EDITION 24

AUGUST

THREATSPLOIT ADVERSARY REPORT

2020

INTRODUCTION

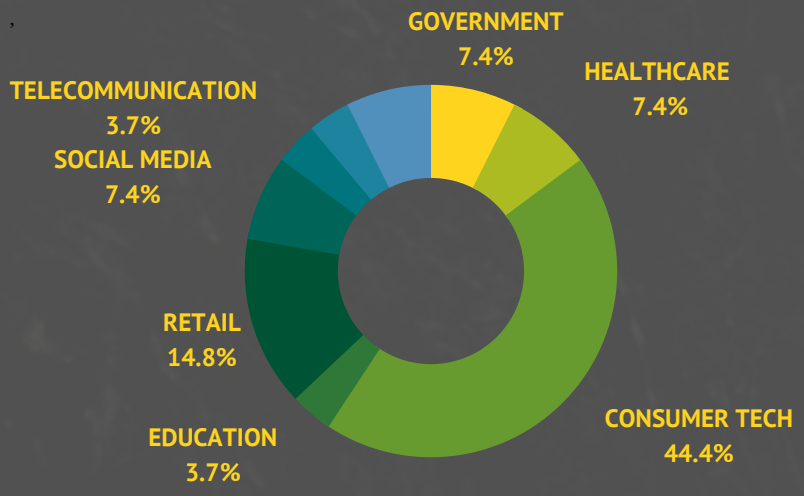
Welcome to the World of Threatsploit Adersary report which contains the global occurrence of most significant and awful cyberattacks identified by Briskinfosec during the month of JULY 2020. At this New Normal situation keeping our data and systems safe is been a great challenge for several companies. Nowadays most of the organizations are stuck in the hands of the hackers. In this Report we have compiled threats that are currently faced by several companies to give you a small walkthrough about the day today cyber issues. At present, companies are looking to have security embedded in their strategy and solutions, In order to minimize their exposure to risk as much as possible.

As many of us are settling into a routine of working from home we have to be more cautious in saving our business from the cyber criminals. As Covid 19 is a threat to human life, currently cyber attack equally threatens all Public and Private Companies. They are also not aware, if their data is safe or is been watched by the hacker. To be away from those kinds of security issues, just contact a best Security Company. As several companies have not yet decided to get back to office in this pandemic situation contacting a security company is the best way for them to keep their system and data safe. As Covid 19 is a threat to human life, currently cyber attack equally threatens all Public and Private Companies. They are also not aware, if their data is safe or is been watched by the hacker. To be away from those kinds of security issues, just contact a best Security Company.

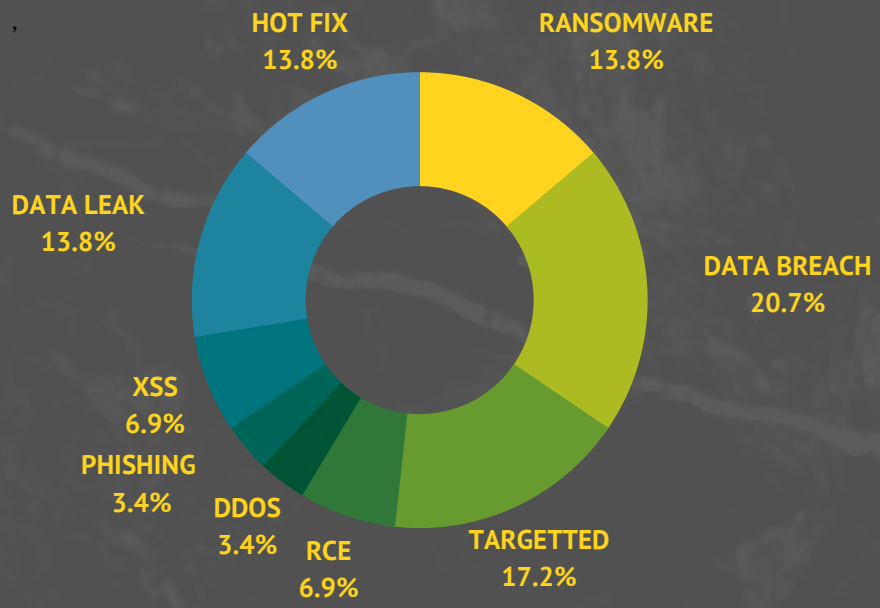
To keep their business safe companies should have cybersecurity awareness, prevention and security best practices as a part of their culture.

SECTORS AFFECTED BY ATTACKS

The below Pie-chart shows the percentage of distinctive sectors that've fallen as victims to the horrendous cyber threats. From it, it's evident that the Consumer Technology has been hit the most.



TYPES OF ATTACK VECTORS



Below, there's a bar-chart that indicates the percentage of nefarious cyber attacks that have broken the security mechanisms of distinct organizations.

Many cyberattacks initiate from various sectors. But, a majority of them seemed to have originated from consumer technology sector, holding about 44%. To prevent these, it's evident that top-notch reliable security is mandatory.

ENTERTAINMENT

- Online poker operator hit by DDoS attack
- US actor casting company leaked private data of over 260,000 individuals

SOCIAL MEDIA

- Several High-Profile Accounts Hacked in the Biggest Twitter Hack of All Time
- Chingari App (Indian TikTok Clone) Accounts Can Be Hacked Easily

RETAIL

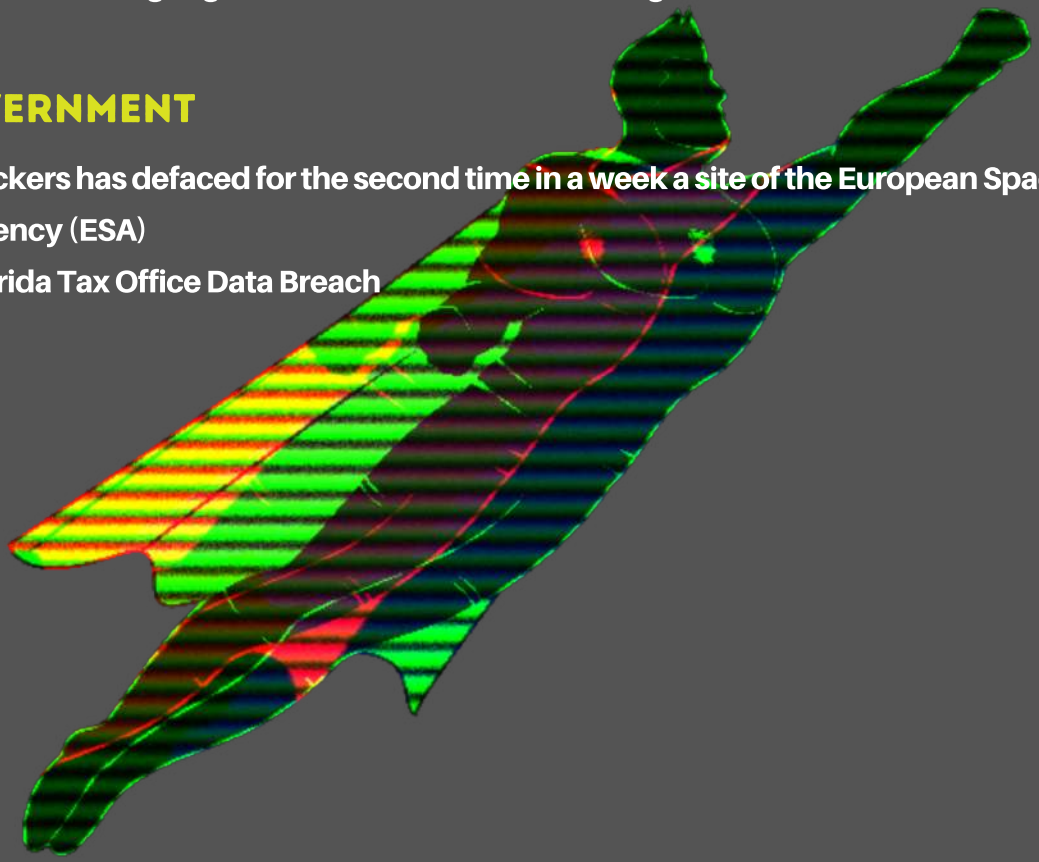
- DeepSource resets logins after employee falls for Sawfish phishing
- Seven VPN Services Including UFO VPN, Rabbit VPN, Fast VPN Leaked Over 1.2TB of Private User Data: Report
- Garmin services and production go down after ransomware attack
- Critical RCE Flaw Affects F5 BIG-IP Application Security Servers

TELECOMMUNICATION

- Orange confirms ransomware attack exposing business customers' data
- Ransomware gang demands $7.5 million from Argentinian ISP

GOVERNMENT

- Hackers has defaced for the second time in a week a site of the European Space Agency (ESA)
- Florida Tax Office Data Breach



CONSUMER TECH

- Roundcube XSS vulnerability opens the door to email account takeover
- WordPress security: RCE flaw in Adding Advertising plugin exploited in the wild
- BadPower attack corrupts fast chargers to melt or set your device on fire
- Malicious‘Blur’Photo App Campaign Discovered on Google Play
- Critical SharePoint flaw dissected, RCE details now available
- ASUS Home Router Bugs Open Consumers to Snooping Attacks
- Cisco releases security fixes for critical VPN, router vulnerabilities
- New Zealand property management company leaks 30,000 users passports, driver’s licenses and other personal data
- Data Viper Servers Hacked; Over 8,000 Databases Leaked
- Apache Guacamole Critical Vulnerabilities Put Remote Desktops at Risk
- A New Flaw In Zoom Could Have Let Fraudsters Mimic Organisations
- Adobe Issues July 2020 Critical Security Patches for Multiple Software

HEALTHCARE

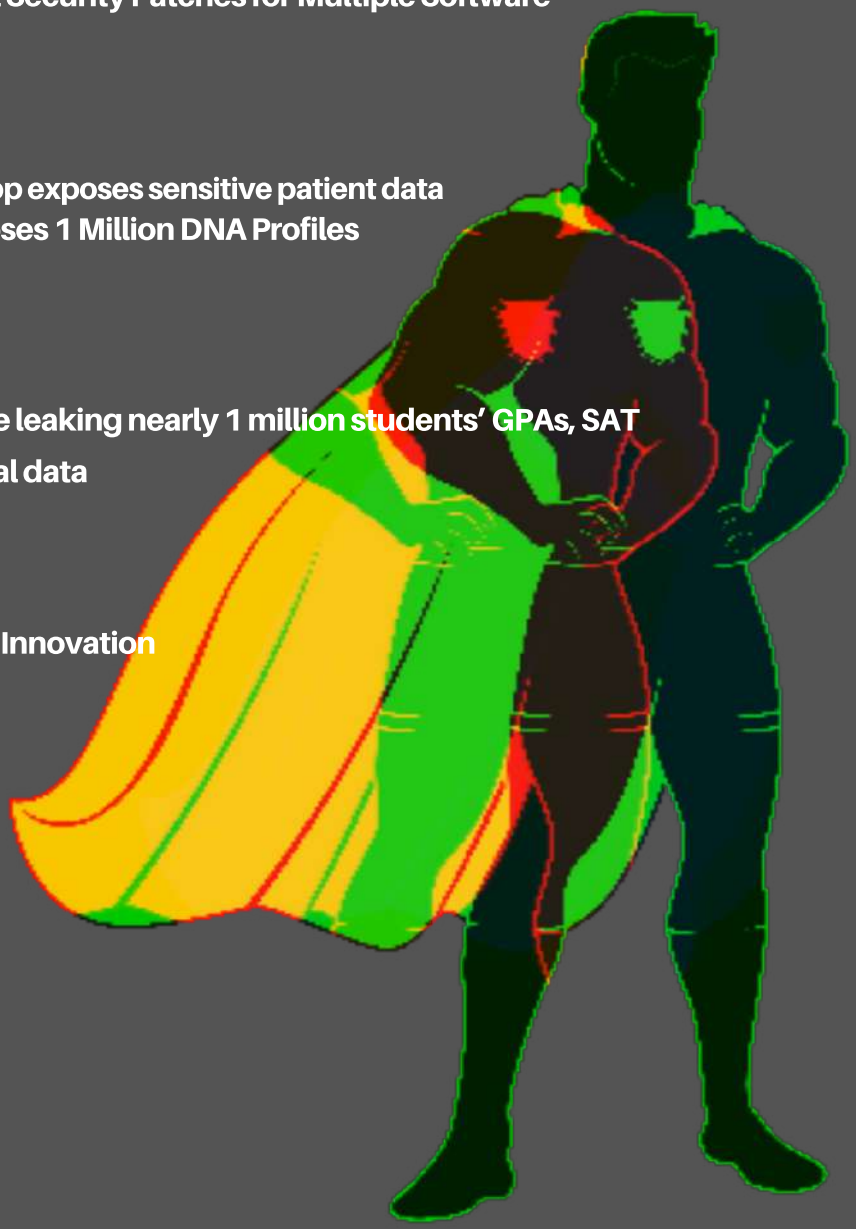
- LibreHealth medical records app exposes sensitive patient data
- Website Security Breach Exposes 1 Million DNA Profiles

EDUCATION

- College recruitment database leaking nearly 1 million students’ GPAs, SAT scores, IDs, and other personal data

OIL & GAS

- OilRig APT Drills Into Malware Innovation



ENTERTAINMENT

Online poker operator hit by DDoS attack

GGPoker a popular poker company has suffered a DDOS while conducting world poker online tournament, confirmed the officials in the organization. The organization said that they witnessed an overflowing of request load from distinct locations and this resulted in shutting down the website for 2 hours. The reason is cited as the tech team not implementing the DDoS protection service to defend against such attacks. Organization decided that fixes will be applied and affected poker players during the incident will be compensated.

ATTACK TYPE
DDos attack

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

US actor casting company leaked private data of over 260,000 individuals

ATTACK TYPE
Data leak

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

New Orleans-based MyCastingFile.com, an online casting agency that've provided actors for productions including True Detective, Pitch Perfect, NCIS: New Orleans, and Terminator Genisys faced a data breach. Their Elastic search server was discovered and left unsecured that exposed 10 million records of 260,000 users summing to 1GB size. Many sensitive information were exposed in it. The company has been notifed on this and they are yet to respond.

SOCIALMEDIA

Several High-Profile Accounts Hacked in the Biggest Twitter Hack of All Time

Several sublime twitter profiles like Joe Bide, Jeff Bezos, Bill Gates, Elon Musk, Uber, and Apple, were breached simultaneously in big hacking campaign carried out to promote a cryptocurrency scam. The broadly targeted hack posted similar worded messages urging millions of followers to send money to a specific bitcoin wallet address in return for larger payback. The twitter team acknowledged it and are working on the issue root cause.

ATTACK TYPE
Tragetted

CAUSE OF ISSUE
Lack of awarness

TYPE OF LOSS
Reputation/Data

Chingari App (Indian TikTok Clone) Accounts Can Be Hacked Easily

ATTACK TYPE
Accout takeover

CAUSE OF ISSUE
Security flaw

TYPE OF LOSS
Reputation/Data

Indian TikTok Clone Chingari App can be easily hacked without takeover on Username and Password. Chingari app has found vulnerable to a critical but easy-to-exploit authentication. This allows anyone to hack any user Chingari account and harm their information, content and the videos which are uploaded. Users of that app are asked to update to the latest version.

RETAIL

DeepSource resets logins after employee falls for Sawfish phishing

DeepSource a company that provides automated coding tools from various repositories was identified with a security breach after one of it's employees fell prey to Sawfish phishing campaign. GitHub Security team informed DeepSource that one of their employees was compromised and had his GitHub app's credentials stolen in the Sawfish phishing campaign. The affected users were notified via email.

ATTACK TYPE
Phishing

CAUSE OF ISSUE
Lack of awarness

TYPE OF LOSS
Reputation/Data

Seven VPN Services Including UFO VPN, Rabbit VPN, Fast VPN Leaked Over 1.2TB of Private User Data: Report

ATTACK TYPE
Data leak

CAUSE OF ISSUE
Phishing campaign

TYPE OF LOSS
Reputation/Data

VPN services including Fast VPN, Free VPN, Super VPN, UFO VPN, Rabbit VPN, Free VPN, and four more have been found to have leaked over 1TB of private user information. Over 30 million users data were leaked. This massive data leak could lead to phishing and fraud, blackmail, viral attack, hacking, doxing, and other forms of cybercrimes. As a precautionary, users are advised change their passwords or to switch to a more secure VPN service provider.

Garmin services and production go down after ransomware attack

Ransomware attack has struck one of the most familiar smartwatch and wearables maker, Garmin, shutting down many services and encrypting the internal network and production systems. The data sync service, aviation DB services and other production services of Garmin were highly affected. The employees called it a ransomware on their firm through social media accounts nevertheless the organization denied it. Whatsoever, official investigation is underway to fix the issue ASAP.

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
none

TYPE OF LOSS
Reputation/Data

Critical RCE Flaw Affects F5 BIG-IP Application Security Servers

ATTACK TYPE
RCE

CAUSE OF ISSUE
Security vulnerability

TYPE OF LOSS
Reputation/Data

Mikhail Klyuchnikov, a sec researchers from positive technologies discovered a vulnerability CVE-2020-5902 (a critical one) could let remote attackers take complete control of the targeted systems, eventually gaining surveillance over the application data they manage. The issue resides in a configuration utility called Traffic Management User Interface (TMUI) for BIG-IP application delivery controller (ADC). Successful exploitation of this vulnerability could allow attackers to gain full admin control.

TELECOMMUNICATION

Orange confirms ransomware attack exposing business customers' data

A French telelcommuniations firm, Orange, suffered a Nefilim ransomware attack thrugh which attackers gained access to 20 of their enterprise customers data and exposed it. As part of the ransom operators' leak, a 339MB archive file was published titled 'Orange_leak_part1.rar'. The company has been notified about this and they are yet to fix this issue.

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Poor security pratice

TYPE OF LOSS
Reputation/Data

Ransomware gang demands $7.5 million from Argentinian ISP

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

One of Argentina's largest ISP providers, Telecom, has been hit by a ransomware. Sources inside the ISP said hackers caused extensive damage to the company's network after they managed to gain control over an internal Domain Admin, from where they spread and installed their ransomware payload to more than 18,000 workstations. The website has been down since the hit.

GOVERNMENT

Hackers has defaced for the second time in a week a site of the European Space Agency (ESA)

Ghost Squad Hackers has defaced for the second time in a week a site of the European Space Agency (ESA). They have found for the second time in a few days a Server-side request forgery (SSRF) remote code execution vulnerability in the server of the agency. This time they have exploited the issue to gain access to the 'https://space4rail.esa.int' domain and deface it. As per reports, the issue hasn't been fixed yet.

ATTACK TYPE
RCE, SSRF

CAUSE OF ISSUE
Security flaw

TYPE OF LOSS
Reputation/Data

Florida Tax Office Data Breach

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

A computer system at a Tax collector office in Florida has been discovered to leak about 450,000 data of the Polk County residents due to being infected by a malware. The information exposed include social security numbers and driver license numbers. However, the issue is being reported to the concerned people and investigation is ongoing to fix the issue and contain the data leak ASAP.

Roundcube XSS vulnerability opens the door to email account takeover

ATTACK TYPE
Cross site scripting

CAUSE OF ISSUE
Existing Vulnerability

TYPE OF LOSS
Reputation/Data

Roundcube is an open source webmail project which offers a browser-based skinnable IMAP client in multiple languages is urging users to update their installations to resolve a security vulnerability that can be exploited to conduct XSS. Roundcube uses a customized version of the Washtml HTML sanitizer to display untrusted HTML code in emails. This if exploited could lead to XSS.

WordPress security: RCE flaw in Adding Advertising plugin exploited in the wild

ATTACK TYPE
RCE

CAUSE OF ISSUE
security vulnerbility

TYPE OF LOSS
Reputation/Data

Webmasters who use WordPress plugin Adning Advertising are urged to patch against a critical vulnerability that is reportedly being exploited in the wild. Exploitation of the flaw enables an unauthenticated attacker to upload arbitrary files, leading to remote code execution (RCE) and potentially a full site takeover. Such is the flaw's seriousness, MITRE has assigned it the highest possible CVSS score – 10.0.

BadPower attack corrupts fast chargers to melt or set your device on fire

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Unknown

TYPE OF LOSS
Reputation/Data

Chinese security researchers said they can alter the firmware of fast chargers to cause damage to connected (charging) systems through Badpower that works by corrupting the firmware of fast chargers and by altering the default charging parameters to deliver more voltage than the receiving device can handle, which degrades and damages the receiver's components.

Malicious'Blur'Photo App Campaign Discovered on Google Play

ATTACK TYPE
Malicious code

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

Researchers at the White Ops Satori Threat Intelligence and Research Team discovered the Android apps — 29 in total — which they said "manifested suspiciously high volumes of ad traffic" during threat-hunting investigations. There have been about 3.5 million downloads of them. Researchers pointed out that reviews can be helpful in avoiding in preventing the download of malicious apps like these.

Critical SharePoint flaw dissected, RCE details now available

A critical vulnerability CVE-2020-1147 that primarily impacts Microsoft sharepoint besides .NET framework and Visual studio. This vulnerability if exploited can be used to perform RCE. The issue was reported to the organization. Efforts are put to fix the issues ASAP. Moreover, users are asked to use the latest version that has patches for the above cited vulnerabilities.

ATTACK TYPE
RCE

CAUSE OF ISSUE
Security flaw

TYPE OF LOSS
Reputation/Data

ASUS Home Router Bugs Open Consumers to Snooping Attacks

ATTACK TYPE
XSS, MITM

CAUSE OF ISSUE
Security flaw

TYPE OF LOSS
Reputation/Data

ASUS home router has been identified with two severe vulnerabilities. The attacks that could be performed on them by exploiting those included Cross Site Scripting attacks and MITM (Man-In-The-Middle) attacks. These flaws were reported to the organization and they've been fixed. Post that, a new version has been released that's devoid of these vulnerabilities.

Cisco releases security fixes for critical VPN, router vulnerabilities

Cisco has released patches for 34 bugs amongst which 5 of them are cited critical. The worst bugs can be exploited for remote code execution, authentication bypass and privilege escalation attacks. Other severity issues include SQL injections, cross-site scripting (XSS) bugs, filter bypass, information leaks, and denial-of-service. It is recommended that Cisco customers accept automatic updates or manually apply the latest round of security fixes as soon as possible.

ATTACK TYPE
Hot fix

CAUSE OF ISSUE
Security vulnerabilities

TYPE OF LOSS
Reputation/Data

New Zealand property management company leaks 30,000 users passports, driver's licenses and other personal data

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Poor security pratice

TYPE OF LOSS
Reputation/Data

Jake Dixon, a security researcher discovered an unsecured Amazon Simple Storage Solution (S3) database containing more than 31,000 images of users' passports, driver's licenses, evidence of age documents, and more. These files are publicly accessible to anyone who has the URL and appears to be owned by the Wellington, New Zealand company whom are maintaining an unsecured DB. The company were unresponsive when contacted and thus AWS were contacted on this and got the DB secured.

CONSUMER TECH

Data Viper Servers Hacked; Over 8,000 Databases Leaked

A hacker with the pseudo-name Nightlion claims to have stolen 8200 backend servers of threat intelligence, data monitoring service and sold around 2 billion records from data viper's DB on darknet forums. He also provided the proof of the access to a list of 482 downloadable JSON files that are stolen from the breached servers. The company have accepted this breach and suspected the hacker to be from hacking groups like TheDarkOverlord, Shiny Hunters, and GnosticPlayers.

ATTACK TYPE
Data leak

CAUSE OF ISSUE
Poor security pratice

TYPE OF LOSS
Reputation/Data

Apache Guacamole Critical Vulnerabilities Put Remote Desktops at Risk

ATTACK TYPE
Reverse RDP

CAUSE OF ISSUE
Existing Vulnerability

TYPE OF LOSS
Reputation/Data

Check Point researchers have uncovered multiple critical reverse RDP vulnerabilities in the Apache Guacamole. Apache Guacamole is a clientless remote desktop gateway that supports VNC, RDP and SSH. This vulnerability is exploited could allow the attacker to compromise the entire user account and also of the Guacamole server. Since WFH began, the panic of being attacked by this is higher now.

A New Flaw In Zoom Could Have Let Fraudsters Mimic Organisations

Checkpoint researchers confirmed that a vulnerability in Zoom could help hackers mimic the activities of employees in an organization. Also, it is said that the vulnerability was very easy to exploit. The vulnerability exists in Zoom's URL helping companies to create custom URL. There are two ways to exploit this.....one, through direct links and the other dedicated Zoom web interfaces. Under OWASP, this vulnerability gets defined under improper account validation. The issues was addressed to zoom and efforts are made to fix that ASAP.

ATTACK TYPE
Improper account validation

CAUSE OF ISSUE
Security vulnerability

TYPE OF LOSS
Reputation/Data

Adobe Issues July 2020 Critical Security Patches for Multiple Software

ATTACK TYPE
Hot fix

CAUSE OF ISSUE
Unknown

TYPE OF LOSS
Reputation/Data

Adobe today released software updates to patch a total of 13 new security vulnerabilities affecting 5 of its widely used applications. The affected products that received security patches today include:· Adobe Creative Cloud Desktop Application· Adobe Media Encoder· Adobe GenuineService· Adobe ColdFusion· Adobe Download ManagerAdobe users are urged to download them and apply immediately.

HEALTHCARE

LibreHealth medical records app exposes sensitive patient data

LibreHealth EHR, a free and open source electronic health records for medical folks to manage patients data has been discovered with 5 critical vulnerabilities such as cross-site scripting, SQL injection, [and] CSRF, as well as some less common issues including local file inclusio that could allow an unauthenticated attacker to compromise the application's underlying server and access sensitive healthcare records. Librehhealth EHR are working on fixing the issue.

ATTACK TYPE
Data leak

CAUSE OF ISSUE
Critical vulnerability

TYPE OF LOSS
Reputation/Data

Website Security Breach Exposes 1 Million DNA Profiles

ATTACK TYPE
Security breach

CAUSE OF ISSUE
Security flaw

TYPE OF LOSS
Reputation/Data

GEDmatch, the DNA analysis site that police used to catch the so-called Golden State Killer, was pulled briefly offline on Sunday while its parent company investigated how its users' DNA profile data apparently became available to law enforcement searches. The permissions change was caused by a breach. They also issued a warning to users on this.

EDUCATION

College recruitment database leaking nearly 1 million students' GPAs, SAT scores, IDs, and other personal data

An unsecured Amazon S3 (Simple Storage Service) bucket, or database, containing nearly 1 million records of sensitive high school student academic information is owned by CaptainU, which is a college recruitment website. Included in this unsecured bucket are GPA scores, ACT, SAT, and PSAT scores, unofficial transcripts, student IDs, and students' and parents' names, email addresses, home addresses, phone numbers and more.

ATTACK TYPE
Data leak

CAUSE OF ISSUE
Security misconfiguration

TYPE OF LOSS
Reputation/Data

BANKING

Tech unicorn Dave admits to security breach impacting 7.5 million users

ATTACK TYPE
Security breach

CAUSE OF ISSUE
Unauthorized access

TYPE OF LOSS
Reputation/Data

Digital banking app and tech unicorn Dave.com confirmed today a security breach after a hacker published the details of 7,516,625 users on a public forum. Due to that, one of Dave's former third party service providers, a malicious party recently gained unauthorized access to certain user data at Dave. The company hired security firm Crowdstrike to assist the investigation.

OilRig APT Drills Into Malware Innovation

The attacks also revealed a revised backdoor tool in the group's arsenal, called RDAT. The attacks were observed by Palo Alto Networks' Unit 42. Researchers there said that the version of RDAT in question was uncovered during the course of its investigation, standing out by using a unique command-and-control (C2) channel. To wit, it uses steganography to hide commands and data within bitmap images attached to emails.

ATTACK TYPE
Malware

CAUSE OF ISSUE
social engg

TYPE OF LOSS
Reputation/Data

CONCLUSION

According to an article, online threats has risen by as much as six-times their usual levels recently, as the Covid 19 pandemic provides new ballast for cyber attacks. A journal analysed the UK traffic figures for four weeks and reported that hacking and phishing attempts were up to 37% month-on-month.

As mentioned previously, it's smart to develop strong cyber safety habits to help prepare for a cyberattack or data breach. Large-scale attacks and breaches would occur at major organizations, but it's also important to secure your personal information and networks too. So, in order to protect your files and system, keep your software up to date, secure your files, encrypt your devices, use strong passwords and keep changing it frequently.

In addition to these steps the most important step to be followed is contacting a best security company like us.

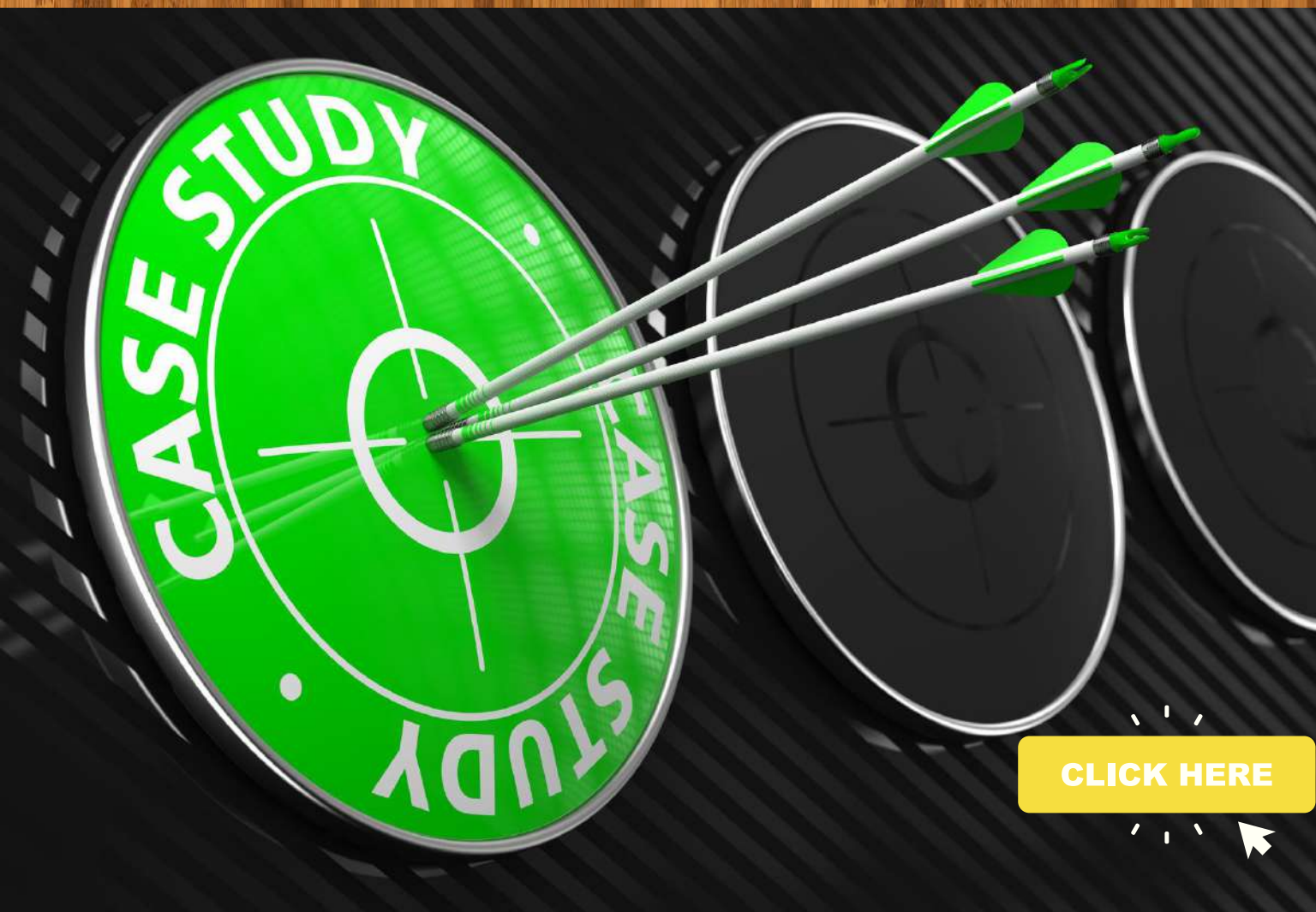
Here we would give you a clear view regarding the security issues and we would also help you out to keep your data secure at this New Normal.

Contact us for more information.

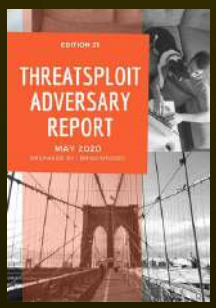
REFERENCES

- https://portswigger.net/daily-swig/online-poker-operator-hit-by-ddos-attack-on-opening-day-of-wsop-event?&web_view=true
- https://thehackernews.com/2020/07/zoom-vanity-url-vulnerability.html
- https://thehackernews.com/2020/07/verified-twitter-hacked.html
- https://www.bleepingcomputer.com/news/security/deepsource-resets-logins-after-employee-falls-for-sawfish-phishing/?&web_view=true
- https://www.zdnet.com/article/ransomware-gang-demands-7-5-million-from-argentinian-isp/?&web_view=true
- https://gadgets.ndtv.com/apps/news/seven-vpn-apps-ufo-fast-secure-flash-rabbit-1-2tb-private-data-leaked-play-store-2265917
- https://securityaffairs.co/wordpress/106111/hacking/esa-site-defaced-again.html?utm_source=feedly&utm_medium=rss&utm_campaign=esa-site-defaced-again
- https://thehackernews.com/2020/07/adobe-security-patch-july.html
- https://techviral.news/chingari-app-accounts-can-be-hacked/
- https://thehackernews.com/2020/07/f5-big-ip-application-security.html
- https://www.secpod.com/blog/critical-vulnerabilities-in-popular-remote-desktop-application-apache-guacamole/
- https://www.bleepingcomputer.com/news/security/orange-confirms-ransomware-attack-exposing-business-customers-data/?&web_view=true
- https://www.zdnet.com/article/us-actor-casting-company-leaked-private-data-of-over-260000-individuals/?&web_view=true
- https://cisomag.eccouncil.org/data-viper-breach/
- https://cybernews.com/security/new-zealand-property-management-company-leaks-30000-passports-drivers-licenses/?web_view=true
- https://www.zdnet.com/article/garmin-services-and-production-go-down-after-ransomware-attack/
- https://www.zdnet.com/article/cisco-releases-fixes-for-critical-vpn-router-vulnerabilities/
- https://www.infosecurity-magazine.com/news/florida-tax-office-blames-data/
- https://threatpost.com/asus-home-router-bugs-snooping-attacks/157682/?web_view=true
- https://www.bleepingcomputer.com/news/security/critical-sharepoint-flaw-dissected-rce-details-now-available/
- https://portswigger.net/daily-swig/roundcube-xss-vulnerability-opens-the-door-to-email-account-takeover#:~:text=Roundcube%20XSS%20vulnerability%20opens%20the%20door%20to%20email%20account%20takeover,-Charlie%20Osborne%2022&text=Roundcube%20is%20urging%20users%20to,site%20scripting%20(XSS)%20attacks.
- https://portswigger.net/daily-swig/librehealth-medical-records-app-exposes-sensitive-patient-data
- https://portswigger.net/daily-swig/wordpress-security-rce-flaw-in-adning-advertising-plugin-exploited-in-the-wild
- https://www.zdnet.com/article/cisa-says-62000-qnap-nas-devices-have-been-infected-with-the-qsnatch-malware/?&web_view=true
- https://www.zdnet.com/article/badpower-attack-corrupts-fast-chargers-to-melt-or-set-your-device-on-fire/
- https://www.threatshub.org/blog/oilrig-apt-drills-into-malware-innovation/
- https://threatpost.com/malicious-photo-app-campaign-google-play/157712/
- https://www.zdnet.com/article/tech-unicorn-dave-admits-to-security-breach-impacting-7-5-million-users/#:~:text=Digital%20banking%20app%20and%20tech,users%20on%20a%20public%20forum.&text=The%20company%20said%20it%20has,notifying%20customers%20of%20the%20incident.
- https://www.usnews.com/news/best-states/california/articles/2020-07-23/website-security-breach-exposes-1-million-dna-profiles
- https://cyware.com/news/nefilim-ransomware-attack-on-orange-sa-exposed-customer-data-5b0b8255
- https://cybernews.com/security/college-recruitment-database-leaking-nearly-1-million-students-gpas-sat-scores-ids-and-other-personal-data/?web_view=true


BLOG
CLICK HERE


CASE STUDY
CLICK HERE

YOU MAY ALSO BE INTERESTED IN OUR PREVIOUS REPORTS



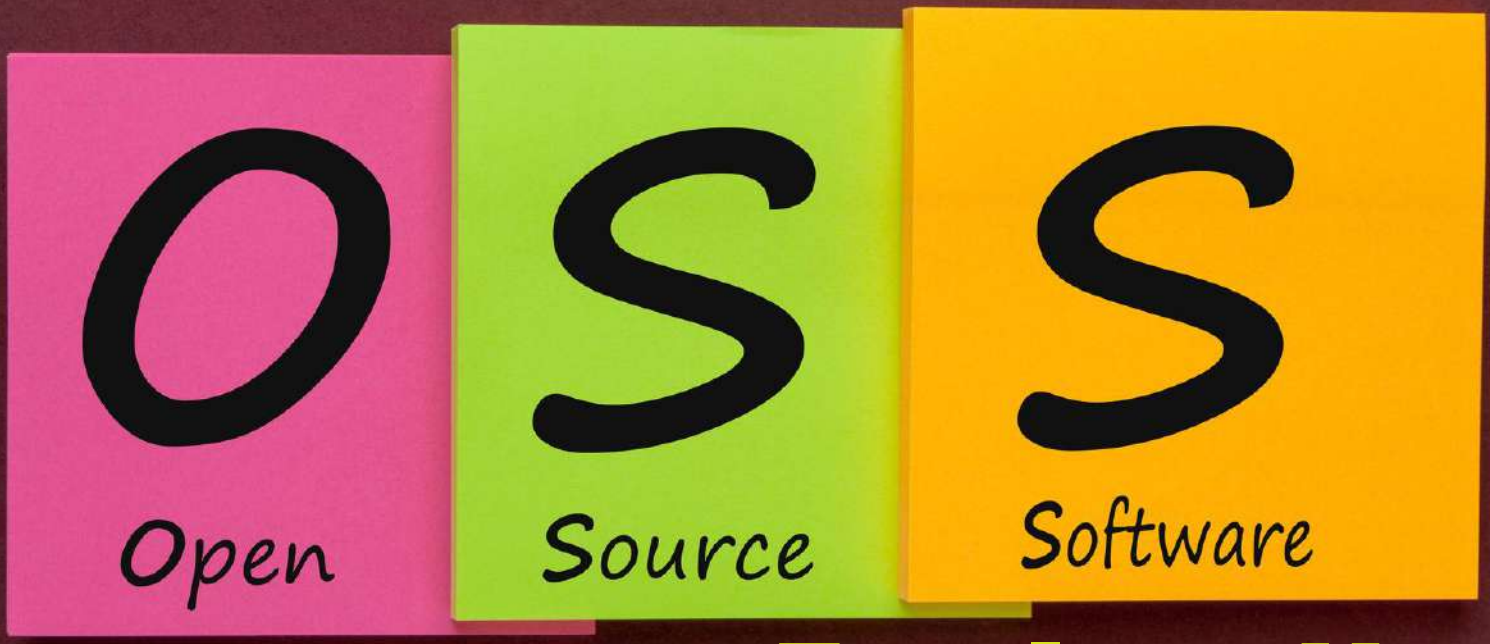
CLICK HERE

CLICK HERE

CLICK HERE

Briskinfosec

CLICK HERE



Tool set's

Your Cybersecurity is Our Responsibility!!

contact@briskinfosec.com | www.briskinfosec.com

Affiliated by

certin
www.cert-in.org.in

BQS
Bureau of Quality Standard
ISO/IEC 27001
ISMS CERTIFIED

ASQS

Awards

CIO Review 10 MOST PROMISING CYBERSECURITY SOLUTION PROVIDER 2019

THE LEADERS GLOBE
THE MOST POWERFUL
CYBER SECURITY SOLUTION PROVIDER