THREATSPLOIT ADVERSARY REPORT

MARCH 2019 | EDITION 7

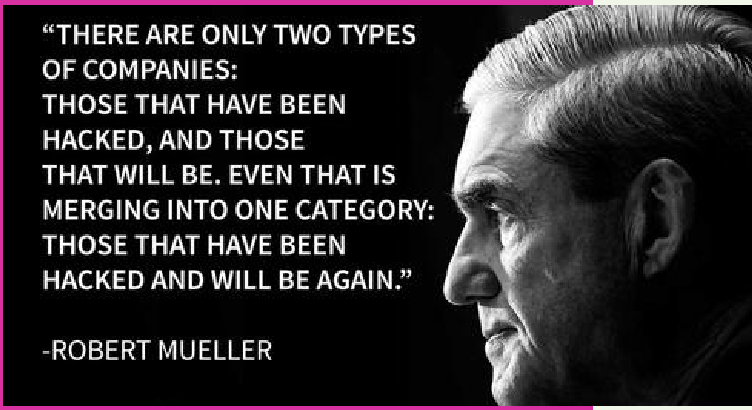
BRISK INFOSEC

CYBER TRUST & ASSURANCE

www.briskinfosec.com

THE WORD DATA BREACH HAS EVER BEEN A THREAT DUE TO WHICH COMPANIES IN THE PAST AND IN PRESENT HAVE FACED THEIR REGRET. SECURITY ASSESSMENTS ARE DONE AND COMPANIES ARE MADE TO BELIEVE THAT THEIR SECURITY IS OF TOP-NOTCH QUALITY. YET, THOSE FIRMS GET BREACHED INEVITABLY.

ISN'T THIS SHOCKING?
MOREOVER, ISN'T THIS FEAR-INVOKING IF WE THINK ABOUT OUR COMPANY'S SECURITY?



"THERE ARE ONLY TWO TYPES OF COMPANIES:
THOSE THAT HAVE BEEN HACKED, AND THOSE THAT WILL BE. EVEN THAT IS MERGING INTO ONE CATEGORY:
THOSE THAT HAVE BEEN HACKED AND WILL BE AGAIN."

-ROBERT MUELLER

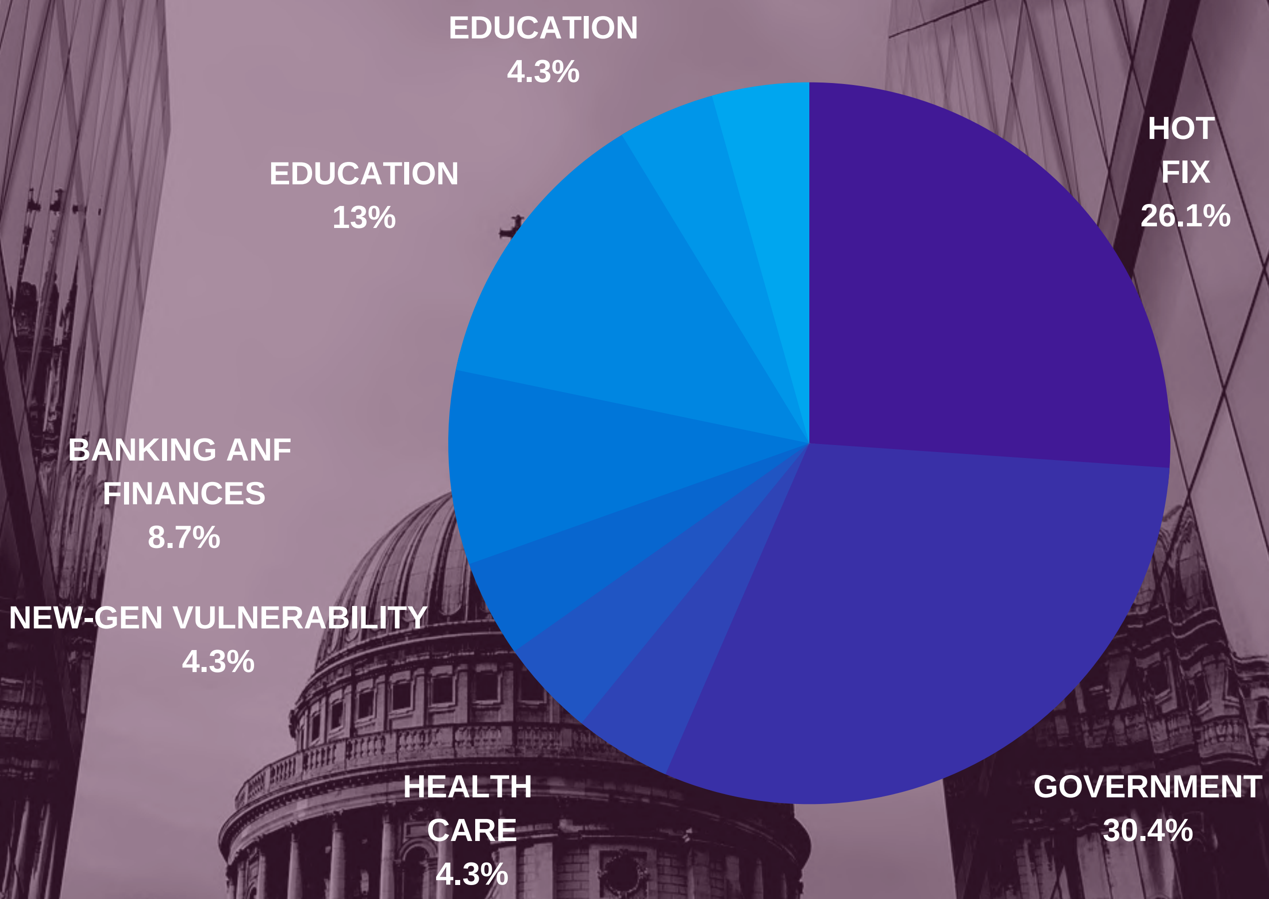
THIS THREATSPLOIT REPORT GATHERS VARIOUS CYBER BREACHES FROM VARIOUS PARTS OF THE EARTH. WE HAVE PREPARED IT BECAUSE WE WANT TO CREATE AWARENESS ON SECURITY AND TO PREVENT YOUR COMPANY REPUTATION FROM GETTING TARNISHED.

YOU MAY EVEN ASK WHY?

IT'S SIMPLE. WE AS DEDICATED CYBER SECURITY FOLKS CARE FOR YOUR DIGITAL SAFETY!

DATA STRUCTURE OF FEBRUARY 2019

GOVERNMENT SECTORS HAVE FACED THE MAJOR AMOUNT OF CYBER BREACHES IN FEB 2019, AMONG OTHER SECTORS. DIFFERENT ATTACKS FROM DIFFERENT SOURCES HAVE CAUSED GOVERNMENT DIFFERENT LOSES, WITH THESE BEING STILL ON THE RISE. THESE CYBER BREACHES CONTINUE TO ASCEND AND SHOW NO SYMPTOMS OF ALLEVIATION.



ARE YOU AWARE OF THESE?.....

CONTENTS TABLE

HOT FIX

GOVERNMENT

HEALTH CARE

AUTOMOTIVE

NEW GEN VULNERABILITY

BANKING AND FINANCE

RETAIL

EDUCATION

TELECOMMUNICATION

Serious flaw found and patched in WordPress, but it might lurk in plugins

A long lurking dreaded vulnerability was just patched by WordPress in its core code. But a same flaw existing in third party plugin can still allow hackers to compromise websites which are using the popular publishing software, says German web security company RIPS technologies. To exploit the vulnerability, perpetrator must have access to the account with "author" privileges - a common designation for WordPress users. Once the hacker gains access, he can manipulate the data and use it for his own selfish motives. An attacker obtaining access with author privileges on WordPress can execute arbitrary PHP code on the server, waving a green signal for remote takeover, says RIPS researcher Simon Scannell in a blog post. The bug classified as a path traversal vulnerability has been running on one-third of all the websites for almost six years, said researchers. Scannell says in-spite the WordPress websites patching their core code, the software is still susceptible to be attacked through plugins. He further adds that any WordPress site installed with improper plugin can make exploitation, certainly with reference cited towards the code part handling image metadata. WordPress plugins have of late been trending in news for vulnerabilities.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Zero day	lack of awareness	Reputation/Data	USA

Researchers found a way to hack those ubiquitous electric scooters

Electric scooters are hacked!.... Isn't this news like curiosity provoking?

Yes, a Xiaomi M365 scooter which can be manipulated through a Bluetooth connection was discovered by Rani Idan, a researcher with Dallas-based Zimperium whom also said that users with authenticated passwords alone can connect and access the scooter. But, he later disclosed that the password completely fails to protect the user. It was found that the password is validated on the application side but the scooter itself isn't cognitive of the authentication state. From there, an app was written for his mobile device by him which allowed to mess with a Xiaomi scooter that was in motion. Due to this flaw, any M365 scooter can be locked and installed with corrupt firmware. Other top scooter sharing companies like Bird and Spin have used Xiaomi in past. But, CyberScoop figured out that Bird updated the firmware on M365 models before a year. A spokesperson told CyberScoop that buying of Xiaomi models were stopped. Xiaomi told Zimperium researchers that they knew the issue and blamed the "third-party products" for it.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Zero day	lack of awareness	Reputation/Data	USA

WordPress plugin patches flaw that gave hackers potential access to 40,000 websites

Luka Sikic, a security developer at WebARX published a report briefing about the bug in Simple Social Buttons plugin. More than 40,000 websites leveraged them to spread their content on social media like Facebook, Twitter and many. WPBrigade have patched the issues in 2.0.22 software after the acknowledgement of Sikic, which had a Friday release. This was the firm that developed Simple Social Buttons. Last year, there was another similar case where hackers manipulated a vulnerability in the plugin WP GDPR compliance to develop their indigenous administer accounts on the WordPress websites.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Zero day	lack of awareness	Reputation/Data	USA

Apple patches FaceTime flaw and two exploited zero-days in new security update

A security update was released on Thursday which comprised the patch for 3 already exploited vulnerabilities. If users jeopardize to update the security patch, then they are vulnerable to threats. The much familiar Face Time bug which permissioned the attackers to espy on others through audio and video was fixed by the security patch iOS 12.1.14. It also rectifies the two zero-day vulnerabilities, says Google's project Zero security team researcher, Ben Hawkes. The bugs CVE-2019-7286 and CVE-2019-7287 can let hackers to escalate privileges as well could also execute arbitrary code with kernel privileges, respectively. To know about these, users must update their phone and must visit the "Settings" page on their iPhone and then must follow "General" to "Software Update". Next, click "Download and Install". Another update insisting iOS users to update to 12.1.4 which the zero day issues fixed, has been a week later since the announcement from New York Governor Andrew Cuomo and Attorney General Letitia James about the state investment on the handling strategy of the FaceTime flaw. A 14-year-old boy from Arizona first found the problem while chatting with friends and playing the video game "Fortnite." The boy's mother spent roughly a week trying to notify Apple about the issue, with little feedback. The company now says it will compensate the family for an undisclosed amount for reporting the issue.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Zero day	lack of awareness	Reputation/Data	USA

E-ticketing system exposes airline passengers' personal information via email

A research published by the mobile security company named as Wandera said that at least 8 airlines used e-ticketing systems which could permit hackers to exploit the sensitive information about travellers. The systems didn't secure the users personally identifiable information (PII) comprising names, boarding passes, passport numbers and flight numbers, said Wandera. Nevertheless, the email vulnerabilities continued to persist even after the notification of researchers to the attacked organisations, Wandera found. The reason for these attacks was found to be the usage of unencrypted and re-usable links which lured perpetrators to hack, says Michael Covington - vice president of product at Wandera. There isn't proof about the vulnerability exploitation from external attackers. Southwest airlines is the best low-cost functioning airline in U.S as of 2019, as per the industry analysts at Center for Aviation. In a statement regarding the security of customers, a spokeswoman told "security of our customers is of utmost significance and we ponder into this issue to strengthen the security of our customers data. A spokesperson for the JetStar told "If users were using Wi-Fi or a physical network, this wouldn't have been an issue. Further, we aren't a testing company but the airlines with whom we've engaged are keen to listen more", he concludes.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Zero day	lack of awareness	Reputation/Data	USA

Drupal critical flaw: Patch this remote code execution bug urgently, websites warned

Website admins are forced to install updates from the Drupal (popular CMS) project instantly, since the find of a highly critical remote code execution bug. Drupal security team identified the bug as CVE-2019-6340 and alerted it as extremely dangerous. According to Drupal, the bug is due to few file types not lucid from non-form sources like RESTful web services. If this jeopardizes, it warns of directing to arbitrary PHP code execution. Till the completion of update to a secure version, admins can disable all web services modules for alleviating the bug. Corrupted branches of Drupal core encompasses Drupal 8.6.x and Drupal 8.5.x. These must be upgraded to Drupal 8.6.10 and Drupal 8.5.11. Drupal warns that after updating Drupal core, admins must install security updates for affected 3rd party Drupal projects comprising of Font Awesome Icons, Transalation Management tools, video, metatag, JSON, and API. Recently, hackers used Drupal sites to address 'Drupalgeddon 2' flaws, with main connotation of installing cryptocurrency miners on affected web servers.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Zero day	lack of awareness	Reputation/Data	USA

GOVERNMENT

Australian parliament hacked by 'sophisticated state actor,' prime minister says

Suspicion over a reputed state actor for breaching the computer network of the Australian parliament has been making the hot news, says the country's prime minister to law makers. Australian Prime Minister Scott Morrison said that our security agencies have spotted this issue and are striving towards securing these systems as well as in protecting users. A federal election is awaiting for Australia within 3 months. With regards to this, the Australian Prime Minister said that Government technical veterans are willing to provide cybersecurity support to any political party, if needed. Morrison didn't reveal the culprit, stating disinterest to say in a public forum. The Sydney morning Herald newspaper reported that intrusions carry the Chinese digital fingerprints. However, Chinese foreign ministry disapproved of these citing as "baseless speculations". However, an anonymous man named as Eialhi Priest has been making unapproved claims on social media platforms with a smirk that, he is the actual culprit. CyberScoop were unable to validate Eliahi's words and are waiting to receive official response from Australian authorities.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Data Breach	lack of awareness	Reputation/Data	AUSTRALIA

Two hackers charged for DDoS attacks, threats to LAX

Southern Californian school districts and Los Angeles International Airport have faced cyber attacks (DDoS) and dreadful physical violence by two men (an American and a British), reports the U.S prosecutors on Tuesday. The perpetrators were identified as George Duke Cohan, a 19 year old British whom taunted the Switzerland based email providers on Twitter. Another one is a 20 year old North Carolina guy named Timothy Dalton Vaughn, who is accused of launching DDoS attack on a Californian motorsport company and persuading for bitcoin to terminate the attack. The threats made by these two men even panicked the Mayor of London. Vaughn and Duke-Cohan also jointly worked over a week for initialising DDOS attack on ProtonMail, an encrypted email service.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
DDoS	lack of awareness	Reputation/Data	USA

How hackers used a PowerPoint file to spy on Tibet’s government-in-exile

A hint on how hackers are persuading to spy on Tibet’s government in-exile is identified through a recently found PowerPoint file. The malicious content was mailed to subscribed users of a mailing list administered by the Central Tibetan Administration (CTA). It is the organization that represents the Tibet’s exiled government, reports Talos, Cisco’s threat intelligence unit. Tibet is an official part of China, but the Tibetan Alphas have been in exile at India for decades. The email was impersonated as a file that would appeal to their politics. The name of the PowerPoint file was “Tibet –was-never-a part-of-China.ppsx”. The research demonstrates the fact that PowerPoint file yielded hackers to execute many JavaScripts for delivering the payload. Further, it also paved inroads for other malicious infrastructure. From there, other dreadful issues like Windows Trojans and updated version of Android malware were also detected. Researchers figured out this 7 year old malware permitted hackers to record audio and pilfer user’s location and personal contacts. However, in spite of blocking this attack, we believe the adversity caused by Cisco Talos will ensure the regrouping of Adversaries, researchers concluded.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Malware	lack of awareness	Reputation/Data	TIBET

'Chafer' group advances espionage tactics by hacking Windows machines in Middle East

A unique malware variant was used a hacking group for the past 3 years to spy on “foreign diplomatic entities” functioning in Iran, expanding its heritage as an espionage group whom were the ones to initially zero down the telecoms entirely on Middle East. The Chafer cyber espionage group deployed a malware known as Remexi to extract user credentials, record keystrokes, browser history and secretly take screenshots on targeted machines through the end of 2018, reports Kaspersky research published on Wednesday. Few hints are acknowledged about the operation, comprising solid evidences on how the malware proliferates. However, Kaspersky’s latest research develops on earlier Symantec findings which determined that Chafer attacked telecommunication companies, an airline in the Middle East and at least one business in the U.S. The group now appears to be targeting Windows machines located inside Iran, Kaspersky said this week. Chafer was first spotted by Symantec in 2015. Since then, hacking tools like EternalBlue pilfered from National Security Agency were used by Chafer whom have also used EternalBlue to target its own campaigns.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Malware	lack of awareness	Reputation/Data	MIDDLE EAST

Civil Defence website hacked by Syrian group

The website for the Civil Defense was hacked on Tuesday, displaying an image of the Syrian flag and calling for the fair treatment of Syrians in Lebanon, along with a message for Prime Minister Saad Hariri. The hackers identified themselves as "Wolftartous and Nightmare," signing their message as "Federal Russian Union". Hariri told An-Nahar newspaper earlier this month that shaking hands with Syrian President Bashar Assad was one of the hardest moments in his life, saying it would never happen again. Last month, the website of Beirut's Rafik Hariri International Airport and the Energy Ministry's were also hacked. Although it wasn't clear who had hacked the airport's website, the Energy Ministry's website was hacked by a Syrian group condemning the death of Syrian teen named as Ahmad al-Zoubi.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Phishing	lack of awareness	Reputation/Data	LEBANON

Hun Sen's Facebook hacked

Prime Minister Hun Sen's official Facebook page was hacked on Monday, with analysts saying a post threatening to shut down the social media platform in Cambodia which was designed to portray him in a negative light. Duong Dara, the one managing Fb account of Hun Sen said that "Hackers erased posts which were familiar among people and this isn't the 1st time of such incident".Ministry of Interior spokesperson Phat Sophanit said that the issue is investigated by the technical authorities. A Facebook user said named as Kea wrote "Too much selfish and Cambodia isn't the absolute property of your family". Another one named as "Assembly" slammed Hun Sen for trying to shut FB completely in Cambodia due to his hacked issue.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Data Breach	lack of awareness	Reputation/Data	CAMBODIA

GOVERNMENT

Allerdale Council leader's Facebook account hacked

Coun Alan Smith made the claims after a “golliwog” post appeared online under his name although he has strictly refused on sharing the racially-charged caricature. This isn’t the 1st time his account is shared. Mr Smith now deleted his social media account after acknowledging his account got hacked. With 2 months down the timeline for council elections, he denied the fact that it was done with selfish political motives.

During the recent meeting of Cockermouth Town Council, Mr. Smith portrayed social media as “Dynamite”. The Golliwog post was shared on the official account of Mr. Smith on 20th February and was simultaneously deleted on the same day as well.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Phishing	lack of awareness	Reputation/Data	CUMBRIA

HEALTH CARE

Patient files leaked Cabrini hospital AUS Ransomware

Medical files of 15,000 patients at Cabrini hospital were hacked. To regain them, ransom was forced through cryptocurrency. Due to this, the Melbourne Heart Group couldn’t monitor patients data. Suspects are believed to be from North Korea or Russia. However, origin of attacks isn’t disclosed. Patients have complained that their files and appointment times had lost in vain. The Australian Cyber Security Centre informed that they are facilitating the hospital with cybersecurity awareness. A Melbourne Heart Group spokeswoman said that they are working with government agencies to set things right. She emphasized the necessity of data protection and also informed that patients data aren’t compromised, as of now. But there wasn’t disclosure of ransom, paid or not. The healthcare care domain has become the primary target for hackers, since the payment of $17,000 bitcoin by Hollywood Presbyterian Hospital, situated in Los Angeles whose computer networks were seized by hackers.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Data Breach	lack of awareness	Reputation/Data	AUSTRALIA

AUTOMOTIVE

Toyota car company hacked -no employee and customer

Toyota car manufacturer on their Australian base faced a cyber attack as its email accounts couldn't be accessed. The Australian Toyota servers were hacked recently and the reasons for this attack remain unknown. Through a statement, Toyota Australia made clear that "No evidence of employee data compromise is found. We don't have further details of the incident." The affected employees aren't able to continue with their work due to this adversity. As an alternative, they have received updates from Toyota's network security team. This incident aids a significant part to the growing count of cyber breaches in Australian territory. With utmost regret, the customer service has placed a notice of "Under maintenance and we apologize for this inconvenience". cyber security experts accept the fact that the breach can be caused due to many reasons like greedy financial aspirations, exploitations of users data, or an espionage campaign.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Data Breach	lack of awareness	Reputation/Data	AUSTRALIA

NEW-GEN VULNERABILITY

DrainerBot rinsing Android users of data and battery life

Oracle says that more than 10 GB of data could be consumed in your phone by downloading hidden vids. The database vendor says that DrainerBot uses corrupted code on Android devices to deliver deceiving invisible video ads. Corrupted apps take "significant bandwidth and battery", says Big Red. The discovery were done by Oracle's team in two named as oracle's fairy recent acquisitions-ad tracking biz and internet infrastructure outfit Dyn. Corrupted apps which is said to be eliminated from google play store is said to reappear as augmented reality like beauty app perfect 365, sketching out the characters of clash of clans, Touch 'n' beat (musical app) and many have been downloaded innocently by users throughout the globe. Once these are downloaded, a code update invokes new functions along with fraudulent ad videos. These don't appear on-screen but lurk, surreptitiously. Apart from this, these apps are instigating false ad opinions like reporting to the ad network but actually, not. Ad fraud isn't a stranger but Oracle says this kind is something beyond danger.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Bot	lack of awareness	Reputation/Data	USA

Bank of Valletta Through €13M Cyber Attack

On 13th February, Times of Malta reported the Bank of Valletta terminated all its operations due to a cyber breach that costed 13 million Euros. With regards to this, the country's Prime Minister said the swindling transactions had been traced. Bank promised its customers that none of their accounts are compromised. Despite assurance from Government and bank officials, customers payments weren't processed. Also, their businesses faced negative impacts. And while Bank of Valletta might actually solve its issues, the question remains – when?

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Data Breach	lack of awareness	Reputation/Data	MALTA

Olympia Financial Group Inc under Ransomware Cyber Attack

Ransomware attack has attacked the information technology systems of Olympia Financial Group on 2nd Feb, 2019. Investigations reveal that the information have been encrypted. Status of other customer data are unavailable. But measures are taken to call and remedy the affected Person's needs. Olympia instantly implemented countermeasures to stop further infection in accordance with Olympia's established cyber security policies that have been developed and implemented in consultation with industry leading cyber security specialists. Olympia has also contacted the RCMP cyber crime division with respect to this attack and has enlisted help from several malware response and recovery industry specialists.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Data Breach	lack of awareness	Reputation/Data	USA

Huddle House Restaurant Chain Suffers POS Malware Breach

US restaurant chain Huddle House announced a possible malware attack on its point of sale (POS) systems. The cyber-attack is believed to have compromised many number of systems at corporate and franchised locations, after a third-party POS system was targeted. Stolen data includes credit/debit card numbers, cardholder names, expiration dates, and other information. Customers who visited Huddle House locations from August 1, 2017, to February 1, 2019, also could have been affected. Customers are advised to check their bank accounts and report any suspicious activity to their local law enforcement, if detected. They are also advised to use free credit monitoring services and freeze their accounts, if they think they may have been impacted. Huddle House, based in Atlanta, Georgia, has 339 restaurants across 39 states. A spokeswoman for Huddle House said they do not know how many locations have been infected with malware. She added: "The investigation is still ongoing."

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Malware	lack of awareness	Reputation/Data	USA

Cyber criminals jeopardize VFEmail's operations after deleting their data

VFEmail, an email service provider which delivered services since 2001, faced a devastating cyber blow. The US users servers with any data were completely washed out by cyber attackers. It seems like even the company's backup servers have been annulled. It was believed that all the VM's were lost. Ironically, not all VM shared the same authentication, yet all were destroyed. However, VFEmail told that their employees are toiling hard to replenish an efficient and more secure server. Company informed users to be away from sending emails, due to delivery mechanism disabled. For paid users, this wasn't an issue.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Data Breach	lack of awareness	Reputation/Data	USA

Malware Attack Shuts Down Columbia State for 2 Days

On 28th February 2019, a computer virus penetrated Columbia state community college campuses, which remained closed for 2 days. This spread everywhere after an employee opened and clicked on a malicious email attachment, says the President Janet Smith. Two days of college was off. This was mandatory for ensuring remediation, says Richard locker- Tennessee Board of regents Director of Communications. Officials comforted the students saying no data of theirs were compromised. Ironically, many students were perplexed as of why the college was closed. As per the Director of Communications Amy Spears-Boyd, students were sent an email about the situation Tuesday afternoon. “Our information technology department has been working incessantly with expert consultants around the clock to safeguard sensitive data and to annul the virus,” the email said.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Malware	lack of awareness	Reputation/Data	COLUMBIA

EDUCATION

University of Albany Targeted with DDoS Attacks

DDoS attacks have struck the University of Albania (UA) on Feb 19th. These attacks have impacted the availability and functionality of several UA IT systems, particularly Blackboard. According to Martin Manjak (CISO of UA), neither the integrity nor confidentiality of university information has been compromised. He also says all we know is that the resource being targeted is Blackboard. “We’re able to maintain access to electronic resources from on-campus through a combination of firewall and filtering rules,” Manjak said, “but access from off-campus was affected because the attacker(s) filled our internet pipe.” “Communication is sent to the University community as when an active threat with the potential to impact the entire campus is identified, it will also be reported” Manjak said,

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
DDoS	lack of awareness	Reputation/Data	USA

EDUCATION

Madras University comes under Ransomware attack

The University of Madras database was struck by a ransomware attack which encrypted the data. To regain normality, hackers demanded Rs 18 lakh as ransom.
Fortune favoured the university as they had back-up data on the non-network system. Technical team recovered the data and restored it on the new built server, said sources in the university. The ransomware gets sent through various ways like email. When such staff member opened it, it got proliferated throughout the system and encrypted the data. The university plans for a security audit and will implement more security schemes to thwart such issues. Apart from this, plans for group-wise firewall as level 2 and level 3 security measures are also in pipeline, says professor Sivaji. The cybersecurity connoisseurs said the upgradation of security will lessen future threats. “If any outside threat is detected, an alert would be issued and the server would automatically shut down,” they concluded.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Ransomware	lack of awareness	Reputation/Data	INDIA

TELECOMMUNICATION

Optus investigating potential privacy breach after customers logged in as other users

Optus customers feared a possible breach since few users attempted to access their accounts masquerading as someone else. The suspicious account activity witnessed customers logged in as “Vladimir” while other customers said they had seen being logged as “Sarah”. Optus verified the issue and said it is striving hard with 3rd party vendors to eliminate this. As a precaution, Optus shortly disabled the account and later re-enabled it. They also conveyed their apologies for this inconvenience. One of the customer reported that he could see another customer personal information when he logged in his own account. Apart from him, others also shared similar experiences. Using the domain “optusnet.com.au”, customers are sent an email telling them a document is available for them to download via the link provided. Once clicked, the victim’s computer will be infected by the malicious file.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Privacy Breach	lack of awareness	Reputation/Data	AUSTRALIA

CONCLUSION

Various security breaches have been reported. The main reasons for these are:

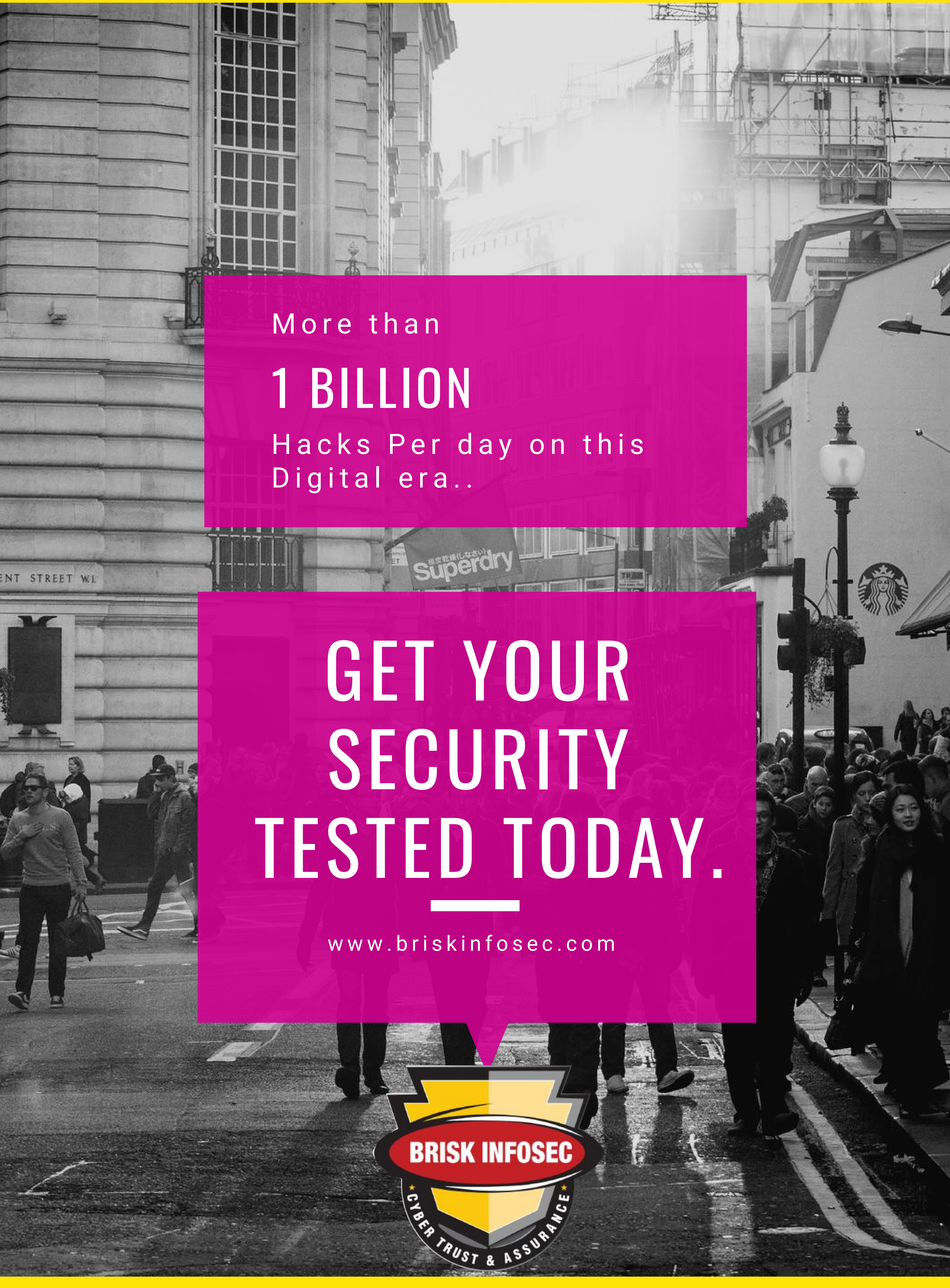
- Improper security configuration.
- Using outdated software.
- Failing to update to the contemporary version available in the security sector
- Lack of awareness of the past, present and about future issues.
- Failing to check the URL sources.
- Failing to validate whether the URL's are from legitimate sources.
- Failing to maintain secondary back up for data storage.
- Inconsistent security assessments.
- Developers using SDLC instead of Secure SDLC (Software Development Life Cycle) for development.
- Lack of proactive approach towards cyber security.
- Last but not the least, negligence in hiring a competent cyber security firm.

To be on the safer side, a lucid security assessment from a dedicated and competent firm needs to be done without fail, in a consistent way. Apart from this, proper awareness must be gained about all possible issues on cyber security. To know more, feel free to contact us anytime. We will assist you with our efficient cyber security services for sure.

> "IT IS BEST TO PREVENT CYBER ATTAKCS THAN TO LAMENT AFTER CYBER HAVOCS!"

REFERENCES

https://www.cyberscoop.com/wordpress-remote-code-vulnerability-rips/
https://www.cyberscoop.com/scooter-hack-zimperium-bluetooth-bird-spin/
https://www.cyberscoop.com/wordpress-plugin-simple-social-buttons-flaw/
https://www.cyberscoop.com/iphone-update-facetime-flaw/
https://www.cyberscoop.com/airlines-ticketing-email-hackers-wandera-southwest/?category_news=technology
https://www.cyberscoop.com/australian-parliament-hacked-sophisticated-state-actor-prime-minister-says/
https://www.smh.com.au/politics/federal/australia-s-major-political-parties-hacked-in-sophisticated-attack-ahead-of-election-20190218-p50yi1.html
https://www.cyberscoop.com/apophis-squad-hackers-lax-ddos/
https://www.cyberscoop.com/hackers-used-powerpoint-file-spy-tibets-government-exile/
https://www.cyberscoop.com/chafer-kaspersky-nsa-eternal-blue/
https://www.theage.com.au/national/victoria/crime-syndicate-hacks-15-000-medical-files-at-cabrini-hospital-demands-ransom-20190220-p50z3c.html
https://www.news.com.au/national/victoria/cybercrime-gang-hacks-thousands-of-medical-files-and-demands-ransom-from-melbourne-hospital/news-story/9e43486ad406d48d845be734a9764a4a
https://www.timesandstar.co.uk/news/17458394.allerdale-council-leaders-facebook-account-hacked/
https://www.phnompenhpost.com/national/hun-sens-facebook-hacked
https://www.deccanchronicle.com/nation/current-affairs/260219/madras-university-comes-under-ransomware-attack.html
http://www.dailystar.com.lb/News/Lebanon-News/2019/Feb-26/477494-civil-defense-website-hacked-by-syrian-group.ashx
https://www.zdnet.com/article/drupal-critical-flaw-patch-this-remote-code-execution-bug-urgently-websites-warned/
https://cyware.com/news/cybercriminals-jeopardize-vfemails-operations-after-deleting-their-data-37f07d50
https://globenewswire.com/news-release/2019/02/04/1709513/0/en/Olympia-Financial-Group-Inc-Announces-Ransomware-Cyber-Attack.html
https://brica.de/alerts/alert/public/1246096/olympia-financial-group-inc-announces-ransomware-cyber-attack/
https://bitcoinist.com/bank-of-valletta-cyber-attack-bitcoin/
https://www.zdnet.com/article/hackers-tried-to-steal-eur13-million-from-maltas-bank-of-valletta/
https://portswigger.net/daily-swig/restaurant-chain-huddle-house-hit-by-pos-malware-attack
https://www.9news.com.au/2019/02/15/08/28/news-australia-optus-investigating-potential-privacy-breach



More than

1 BILLION

Hacks Per day on this Digital era..

GET YOUR SECURITY TESTED TODAY.

www.briskinfosec.com

BRISK INFOSEC
CYBER TRUST & ASSURANCE