EDITION 15

THREATSPLOIT

ADVERSARY REPORT

NOVEMBER 2019

AFFILIATED BY

NCDRC (NATIONAL CYBER DEFENCE RESEARCH CENTRE)
IN COLLABORATION WITH BINT LABS
www.ncdrc.res.in

PREPARED BY

www.briskinfosec.com
CERT-IN EMPANELLED FIRM

INTRODUCTION

Certain things are unstoppable. The forces of nature like rain, sun, wind, storms are unstoppable. Volcanic eruption and tsunami disasters are unstoppable. But, one such thing apart from nature has seemingly got its place in the list of “Unstoppables”. It's none other than ‘cyberattacks’. These seem to be just something, take off many things and keep growing beyond anything.

For example:

Regarding ransomware…. they’ve predominantly occurred in many places on this month, have encrypted the data and demanded in bitcoins for victims to seek data manumission. Months of earning are gone in seconds.

Regarding phishing… I’d like to name these threat actors as ‘witty hitters.’ Because, these threat vectors appear to be so exact like the authenticated ones but in reality, they aren’t. A single click is what they need to prove how notorious they can be towards you. It’s becoming hard to distinguish the true and fake ones due to their spectacular evolution.

Regarding malware… Remember how silently yet brilliantly a leopard enters into a place to get its prey? This is how a malware is. Stealthily yet brilliantly, it gets into your security environment, helps intruders gain remote access and in executing their malicious actions. Moreover, these are becoming very hard to trace these days.

Well, these attacks are like ‘a’ in ‘attacks’. There are many such occurrences in this report. Just check them out! It's exclusively prepared for you with the noble intension of creating cyber security awareness!

CONSUMER TECH

- Critical Remote Code Execution Vulnerability Patched in Exim Email Server.
- Nasty PHP7 remote code execution bug exploited in the wild.
- Firefox, Chrome Bugs Allow Arbitrary Code-Execution
- Data leak exposes more than 200K job seeker CVs
- iOS Clicker Trojan Malware Found in 17 Apps in Apple's App Store.
- 7.5 Million Records of Adobe Creative Cloud User Data Exposed
- Critical command execution vulnerability in iTerm2 patched, upgrade ASAP!
- Critical Command Execution Vulnerability Found in D-Link Routers That Will Not Be Patched Attribution link

RETAIL

- Ransomware attack on cosmetics brand, The Heat Group and BillTrust
- Shipping giant Pitney Bowes hit by ransomware
- Home Group: Thousands warned over data breach
- Toms Shoes' Mailing List Hacked to Tell Users to Log Off
- P&G Online Beauty Store Hacked to Steal Payment Info
- AWS hit by DDoS attack dragging half of web down
- Malicious Malware Detected On American Cancer Society’s eComm Site
- Avast Vulnerability Potentially Allows DLL Hijacking
- Avast's internal network was hacked via a compromised VPN profile
- Pos Malaysia confirms attempted malware attack, lodges police report

- Ransomware Attack Reportedly Hits Practice Management Company,Locking Lawyers Out of their Case Files
- The Nationals' Ticket System Got Hacked and Somebody Stole a Bunch of World Series Tickets

BANKING AND FINANCE

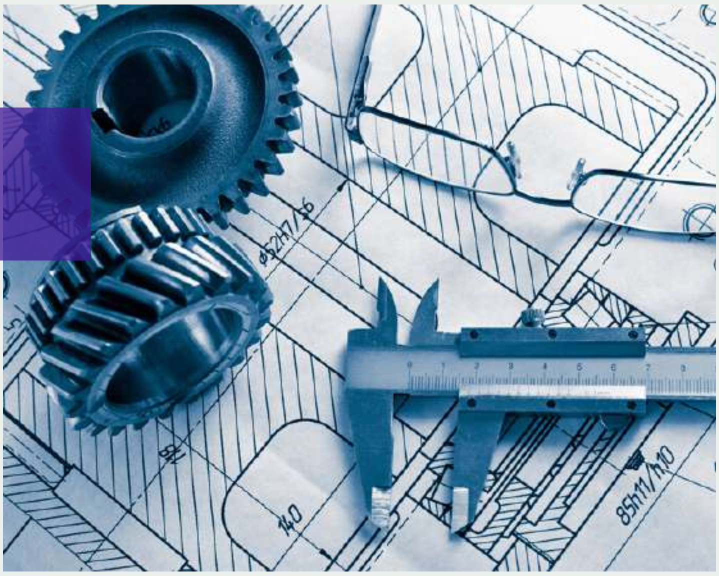
- City of Joburg, banks under cyber attack
- Russia's Sberbank hit with huge data leak
- UM E-Payment Site Gets Anonymously Hacked & Now Displays Bold Protest Message

GOVERNMENT

- Georgia hit by massive cyber-attack
- Ocala gets scammed in 'spear phishing' attack.
- City of Carrollton Computer Network Hacked

ENTERTAINMENT

- Discord Turned Into an Info-Stealing Backdoor by New Malware
- EA leaks personal data for 'FIFA 20' Global Series players



AUTOMOTIVE

- Major German manufacturer still down a week after getting hit by ransomware

RESTAURANT

- Japanese hotel chain sorry that hackers may have watched guests through bedside robots

SOCIAL MEDIA

- Shane Watson's Instagram and Twitter accounts hacked, ex-cricketer apologises for illicit photos

EDUCATION

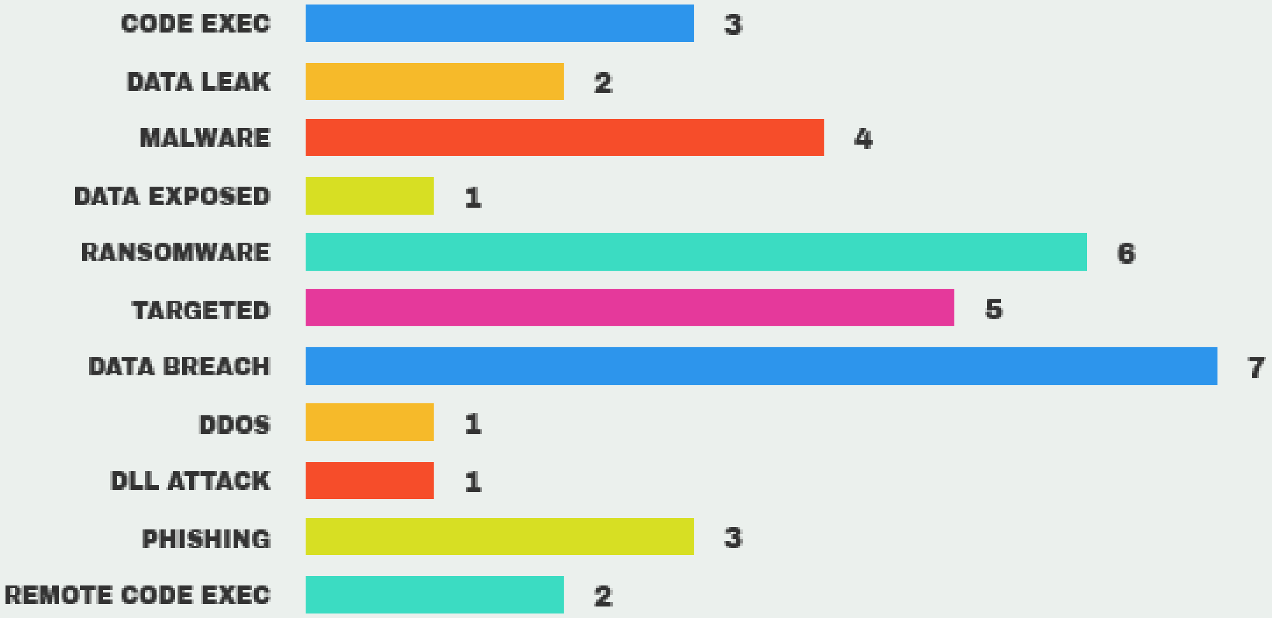
- Downingtown Area School District investigating data breach; multiple students being questioned

HEALTHCARE

- Data breach at St. Louis health center impacts up to 152,000
- Alabama hospitals have been hit by a massive ransomware attack

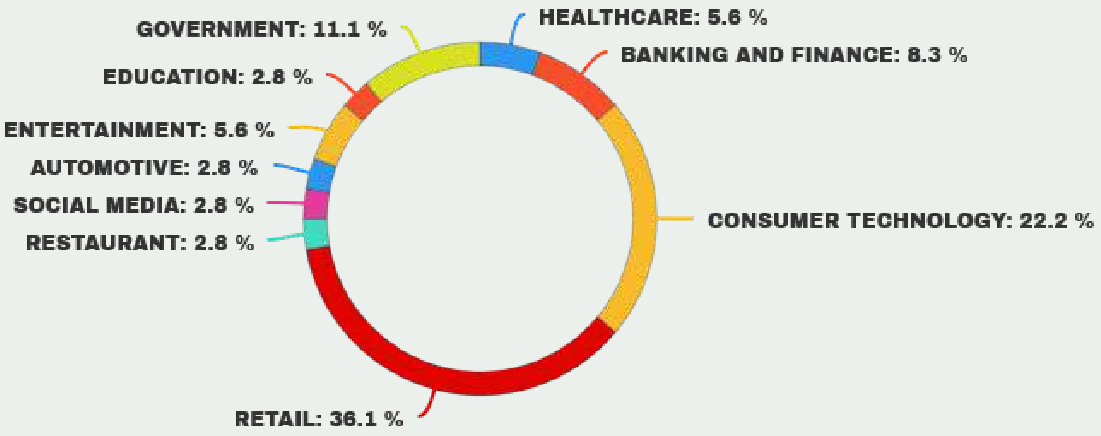
TYPES OF ATTACK VECTORS

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



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 and Retail has been hit the most.



39.4%

Retail

Critical Remote Code Execution Vulnerability Patched in Exim Email Server

Exim recently patched a critical vulnerability that could enable threat actors to execute arbitrary codes on servers running certain versions of the company's software. The vulnerability identified as CVE-2019-16928, put numerous systems at risk. Exim is used by 57% of all email servers worldwide. Exim versions 4.92, 4.92.1 and 4.92.2 are all vulnerable, so users are urged to update their servers to Exim 4.92.3. It was also revealed last month, that a new ransomware strain dubbed Lilocked or Lilu was targeting servers, running outdated instances of Exim.

ATTACK TYPE
RCE attack

CAUSE OF ISSUE
Security flaws

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

Nasty PHP7 remote code execution bug, exploited in the wild

A recently patched security vulnerability CVE-2019-11043 in modern PHP versions is again being exploited in the wild. This vulnerability was discovered by Andrew Danau, through CTF challenge. It lets attackers to run malicious commands on the server by accessing a specially crafted URL. Fortunately, only NGINX servers with PHP-FPM enabled are vulnerable. Due to publicly available POC codes and simplicity of exploiting this bug, website owners are urged to update to the latest PHP versions 7.3.11 and 7.2.24, which had been released with patches for CVE-2019-11043.

ATTACK TYPE
RCE Flaw

CAUSE OF ISSUE
Security flaws

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

Firefox, Chrome Bugs Allow Arbitrary Code-Execution

Two of the greatest browsers, Firefox and Chrome, have been discovered with serious bugs.

In Firefox: Some of the major vulnerabilities found were CVE 2019-5903, CVE 2019-11758 and CVE 2019-11757. These vulnerabilities are capable of allowing hackers to bypass content security policy (CSP), heap buffer overflow, launch injection attacks and much more. Finally, somehow Firefox managed to patch these issues.

In Chrome: It identified 37 security issues. Main includes CVE-2019-13699, a high severity use-after-free bug in media. By exploiting, the browser's sensitive information can be obtained, security restrictions can be bypassed and unauthorized actions can be performed. Somehow, finally, Google patched all the 37 security issues.

ATTACK TYPE
Arbitrary Code-Execution

CAUSE OF ISSUE
Security flaw

TYPE OF LOSS
Reputation

COUNTRY
GLOBAL

Data leak exposes more than 200K job seeker CVs

Authentic Jobs and Sonic Jobs, two recruitment firms from America and Great Britain, together have leaked the CV details of about 250,332 job applicants online. Their exposed details comprised of names, addresses, phone numbers and career statistics. The reason behind this is because of improperly configuring their Amazon Web Server's S3 Buckets. It wasn't secured enough and thus became exposed publicly with all the stored data alongside it. The companies admitted their blunder and ensured to set things right without delay.

ATTACK TYPE
Unauthorised access

CAUSE OF ISSUE
Improper AWS config

TYPE OF LOSS
Reputation/Data

COUNTRY
USA & GBR

iOS Clicker Trojan Malware Found in 17 Apps in Apple's App Store

17 iOS apps were infected with a clicker Trojan malware and spread through Apple App Store to perform ad fraud-related tasks by using the command and control servers. This malware simulates ad clicks and opens web pages in the background without the need of user interaction, thus carrying out an ad fraud campaign by abusing all iPhones, iPads, and iPods it compromises. Once executed, the malware starts collecting system info like the OS version, the device's manufacturer and model, the user's country of residence, the internet connection type, the user's time zone, and info on the app with the clicker Trojan module.

ATTACK TYPE
Malware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

7.5 Million Records of Adobe Creative Cloud User Data Exposed

ATTACK TYPE
Data Exposed

CAUSE OF ISSUE
Improper server config

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

A whopping amount of 7.5 million records of Abode's data in Adobe's Elasticsearch server was exposed. The exposed data comprised of user's subscription status, member ID's, country and previous logins. This server was discovered by actively scanning the web in search for insecure databases. However, there is no information about information misuse, if yes, could be used for phishing campaigns. Moreover, sensitive details like passwords and payment details weren't secured. This was informed to the company and they fixed this quickly without further ado's.

Critical command execution vulnerability in iTerm2 patched, upgrade ASAP!

A critical vulnerability (CVE-2019-9535) present in the tmux integration feature of iTerm2, a macOS terminal emulator frequently used by developers and system administrators, could allow attackers to take control of the target system. The vulnerability has been present for at least seven years. It was discovered by Radically Open Security researchers. iTerm2 developer, George Nachman, says to use v3.3.6, which fixes the flaw. The issue affects all versions released before this last one. Users are urged to update manually instead of waiting for an update prompt from the software.

ATTACK TYPE
command execution

CAUSE OF ISSUE
Security flaw

TYPE OF LOSS
Reputation

COUNTRY
GLOBAL

Critical Command Execution Vulnerability Found in D-Link Routers That Will Not Be Patched

ATTACK TYPE
Command Execution

CAUSE OF ISSUE
Lack of maintenance

TYPE OF LOSS
Reputation

COUNTRY
GLOBAL

An unauthenticated vulnerability (FG-VD-19-117/CVE-2019-16920) has been identified in some older D-Link routers which if exploited could make hackers gain remote access. Despite acknowledging this, the company is hesitant to amend this. They say the affected models "DIR-652, DIR-655, DIR-866L and DHP-1565" are outdated and no longer newly manufactured. As this will never be patched, the only real solution for users is to use the updated device.

Gillian Franklin hit by $2 million cyber attack

Ms. Gillian Franklin, the founder of cosmetic business company named, The Heat Group, has been hit by a cyberattack causing about $2 million on her business. She just logged in to her business from London and found out that all online documents and files were missing. She also found out a ransom message in website, which indicated to pay $40,000 in Bitcoin. When collaborating with the security team, it was identified that few data were already deleted and many compromised,, with no point in paying ransom. Instead, she said her security team to restore the systems. She also cautioned other businesses to scrutinise their security quality and amend it consistently.

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Lack of maintainces

TYPE OF LOSS

Reputation/Data

COUNTRY

NEW JERSY (USA)

Shipping giant Pitney Bowes hit by ransomware

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation/Data

COUNTRY

USA

Pitney bowes, a familiar shipping tech company with over 1.5 million clients and users worldwide, recently fell as a victim to cyber threat.
Wondering what?
The attacked threat vector is identified as a ransomware that has encrypted many information on its systems. However, the company ensured that no data was lost. But, many of their internal systems were taken offline causing hindrances for their business. The company notified their customers about this and also said that they're working with an external security firm to fix this issue. Details on the type of ransomware isn't known yet!

Toms Shoes' Mailing List Hacked to Tell Users to Log Off

One of the most popular footwear retailers 'Toms' have got their email newsletter hacked by someone who calls himself as "a nice man." This message was sent by Nathan. Nathan instead of warning the company's security issues directly communicated with its newsletter's subscribers. During investigation, it was confirmed that 'Toms' newsletter had truly been compromised. They later informed their subscribers to stay alert. However, their customers weren't happy as it was informed way too late.

ATTACK TYPE

Targetted

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation/Data

COUNTRY

CALIFORNIA
(USA)

Home Group data breach hits 4,000 housing association customers

ATTACK TYPE

Data breach

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation/Data

COUNTRY

UK

One of the UK's biggest housing associations named Home Group, became the latest sensation of a data breach victim. The data breach is believed to have exposed the personal details of over 4000 people including their names, addresses and contact information from England and Yorkshire. This information came into light after being discovered and notified by an external security researcher (name unrevealed). Without delay, the company worked with a security team and swiftly contained the situation within 30 minutes. However, the culprit behind this remains unfound yet!

AWS (Amazon Web Server) hit by a major DDoS attack

AWS recently experienced a powerful DDoS attack that appears to have lasted for around eight hours. As a result of this powerful DDoS attack, many users globally were halted from using some Amazon S3 services. Even Amazon's router 53 DNS web services were affected. The main cause for this is, Amazon used Shield Advanced as a DDoS mitigation measure but the notoriety of the DDoS attack was just too much to be stalled. However, an official investigation regarding this security disaster is ongoing and further details are to revealed post that.

ATTACK TYPE
DDOS

CAUSE OF ISSUE
Improper maintainance

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

Malicious Malware Detected On American Cancer Society's eComm Site

ATTACK TYPE
Malware

CAUSE OF ISSUE
Lack of maintainance

TYPE OF LOSS
Reputation/Data

COUNTRY
GEORGIA

William De Groot, a security researcher discovered that a deep hidden credit card stealing malware was inserted into the code of American Cancer Society's online store. It's reported that this malware was injected for doing hot sales on dark web and for other malicious activities. De Groot decoded the information and discovered the web address of the server to be hosted from Moscow, but it was just a decoy. However, this malicious malware was removed on Oct 25th but victims affected remain unknown. It's further advised that people using credit card on this forum should contact their payment provider.

RETAIL

Avast Vulnerability Potentially Allows DLL Hijacking

Avast software has been identified with a vulnerability CVE-2019-17093 that allows an attacker to load a malicious DLL file to bypass defences and escalate privileges. Usually, even administrators are not allowed to write DLL to the AM-PPL (Anti-Malware Protected Process Light). However, this restriction can be bypassed by writing the DLL file to an unprotected folder from which components are loaded by the application. The cause of this is due to lack of safe DLL loading and the code integrity is not enforced in the AM-PPL process. As a remediation, Avast recommended users to update to the latest version ASAP.

ATTACK TYPE
DLL attack

CAUSE OF ISSUE
Poor security

TYPE OF LOSS
Reputation/Data

COUNTRY
CZECH REPUBLIC

Avast's internal network was hacked via a compromised VPN profile

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
CZECH REPUBLIC

Avast, a popular security antivirus provider, has recently become the victim of a vicious supply chain attack targeting its internal network. "The evidence we gathered pointed to activity on MS ATA/VPN [Microsoft Advanced Threat Analytics] on 1 October, when we re-reviewed an MS ATA alert of a malicious replication of directory services from an internal IP that belonged to our VPN address range, which had originally been dismissed as a false positive, reports the company. They've confirmed their domain's admin privilege has been comprised through privilege escalation. However, the issue was fixed by Oct 15th and additional security measures were also implemented.

Pos Malaysia confirms attempted malware attack, lodges police report

POS Malaysia confirmed that a malware attack was inferred in their systems which rendered them inaccessible to use it. The malware was identified in its core systems and online services while doing system upgrade. Further, the company claimed that no users nor customers were affected by this. They said that they've shut down the services to prevent it from spreading. They said that the services will be brought back to normal soon. An official investigation is ongoing to find out the intruders behind this. As of now, it's being reported that the malware has been contained.

ATTACK TYPE

Malware

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation/Data

COUNTRY

MALAYSIA

RETAIL

Ransomware Attack Reportedly Hits Practice Management Company, Locking Lawyers Out of their Case Files

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Lack of awarenesss

TYPE OF LOSS

Reputation/Data

COUNTRY

USA

TrailWorks, one of the world's largest legal case management software providers for law organizations and attorneys was hit by a severe ransomware attack. This made lawyers paralysed towards accessing the legal documents hosted on 'TrailWorks' platform. An email was sent, cautioning lawyers regarding this incident. They said they are working with top security firms to fix this situation ASAP. Prior to it, 2 days after the attack, the affected systems were disinfected, suggesting that ransom was paid.

The Nationals' Ticket System Got Hacked and Somebody Stole a Bunch of World Series Tickets

The National Ticketing System got recently hacked and tickets were stolen. But, identifying the issue didn't take too much time. According to a spokesperson from Washington Nationals, "We've identified a fraudulent activity presence in our ticketing system. Any ticket that was taken illegitimately was blocked. Most importantly, no personal information was breached. We've also taken remediation measures to prevent such threats in the future."

ATTACK TYPE

Targetted

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation/Data

COUNTRY

USA

BANKING AND FINANCE

City of Joburg, banks under cyber attack

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation/Data

COUNTRY

SOUTH AFRICA

A cybercriminal group named the Shadow kill hackers, launched a severe ransomware attack on the city of Johannesburg, disrupting the city's network and shutting down the websites of many banks there. As a precautionary, the city's email services, websites and billing systems were halted. Customers will not be able to transact on e-services nor log queries via the call centre. To seek redemption, hackers have demanded a ransom of 4.0 bitcoins by October 28th. If failed, then all the data would be exposed online, said their message. An official investigation is ongoing by the city's cybersecurity professionals, who are keen on getting this resolved ASAP.

BANKING AND FINANCE

Russia's Sberbank hit with huge data leak

Sberbank, a hugely familiar bank in Russia has suffered a data breach. About 200 customers are said to be affected by this data leak. This is speculated to be the biggest data breach in Russian history. It is said that through these 200 entries, financial details of over 60 million were known. The illegitimate seller has claimed 8 cents per entry. The suspect behind this disastrous cause is said to be caused due to a disgruntled insider. Further, an official investigation is underway to find who did this and how to fix this ASAP.

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

COUNTRY
RUSSIA

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Clicking malicious links

TYPE OF LOSS
Reputation/Data

COUNTRY
MALAYSIA

UM E-Payment Site Gets Anonymously Hacked & Now Displays Bold Protest Message

University of Malaya has joined as the new member in the hacked victims list. Yes, the university's e-payment page on its website was hacked on October 18th. The link when clicked redirected towards a page containing some disdain messages (like religious and religious comments) in the website. It also had resenting hashtags against the university's Vice-chancellor.

The backstory behind this was, a student during convocation shouted and protested against the unrevealed injustices happening in the university. The next day, when another student was suspected of causing the same commotion, he was stopped from going to the ceremony. However, police have arrested the person for violating graduation ceremony protocols and said that it isn't the place to protest. They are investigating under Section 504 Penal code.

GOVERNMENT

Georgia hit by massive cyber-attack

Georgia has faced the biggest data breach in its history. Yes, thousands of websites in Georgia have been defaced and many National TV channels were taken offline. Affected websites displayed the photo of former Georgia President, Mikheil Saakashvili, with a caption "I'll be back". The affected websites were hosted on a compromised server managed by Proservice, a hosting provider in Russia. Further details reveal that the attack wasn't a sophisticated one but the security defences of Georgia used were fragile. However, an official investigation is ongoing under Article 284 and 286 of the criminal code of Georgia.

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Poor server maintainces

TYPE OF LOSS
Reputation

COUNTRY
GEORGIA (USA)

GOVERNMENT

Ocala gets scammed in ‘spear phishing’ attack

A “spear phishing” email attack led an Ocala employee to mistakenly transfer $640,000 to a fraudulent bank account set up by a scammer. City spokeswoman, Ashley Dobbs, said someone sent an email to a city department requesting payment for services via electronic transfer. When paid, there was no positive signs. Suspicions arouse and the city’s officials reported the incident to the Ocala Police Department, which in turn notified the FBI. In light of the incident, the city conducted an internal investigation into how they got scammed and found it was a spear phishing attack from the scammers. To thwart such miseries in future, changes in policies and better security features are to be implemented, so said Dobbs.

ATTACK TYPE
Phishing

CAUSE OF ISSUE
Lack of awarness

TYPE OF LOSS
Reputation/Data

COUNTRY
OCALA

City of Carrollton Computer Network Hacked

ATTACK TYPE
Security breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
TEXAS (USA)

The City of Carrollton's computer network experienced a cyberattack. Public safety response and Carrollton's 911 emergency response were not affected, but some city services were impacted. The City of Carrollton says it currently has no reason to believe that resident information has been accessed or will be affected. Water, sewer, and trash services are running on schedule. Most residents should not experience interruptions. The City of Carrollton says it’s working with state and federal officials to investigate this criminal act and will pursue prosecution to the fullest extent of the law. Further, they said that they’ll update citizens as more information becomes available.

ENTERTAIMENT

Discord Turned Into an Info-Stealing Backdoor by New Malware

Researchers from malware hunter team discovered a new malware named “Spidey Bot” that’s targeting Discord users by modifying the Windows Discord client, so that, it’s transformed into a backdoor and an information-stealing Trojan. This allows the malware to modify its core files so that the client executes malicious behaviour. Vitali kremez, a reverse security engineer says that Discord messaging app is being used to spread the malware. Moreover, this malware is very hard to be detected, even through virus total. The best way to quarantine this malware if you’re infected is by uninstalling this malware and then by legitimately reinstalling it.

ATTACK TYPE
Malware

CAUSE OF ISSUE
Poor security pratices

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

EA leaks personal data for 'FIFA 20' Global Series players

ATTACK TYPE
Data leak

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
GLOBAL

EA Games has leaked the personal information of 1600 game contestants for FIFA 20 Global series competition who registered through the company’ website. They registered in a link in the company’s website for verifying their EA account, instead, the forms displayed the registrant’s personal information. The compromised info included email addresses, account ID, DoB’s. Upon acknowledging this, EA Games sooner within 30 minutes responded, “We’ve identified the security problem and have successfully fixed it. Further, users won’t experience such inconvenience from us in the times ahead.”

AUTOMOTIVE

Major German manufacturer still down a week after getting hit by ransomware

Pilz, one of the world's most popular automated tools manufacturers from Germany, has been dormant over a week after being hit by a severe ransomware named BitPaymer. Due to it, several users across 76 countries worldwide using the company's products and services have been stalled. As a precautionary, the company isolated the affected computers and blocked access to the corporate network. However, it took six days for the company to seek a redemption from this blow, and normal services were restored.

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of awarness

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

TRAVEL & HOSPITALITY

ATTACK TYPE
Security breach

CAUSE OF ISSUE
Security flaw

TYPE OF LOSS
Reputation/Data

COUNTRY
JAPAN

Japanese hotel chain sorry that hackers may have watched guests through bedside robots

HIS hotel chain in Japan have robots and humanoids that uses facial recognition technology and lets customers in their room, and a bedside robot will look over other requirements. Recently, a security researcher discovered a vulnerability that allows intruders to gain access to cameras and microphones in the robot remotely so they could watch and listen to anyone in the room in the future. Initially, he warned the company but later exposed it online when they showed riddance towards him. However, the hotel finally updated their robots and have fixed their flaws.

SOCIAL MEDIA

Shane Watson's Twitter account hacked

Former Australian cricket star 'Shane Watson's' Twitter account recently got hacked. In addition to a series of objectionable tweets, the account's profile picture and name were also changed. Watson's account was active for nearly half-an-hour during which there were a series of tweets, which included fat-shaming statements and racial slurs among others. Watson's name was also changed to 'crimin.al.' After fans raised an alarm, Watson's account was restored to its original status, and all the offensive tweets were deleted.

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
AUSTRALIA

EDUCATION

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
PENNSYLVANIA

Downingtown Area School District investigating data breach; multiple students being questioned

A high school in Downingtown, a district in Pennsylvania has recently experienced a cyberattack. Officials at Downingtown Area School District (DASD) are investigating this issue pertaining to teacher-student software. But, the students said it was just done for a game. Investigation reveals that a potential hack was observed in the school's Naviance accounts. Naviance is a college and career guidance website for students. Further analysis says hackers have compromised the profile information of entire students from DASD. This is cited to be one of the biggest hacks in Pennsylvania. Regarding this, DASD officials have said that student's safety is our prime concern and work is ongoing to remedy this ASAP.

Data breach at St. Louis health center impacts up to 152,000

About 152,000 people were affected by a cyberattack at St. Louis health Center, said officials. The attack targeted and compromised patient information such as addresses, social security numbers, medical providers. But, medical records of patients were affected. A hefty ransom was demanded to unlock it. However, the Center says it refused to pay the ransom and Instead contacted police. CEO Dwayne Butler says there is no way to know if the information has been viewed or accessed by the attacker. He says the Center regrets "any inconvenience this incident may have caused our patients and customers."

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

lack of awarness

TYPE OF LOSS

Reputation/Data

COUNTRY

ST. LOUIS COUNTY

Alabama hospitals have been hit by a massive ransomware attack

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation/Data

COUNTRY

ALABAMA & AUSTRALIA

10 hospitals, 7 from Australia and 3 from Alabama, have been hit by ransomware attack. Regarding this, a spokesperson said, this attack hasn't affected any patient records but created a disruption for hospital services like surgeries and OP (Out Patient) services. The hospitals in Australia somehow identified the affected systems and separated them while Alabama hospitals found this difficult. Moreover, many patients were shifted towards other hospitals. The hospital's brass said that, "Details regarding the ransom isn't revealed by the hackers yet. Ransomware attacks are growing rapidly and in 2019, ransomware holds the second most highly occurred cyberattack. Further, official investigation is ongoing to fix this ASAP."

CONCLUSION

Due to some restrictions, we weren't allowed to reveal many such notorious occurrences of cyberattacks from worldwide, but the above ones are just the significant ones among many that are unsaid.

Every month, at least one entire nation is creating a history with cyberattacks. In August, **Bulgaria** faced the biggest data breach in its history exposing 5.1 million citizens data. In September, **Ecuador** faced the biggest data breach in its history exposing 20+ million citizens data.

In October, **Georgia** and **Pennsylvania** faced the biggest **data breach** in its history with many data loss.

Next month, who it's going to be? Where it's going to be? How much data loss it's going to be?

Well, honestly, we don't know! But, we have the best and the advanced security solutions to secure your security environment against the ever growing and ever evolving cyber threats.

Just reach us out.

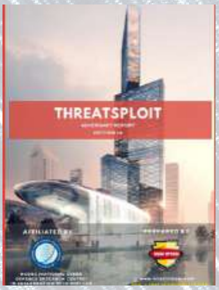
We'll secure your data like no one else does!

```
r-top: 1px solid #ccc !important;}
left;}
z-index: 10;}
border: 1px solid #ccc !important; bo
one; [illegible] none; user-selec
e-out 0s;}
gba(0,0,0,.2)}
```

REFERENCES

- https://www.oodaloop.com/briefs/2019/10/01/critical-remote-code-execution-vulnerability-patched-in-exim-email-server/
- https://www.zdnet.com/article/nasty-php7-remote-code-execution-bug-exploited-in-the-wild/
- https://threatpost.com/critical-firefox-bugs-arbitrary-code-execution/149455/
- http://www.digitaljournal.com/tech-and-science/technology/data-leak-exposes-more-than-200k-job-seeker-cvs/article/560196
- https://www.bleepingcomputer.com/news/security/ios-clicker-trojan-malware-found-in-17-apps-in-apples-app-store/
- https://www.bleepingcomputer.com/news/security/75-million-records-of-adobe-creative-cloud-user-data-exposed/
- https://www.helpnetsecurity.com/2019/10/10/iterm2-vulnerability/
- https://blog.mozilla.org/security/2019/10/09/iterm2-critical-issue-moss-audit/
- https://www.techradar.com/news/gaping-security-hole-means-owners-of-these-d-link-routers-should-upgrade
- https://www.cybersecurity-insiders.com/ransomware-attack-on-cosmetics-brand-the-heat-group-and-billtrust/
- https://techcrunch.com/2019/10/14/pitney-bowes-ransomware-attack/
- https://www.bbc.com/news/uk-england-50132533
- https://www.grahamcluley.com/toms-shoes-newsletter-hacked-by-a-nice-man/
- https://www.bleepingcomputer.com/news/security/pandg-online-beauty-store-hacked-to-steal-payment-info/
- https://www.crn.com.au/news/aws-hit-by-ddos-attack-dragging-half-of-web-down-532842
- https://www.pymnts.com/news/security-and-risk/2019/malicious-malware-detected-on-american-cancer-society-ecomm-site/
- https://cyware.com/news/avast-vulnerability-potentially-allows-dll-hijacking-14ad6bff/
- https://www.bleepingcomputer.com/news/security/discord-turned-into-an-info-stealing-backdoor-by-new-malware/
- https://www.infosecurity-magazine.com/news/ea-games-leaks-personal-data/
- https://www.charlotteobserver.com/news/science-technology/article236661538.html
- https://searchsecurity.techtarget.com/news/252471758/Hospital-ransomware-attacks-lead-to-patients-being-turned-away
- https://6abc.com/downingtown-area-school-district-investigating-data-breach/5629227/
- https://www.nbcphiladelphia.com/on-air/as-seen-on/Downingtown-Area-School-District-Data-Breached-By-Student-Hackers_Philadelphia-563441232.html
- https://twitter.com/CityofJoburgZA/status/1187476208872636416
- https://blockpublisher.com/johannesburgs-civil-website-hacked-hackers-demanding-ransom-in-bitcoin/
- https://www.bbc.com/news/technology-50207192
- https://www.ocala.com/news/20191024/ocala-gets-scammed-in-spear-phishing-attack
- https://www.nbcdfw.com/news/local/City-of-Carrollton-Computer-Network-Hacked-562771671.html
- https://www.msn.com/en-us/news/us/city-of-carrollton-computer-network-hacked/ar-AAIBakV
- https://www.businesslive.co.za/bd/national/2019-10-25-city-of-joburg-banks-under-cyber-attack/
- https://www.techradar.com/news/russias-sberbank-hit-with-huge-data-leak
- https://www.worldofbuzz.com/um-e-payment-site-gets-anonymously-hacked-now-displays-bold-protest-message/
- https://www.zdnet.com/article/major-german-manufacturer-still-down-a-week-after-getting-hit-by-ransomware/
- https://www.theregister.co.uk/2019/10/22/japanese_hotel_chain_sorry_that_bedside_robots_may_have_watched_guests/
- https://www.indiatoday.in/sports/cricket/story/former-australia-all-rounder-shane-watson-instagram-and-twitter-accounts-hacked-1609837-2019-10-16

YOU MAY ALSO BE INTERESTED IN OUR PREVIOUS WORKS



REFERENCES ABOUT BRISKINFOSEC

CASE STUDIES

SOLUTIONS

SERVICES

RESEARCH

COMPLIANCES

BLOGS

BRISK INFOSEC

CYBER TRUST & ASSURANCE

FEEL FREE TO REACH US FOR ALL YOUR CYBERSECURITY NEEDS

contact@briskinfosec.com | www.briskinfosec.com