

EDITION 27
NOVEMBER

THREATSPLOIT ADVERSARY REPORT

2020

Key Highlights:

- Major cloud breaches
- Zero Day storm hits consumer electronics
- Mass data leakage in Social Media platforms
- Gov still struggle to protect civilians data



www.briskinfosec.com

INTRODUCTION

Greetings our dear reader! Welcome to the world of threatsploit report for the month of October 2020. Some important things that were repeatedly emphasized by us as a passionate and user-focused security professional will be repeated even now as security threats just keep growing like population. Again and again, the same security attacks keep troubling countless organizations (amongst which many are new and many are hacked again) predominantly due to two contrasting approach: complacency and ignorance towards security.

To elaborate further, many new vulnerabilities have also had their inception and found new ways to perpetrate inside the organization's security environment despite the deployment of security defensive software's like firewall and antivirus solutions. It's no wonder that traditional defences can't block the updated and modern attacks.

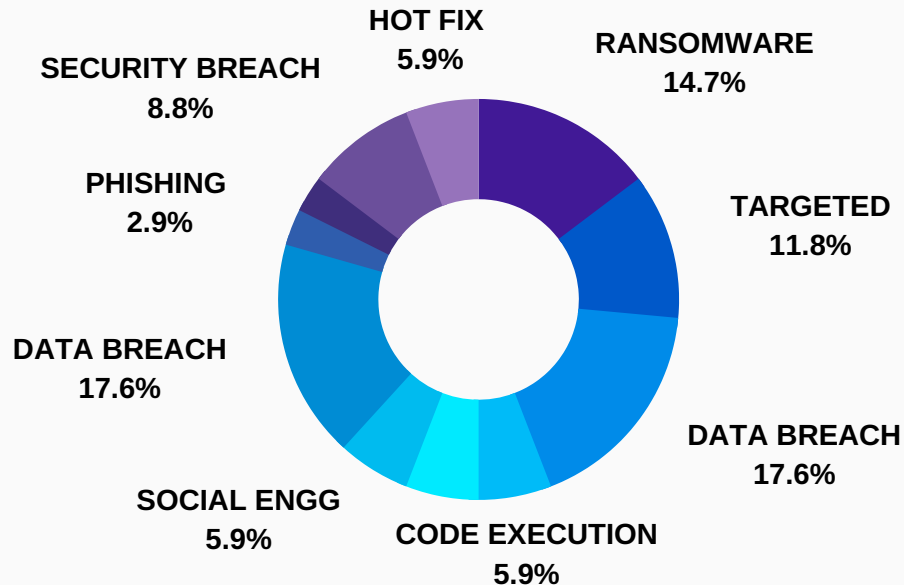
We've been stressing that cloud security is a shared responsibility and not the cloud operators alone and this has proven right ever since that and as a proof, Microsoft cloud Azure services were affected with critical level vulnerabilities that's been briefed below.

Many such of those are gathered and covered and so, kindly read over to know further.



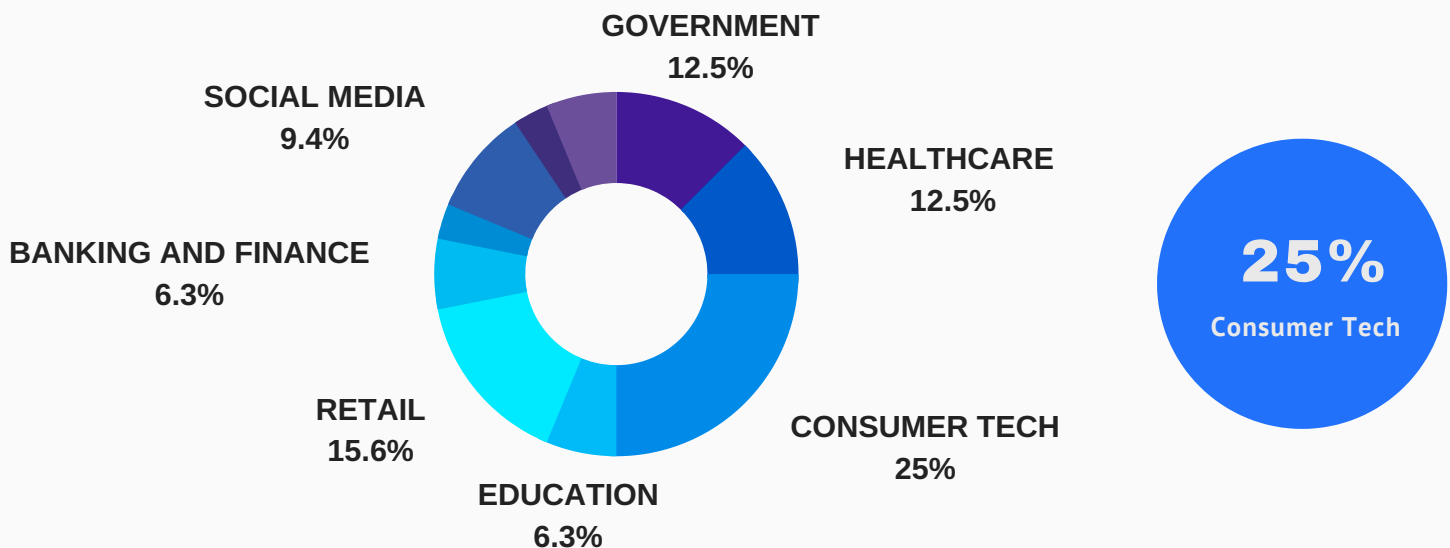
TYPES OF ATTACK VECTORS

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 25% 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

- Researcher Find Vulnerabilities in Microsoft Azure Cloud Service
- Microsoft Releases Patches For Critical Windows TCP/IP and Other Bugs
- Google Warns of Zero-Click Bluetooth Flaws in Linux-based Devices
- New Chrome 0-day Under Active Attacks
- Browser Bugs Exploited to Install 2 New Backdoors on Targeted Computers
- Over 100 irrigation systems left exposed online without a password
- Nando's Customers Hit by Credential Stuffing Attacks
- Sopra Steria Hit by New Ryuk Variant

HEALTHCARE

- Medical Records of 3.5 Million U.S. Patients Can be Accessed and Manipulated by Anyone
- Cyberattack targets networks of Vermont, New York hospitals
- Japanese drug firm Shionogi hit by cyberattack and data breach
- Hackers hold patient information for ransom in psychotherapy data breach

RETAIL

- New Flaws in Top Antivirus Software Could Make Computers More Vulnerable
- Mobile Browsers Found Vulnerable To Address Bar Spoofing Attacks
- Alibaba-owned Lazada suffers data hack of 1.1 million accounts
- Amazon sacks insiders over data leak, alerts customers
- German tech giant Software AG down after ransomware attack

EDUCATION

- DDoS Attacks Disrupt Massachusetts Schools
- University Email Hijacking Attacks Push Phishing, Malware

ENERGY & GAS

- Enel Group hit by ransomware attack



SOCIALMEDIA

- True, the social networking app that exposed private messages and user locations
- Twitter-Owned SDK Leaking Location Data of Millions of Users
- Social media app leaks data of 172,000 users, including location coordinates

TELECOMMUNICATION

- Hackers hijack Telegram, email accounts in SS7 mobile attack


GOVERNMENT

- German infectious disease agency hit by DDOS
- Trump's campaign website hacked by cryptocurrency scammers
- Georgia Election Data Hit in Ransomware Attack
- Cyberattacks hit Louisiana government offices

MANUFACTURING

- Giant Steelcase Hit by Suspected Ransomware Attack
- Kleenheat customer names and addresses exposed in system breach

BANKING & FINANCE

- Hacker steals \$24 million from cryptocurrency service 'Harvest Finance'
 - Uganda's banks have been plunged into chaos by a mobile money fraud hack
- 

Researchers Find Vulnerabilities in Microsoft Azure Cloud Service

Two security flaws in Microsoft's Azure App Services could have enabled a bad actor to carry out server-side request forgery attacks or execute arbitrary code and take over the App Service's git server administration server. As a general best practice, runtime cloud security is an important last line of defense and one of the first actions you can take to reduce risk to prevent further attacks striking the surface.

ATTACK TYPE

SSRF & Code execution

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation/Data

REFERENCES

<https://bit.ly/3mH2DWb>

Microsoft Releases Patches For Critical Windows TCP/IP and Other Bugs

ATTACK TYPE

RCE

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation/Data

REFERENCES

<https://bit.ly/324XmzR>

Microsoft issued fixes for 87 vulnerabilities affecting Windows, Office and Office Services and Web Apps, Visual Studio, Azure Functions, .NET Framework, Microsoft Dynamics, Open Source Software, Exchange Server, and the Windows Codecs Library (out of which newly 11 critical) discovered security vulnerabilities as part of its October 2020 Patch Tuesday, including two critical remote code execution (RCE) flaws in Windows TCP/IP stack and Microsoft Outlook. Users are also asked to update to the latest security versions released.

Google Warns of Zero-Click Bluetooth Flaws in Linux-based Devices

Google security researchers are warning of a new set of 3 zero-click vulnerabilities called Bleeding Tooth in the Linux BlueZ protocol stack that can allow a nearby unauthenticated, remote attacker to execute arbitrary code with kernel privileges on vulnerable devices. As a remediation, Intel has recommended installing the kernel fixes to mitigate the risk associated with these issues.

ATTACK TYPE

Bleeding tooth

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation

REFERENCES

<https://bit.ly/3ehgw49>

New Chrome 0-day Under Active Attacks

ATTACK TYPE

Hot fix

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation

REFERENCES

<https://bit.ly/3en8DjZ>

If you are users of Google Chrome browser on your Windows, Mac, or Linux computers, you need to update your web browsing software immediately to the latest version Google released 86.0.4240.111. The earlier versions were identified with 5 critical level vulnerabilities. Although the Chrome web browser automatically notifies users about the latest available version, users are recommended to manually trigger the update process by going to "Help → About Google Chrome" from the menu.

Browser Bugs Exploited to Install 2 New Backdoors on Targeted Computers

Security researchers have disclosed details about a new watering hole attack targeting the Korean diaspora that exploits vulnerabilities in web browsers such as Google Chrome and Internet Explorer to deploy malware for espionage purposes. A secret and powerful group is linked to be behind this carrying such attacks since May. Experts predict they will continue to do this.

ATTACK TYPE

Watering hole

CAUSE OF ISSUE

Lack of maintainances

TYPE OF LOSS

Reputation/Data

REFERENCES

<https://bit.ly/3oNbHL6>

Over 100 irrigation systems left exposed online without a password

ATTACK TYPE

Authentication

CAUSE OF ISSUE

Poor security practice

TYPE OF LOSS

Reputation/Data

REFERENCES

<https://zd.net/3eqjdlo>

More than 100 smart irrigation systems were left exposed online without a password last month, allowing anyone to access and tamper with water irrigation programs for crops, tree plantations, cities, and building complexes. Companies and city officials had installed ICC PRO systems without changing default factory settings, which don't include a password for the default account that could be found using Shodan.

Nando's Customers Hit by Credential Stuffing Attacks

Some customers of popular high street eatery Nando's have been left hundreds of pounds poorer after cyber-attackers hijacked their online accounts to place large orders. Due to COVID-19 restrictions, customers need to now scan a QR code in store and order online to get their food. However, that has left the door open to attackers trying previously breached log-ins from other sites to hijack their accounts, when those credentials are reused by the victims.

ATTACK TYPE

Credential stuffing

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation/Data

REFERENCES

<https://bit.ly/3mKsCMG>

Sopra Steria Hit by New Ryuk Variant

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Poor security practice

TYPE OF LOSS

Reputation/Data

REFERENCES

<https://bit.ly/3oRDQkf>

European IT services group Sopra Steria is battling a suspected ransomware attack on its network. "The virus has been identified: it is a new version of the Ryuk ransomware, previously unknown to anti-virus software providers and security agencies," it claimed. Investigation teams immediately provided the competent authorities with all information required. The group was able to quickly make this new version's virus signature available to all anti-virus software providers, in order for them to update their anti-virus software."

Cyberattack targets networks of Vermont, New York hospitals

A cyberattack on the University of Vermont (UVM) Health Network negatively impacted systems at multiple hospitals in Vermont and New York, as hospitals across the country are facing a surge in both COVID-19 patients and cyber targeting. "The University of Vermont Health Network is working with the Federal Bureau of Investigation and the Vermont Department of Public safety to investigate a now confirmed cyberattack that has affected some of our systems," the health care network said in a statement

ATTACK TYPE

Targeted

CAUSE OF ISSUE

Lack of maintainances

TYPE OF LOSS

Reputation

REFERENCES

<https://bit.ly/361vm0H>

Medical Records of 3.5 Million U.S. Patients Can be Accessed and Manipulated by Anyon

ATTACK TYPE

Data exposed

CAUSE OF ISSUE

Poor security practice

TYPE OF LOSS

Reputation/Data

REFERENCES

<https://bit.ly/2HSI7V9>

The results of 13 million medical examinations relating to around 3.5 million U.S. patients are unprotected and available to anyone on the internet which resulted in more than 2 Petabytes of Unprotected Medical Data Found on Picture Archiving and Communication System (PACS) Servers. The records can be accessed and downloaded from the internet by anyone and causing three separate threats: personal identity theft, personal extortion and healthcare company breaches. Whether all these data are tampered remains unknown.

Japanese drug firm Shionogi hit by cyberattack and data breach

Japanese pharmaceutical firm Shionogi & Co. said Thursday that its Taiwanese subsidiary was hit by a cyberattack earlier this month. Reports say leading to a data breach import licenses for medical equipment and employee residency permits were released on the "dark web" after a computer in its Taipei sales office was infected with a virus. Moreover, the attacker has threatened to release more information unless a ransom is paid.

ATTACK TYPE

Data breach

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation/Data

REFERENCES

<https://bit.ly/3mWcS9r>

Hackers hold patient information for ransom in psychotherapy data breach

ATTACK TYPE

Data breach

CAUSE OF ISSUE

Ransomware

TYPE OF LOSS

Reputation/Data

REFERENCES

<https://bit.ly/2GqU6ax>

Vastaamo, a famous finland company that offers psychotherapy to thousands of patients says it's been the victim of a data breach due to ransomware, with the personal information of customers held for ransom. "As a company providing psychotherapy services, the confidentiality of customer information is extremely important to us and the starting point for all our operations and so we deeply regret the leak due to the data breach" said the head.

New Flaws in Top Antivirus Software Could Make Computers More Vulnerable

Familiar antivirus solutions including like Kaspersky, McAfee, Symantec, Fortinet, Check Point, Trend Micro, Avira, and Microsoft Defender have been identified with vulnerabilities that could elevate privileges, perform DLL hijacking and allow hackers to delete files from directories and install malware. Majority of bugs result from default DACLS (Discretionary Access Control Lists) i.e., C:\ProgramData" folder of Windows. As a remedy, the software's must be updated to the latest version.

ATTACK TYPE

DLL Hijacking

CAUSE OF ISSUE

Lack of maintainances

TYPE OF LOSS

Reputation

REFERENCES

<https://bit.ly/35Tx84y>

Mobile Browsers Found Vulnerable To Address Bar Spoofing Attacks

ATTACK TYPE

Bar spoofing

CAUSE OF ISSUE

Poor security practice

TYPE OF LOSS

Reputation

REFERENCES

<https://bit.ly/2TKX1ao>

Security researchers on Tuesday disclosed details about an address bar spoofing vulnerability affecting multiple mobile browsers such as UCWeb, Yandex Browser, Bolt Browser, RITS Browser, Apple Safari and Opera Touch, leaving the door open for spear-phishing attacks and delivering malware. Amongst these, UCWeb and Bolt Browser remain unpatched as yet while Opera Mini is expected to receive a fix on November 11, 2020.

Alibaba-owned Lazada suffers data hack of 1.1 million accounts

Singapore based e-commerce firm Lazada said on Friday that personal information including addresses, email, passwords, partial credit card numbers and many such of from 1.1 million accounts had been hacked, a major breach in the city-state of 5.7 million. Hackers targeted database of it's grocery arm Redmart. However, ingapore e-commerce firm Lazada said on Friday that personal information including addresses and partial credit card numbers from 1.1 million accounts had been hacked, a major breach in the city-state of 5.7 million.

ATTACK TYPE

Data leak

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation/Data

REFERENCES

<https://reut.rs/2Ghh0Wu>

Amazon sacks insiders over data leak, alerts customers

ATTACK TYPE

Data leak

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation/Data

REFERENCES

<https://bit.ly/37Z2QA0>

Amazon has recently terminated employees responsible for leaking customer data, including their email addresses, to an unaffiliated third-party in violation of company policies. The company sent an alert mail and an apology mail to all its customers informing of the data breach as well cautioning them to change their passwords. Frustrations from users have been faced from many.

German tech giant Software AG down after ransomware attack

Software AG, one of the largest software companies in the world, has suffered a ransomware attack over the last weekend, and the company has not yet fully recovered from the incident. A ransomware gang going by the name of "Clop" has breached the company's internal network on Saturday, October 3, encrypted files, and asked for more than \$20 million to provide the decryption key.

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation/Data

REFERENCES

<https://zd.net/36bzRGP>

University Email Hijacking Attacks Push Phishing, Malware

ATTACK TYPE

Phishing & Malware

CAUSE OF ISSUE

Security misconfiguration

TYPE OF LOSS

Reputation

REFERENCES

<https://bit.ly/3eftDs5>

Attackers are compromising email accounts from popular universities, including Purdue and Oxford, to launch attacks that get around DMARC and SPF to bypass detection and trick victims into handing over their email credentials or installing malware. Also SMTP servers were identified to be to be improperly configured. "We started to detect these types of attacks in summer 2019, and the number of hijacked accounts increased during the pandemic lockdowns," said the chief.

DDoS Attacks Disrupt Massachusetts Schools

Students learning remotely in Massachusetts have had their lessons disrupted by distributed-denial-of-service, or DDoS, attacks. Sandwich Public Schools suffered a week of connection issues after what was first identified as a firewall failure occurred on October 8. A new firewall put in place to resolve the issue subsequently crashed. After further connectivity issues were experienced with the schools' OpenCape Network despite the new firewall, the source of the problem was determined to be a DDoS attack

ATTACK TYPE

Data leak

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation/Data

REFERENCES

<https://bit.ly/328jqd4>

Enel Group hit by ransomware

Multinational energy company Enel Group has been hit by a ransomware attack for the second time this year. This time by Netwalker, who is asking a \$14 million ransom for the decryption key and to not release several terabytes of stolen data Enel's internal network was attacked by Snake ransomware, also referred to as EKANS, but the attempt was caught before the malware could spread.

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation/Data

REFERENCES

<https://bit.ly/3oNLHn>

True, the social networking app that exposed private messages and user locations

True bills itself as the social networking app that “protect your privacy.” But a security lapse left one of its servers exposed — and spilling private user data to the internet for anyone to find details about it. But a dashboard for one of the app’s databases was exposed to the internet without a password, allowing anyone to read, browse and search the database — including private user data. This is another example of how mistakes can happen at any organization, even those that are privacy-centric.

ATTACK TYPE

Authentication

CAUSE OF ISSUE

Poor security patch

TYPE OF LOSS

Reputation/Data

REFERENCES

<https://tcrn.ch/35Uqx06>

Twitter-Owned SDK Leaking Location Data of Millions of Users

Seven apps have been sending users’ unencrypted GPS location data to MoPub’s servers, according to a report by International Digital Accountability Council (IDAC). Twitter's MoPub provides monetisation services for global mobile app developers and publishers. MoPub's clients include popular gaming companies like Zynga, the creator of games such as Words with Friends 2 and Farmville. MoPub’s failure to protect unencrypted data transmission is responsible for the data leak, the report stated.

ATTACK TYPE

Data leak

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation/Data

REFERENCES

<https://bit.ly/3jQv1q>

Social media app leaks data of 172,000 users, including location coordinates

The Cyber investigations team discovered an unsecured data bucket that belongs to Panion, a Swedish software company. The unprotected bucket contains more than 2.5 million user records, including full names, email addresses, genders, interests, location coordinates and last login dates, as well as selfies and document photos. The files containing the records were left on a publicly accessible Amazon Web Services (AWS) server, allowing anyone to access and download the data.

ATTACK TYPE

Data leak

CAUSE OF ISSUE

Improper authentication

TYPE OF LOSS

Reputation/Data

REFERENCES

<https://bit.ly/2HRvAQa>

Hackers hijack Telegram, email accounts in SS7 mobile attack

The hackers used SS7 to steal 2-Factor Authentication (2FA) codes sent to victims through SMS. The attacker spoofed a message of a mobile network operator to send an update location request to the targeted phone number. Since the attacker was in control of the spoofed message service center, they managed to gather all of the messages sent to the phone. Telegram was the main application that was targeted where the attackers would private message others trying to exchange cryptocurrency.

ATTACK TYPE

SS7

CAUSE OF ISSUE

Poor security practice

TYPE OF LOSS

Reputation/Data

REFERENCES

<https://bit.ly/3jQjunR>

German infectious disease agency hit by DDOS

Germany's Robert Koch Institute for infectious disease control was hit by a DDOS cyber attack days before its headquarters was the target of an arson attempt. Regarding this, the Federal Office for Information Security did not immediately respond to a request for comment. The Federal Centre for Information Technology, said the website was knocked out for two hours on Oct. 22 by a distributed denial of service attack. No sensitive data was lost

ATTACK TYPE
DDOS

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

REFERENCES
<https://bit.ly/34laq9G>

Trump's campaign website hacked by cryptocurrency scammers

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

REFERENCES
<https://tcrn.ch/3mWJ4cP>

President Trump's campaign website was briefly and partially hacked as unknown adversaries took over parts of the page, replacing them with what appeared to be a scam to collect cryptocurrency. However, this is not the first time Trump has been hacked recently. Trump recently stated, mistakenly it seems, that "Nobody gets hacked. To get hacked you need somebody with 197 IQ and he needs about 15% of your password."

Georgia Election Data Hit in Ransomware Attack

Ransomware gangs have officially entered the 2020 election fray, with reports of one of the first breaches of the voting season, on Hall County, Ga. The county's database of voter signatures was impacted in the attack along with other government systems. Although the county said the voting process hasn't been impacted by the ransomware attack, the incident is a warning to other municipalities to lock down their systems, particularly in these last days leading up to the election.

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

REFERENCES
<https://bit.ly/3oQb144>

Cyberattacks hit Louisiana government offices

ATTACK TYPE
Security breach

CAUSE OF ISSUE
Poor security practice

TYPE OF LOSS
Reputation/Data

REFERENCES
<https://politi.co/3jWkqHm>

Hackers breached several local government offices in Louisiana in recent weeks, prompting state officials to enlist the National Guard to stem the attacks. The Louisiana cyberattacks involved a remote access trojan, or RAT, the kind of malware often used to lay the groundwork for additional breaches. The hacking tool, called "KimJongRat," has been used. Officials are increasingly worried, however, about hackers testing states' defences ahead of possible disinformation or sabotage efforts closer to the election.

Giant Steelcase Hit by Suspected Ransomware Attack

Steelcase, the world's largest maker of office furniture and a multibillion-dollar furniture maker has become the latest big name apparently hit by a major ransomware attack. At this stage it's unclear which variant was responsible for the attack, although Steelcase said it is not aware of any data being stolen from its systems. A series of containment measures were said by the company. Steelcase attack came in the same week that French IT services giant Sopra Steria fell victim to what it claimed to be a new variant of the prolific Ryuk family.

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation/Data

REFERENCES

<https://bit.ly/3mGw4b1>

Kleenheat customer names and addresses exposed in system breach

ATTACK TYPE

System breach

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation/Data

REFERENCES

<https://zd.net/2THW1t4>

Australian gas producer Kleenheat has warned a number of its customers about a data breach that may have resulted in information such as name and address being exposed. Kleenheat referred to data at potential risk as being "general contact information", confirming that it included name, residential address, and email address. It "reassured" phone number, date of birth, or bank, credit card, and account details were not breached

Hacker steals \$24 million from cryptocurrency service 'Harvest Finance'

A hacker has stolen roughly \$24 million worth of cryptocurrency assets from decentralized finance (DeFi) service Harvest Finance, a web portal that lets users invest cryptocurrencies and then farm the price variations for small profit yields. A hacker invested large quantities of cryptocurrency assets in its service and then used a cryptographic exploit to siphon the platform's funds to their own wallets. The issue has been noticed and efforts to contain are done.

ATTACK TYPE

Targetted

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation/Data

REFERENCES

<https://zd.net/34MuKqE>

Uganda's banks have been plunged into chaos by a mobile money fraud hack

ATTACK TYPE

Security breach

CAUSE OF ISSUE

Poor security practice

TYPE OF LOSS

Reputation/Financial

REFERENCES

<https://bit.ly/3jRa1wg>

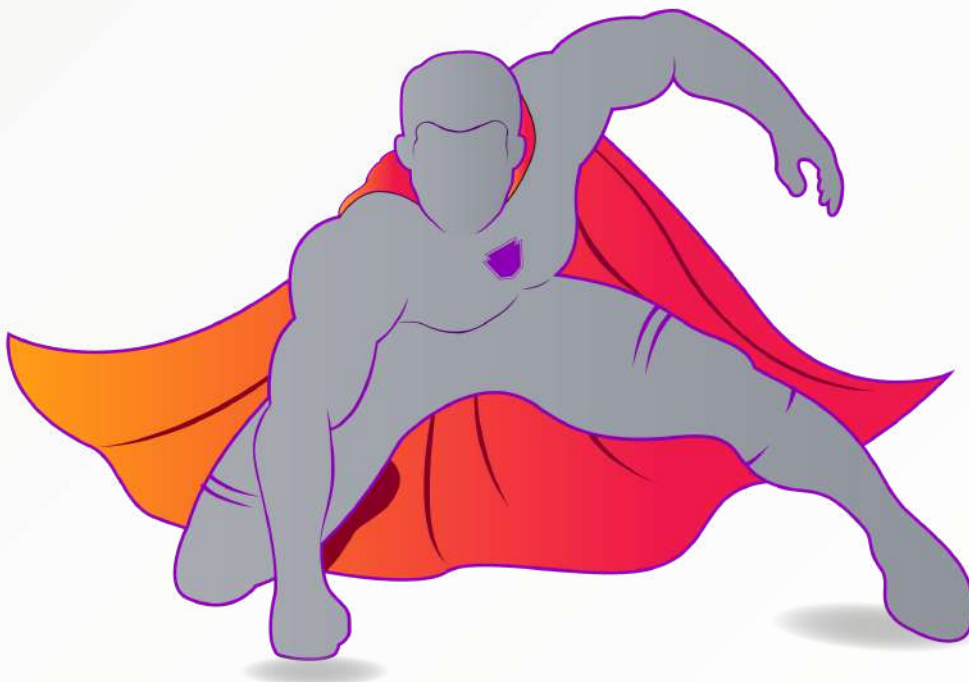
A major hack that compromised Uganda's mobile money network has plunged the country's telecoms and banking sectors into crisis. It is security breach on a consumer finance aggregator, Pegasus Technologies, which mainly affected bank to mobile wallet transfers. At least \$3.2 million is estimated to have been stolen in this latest incident. The hackers used around 2,000 mobile SIM cards to gain access to the mobile money payment system, according to local papers.

CONCLUSION

These attacks that we've covered have been covered and briefed to the level someone could normally engage themselves towards reading something fully. Rest unsaid are millions and covering and detailing all of them wouldn't completely reach the eyes of readers as too much of anything becomes overfed. Henceforth, we've encompassed the most significant ones that would represent most of the uncovered cyber threats.

Millions of organizations and individuals have clicked phishing links and fallen victims to the deceiving baits of hackers with 'lack of awareness' being one of the obvious reasons for it. To go deeper, cybercrimes have caused about 1 lakh 25 thousand crores of losses in India alone as per the National Cyber Security Coordinator Lieutenant General Dr. Rajesh Pant in 2019. Now, it has been multiplied many times in 2020 due to this WFH with least employees, many security voids were unfulfilled. As a proof to this, the director of CERT-In has blatantly agreed and declared that even since WFH began, there has been whopping 4300% of increase in cyber threats caused by phishing under COVID 19 protection click baits. Unless and until awareness is attained, nothing can be changed.

For further details, feel free to reach us out anytime.





Blog

[CLICK HERE](#)



[CLICK HERE](#)

YOU MAY ALSO BE INTERESTED IN OUR PREVIOUS REPORTS



CLICK HERE



CLICK HERE

[CLICK HERE](#)



[CLICK HERE](#)



FREE TOOL SETS



FEEL FREE TO REACH US FOR ALL YOUR CYBERSECURITY NEEDS

contact@briskinfosec.com | www.briskinfosec.com