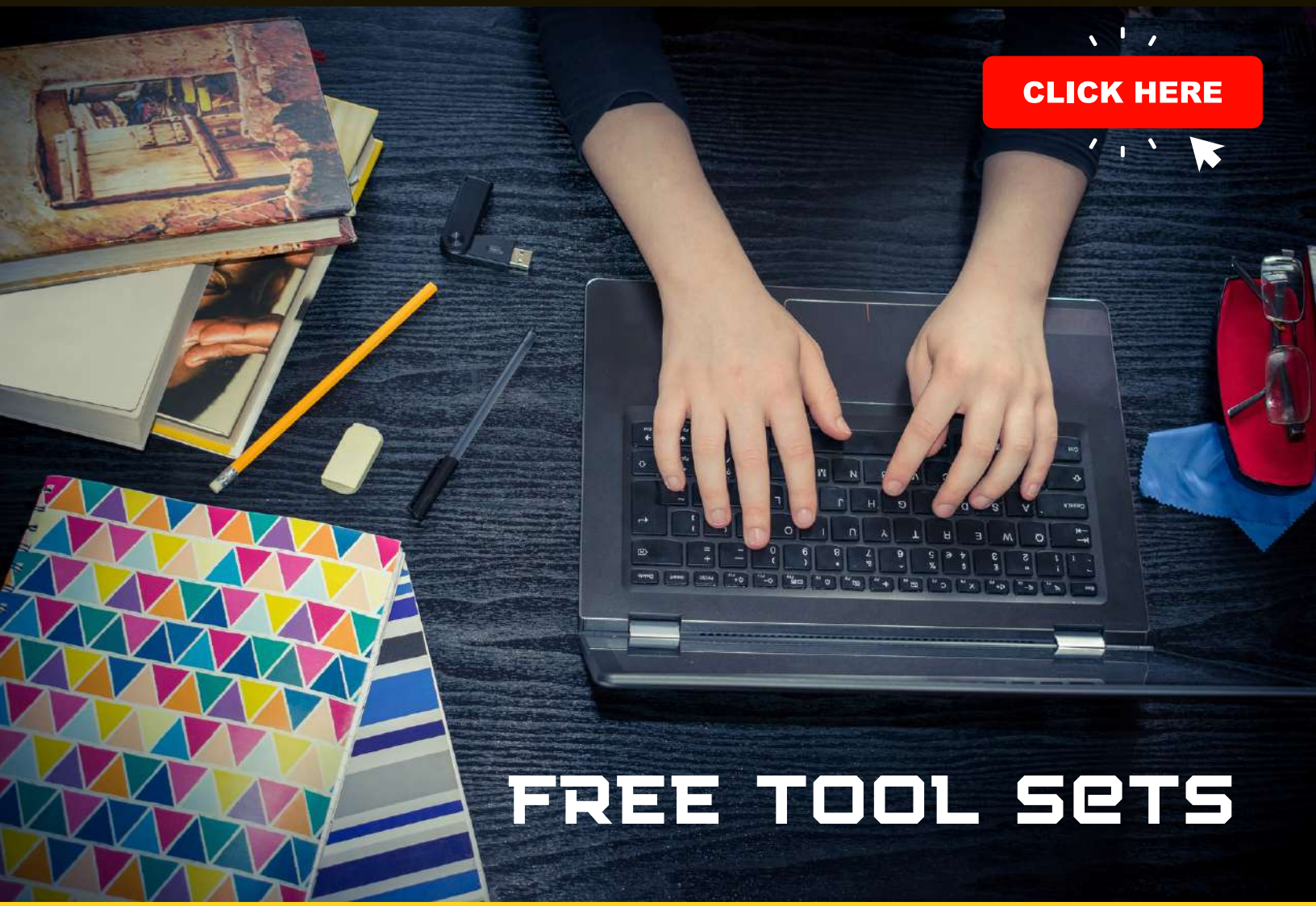
YOU MAY ALSO BE INTERESTED IN OUR PREVIOUS REPORTS

CLICK HERE

CLICK HERE

WAKE UP CXO

AN INITIATIVE BY BRISKINFOSEC



CLICK HERE

FREE TOOL SETS

FEEL FREE TO REACH US FOR ALL YOUR CYBERSECURITY NEEDS

contact@briskinfosec.com | www.briskinfosec.com