EDITION 26

OCTOBER 2020

THREATSPLOIT

ADVERSARY REPORT

PREPARED BY

Briskinfosec Technology

www.briskinfosec.com

INTRODUCTION

We welcome you to the October 2020 edition of the Threatsploit report covering some of the important cyber security exploits, incidents and events that occurred in the last month. Overall, organisations across the globe witnessed a massive rise in ransomware and data breach attacks, besides many other attack types were seen spiking during these recent months.

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

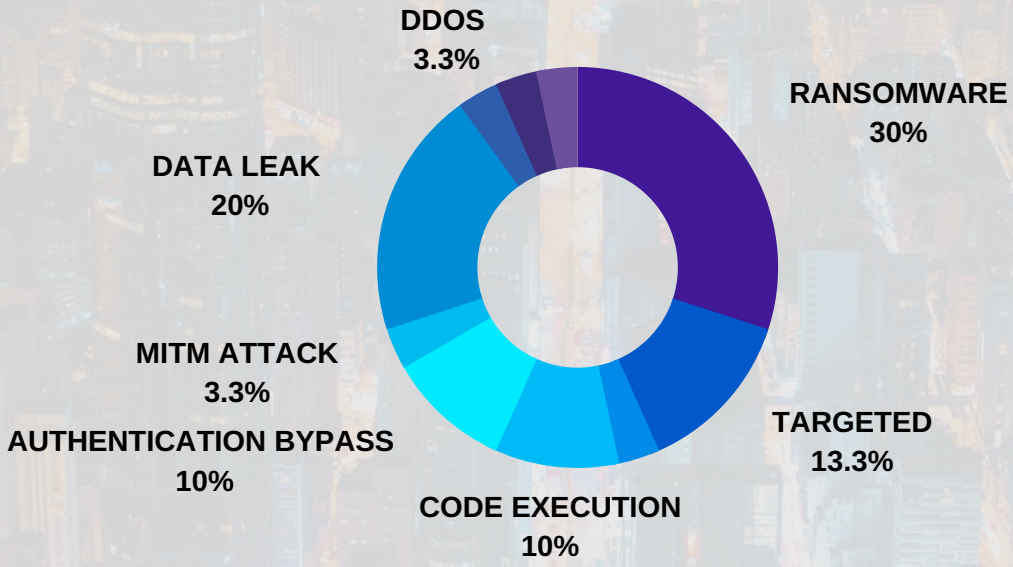
"employees and stakeholders have limited or no perception or understanding of threats and misplaced understanding of cyber threats or its consequences".

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 October 2020.

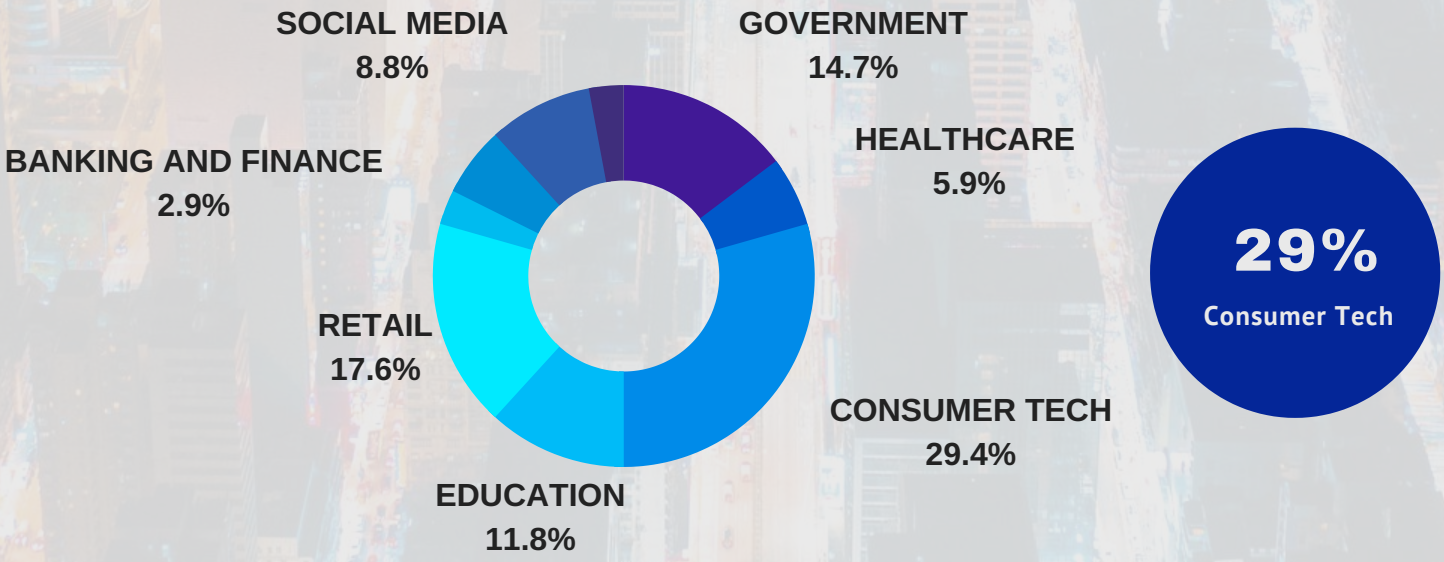
TYPES OF ATTACK VECTORS

The pie-chart indicates the percentage of malicious cyber-attacks that exploited the information infrastructure and compromised the security mechanisms across organisations from various business verticals.



SECTORS AFFECTED BY ATTACKS

This chart highlights the percentage of Industry-wise organisations that were 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 (with 29% of victims). To prevent any attack, organisations need the best of cyber security partners. Needless to say, Cyber security as a function is assuming very high importance like the Operations, Sales, Finance or Human Resources.

CONSUMER TECH

- Cisco IOS XR Zero Day Vulnerability Being Actively Exploited in the Wild
- Ransomware attack hits Laser developer firm, IPG Photonics
- Unsecured Microsoft Bing Server Leaks Search Queries, Location Data
- Tutanota encrypted email service suffers DDoS cyberattacks
- The Windows XP source code was allegedly leaked online
- A bug in Joe Biden's campaign app gave anyone access to millions of voter file
- Fortinet VPN with Default Settings Leave 200,000 Businesses Open to Hackers
- Critical ZeroLogon Windows Server Vulnerability
- Apple Bug Allows Code Execution on iPhone, iPad, iPod

HEALTHCARE

- University Hospital New Jersey hit by SunCrypt ransomware, data leaked
- UHS hospitals hit by reported country-wide Ryuk ransomware attack

RETAIL

- US fitness chain, Town Sports suffers Data Breach Exposing 600K Customer Data online
- Shopify says customer data likely exposed as employees accessed records
- Details of 540,000 sports referees taken in failed ransomware attack
- Popular shopping site leaks miners' data in 6TB of database mess up
- Suspicious logins reported after ransomware attack on US govt contractor
- KuCoin cryptocurrency exchange hacked for $150 million

TRANSPORTATION

- Two major flight tracking services hit by crippling cyberattacks
- Shipping Giant CMA CGM Hit by Ransomware Cyber Attack

GOVERNMENT

- Ukraine police website shut down after hackers gain access
- Hackers leak details of 1,000 high-ranking Belarus police officers
- Department of Veteran Affairs discloses breach impacting 46,000 veterans
- Wales says personal data of 18,000 COVID patients accidentally published
- US Court Hit by "Conti" Ransomware

SOCIALMEDIA

- Researcher hacked Facebook by exploiting flaws in MobileIron MDM
- Major Instagram App Bug Could've Given Hackers Remote Access to Your Phone
- PM Modi’s Twitter account hacked

EDUCATION

- Ontario nurses’ college hit by ransomware attack, personal data at risk
- University of Tasmania students' personal information exposed in email bungle
- California Elementary Kids Kicked Off Online Learning by Ransomware
- Fairfax County Public Schools hit by Maze ransomware

BANKING AND FINANCE

- Hungarian Banks, Telecoms Services Briefly Hit By Cyber Attack

MEDIA AND ENTERTAINMENT

- Over 500,000 Activision accounts hacked, Call of Duty players’ data, password at risk

CONSUMER TECH

Cisco IOS XR Zero Day Vulnerability Being Actively Exploited in the Wild

Cisco has warned of an active zero-day vulnerability tracked as CVE-2020-3566 in its router software that's being exploited in thewild and could allow a remote, authenticated attacker to carry out memory exhaustion attacks by sending crafted IGMP traffic to an affected device. A software fix is slated to be released by the company but timeline hasn't been said yet.

ATTACK TYPE
Memory exhaustion

CAUSE OF ISSUE
Zero day vulnerability

TYPE OF LOSS
Reputation/Data

REFFERENCES
https://zd.net/3iqusSv

Ransomware attack hits Laser developer firm, IPG Photonics

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of maintenance

TYPE OF LOSS
Reputation/Data

REFFERENCES
https://bit.ly/36m1c07

U.S Laser company IP Photonics Corp. has been hit by ransomware attack that shut down its information technology systems worldwide. The ransomware attack involved theRansomExx strain of ransomware, sometimes also dubbed RansomX. The ransom demand against IP Photonics included a message stating that law enforcement should not be contacted because ransom payments could be blocked.

Unsecured Microsoft Bing Server Leaks Search Queries, Location Data

Microsoft has suffered a rare cyber-security lapse earlier this month when the company's IT staff accidentally left one of Bing's backend servers exposed online is believed to have exposed more than 6.5TB of log files containing 13 billion records originating from the Bing search engine. They then fixed that mis-configuration that caused asmall amount of search query data to be exposed.

ATTACK TYPE
Data Leak

CAUSE OF ISSUE
Security misconfiguration

TYPE OF LOSS
Reputation/Data

REFFERENCES
https://bit.ly/3cK9ydB

Tutanota encrypted email service suffers DDoS cyberattacks

ATTACK TYPE
DDOS

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

REFFERENCES
https://bit.ly/3ilMnHD

Encrypted email service, Tutanota has experienced a series of DDoS attacks this week, first targeting the Tutanota website and further its DNS providers. This had caused downtime for several hours for millions of Tutanota users. This incident caused issues for a few hundred users, but was remedied shortly by restricting an "overreacting IP-block" responsible for the attack

CONSUMER TECH

Critical ZeroLogon Windows Server Vulnerability

Windows Server users, make sure it's up to date with all recent patches issued by Microsoft, especially the one that fixes a recently patched critical vulnerability Dubbed 'Zerologon' (CVE-2020-1472) that could allow unauthenticated attackers to compromise the domain controller. The privilege escalation vulnerability exists due to the insecure usage of AES-CFB8 encryption for Netlogon sessions, allowing remote attackers to establish a connection to the targeted domain controller over Netlogon Remote Protocol (MS-NRPC).

ATTACK TYPE
Privilege escalation

CAUSE OF ISSUE
Lack of maintainces

TYPE OF LOSS
Reputation/Data

REFFERENCES
https://bit.ly/3jjyvPj

The Windows XP source code was allegedly leaked online

ATTACK TYPE
Data leak

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

REFFERENCES
https://bit.ly/30p6P4i

The source code for Windows XP SP1 and other versions of the operating system was allegedly leaked online today. The leaker claims to have spent the last two months compiling a collection of leaked Microsoft source code. This 43GB collection was then released today as a torrent on the 4chan forum. The torrent also includes a media folder containing a bizarre collection of conspiracy theory videos about Bill Gates.

A bug in Joe Biden's campaign app gave anyone access to millions of voter file

A privacy bug in Democratic presidential candidate Joe Biden's official campaign app allowed anyone to look up sensitive voter information on millions of Americans, a security researcher has found. The app uploads and matches the user's contacts with voter data supplied from TargetSmart, a political marketing firm that claims to have files on more than 191 million Americans.

ATTACK TYPE
Unauthorized access

CAUSE OF ISSUE
Security flaw

TYPE OF LOSS
Reputation/Data

REFFERENCES
https://tcrn.ch/3n0UPj0

Fortinet VPN with Default Settings Leave 200,000 Businesses Open to Hackers

ATTACK TYPE
MITM attack

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

REFFERENCES
https://bit.ly/34fbqXN

Over 200,000 businesses that have deployed the Fortigate VPN solution —with default configuration—to enable employees to connect remotely are vulnerable to Man-in-the-Middle (MITM) attacks, allowing attackers to present a valid SSL certificate and fraudulently take over a connection. he researchers set up a compromised IoT device that's used to trigger a MITM attack soon after the Fortinet VPN client initiates a connection, which then steals the credentials before passing it to the server and spoofs the authentication process.

CONSUMER TECH

Apple Bug Allows Code Execution on iPhone, iPad, iPod

Apple has updated its iOS and iPad operating systems, which addressed a wide range of flaws in its iPhone, iPad and iPod devices. The most severe of these could allow an adversary to exploit a privilege-escalation vulnerability against any of the devices and ultimately gain arbitrary code-execution. In total, Apple addressed 11 bugs in products and components, including AppleAVD, Apple Keyboard, WebKit and Siri.

ATTACK TYPE
Code execution

CAUSE OF ISSUE
Poor security patch

TYPE OF LOSS
Reputation/Data

REFERENCES
https://bit.ly/3c0FUDL

BANKING AND FINANCE

Hungarian Banks, Telecoms Services Briefly Hit By Cyber Attack

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

REFERENCES
https://bit.ly/2Sc261r

Some of the Hungarian banking and its telecommunication services were disrupted by a powerful cyber attack. The event was a distributed-denial-of-service (DDoS) attack, a cyber attack in which hackers attempt to flood a network with unusually high volumes of data traffic in order to paralyse it. Hungarian bank OTP Bank confirmed it had been affected by the attack. The volume of data traffic in the attack was 10 times higher than the amount usually seen in DDoS events and it was one of the biggest hacker attacks in Hungary ever, the company said.

University Hospital New Jersey hit by SunCrypt ransomware, data leaked

University Hospital New Jersey (UHNJ) has suffered a massive 48,000 document data breach after a ransomware operation leaked their stolen data. The SunCrypt ransomware operation has leaked data allegedly stolen from UHNJ in a September ransomware attack. Of the 240 GB of data allegedly stolen from University Hospital New Jersey, the attackers have leaked a 1.7 GB archive containing over 48,000 documents.

ATTACK TYPE
Data leak

CAUSE OF ISSUE
Ransomware

TYPE OF LOSS
Reputation/Data

REFERENCES
https://bit.ly/34dP60r

HEALTHCARE

UHS hospitals hit by reported country-wide Ryuk ransomware attack

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Poor security pratice

TYPE OF LOSS
Reputation/Data

REFERENCES
https://tcrn.ch/3cQFCfJ

UHS hospitals in the US including those from California, Florida, Texas, Arizona, and Washington D.C. are left without access to computer and phone systems. The affected hospitals are redirecting ambulances and relocating patients in need of surgery to other nearby hospitals. When the attack happened multiple antivirus programs were disabled by the attack and hard drives just lit up with activity.

RETAIL

US fitness chain, Town Sports suffers Data Breach Exposing 600K Customer Data online

US fitness chain, Town Sports suffers a data breach exposing a database containing 600K customer information exposed online. Bob Diachenko discovered a database belonging to Town Sports International exposed online. The data contained records of around 600,000 staffer members, and the information includes names, addresses, contact numbers, email addresses, last four digits of credit cards, credit card expiration dates, billing histories and limited payment information.

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

REFERENCES
https://bit.ly/341aq4G

Shopify says customer data likely exposed as employees accessed records

ATTACK TYPE
Data expsed

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

REFERENCES
https://reut.rs/3n60BA3

The data exposed includes email, name, and address, as well as order details, but does not involve complete payment card numbers or financial information. Shopify said it immediately terminated the access of HEOS, individuals, who were part of its support team, to its network and was working with the Federal Bureau of Investigation and other international agencies in the investigation.

Details of 540,000 sports referees taken in failed ransomware attack

ArbiterSports, the official software provider for the NCAA (National Collegiate Athletic Association) and many other leagues, said it fended off a ransomware. In a data breach notification letter filed with multiple states across the US, the company said that despite detecting and blocking the hackers from encrypting its files, the intruders managed to steal a copy of its backups.

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

REFERENCES
https://zd.net/2GdJqEw

Popular shopping site leaks miners' data in 6TB of database mess up

ATTACK TYPE
Data leaks

CAUSE OF ISSUE
Poor security practice

TYPE OF LOSS
Reputation/Data

REFERENCES
https://bit.ly/30mr0jp

A misconfigured Elasticsearch database exposed 882 GB worth of data from 70 dating and e-commerce sites. The DB belongs to a German online shopping website "windeln.de" exposing a humongous amount of personal data putting children and parents at all sorts of offline and online risks. It is worth noting that the production database was hosted on the Elasticsearch server exposed on Shodan without any security authentication.

RETAIL

Suspicious logins reported after ransomware attack on US govt contractor

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of maintaince

TYPE OF LOSS
Reputation/Data

REFERENCES
https://zd.net/33iBOfi

Customers of Tyler Technologies, one of the biggest software providers for the US state and federal government, are reporting finding suspicious logins and previously unseen remote access tools (RATs) on their networks and servers after being affected by a ransomware attack locking many internal documents of company in cloud infrastructure. It is recommended to reset passwords on your remote network access.

KuCoin cryptocurrency exchange hacked for $150 million

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Financial/Data

REFERENCES
https://zd.net/3ids2nS

Over $150 million is estimated to have been emptied in a hack of Singapore-based cryptocurrency exchange KuCoin. The security incident saying that it detected some large withdrawals and it found that part of Bitcoin, ERC-20 and other tokens in KuCoin's hot wallets were transferred out of the exchange.The assets in our cold wallets are safe and unharmed, and hot wallets have been re-deployed. Deposits and withdrawals have been temporarily suspended while the company's security team investigates the incident.

TRANSPORTATION

Two major flight tracking services hit by crippling cyberattacks

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

REFERENCES
https://bit.ly/2SeBhJN

Two of the most popular flight tracking websites, Flightradar24 and PlaneFinder had their service disrupted after consecutively suffering multiple cyberattacks.It seems like a well-organized hacking campaign targeting real-time flight tracking service providers. Flightradar24 was attacked thrice in two days, whereas PlaneFinder was attacked multiple times. PlaneFinder confirmed the news and asked its users to remain patient as they are trying to fix the issue.

Shipping Giant CMA CGM Hit by Ransomware Cyber Attack

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Poor security pratices

TYPE OF LOSS
Reputation/Data

REFERENCES
https://zd.net/2SqZqzm

French shipping giant CMA CGM group is currently dealing with ransomware attack impacting peripheral servers. Once security breach was detected, external access to applications was interrupted to prevent the malware from spreading. But, CMA CGM network remains available to the Group's customers for all booking and operation requests. CMA CGM's statement said "An investigation is underway, conducted by our internal experts and by independent experts".

Ukraine police website shut down after hackers gain access

Ukraine's national police website has been temporarily shut down after it was hacked by unknown persons who published false information on the site. As a result, inaccurate information was spread on some websites of the regional police departments. Investigation is going on about the hacker's unauthorized access into the website by cyber forensic experts.

ATTACK TYPE
Unauthorised access

CAUSE OF ISSUE
Lack of Maintaince

TYPE OF LOSS
Reputation/Data

REFERENCES
https://bit.ly/30pRh03

Hackers leak details of 1,000 high-ranking Belarus police officers

ATTACK TYPE
Data leaks

CAUSE OF ISSUE
Poor security practice

TYPE OF LOSS
Reputation/Data

REFERENCES
https://zd.net/3il6bL6

Personal details including names, dates of birth, and the officers' departments and job titles of more than 1,000 high-ranking Belarusian police officers in response to violent police crackdowns against anti-government demonstrations have been leaked. Details for 1,003 police officers were leaked via a Google spreadsheet, with most of the entries being for high-ranking officers, such as lieutenants, majors, and captains.

Department of Veteran Affairs discloses breach impacting 46,000 veterans

The Department of Veterans Affairs (VA) has disclosed today a security breach during which the personal information of around 46,000 veterans was obtained by a malicious third-party. The breach took place after "unauthorized users" accessed an online application managed by the VA Financial Services Center (FSC). Besides investigation, VA believes that the hackers might have also accessed veteran records, including Social Security numbers.

ATTACK TYPE
Security breach

CAUSE OF ISSUE
Unauthorized access

TYPE OF LOSS
Reputation/Data

REFERENCES
https://zd.net/3cN4340

Wales says personal data of 18,000 COVID patients accidentally published

ATTACK TYPE
Human error

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

REFERENCES
https://bit.ly/2ShitKa

Personal data concerning 18,105 residents of Wales who tested positive for COVID-19 was uploaded by mistake to a public server. The data breach was a result of individual human error, the public health body said, adding that it had commissioned an external investigation into the data breach and taken steps to prevent any similar incident. During the time it was online, it was viewed 56 times by unknown users.

GOVERNMENT

US Court Hit by “Conti” Ransomware

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

REFERENCES
https://bit.ly/30odsDO

The infrastructure of US criminal court has been hit by ransomware with court documents published online in what is thought to be the first ransomware attack of its kind and published apparent proof of the attack on its dark web page. It appears to have published documents obtained from the court relating to defendant pleas, witnesses and jurors. Ever since, the court’s website remains offline. It was not clear if infrastructure had been pulled offline for precautionary reasons or if the malware had hit there too.

SOCIALMEDIA

Major Instagram App Bug Could've Given Hackers Remote Access to Your Phone

ATTACK TYPE
Remote access

CAUSE OF ISSUE
Existing vulnerability

TYPE OF LOSS
Reputation/Data

REFERENCES
https://bit.ly/30q4htM

Check Point researchers disclosed details about a critical vulnerability in Instagram's Android app that could have allowed remote attackers to take control over a targeted device just by sending victims a specially crafted image. The flaw not only lets attackers perform actions on the Instagram app—including spying on victim's private messages and even deleting or posting photos from their accounts—but also execute arbitrary code on the device.

Researcher hacked Facebook by exploiting flaws in MobileIron MDM

ATTACK TYPE
Authentication

CAUSE OF ISSUE
Poor security pratices

TYPE OF LOSS
Reputation/Data

REFERENCES
https://bit.ly/36nGvew

Facebook where a researcher Orange Tsai from DEVCORE found Facebook vulnerable to critical attacks because of a flaw in MobileIron. MobileIron is a Mobile Device Management (MDM) system used by the social network giant in order to control employees’ corporate devices. The researcher identified 3 vulnerabilities centered around allowing attackers to engage in:Arbitrary file reading – CVE-2020-15507Remote Code Execution (RCE) – CVE-2020-15505Bypassing the authentication measures in place remotely – CVE-2020-15506

MEDIA & ENTERTAINMENT

Over 500,000 Activision accounts hacked, Call of Duty players’ data, password at risk

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

REFERENCES
https://bit.ly/33nPR8t

More than 500,000 Activision accounts may have been hacked with login data compromised. The credentials to access these accounts are being leaked publicly, and account details changed to prevent easy recovery by the rightful owners. Such breached accounts provide a goldmine for malicious actors intending to plan further attacks – be it phishing or otherwise.

EDUCATION

Ontario nurses' college hit by ransomware attack, personal data at risk

The organization that regulates the nursing profession in Ontario was hit by a ransomware cyber-attack in which personal information might have been compromised. The nurses' college said it was implementing a range of options to resume operations safely and securely. Those options include restoring the inaccessible data from backups.

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

REFERENCES
https://bit.ly/34bTJbL

University of Tasmania students' personal information exposed in email bungle

ATTACK TYPE
Data exposed

CAUSE OF ISSUE
Poor security practice

TYPE OF LOSS
Reputation/Data

REFERENCES
https://bit.ly/2GqfkoF

The University of Tasmania has apologized after an email bungle released almost 20,000 students' personal details to its entire faculty. The data leak, which contained personally identifiable information, was made accessible to all users with a utas.edu.au email address. The breach was unintentional and there was no evidence it was linked to malicious activity, the university said.

California Elementary Kids Kicked Off Online Learning by Ransomware

The attack on the Newhall District in Valencia is part of a wave of ransomware attacks on the education sector, which shows no sign of dissipating. The latest is a strike against a California school district that closed down remote learning for 6,000 elementary school students, according to city officials. Newhall's servers have been shut down while a forensic investigation plays out, and the kids are back to using pencil and paper to work on take-home assignments.

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

REFERENCES
https://bit.ly/2Ge4MjE

Fairfax County Public Schools hit by Maze ransomware

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation

REFERENCES
https://bit.ly/3nbm6j4

Maze ransomware operators have claimed responsibility for a cyber attack affecting the Fairfax County Public Schools (FCPS). The ransomware attack that disrupted some of US school division systems. Also , the group leaked a series of FCPS files containing student information and administrative documents.Us school division says that "we may have been victimized by cyber criminals who have been connected to dozens of ransomware attacks in other school systems and corporations worldwide. We are coordinating with the FBI on the matter".

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. All the attacks mentioned above - their types, the financial and reputation 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. 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. We assure that we will help you to keep your data safe and also give you clear information on your company's current status and what steps to be taken to stay away from any kind of cyber attack.


Blog
CLICK HERE


Analyzing
Circumstances
Data
Case Study
Researcher
Knowledge
Criteria
CLICK HERE

YOU MAY ALSO BE INTERESTED IN OUR PREVIOUS REPORTS

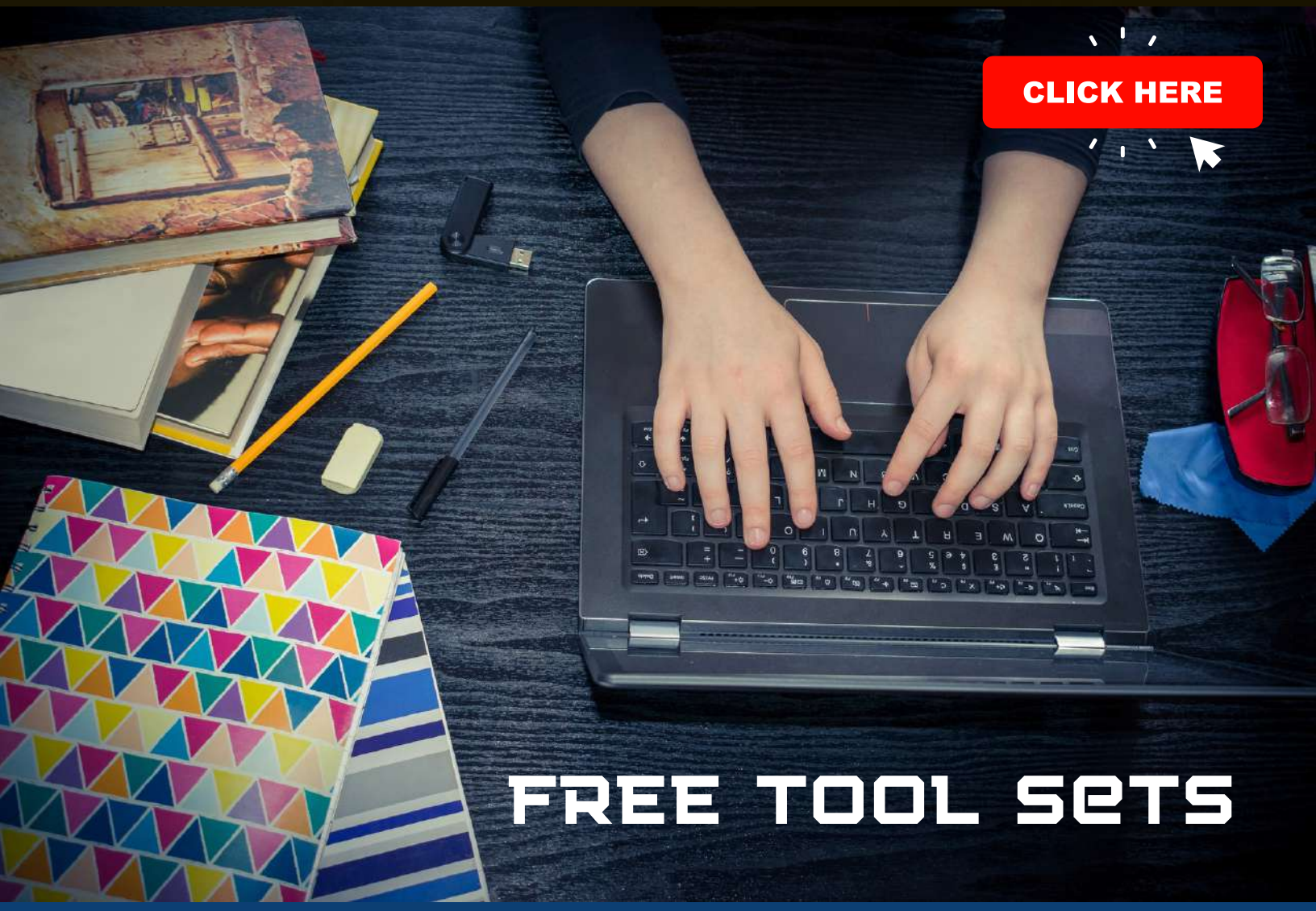
CLICK HERE

CLICK HERE

CLICK HERE

WAKE UP CXO

AN INITIATIVE BY BRISKINFOSEC



CLICK HERE

FREE TOOL SETS

BRISK INFOSEC

CYBER TRUST & ASSURANCE

FEEL FREE TO REACH US FOR ALL YOUR CYBERSECURITY NEEDS

contact@briskinfosec.com | www.briskinfosec.com