December -2019
Edition-16

THREATSPLOIT ADVERSARY REPORT

BRISK INFOSEC
CYBER TRUST & ASSURANCE

INTRODUCTION

First and foremost, an earnest thanks to all of you from Briskinfosec!2019 has been a great year for Briskinfosec and this is the last report of this year.

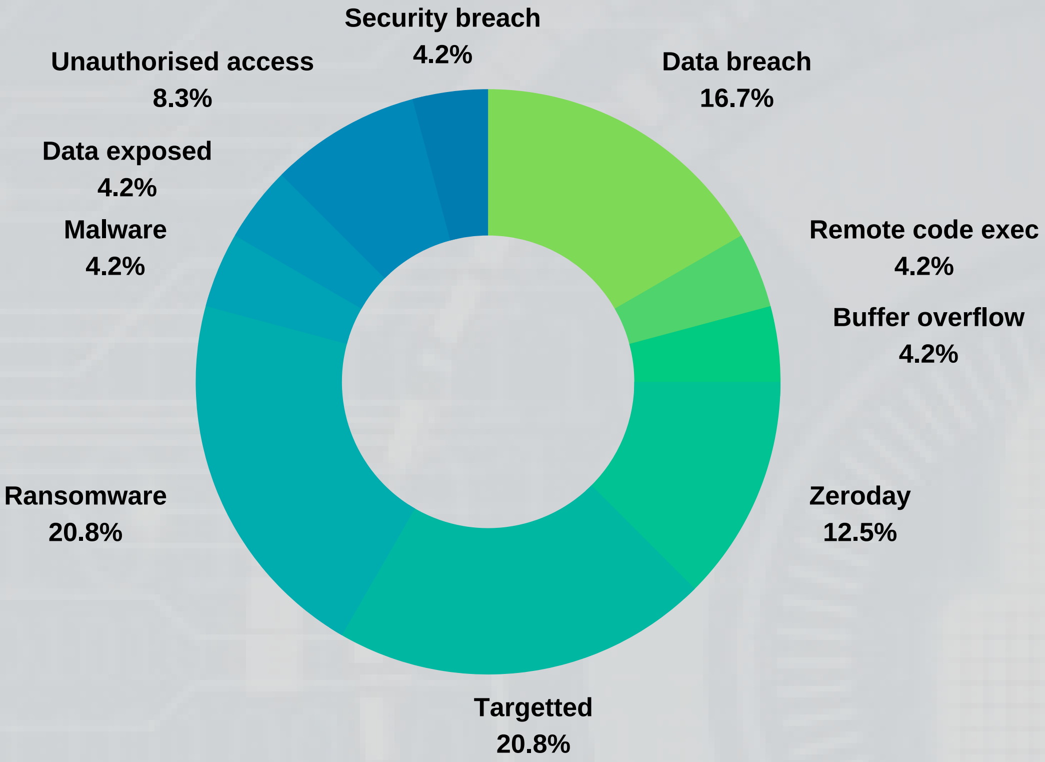
Each month we're continually preparing a threatsploit report consisting of major cyberattacks happening around the world. This new report containing the globally occurred cyberattacks in the month of November 2019.

This report contains a collection of major cyberattacks in widely used devices such as amazon Alexa, Google Voice, and Apple Siri, and many of the Government organization are also been a victim of the cyber attacks From the bottom of our hearts, once again, thank you for the continued support.

Forever, we're grateful for it!

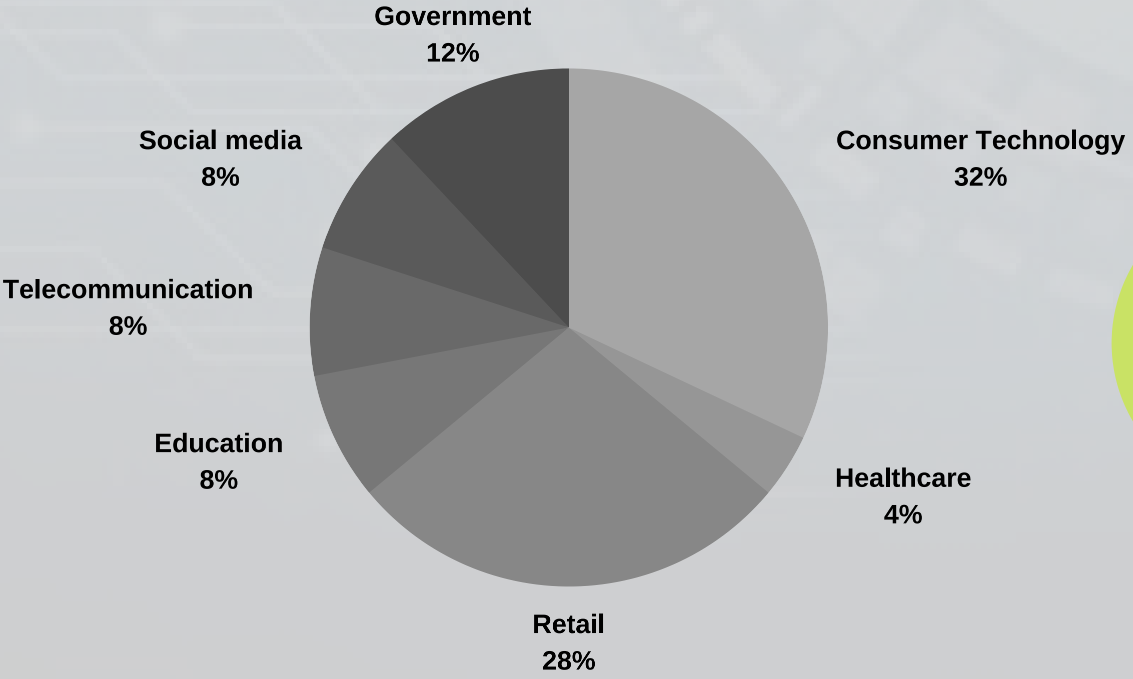
TYPES OF ATTACK VECTORS

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



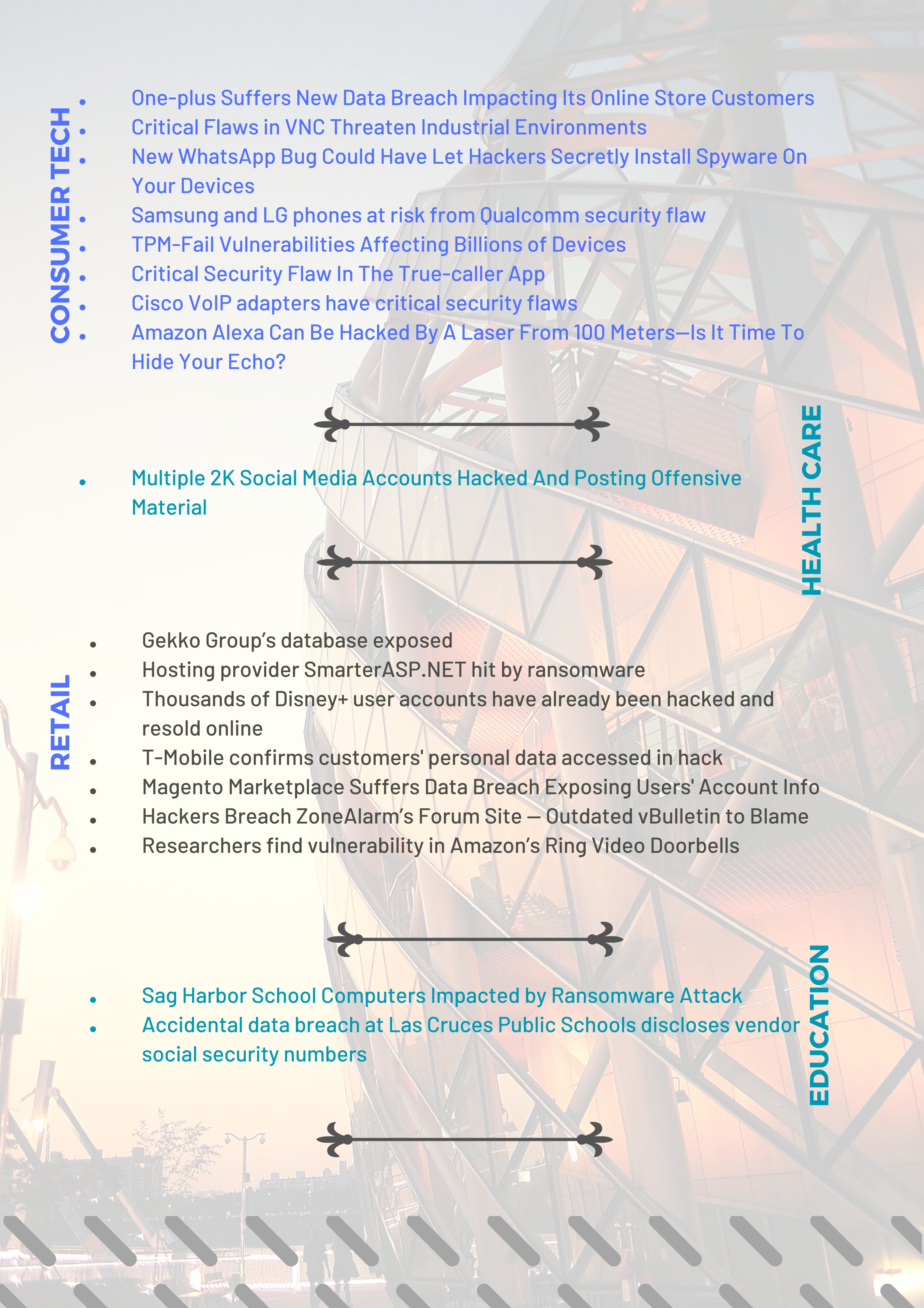
SECTORS AFFECTED BY ATTACKS

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.



32%

consumer Tech



CONSUMER TECH

- One-plus Suffers New Data Breach Impacting Its Online Store Customers
- Critical Flaws in VNC Threaten Industrial Environments
- New WhatsApp Bug Could Have Let Hackers Secretly Install Spyware On Your Devices
- Samsung and LG phones at risk from Qualcomm security flaw
- TPM-Fail Vulnerabilities Affecting Billions of Devices
- Critical Security Flaw In The True-caller App
- Cisco VoIP adapters have critical security flaws
- Amazon Alexa Can Be Hacked By A Laser From 100 Meters—Is It Time To Hide Your Echo?

HEALTH CARE

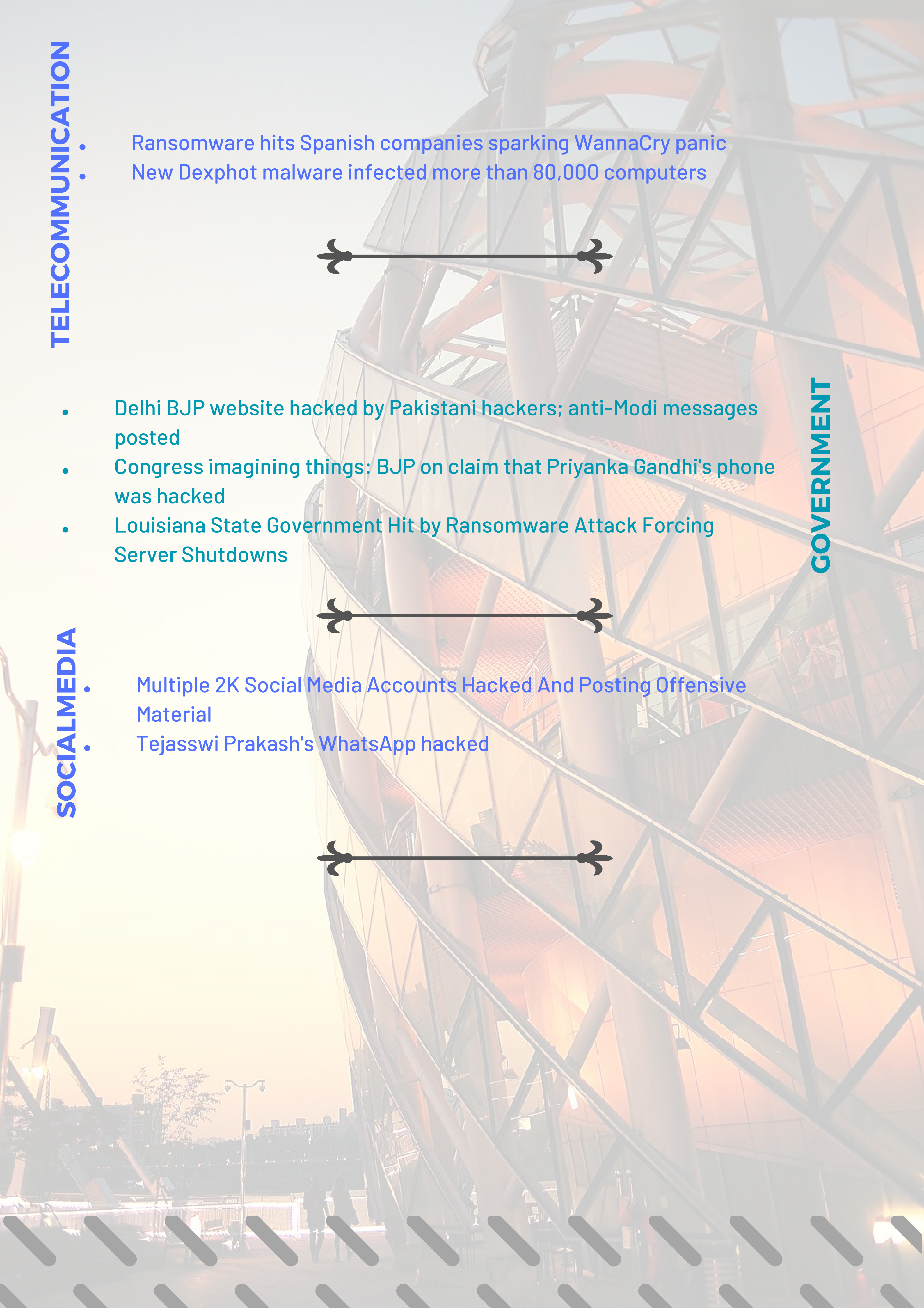
- Multiple 2K Social Media Accounts Hacked And Posting Offensive Material

RETAIL

- Gekko Group’s database exposed
- Hosting provider SmarterASP.NET hit by ransomware
- Thousands of Disney+ user accounts have already been hacked and resold online
- T-Mobile confirms customers' personal data accessed in hack
- Magento Marketplace Suffers Data Breach Exposing Users' Account Info
- Hackers Breach ZoneAlarm’s Forum Site — Outdated vBulletin to Blame
- Researchers find vulnerability in Amazon’s Ring Video Doorbells

EDUCATION

- Sag Harbor School Computers Impacted by Ransomware Attack
- Accidental data breach at Las Cruces Public Schools discloses vendor social security numbers



TELECOMMUNICATION

- Ransomware hits Spanish companies sparking WannaCry panic
- New Dexphot malware infected more than 80,000 computers

GOVERNMENT

- Delhi BJP website hacked by Pakistani hackers; anti-Modi messages posted
- Congress imagining things: BJP on claim that Priyanka Gandhi's phone was hacked
- Louisiana State Government Hit by Ransomware Attack Forcing Server Shutdowns

SOCIALMEDIA

- Multiple 2K Social Media Accounts Hacked And Posting Offensive Material
- Tejasswi Prakash's WhatsApp hacked

OnePlus Suffers New Data Breach Impacting Its Online Store Customers

OnePlus mobile has suffered a data breach and disclosed many information of its customers with causes citing to be a severe vulnerability presence in it. Regarding this, the company said their security team identified this while monitoring and instantly notified all their customers through email. Also, not all users are affected and no financial details of anyone has been exposed nor compromised. As a remedy, users are urged to change their passwords. Also, the company plans for mega bug bounty programs to report flaws if there's any.

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Security flaws

TYPE OF LOSS
Reputation/Data

COUNTRY
CHINA

Critical Flaws in VNC Threaten Industrial Environments

ATTACK TYPE
RCE

CAUSE OF ISSUE
Security flaws

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

The open source Virtual Network Computing (VNC) has been identified with 37 memory corruption vulnerabilities, which if exploited could result in remote execution attacks. It's said that 600,000 web accessible servers use that code. However, when each of these flaws were examined, it was identified that they had further flaws. As a remedy, the developers were contacted and issued the needed patches to fix them.

New WhatsApp Bug Could Have Let Hackers Secretly Install Spyware On Your Devices

What'sApp, one of the world's most popular social media forum is under severe threat once again. A vulnerability named as CVE-2019-11931 is a stack based buffer overflow vulnerability that allows intruders launch DoS and other remote code execution attacks. To exploit this vuln, all that's needed is just the phone number to send a malicious crafted mp4 file over What's App, through which a malware (spyware) could be installed after installing that mp4 file. Over 1400 devices are said to've been affected due to this. However, users are urged to use the latest version and if not, are urged to update ASAP.

ATTACK TYPE
Buffer overflow

CAUSE OF ISSUE
Security flaw

TYPE OF LOSS
Reputation

COUNTRY
GLOBAL

Samsung and LG phones at risk from Qualcomm security flaw

ATTACK TYPE
RCE

CAUSE OF ISSUE
Security flaws

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

The hardware of Qualcomm chipsets in Samsung, LG and Motorola mobiles have been identified with vulnerabilities which could allow attackers to exploit information remotely. There were already few vulnerabilities in Qualcomm which were also patched by them. But, this news came up quickly after those old vulnerabilities were patched. Patches to fix the found issues were issued and Samsung and LG have fixed it. However, Motorola hasn't yet!

TPM-Fail Vulnerabilities Affecting Billions of Devices

TPM (Trusted Platform Mobile), a globally used and highly familiar hardware/firmware technology has been identified with serious vulnerabilities that could allow attackers to retrieve cryptographic keys protected inside TPM chips manufactured by STMicroelectronics or firmware-based Intel TPMs. TMP technology is being used widely by billions of desktops, laptops, servers, smartphones, and even by IoT devices to protect encryption keys, passwords, and digital certificates. However, the issues were patched by the company.

ATTACK TYPE
Zero day

CAUSE OF ISSUE
Security flaws

TYPE OF LOSS
Reputation/Data

COUNTRY
CHINA

Critical Security Flaw In The Truecaller App

Ehraz Ahmed, an Indian Cybersecurity researcher, has discovered a critical flaw in Truecaller app, that's widely used people globally. The flaw has been detected in some of its API service. Through this flaw, malicious links could be exploited and other attacks like brute force attacks and DDoS. All mobile versions are highly vulnerable to this flaw. However, this issue has been patched.

ATTACK TYPE
Zero day

CAUSE OF ISSUE
Security flaws

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

Cisco VoIP adapters have critical security flaws

Security researchers have discovered 19 security flaws in Cisco VoIP adapters from Cisco's SPA100 series. If successfully exploited, hackers can gain remote access and launch and eavesdrop on the user's conversations and other activities. By using Shodan, security researchers were further able to identify 3,662 potentially vulnerable devices in Cisco SPA 100 series. As a security safety, it's recommended to update to the latest firmware before these flaws are exploited in the wild.

ATTACK TYPE
zero day

CAUSE OF ISSUE
Security flaw

TYPE OF LOSS
Reputation

COUNTRY
GLOBAL

Amazon Alexa Can Be Hacked By A Laser From 100 Meters—Is It Time To Hide Your Echo?

Amazon Alexa, Google voice and Apple Siri, all these own a similarity. Guess what?Well all these three can be hacked by a laser, discovered researchers. They say it'd be done by mimicking the voice commands from the electrical signals caused by the laser. The commands can be given even with a cheap and classic laser pointer. Further, many malicious attacks can be launched and even vehicles can be started. The researchers informed about this to the respective firms and the companies in turn swore to take remediation steps ASAP.

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

HEALTHCARE

Multiple 2K Social Media Accounts Hacked And Posting Offensive Material

Great Plains Health in Nebraska hit with a ransomware attack on 25th November forcing the Nebraska hospital to launch downtime procedures as it attempts to recover its IT systems. The attack was first detected by the information security team who has worked through the night to reduce the impact of the attack. Due to the attack, the hospital began canceling non-emergency appointments and other procedures on 26th November, and patients were reschedule scheduled and other processes are continued as planned.

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
NEBRASKA

Gekko Group's database exposed

ATTACK TYPE
Data exposed

CAUSE OF ISSUE
Poor security practices

TYPE OF LOSS
Reputation/Data

COUNTRY
GERMANY

European B2B hotel booking platform provider Gekko Group mistakenly stored over 1 TB of information on a publicly configured server, which was found by the research team on Nov 7. Researchers have found elasticsearch database while performing internet mapping projects. Sensitive client information is exposed because of the poor security practices followed by Gekko's third-party partners. Later this issue was patched and additionally they have integrated two vulnerability detection tools for better security.

RETAIL

Hosting provider SmarterASP.NET hit by ransomware attack

SmarterASP.NET, a well-known web hosting service provider, having over 4 lakh customers has been severely hit with a ransomware named Snatch. According to reports, the ransomware attack hit and encrypted customers' web hosting accounts which give customers access to servers where they can store files and data required to run their websites, thus crippling customer websites. It's said that $500 - $1500 of ransom is being claimed in Bitcoin. Also, their customers were unhappy as they were informed only after being affected by it. However, efforts to contain the situation are being put in by the company.

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

Thousands of Disney+ user accounts have already been hacked and resold online

ATTACK TYPE
Unauthorized access

CAUSE OF ISSUE
Lack of maintainces

TYPE OF LOSS
Reputation

COUNTRY
GLOBAL

Thousands of Disney user accounts from Canada, US and Netherlands have been hijacked and many information were posted on hacking forums ranging between $3 to $11 or free either. The attack commenced on November 12th. The hackers were able to crack the passwords, changed the users info and used it for other malicious purposes. ZDNET, a tech company who identified this problem, recommends users to use very strong and unique passwords for preventing such issues from happening.

T-Mobile confirms customers' personal data accessed in hack

One of the US telecommunications giant T-Mobile disclosed a security breach impacting many customers of it. Information of customers T-Mobile prepaid wireless accounts included their names, billing addresses, phone numbers, account numbers and much more. However, the company discovered the exposed details, contained them and thwarted the chances of fraudulent access. Also, no data of users were harmed. As a better security move, users are urged to change their passwords as well as their pin codes.

ATTACK TYPE
security breach

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

COUNTRY
CHINA

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

Magento Marketplace Suffers Data Breach Exposing Users' Account Info

Magento, a familiar e-commerce platform, has been identified with a data breach that was discovered by Adobe, the company owing Magento. There's news like an undisclosed vulnerability in Magento has been exploited by some remote hackers, causing what happened to happen. The hack commenced on Nov 21 and many details of customers and company were exposed. The company notified customers via mail and remediation work is ongoing by the security team to fix this ASAP.

Hackers Breach ZoneAlarm's Forum Site — Outdated vBulletin to Blame

ZoneAlarm, an Israel based security software company has suffered a data breach that exposed the data of its discussion forum users "forums.zonealarm.com" domain with nearly 4500 subscribes. The company noiselessly sent a notification email to all the affected customers. "The website became inactive in order to fix the problem and will resume as soon as it is fixed and users are requested to reset passwords after joining the forum.

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
GLOBAL

ATTACK TYPE
Unauthorized access

CAUSE OF ISSUE
Security flaws

TYPE OF LOSS
Reputation

COUNTRY
GLOBAL

Researchers find vulnerability in Amazon's Ring Video Doorbells

Bitdefender security researchers discovered security vulnerabilities in Amazon's ring video doorbell Pro IoT device that'd give hackers unauthorized access if successfully exploited. Ring Doorbells are internet-connected doorbells that provide motion-sensing and video surveillance capabilities. Few people who were affected by this thought it was a technical glitch and so changed passwords, but the problem still persisted. Work is underway to resolve this ASAP.

EDUCATION

Sag Harbor School Computers Impacted by Ransomware Attack

The school computers of Sag Harbor Pierson have been affected by a severe cyber threat that's suspected to be from a malware family named ransomware. On November 11th, administrators and school teachers identified that their systems were seized and were inaccessible. Fortunately, things never went beyond control as they had backup of it. Also, security experts from outside have been brought on board to reset all from backups.

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

COUNTRY
NEW YORK, UNITED STATES

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

Accidental data breach at Las Cruces Public Schools discloses vendor social security numbers

Las Cruces Public Schools now confirms it accidentally sent out an email back in September containing the social security numbers of vendors the district uses. That email was sent to about 150 district employees, officials said. Vendors were advised to place a fraud alert on their credit files as a precaution. Those vendors also were told by LCPS to check their credit reports and financial history for any signs of identity theft.

TELECOMMUNICATION

Ransomware hits Spanish companies sparking WannaCry panic

In Spain, NTT data owned Everis, a top IT consulting firm and National Radio Station SER have reported to be the victims of a severe ransomware attack. The most irony is that Everis offers it's own cybersecurity services, solutions and auditing. The type of ransomware is speculated to be either Ryuk or Bitpaymer. It's also said that the attack involved the exploitation of BlueKeep vulnerability, explosion of Bluekeep malware. Investigations reveal that a malicious file was attached to a mail and when both companies clicked, pandora's box opened and has caused troubles to many customers. However, steps to fix this are being made.

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
SPAIN

ATTACK TYPE
Malware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
GLOBAL

New Dexphot malware infected more than 80,000 computers

Dexphot malware has infected more than 80,000 windows computers. The goal of this malware is to stealthily install a coin miner and then steal computer resources. It's a second staged malware, a malware that attacks a system that already hit by a malware. Further, this malware is very hard to be traced by AV's as they just keep changing their signature, rendering them untraceable. Users are urged to be cautious before clicking or downloading anything online.

GOVERNMENT

Delhi BJP website hacked by Pakistani hackers; anti-Modi messages posted

Bharatiya Janata Party's (BJP) official Delhi website was hacked by Pakistan's hacking team, Mohammed Bilal Team. As per the reports, the official website bjp.org was seemed to be landing at a page delhi.bjp.org/Kashmir. This further redirects to a page which contained expletive messages about India, Prime Minister Mr. Modi and about Wing Commander Mr. Abhinandhan. The hack was identified by security aficionado Mr. Elliot Alderson, who said that the page Kashmir.html was loaded from Pastebin allowing users to make dummy web pages. He also released the decoded version of the page.

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

COUNTRY
INDIA

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

Congress imagining things: BJP on claim that Priyanka Gandhi's phone was hacked

Congress General Secretary Priyanka Gandhi's phone has been hacked. The attack vector is identified as WhatsApp spyware. Congress party said that their opposite party BJP are spying them. For this, BJP's spokesperson Amit Malviya refuted back at such claims saying that, "Haven't we seen Congress imagining things that don't exist? Didn't false claims of life threat arise when a green light flashed on Rahul's face?" However, this issue hasn't propelled forward yet.

Louisiana State Government Hit by Ransomware Attack Forcing Server Shutdowns

Louisiana's State Government has been hit by a severe ransomware that's crippled and taken many of its server's offline. As a response to it, Louisiana's Governor John Bel Edwards alerted the cyber incident response team and as a precautionary, it was them who took offline the servers and not the post effect of ransomware attack. The Governor confirmed that there's no data loss and no ransom has been paid as demanded by the hackers yet.

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
USA

SOCIALMEDIA

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
CHINA

Multiple 2K Social Media Accounts Hacked And Posting Offensive Material

The official twitter account of Ronnie 2k alias Ronnie Singh, the Digital Brand manager for the NBA 2k series was hacked on November 16th. Many users experienced their social media accounts hacked and expressed displeasure over it. This is an indication of how globally familiar businesses get their reputation hit overnight due to fragile security defences.

Tejasswi Prakash's WhatsApp hacked

Tejasswi Prakash's WhatsApp hackedTelevision actress Tejasswi Prakash's Whatsapp account has been hacked. The attacker who gained access has performed a distasteful activity. Later she called cybercrime cell then registered a compliant at the nearby police station, unfortunately, she cannot go due to the shooting till 3 a.m. Apart from Tejaswii, her co-star's Whatsapp account has also been hacked

ATTACK TYPE

Targetted

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation/Data

COUNTRY

INDIA

CONCLUSION

These are some of the major cyber attacks, But this is not all!

We have just mentioned only a few attacks. Cyberattacks are becoming day to day struggle. There is a huge increase in data-breaches and ransomeware attacks.One of the main reasons for this cyber attacks is unprotected data and poor cyber security practices. According to **varonis** only 5% of the companies are properly protected on average.

In order to protect the data from cyber attacks many companies are Spending millions to protect the data, A proper cyber awarness to employees will prevent a few.....

Trust me pals,we aren't lying!

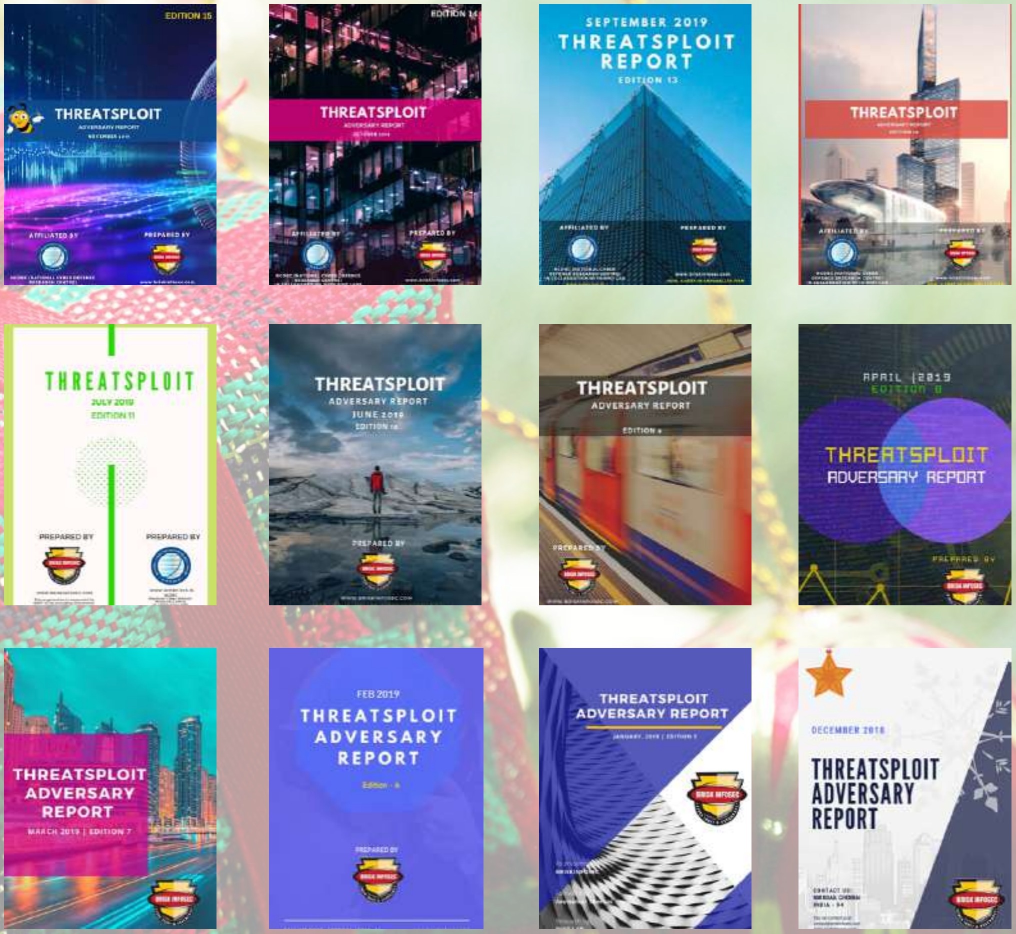
If you truly want to stay secured from all these, reaching out atrustworthy and exquisite cybersecurity firm is mandatory. It's the only best chance you're left to take to remain safe againstcyberattacks.

To know further, reach us out anytime.

REFERENCES

- https://calgaryherald.com/news/thousands-of-disney-user-accounts-have-already-being-hacked-and-resold-online/wcm/af3a5a1f-f5b5-45cd-a39a-c6d88939333d
- https://www.newsclick.in/Marathi-News-Channel-Hacked-Editor-Suspects-Anti-establishment-Reporting-Reason
- https://www.forbes.com/sites/brianmazique/2019/11/16/multiple-2k-social-media-accounts-hacked-and-posting-offensive-material/
- https://brica.de/alerts/alert/public/1287796/multiple-2k-social-media-accounts-hacked-and-posting-offensive-material/
- https://www.pymnts.com/news/security-and-risk/2019/t-mobile-data-breach-puts-personal-data-of-1m-customers-at-risk/
- https://www.zdnet.com/article/t-mobile-discloses-security-breach-impacting-prepaid-customers/
- https://www.engadget.com/2019/11/22/t-mobile-data-breach/
- https://thehackernews.com/2019/11/magento-marketplace-data-breach.html
- https://news.cyberfreakz.com/hackers-breach-zonealarms-forum-site-outdated-vbulletin-to-blame/
- https://www.cisomag.com/researchers-find-vulnerability-in-amazons-ring-video-doorbells/
- https://www.facebook.com/security/advisories/cve-2019-11931
- https://thehackernews.com/2019/11/whatsapp-hacking-vulnerability.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29&m=1
- https://thehackernews.com/2019/11/oneplus-store-data-breach.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29&m=1
- https://threatpost.com/critical-flaws-vnc-industrial/150568/
- https://www.techradar.com/news/qualcomm-security-flaw-puts-samsung-and-lg-phones-at-risk
- https://thehackernews.com/2019/11/tpm-encryption-keys-hacking.html
- https://in.mashable.com/tech/8839/researcher-discovered-a-critical-security-flaw-in-the-truecaller-app
- https://www.techradar.com/news/cisco-voip-adapters-have-critical-security-flaws
- https://www.wweek.com/news/2019/11/18/someone-hacked-phones-at-portland-israeli-street-food-restaurant-shalom-yall-this-weekend-and-left-anti-semitic-outgoing-messages/
- http://www.israelnationalnews.com/News/News.aspx/271903
- https://liistudio.com/newcastle-restaurant-21s-e-mail-hacked-by-fraudsters-demanding-412-from-consumers/33464/
- https://defensemaven.io/bluelivesmatter/news/police-department-website-gets-hacked-graphic-images-populate-google-for-hours-f9T4EwKGXEC-Qqw-4sBrwA/
- https://www.iberianet.com/breaking_news/new-iberia-network-hit-with-virus/article_739fc014-0bd5-11ea-82ec-cf0621e743a1.html
- https://www.katc.com/news/local-news/iberia-parish/city-of-new-iberia-hacked-according-to-mayor
- https://thehackernews.com/2019/11/louisiana-ransomware-attack.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29&m=1
- https://brica.de/alerts/alert/public/1288723/sag-harbor-school-computers-impacted-by-ransomware-attack/
- https://www.databreaches.net/sag-harbor-school-computers-impacted-by-ransomware-attack/
- https://www.databreaches.net/accidental-data-breach-at-las-cruces-public-schools-discloses-vendor-social-security-numbers/
- https://kvia.com/news/education/2019/11/20/accidental-data-breach-at-las-cruces-public-schools-discloses-vendor-social-security-numbers/
- https://www.zdnet.com/article/ransomware-hits-spanish-companies-sparking-wannacry-panic/
- https://www.zdnet.com/article/microsoft-says-new-dexphot-malware-infected-more-than-80000-computers/
- https://www.scmagazine.com/home/security-news/data-breach/leaky-gekko-group-database-exposes-info-on-hotel-brands-travelers/
- https://healthitsecurity.com/news/ransomware-attack-forces-great-plains-health-to-ehr-downtime
- https://www.knopnews2.com/content/news/Database-breached-at-Great-Plains-Health-Hospital-565505671.html
- https://brica.de/alerts/alert/public/1289485/great-plains-health-ransomware-attack-prevents-access-to-patient-medical-records/
- https://www.indiatoday.in/television/celebrity/story/tejasswi-prakash-s-whatsapp-hacked-he-is-using-my-account-to-make-vulgar-video-calls-1615474-2019-11-04

YOU MAY ALSO BE INTERESTED IN OUR PREVIOUS WORKS



REFERENCES ABOUT BRISKINFOSEC

CASE STUDIES

SOLUTIONS

SERVICES

RESEARCH

COMPLIANCES

BLOGS

BRISK INFOSEC

CYBER TRUST & ASSURANCE

BEWARE

Never get trapped on christmas and new year cyber scams

Happy Christmas!!!

contact@briskinfosec.com | www.briskinfosec.com