THREATSPLOIT ADVERSARY REPORT

JANUARY, 2019 | EDITION 5

As presented by
BRISKINFOSEC

Foreword by
Arulselvar Thomas

Research by
BINT LAB
Brisk Intelligence Lab

WWW.BRISKINFOSEC.COM

EXECUTIVE SUMMARY

"Many organizations security defences have been smacked
Their earned reputation within a flash have been jacked
Heartless jokes on them by others also have been cracked
How come they're sure that their firms haven't been hacked?"

This Threatsploit research report DEC 2018, reports various cyber catastrophes from distinguished sectors, with healthcare domain being highly affected, obviously leading the breached list. Our Threatsploit report encompasses various interesting attacks meant to caution readers about the proliferating cyber hacks which are stealthy in spreading but vociferous in menacing.

This report will surely leave you spellbound. This report is prepared with a sole intention of empowering you in understanding from these attacks, the undeniable fact that the need for a high quality security is mandatory.

Technology and healthcare „indeed the most indispensable horizons have benefited humans in humongous quantity .Both of these have comforted the life of us with their spell - bound inventions and accomplishments for human race. In spite of all these glories, there are pathetic stories of various cyber breaches, both in the past and in the present which seemed to have the majority of their inception from these both sectors.,encompassing of a total of 80 % breaches from these two alone.

DATA STATISTICS OF DECEMBER

40%

HEALTHCARE

10%

SOCIAL MEDIA

Various security breaches from various sectors have commenced in various ways. Among these, healthcare sector shines predominantly in the waning moon with 40% of cyber hacks originating from it. Due to the existence of fragile security measures

While the technology is continuing to captivate people with its awe-strucking inventions, it is also the cause for 40% breaches to exist.

40%

TECHNOLOGY

10%

RANSOMEWARE

CONTENTS TABLE

Email Error, Lack of Encryption Breaches a Nebraska Patient Data

This week's breach roundup highlights the healthcare sector's ongoing struggle with email, with three breaches caused by email errors.

Because of a faulty email sent inadvertently by an employee to a rogue recipient, 6450 patients data's including patient names, birthdates, telephone numbers, sex, race, insurance details, account numbers were breached and this was informed by Nebraksa based Prairie field family on December 13,2018. In this breached list, financial and health information weren't involved. In-spite of the repeated attempts made in contacting the email owner to caution about deleting the database, no response was seen. This unresponsiveness from the email address owner aroused a suspicion among officials, "Is the account active or dormant?".
Similar to this breach, there were also breaches happening in Butler Country causing health data's of 1350 people on September and also from Iowa based Thielan student health centre on November 5th with names, insurance information, appointment date's and many things compromised. As a sign of remediation from Officials, the provider amended their security features and cautioned people to stay alert for thwarting any such kind of massacres in the yet to come times.

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

30 Percent of Online Health Databases Expose Patient Data

IntSights researchers found about 1.5 million patient records exposed online through FTP servers, FHIR apps and other platforms that required no intrusive methods to obtain.

Hackers gained access to various online data's through various google methods like technical documentation, subdomain documentation and through other exploiting methodologies through which Hackers exposed 30% of online breaches pertaining to the Healthcare sector. Post investigation, it was revealed that 1.5 million records were exposed from 15 databases among 50. Similar scrutiny of DevOps sites found 23% of servers being open to internet. To add more fuel to the flame, it was discovered that Hova health- a telemedicine vendor beached 2.4 million patients data's at a rate of 16,667 per hour. This was due to the misconfiguration of MongoDB database in August 2018. SMB (Server Message Block) ports were also accessed by researchers and was noted that their security features are damn fragile and they shouldn't be exposed to the public. These were also the cause for Wanna-cry attacks of May 2017.
Researchers further said that healthcare firms aren't doing a great job in protecting patients data's.
To prevent these, researchers recommend the use of 2FA, proper Pen-Testing, incessant monitoring and placing the security controls in a proper place to help organizations remain secure under the umbrella of cyber rains. As a final note, researchers concluded that "Healthcare organizations increased their attack surfaces and have provided cybercriminals new aspects to abduct ePHI. Still no proper investments towards cybersecurity tools or procedures have been implemented".

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

Third-Party Vendor Hack Breaches 48,000 Baylor Frisco Patients

The credit card processing system of Baylor Scott and White Medical Center-Frisco was hacked for about a week in September, exposing the financial data of patients.

A hack on credit card processing system caused a breach of 47,948 patients data with their information's like names. Medical record numbers, account data, credit card numbers, insurance provider information, CCV numbers, credit card type, recurring payment details, account balances, transaction status, invoice numbers and much more being exposed for a week, notified by Baylor Scott and Center-Frisco on December 11, 2018. After detecting the issue on September 29th, instant notification was sent to the vendor and was later followed with substantial investigations to figure out the cause of breach. The reason was found out to be some inappropriate access. All victims have been offered free credit monitoring for 1 year. The online payment function of Baylor Scott and White medical Center-Frisco is still dormant even on December 11th. These attacks are uncountable just like the count of stars on sky. As many healthcare provider have multiple vendors, it is indispensable to build a sane relationship through perfect security assessments.

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

Malware Attack Hits University of Maryland Medical System

The majority of systems were brought back online Monday morning, but officials are still working with forensics and law enforcement to determine the scope of the cyberattack.

On December 11, 2018, a malware attack purged the data's of the University of Maryland medical system in an persuasion to penetrate the IT systems, at 4.30 A.M on Sunday. UMMS' IT team helping patients across Maryland and serving beyond 150 locations, disabled the services of more than 250 IT systems to stop malware from passing to other systems. However under EMS protocols, some patients privileges were escalated to other facilities and through redress measures like identification, isolation and infiltration of threats, the UMMS systems were brought back online and with proper working condition, reports Jon Burns-Senior Vice president and Chief Information Officer of UMMS.
According to Officials, distinct healthcare's like East Ohio Regional Hospital, Ohio Valley medical Center, Rhode Island based Thundermist health center have suffered disastrous cyber breaches. To control these disguised morons, the health system is hiring competent external forensics team and expediting law enforcement collaborations to determine the attack origin.

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

HEALTHCARE

OCR Settles with Colorado Provider for $111,000 over HIPAA Failures

Pagosa Springs Medical Center failed to terminate a former employee's access to electronic patient data and also failed to obtain a business associate agreement with its scheduling vendor

The department of Health and Human services office for civil rights settled with Pagosa Springs Medical Center for $111,400 for waning to end an ex-employee's access whom continued to have remote contact to PSMC's electronic protected health information consisting the ePHI of 557 patients.Corrective action plans like updating the security management and business associate agreement, its policies and procedures, designating an individual who must bear the responsibility for ensuring all the third party vendors enter into a business associate agreement under HIPAA (health Insurance Portability and accountability Act) and all these must be followed for two years under the settlement.OCR Director Roger Severino said that
Its basic sense that left employees connection must be discarded from their termination.
Under HIPAA, covered entities must secure their business with all vendors.
Identity access management must be imbibed with identity access management to determine access to data is with whom and other employee stuff.Severino has reiterated that HIPAA will surge at OCR and this isn't the 1st but 2nd OCR settlement related to the devoid of business associate agreement.

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

EmblemHealth Fined $100K for 2016 Healthcare Data Breach

The New York nonprofit insurer inadvertently revealed the Medicare beneficiary identifications numbers of about 81,000 customers in 2016; 6,000 were New Jersey residents.

Gurbir Grewal- New Jersey attorney general fined health insurance vendor EmblemHealth a fine of $100,000 for its breach on health data's on more than 6,000 New Jersey residents during 2016. In October 2016, a letter was sent by the vendor to customers with their Medicare beneficiary identification numbers composed of 9 digits social security numbers was termed as "Package ID".The investigation figured out that EmblemHealth was at mistake, as the employee who took care of the Evidence of Coverage mailings left the organization without excluding the patient's HICNs, and was replaced by another folk with minimum experience in that department.Whenever highly sensitive personal information are asked by companies to consumers like social security numbers, the information will be stored securely and used discretely, says Paul Rodriguez- Acting Director of New Jersey's Division of Consumer Affairs, in a statement."Sensitive personal information have to be prevented from getting disclosed and health insurers must be entrusted in it", says Grewal in a statement. .A whopping sum of $575,000 was settled already by EmblemHealth with new York in March 2018. The fine reflects the quantity of New York residents impacted.This is just the second settlement between New Jersey and a Healthcare vendor in this month. The first was Attorney General settled with the vendor due to the cause of 2016 Virtua health patient data breach on November 2nd by a extravagant sum of $200,000.

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

EMR Vendor Ransomware Attack Impacts 16,000 Patient Records

A cyberattack on IT Lighthouse, an EMR hosting vendor, breached the data of Redwood Eye Center patients, prompting the eye specialist to switch vendors.

16,055 patients records comprising of names, health insurance information, medical treatment details and many more have been notified to the California Attorney General of a potential breach by California based Redwood Eye Center on Dec 7th, 2018. The type of breach is identified as ransomware that was caused on 20th Sept at IT Lighthouse.
Redwood hired a 3rd party vendor, a digital forensic consultant and a software specialist to inspect the case and since then, Redwood has amended its medical records hosting vendor and has improvised its security program.
However there have indications of large breaches reported to have occurred in the past few months on places like the Center for Vitreo-Retinal Diseases on Illinois with 20,000 breached patient records, Thundersmit Health center being hit last week with a horrendous virus and the previous week, two Ohio hospitals experienced a security breach. As a saving grace factor, the emergency care patients were sent to the adjacent hospitals.
All these disastrous incidents indicate the disturbing fact that Ransomware and other such attacks are still on the rise.

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

20,000 Patients Impacted by Ransomware Attack on Illinois Specialist

Two errors involving paper records were behind two breach notifications this week, while ransomware continues to hit the healthcare sector.

The Center for Vitreo-Retinal Diseases in Illinois recently notified that 20,371 patients data's like names, DOB's, insurance information, Health data, addresses and phone numbers were breached in September 18, due to unauthorized access. The attack type is identified as ransomware. The incident commenced on Dec 6, 2018. Post investigation, it's was evident whether hackers accessed the viewed data. As a wakefulness initiative, officials said that preventive steps are taken to thwart any such incidents further.Similarly, another breach occurred in the San Mateo Medical Center with more than 5000 patient records being breached due to a female staff whom failed to clean the patient box records.According to SMMC officials, Further, the usage of bins have been eliminated by the officials to prevent hazards. Officials conducted two clinic site visits on November 8 and 16th, where "clinic manager for Daly City instructed that recycling bins no longer be used and confidential information be immediately placed in a confidential shred bin."Healthcare sector has been affected by mailing errors in recent years. Recently, Samba a federal benefit association informed 14,000 patients as IRS tax forms were sent to wrong recipients. Later, Orthopaedic and sports medicine practices network notified Texas Physicians and Surgeons about the 2172 patients of a mailing error that breached their personal data's.

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

HEALTHCARE

OCR Fines Florida Physicians Group $500,000 for HIPAA Failures

Advanced Care Hospitalists contracted with an individual claiming to be part of Doctor's First Choice Billings in 2011, but never entered into a business associate agreement as required by HIPAA.

The office of civil rights for multiple HIPAA compliance failures fined the Florida based advanced care Hospitals (ACH) by a whooping sum of $500,000 on December 4, 2018 for sharing protected information with unknown vendor.ACH was contacted by a local hospital on Feb11, 2014 and informed officials that 8,855 patient data's like names, DOB's, social security numbers were viewable on a website named as First Choice website. OCR launched its own investigation into ACH to see what happened and found that ACH never entered into a business agreement with first choice under HIPAA and also failed in adopting a business associate policy until 2014. Also, no security measures, written HIPAA policies or procedures prior to 2014 were implemented. Under HIPAA, thorough routine risk analysis on potential risks and vulnerabilities must be done for all the covered entities and business associates. "This case is especially troubling because the practice allowed the names and social security numbers of thousands of its patients to be exposed on the internet after it failed to follow basic security requirements under HIPAA," OCR Director Roger Severino reported in a statement. Further, ACH needs to instate HIPAA-compliant policies and procedures."As part of this process, ACH shall develop a complete inventory of all electronic equipment, data systems, and applications that contain or store ePHI which will then be incorporated in its risk analysis," according to the agreement. OCR will analyse the analysis and the findings will be approved or disapproved by the officials.This isn't the first but the second OCR settlement in the past month. $125,000 was settle by Allergy associates with OCR for THE impermissible disclosure of patient data due to "reckless disregard for the patients privacy rights".

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Phishig Attack	lack of awareness	Reputation/Money	USA

RANSOMEWARE ATTACK

Ransomware Attack Impacts EHR of Rhode Island Provider

Thundermist Health Center was hit by a ransomware attack on Thursday, cancelling appointments that would impact patient safety without EMR access.

Ransomware attack has once again struck the Thundermist Health center that is in Rhode island on the early Thursday, impacting some patient care on 3rd December 2018. Rhode Island State Police and Rhode Island Department of Health have joined with the officials and expect access to be fully restored by the weekend. This is the second attack in the last two weeks for the healthcare sector. East Ohio regional Hospital and Ohio Valley medical Center interrupted their emergency care services due to cyberattack and those patients were sent to the adjacent hospital. Proofpoint researches have stated that healthcare sector is highly affected ransomware, despite the declination in attack quantity. However, SamSam kind of ransomware is able to execute its malicious deed without human interaction through brute forcing on remote desktop protocol. The Department of Health and Human services, the FBI and security researchers insist organizations to maintain backups for restoring files and in returning back to normal positions. Payment of ransom for "ransomware manumit" should be prohibited.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Ransomeware Attack	lack of awareness	Reputation	USA

HEALTHCARE

42,000 Records Breached in Cancer Treatment Center Phishing Hack

A Cancer Treatment Centers of America employee fell victim to a targeted phishing email in May, providing the hacker with their network credentials.

Cancer treatment Centers of America at western regional medical center informed about 41,948 patients of their personal data breach on December 4th 2018 due to an illegitimate email being responded back by an employee on September 26th with its origin from a CTCA executive.The breached data's contained patient information like names, addresses, sensitive data's like the medical record number, facility visited, treatment date, physician name, cancer type and or health data. Social Security numbers were also included in the breached data list. Post investigation, the types of information seen and influenced by the hackers were unable to be figured out by the forensic team.Post the incident, CTCA notified all the impacted patients and provided free credit monitoring and identity services for people whose Social Security number was involved. Further indoctrination of how to identity rogue emails were also facilitated by the Officials.These phishing attacks have been proliferating throughout 2018. Last week, Georgia Spine and Orthopaedics of Atlanta notified 7000 patients of a breach due to a phishing attack on employee account. Similarly, new York Oncology hematology notified 128,000 patients last month of a breach caused by 15 employees whom fell prey to the phishing traps in April.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Phishig Attack	lack of awareness	Reputation	USA

TECHNOLOGY

New Shamoon Malware Variant Targets Italian Oil and Gas Company

Saudi Arabia's largest oil producer who was tormented by Shamoon- one of the most destructive malware now targeted energy sectors primarily operating in the Middle East

Saudi Arabia's largest oil producer who was tormented by Shamoon- one of the most destructive malware families in 2012 has now targeted energy sectors primarily operating in the Middle East. Prior this week, Saipem-an Italian oil drilling company was attacked and about 10% of servers were destroyed, especially in the Middle East that includes Saudi Arabia, UAE, Kuwait, India and also in Scotland. Saipem admitted on Wednesday that virus used for latest cyberattack is a variant Shamoon-a disk wiping malware was being used against Saudi Aramco and RasGasco Ltd and destroyed data's on more than 30,000 systems. The recent attack against Saipem made more than 300 servers and 100 personal computers to go haywire among 4000 machines. The company pacified the people saying that they had backed up the data's and so contingencies for data loss is not possible.Shamoon alias Disttrack functions by disabling systems and by overwriting key computer files that includes Master boot record (MBR), making it capable for systems to start up. The malware can also easily spread through infected networks using Windows Server message Block (SMB) protocol that is similar to other damaging malware's like WannaCry and Not-Petya.Shamoon had its inception in 2012. Amongst all these chaos spinning in the heads for many, it is still unclear that who is behind its arise. Suspicions steer towards the Iranian hacking groups like OilRig, R. However, the Iranian Government has firmly refused this baseless allegation.

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

RANSOMEWARE

New Ransomware Spreading Rapidly in China Infected Over 100,000 PCs

Presented on December , Repercussions-a new ransomware strain started to target Chinese users and corrupted more than 100,000 systems

Due to supply chain attack on December 1, a new ransomware strain started to target Chinese users and corrupted more than 100,000 systems by encrypting the system files, abducting login credentials of Chinese online services like taobao, Baidu Cloud, NetEase 163, Tencent QQ, Jingdong and Alipay.Velvet security researchers after scrutiny on ransomware determined that the attackers added malicious code and combined with more than 50 poisoned software to be injected into various software's compiled with it. Further, it also tracks the software details installed on the victim's computer. The following data's were procured from the Victim machines. They are cited below:
System version information, current system login username, system login time
CPU model, Screen resolution, IP and broadband provider name, Software installation information.Security software process information, Online shopping account login information, email login information, QQ number login information, network disk login information, etc.Ransomware authors order victims to make payments through Bitcoins but in this scenario, payment was levied to be paid through WeChat payment app. Ransomware operators demand victims to imbue a sum of 110 yuan (app $16).

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Ransomeware Attack	lack of awareness	Data/Money/Reputation	CHINA

TECHNOLOGY

500 Million Marriott Guest Records Stolen in Starwood Data Breach

Presented on December Repercussions-500 Million Marriott Guest Records Stolen in Starwood Data Breach

327 million records containing guest's names, postal address, phone number, DOB, gender, email address, passport number, starwood's rewards information, arrival and departure information, reservation date and communication preferences was breached. During forensic investigation on November 19th, they decrypted the database and figured out that the breach is from Starwood Hotels database. The cause of this is due to unauthorized access to database on Sept10, 2014. Marriott learned during the investigation that there had been unauthorized access to the Starwood network since 2014, and also said that an unauthorized party has copied and encrypted information, and took steps towards removing it."
Starwood said that unknown number of databases contained encrypted credit card data but hasn't been able to rule out the contents needed to decrypt the data.
"Marriott reported this incident to law enforcement and continues to support their investigation," said the statement.
The company said that its Marriott hotels are not believed to be affected as its reservation system is "on a different network," following Marriott's acquisition of Starwood in 2016.
The firm started to notify customers of the breach to people across U.S, Canada and U.K.
4% of financial penalties maybe faced by Starwood if found to be in the breach rules, under the European wide GDPR rules.

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

HEALTHCARE

Dell Resets All Customers Passwords After Potential Security Breach

Presented on december 2018, Dell Resets All Customers Passwords After Potential Security Breach

Dell- A Multinational computer technology disclosed on Wednesday that its online electronics marketplace faced an unfortunate “cybersecurity incident” when an unknown mass of hackers penetrated into the internal network which was later found out by Dell on November 9th.
The initial investigation according to the company found no lucid evidence of hackers triumphing in stealing any information. As a wakefulness measure, Dell reset its passwords for all accounts on its website Dell.com, irrespective of the fact whether the data was pilfered or not.Dell never shared the information’s on how hackers penetrated their networks and how much accounts were affected. The company confirmed that payment information, Social Security numbers, Credit card, sensitive information’s and Dell products/services weren’t targeted. If any account has been created on dell website for purchasing products, then contingencies for those data’s to get corrupted are evident."Upon detection of the attempted extraction, Dell immediately implemented countermeasures and initiated an investigation. Dell also retained a digital forensics firm to conduct an independent investigation and has engaged law enforcement," the company said.

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

SOCIAL MEDIA

Quora Gets Hacked – 100 Million Users Data Stolen

Presented onDecember 2018, Repercussions-100 Million Users Data Stolen

Quora- world’s most familiar Q&A site suffered a humongous data breach due to hackers gaining access to potentially sensitive personal information comprising the data’s of 100 million users.
Adam D Angelo, CEO and Co-founder of Quora, the personal user information compromised in the breach includes: Account information, such as names, email addresses, encrypted (hashed) passwords, and data imported from linked social networks like Facebook and Twitter when authorized by users.
Public content and actions, like questions, answers, comments, and upvotes.
Non-public content and actions, including answer requests, downvotes, direct and messages (note that a low percentage of Quora users have sent or received such messages)
Quora said it stores salted and hashed passwords to thwart them from cracking, but as a precautious awareness, the company has logged all compromised users out of their Quora accounts, and are urging them to reset their password. Quora said it’s still investigating the breach and promised its users that it is working swiftly to "take the appropriate steps to prevent such incidents in the future." Quora's data breach news is the newest in a sequence of high-profile hacks..

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

TECHNOLOGY

Someone Hacked 50,000 Printers to Promote PewDiePie YouTube Channel

Presented on december 2018, Repercussions-Hacked 50,000 Printers to Promote PewDiePie YouTube Channel

The clash for the "most-subscribed Youtube channel" crown between T-Series and PewDiePie took an exciting turn after a hacker yesterday hijacked more than 50,000 internet-connected printers globally to print out flyers requesting all people to subscribe “PewDiePie” YouTube channel, a Bollywood record label T-series with 72.5 million YouTube subscribers. PewDiePie, whose pristine name is Felix Kjellberg, is a highly familiar YouTuber from Sweden, who is specially known for his game commentary and pranks. He has also had the most subscribers on YouTube, ever since 2013. With the Twitter username as “TheHackerGiraffe”, an anonymous hacker emerge with a Hacking driven notion by scanning the list of vulnerable printers, with 9100 ports being open through the scan of Shodan for spewing out a message articulating as ““PewDiePie is in trouble, and he needs your help to defeat T-Series!” . Obviously, post the message display, the hacked victims were pressured to unsubscribe from T-series channel and immediately subscribed to PewDiePie, without procrastination. tter,” the hacker tweeted. Honestly speaking from the atrium of my heart, trust me as even your fax number is more than sufficient for hackers to infiltrate into your data’s and take complete control over the printer and even penetrate the remaining part of the networks connected to it. Indeed, the space between the two epic channels is seeking a confrontation as the intriguing battle is about to halt. Let’s see if PewDiePie can win the prestigious tiara of being the “Most followed YouTube channel”.

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

RANSOMEWARE

U.S Charges Two Iranian Hackers for SamSam Ransomware Attacks

Presented on December 2018, Repercussions-U.S Charges Two Iranian Hackers for Ransomware Attacks

Faramarz Shahi Savandi and Mohammad Mehdi Shah were charged by the authorities in the U.S for being in link with a series of more than 200 notorious ransomware attacks.Unlike normal ransomware attacks, SamSam attacks hack organizations data’s manually one by one through a variety of techniques like brute-forcing their way into exposed RDP connections on a vulnerable server and making the use of pilfered login credentials.Harvesting of admin passwords and escalation of privileges would be done by hackers once with a intention to check out the gathering of further intelligence on the compromised network. Through this strategy, they mark and expand their foothold and unleash the SamSam ransomware to compromise and encrypt PC’s. By this, victims were steered to the webpages under the control of hackers whom contained their ransomware demands parallel with a threatening countdown, post which it was said that decryption keys will be deleted and recovery of the lost stuffs will be impossible. A mindboggling sum of US $8000 worth of Bitcoin would be demanded from the SamSam extortionists to recover the lost files or a US $55,000 whopping sum to decrypt the affected PC’s on a network. FBI’s investigation reveal that the existence both men is speculated to be in Tehran, the capital of Iran.In the absence of a physical person to place before a judge, the US authorities have instead published the Bitcoin addresses used by the pair for allegedly collecting their ransomware payments. Processing transactions relating to direct addresses is not being encouraged under the Cryptocurrency exchanges

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Ransomeware Attack	lack of awareness	Reputation/Money	USA

Uber fined $1.1 million by UK and Dutch regulators over 2016 data

Presented on December 2018, Repercussions- Uber fined $1.1 million by UK and Dutch regulators over 2016 data

Uber-a renowned ride-sharing company was hit on Tuesday by the British and Dutch with an alleged fine of $1,170,892 (app 1.1 million) for failing to protect users sensitive personal information during a cyberattack on 2016, involving the data's of millions of users.The massive data breach in October 2016 experienced by Uber unveiled the fact the breached data's contained names, email addresses and phone numbers of about 57 million Uber riders and drivers with Driving license numbers of 600,000 drivers. Apart from this, a ransom of $100,000 for maintaining the incident with secrecy and in privacy.Today Britain's Information Commissioner's Office (ICO) fined Uber 385,000 pounds ($491,102), while the Dutch Data Protection Authority (Dutch DPA) levied a 600,000 euro ($679,790) penalty on Uber for failing to protect the personal information of its 3 million British and 174,000 Dutch citizens, respectively.. . It gains the fame as the most widely used and deployed database engine in the world today that is used by countless of applications with billions of deployments including IoT devices, macOS and Windows apps, including major web browsers, such as Adobe software, Skype and more.Google Chrome, Opera, Vivaldi and Brave – all these Chromium based web browsers also support SQLite through the deprecated Web SQL database API, through which a remote attacker can target the affected browsers by conjuring them and then influencing them to visit a specially crafted web-page.Updated version3.26.0 of its software has been released by SQLite to address the issue and Google has also released Chromium version 71.0.3578.80 to patch the issue and pushed the patched version to the latest version of Google Chrome and Brave web-browsers.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Stuffing Data Breach	lack of awareness	Data/Money/Reputation	UK/Dutch

TECHNOLOGY

Critical SQLite Flaw Leaves Millions of Apps Vulnerable to Hackers

Presented on December, Repercussions-Critical SQLite Flaw Leaves Millions of Apps Vulnerable to Hackers

Cybersecurity researchers have discovered a critical vulnerability in widely used SQLite database software that exposes billions of deployments to hackers by allowing remote attackers to execute malicious codes and by crashing apps.SQLite requires minimal support from operating systems or external libraries, and hence compatible with almost every device, platform, and programming language.SQLite is the most widely deployed database engine in the world today, which is being used by millions of applications with literally billions of deployments, including IoT devices, macOS and Windows apps, including major web browsers, such as Adobe software, Skype and more.Since Chromium-based web browsers—including Google Chrome, Opera, Vivaldi, and Brave—also support SQLite through the deprecated Web SQL database API, a remote attacker can easily target users of affected browsers just by convincing them into visiting a specially crafted web-page.SQLite has released updated version 3.26.0 of its software to address the issue and Google has also released Chromium version 71.0.3578.80 to patch the issue and pushed the patched version to the latest version of Google Chrome and Brave web-browsers.Tencent researchers said they successfully build a proof-of-concept exploit using the Magellan vulnerability and successfully tested their exploit against Google Home.Users and administrators are highly recommended to update their systems and affected software versions to the latest release as soon as they become available.

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

TECHNOLOGY

China hacked HPE, IBM and then attacked clients: Sources

presented on December2018-china hacked HPE,IBM and then attacked clients

Hackers working on behalf of China's Ministry of State Security, breached the networks of Hewlett Packard Enterprise Co and IBM. After the incident, it was used to gain access for hacking into their clients' computers, according to five sources familiar with the attacks.
The attacks were part of a Chinese campaign known as Cloudhopper, which the United States and Britain on Thursday said to the infected technology service providers in order to exploit secrets from their clients.While cybersecurity firms and government agencies have issued multiple warnings about the Cloudhopper threat since 2017, they have not disclosed the identity of technology companies whose networks were compromised.Businesses and governments are increasingly looking to technology companies known as managed service providers (MSPs) to remotely manage their information technology operations, including servers, storage, networking and help-desk support.Cloudhopper attacks date back to at least 2014, according the indictment.They were from industries including finance, electronics, medical equipment, biotechnology, automotive, mining, and oil and gas exploration.One senior intelligence official, who declined to name any victims who were breached, said attacks on MSPs were a significant threat because they essentially turned technology companies into launchpads for hacks on clients."By gaining access to an MSP, you can in many cases gain access to any one of their customers,"

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Sensitive data exposure	lack of awareness	Reputation/Data	USA

SOCIAL MEDIA

Hackers Exploit Malware Attacks Through Twitter Memes

presented on December2018-Repercussions of hackres exploiting malwar attack through twitter memes.

According to a recent report, researchers at Trend Micro have found some malicious Twitter memes that obfuscate malware. When a victim downloads such memes, the malware thrives towards the victim's device and executes its code in secrecy without cautioning the user.
The researchers illustrated that the Hackers exploit this trick using steganography method for injecting malware. In this method, the author hides a malicious payload in an image to evade cybersecurity measures. According to Trend Micro, the hackers may now exploit the same trick via Twitter memes as well.
Reportedly, they noticed an old Twitter account posting memes on October 25, 2018, and October 26, 2018. Regarding how this malware could execute, they state that, "what makes the discovery significant is the reliability of the source bearing the malicious memes, that is, Twitter. Identified as TROJAN.MSIL.BERBOMTHUM.AA. Taking the malicious memes down seemed impossible without suspending the malicious Twitter account".

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

NASA Confirmed Data Breach After an Internal Server Was Hacked

presented on December2018-Nasa confirmed data breach after an internal server was hacked

In a recent memo disclosed to employees, NASA confirmed a data breach that was related to one of their internal servers. Allegedly, the server contained personal information of employees which may have leaked to the hackers, the data included social security numbers.
As revealed, the cybersecurity personnel at NASA found out the breach in October while investigating a server containing employees' . NASA haven't poignantly stated what exactly the leaked data includes, however they confirmed the breach of Social Security numbers.
At the moment, they haven't disclosed any details regarding the impact of the breach. Rather they confirm that investigations are underway. This also includes investigations regarding the identification of hackers.

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

Saint John Parking Ticket System Data Breach Impacts Users

presented on December2018-Repercussions saint john parking tikect system data breach impacting users

A minimal of 6,000 people in Saint John, N.B have been affected by a data breach that impacted the municipality's online parking ticket system.
Alex Cooke of the national news agency The Canadian Press reports, "As many as 6,000 people in Saint John, N.B., could have had their personal information exposed, an analyst group said as the city announced it was one of dozens of municipalities affected by a data breach to its online parking ticket payment system."
The report also reveals that the city has learned about a breach to the third-party software product Click2Gov; HackerCombat has already reported about the data pilferage from local Click2Gov government systems across US cities. Click2Gov, which is being run by CentralSquare Technologies, gives people the options to make online payments and make use of the many government services. The Saint John online parking ticket system, which functioned through this software, permitted people to pay parking tickets through the city's website.

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

Facebook Share Plunges Following Allegations of Data Sharing

Presented on December2018-Repercussions on Facebook share plunges following allegations of data sharing

SOCIAL MEDIA

The shocking news of Facebook allowing companies like Spotify, Bing, Royal bank of Canada to access user's private messages has been the hot news for various people in the earth. This waning news has hit the Facebook shares badly. After an earnings report indication, it is evident that Facebook is witnessing the second steepest fall this year with a drop of 19% on July 26th. It is the only major tech company to see its stock below the red line. By end of Wednesday's Federal Reserve meeting, it became worst when the Nasdaq composite Index steeped down to 2.17 percent.As per the allegations reported in Times may put Facebook in trouble for violating its 2011 agreement with the Federal trade Commission. The agreement needed Facebook to make poignant stands on how much data it shared with 3rd parties and banned it from sharing friends data without their permission. Facebook reportedly considers its "partners" to be extensions of its core business, rather than third-parties.

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

BJC Healthcare: Another Healthcare Provider Becomes a Malware Victim

Presented on December2018-Repercussions on a healthcare provider who becomes a malware victim

HEALTHCARE

BJC HealthCare, a non-profit healthcare organization,, headquartered in St. Louis Missouri became a recent victim of malware which is now being blamed for the loss of personally identifiable information. This includes credit and debit card details of 5,850 patients. BJC HealthCare confirmed the theft of data more than a month ago, November 19. The malware had allegedly intercepted all patient records entered into the system from October 25 - November 19 of all those who received service from BJC HealthCare. The healthcare institution advised the patients and their families to monitor their bank accounts for detection of illegitimate transactions. At the time of this writing, BJC HealthCare has already contacted all the affected patients. "BJC has no indication to date that any information was actually misused. As a precaution, individuals whose payment information may have been exposed are advised to carefully review credit card and bank statements and immediately contact their credit card holder or banking institution about any inconsistencies or suspicious activity

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

TECHNOLOGY

Shamoon Malware from 2016-2017 Evolved With File Wiping Capability, Targets Middle East Countries

Presented on December2018-Repercussions of shamoon Malware evolving wiping capability, targets middle east countries.

McAfee, the Intel subsidiary anti-malware vendor has recently disclosed the evolution of the Shamoon malware, with Europe and the Middle East, stating these both as the two most infected regions. The newer version of Shamoon has an added capability of wiping files off the hard drives, making the new variant highly damaging for the victims. Just like the other complex malware of this generation, Shamoon's new variant is not just a 1-file malware, but comes with a modular layout of related files, as per McAfeeThis tool is responsible to run the second tool, spreader.exe, with the list of each targeted machine.
Spreader.exe: Used to spread the file eraser in each machine previously set. It also gets information about the OS version.SpreaderPsexec.exe: Similar to spreader.exe but uses psexec.exe to remotely execute the wiper.SlHost.exe: The new wiper, which browses the targeted system and deletes every file.Even with the complexity of Shamoon, its behavior was understood by McAfee relatively faster, since the malware was developed under .Net Framework, a toolkit that is well acquainted and understood by the developer community. From the attack pattern of the malware, it can be concluded that the virus author's goal is to focus its attention on oil-exporting countries, which are mostly in the Middle East. Through the usage of Powershell, the next generation command-line scripting utility in Windows, the malware executes Powershell scripts it downloaded from the command and control servers, which includes capturing user credentials and identification of the Windows Active Directory domain, where the PC is undeniably a member of.

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

Almost 19,500 Orange Modems Leaking WiFi Credentials

Presented on December2018-Repercussions leading to almost 19,500 leaking WI-FI Credentials

Over the weekend, a security researcher has discovered that nearly 19,500 Orange Livebox ADSL modems are leaking WiFi credentials.roy Mursch, co-founder of Bad Packets LLC, says his company's honeypots have detected at least one threat actor scanning heavily for Orange modems. Scans started Friday, December 21, Mursch said.The attacker is exploiting a vulnerability affecting Orange LiveBox devices (CVE-2018-20377) that was first described in 2012. The vulnerability allows a remote attacker to obtain the WiFi password and network ID (SSID) for the modem's internal WiFi network just by accessing the modem's get_getnetworkconf.cgiServices like Widle allow an attacker to get the exact geographical coordinates of a WiFi network based only on its SSID. Since the Orange modem also leaks the WiFi password, an attacker can travel to a suspected high-value target, This vulnerability can also be used to build online botnets. .This panel can be used to alter the modem's settings, but also to gain access to sensitive information."They can obtain the phone number tied to the modem and conduct other serious exploits detailed in this Github repository," Mursch said today in a security advisory published by his company.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Phishig Attack	lack of awareness	Reputations/Data	USA

European Union's COREU Network Hacked, Confidential Diplomatic Cables Stolen

Presented on December2018-Repercussions on European union's coreu network,confidential diplomatic cables stolen

Cyberattacks against European Union's diplomatic cables have been happening for a while which was allegedly targeted by Chinese based Hackers whom also targeted the COREU network. A diplomatic cable alias diplomatic correspondence/embassy cable is a short message sent in secrecy between the legitimately involved consulates/embassies or foreign dignitaries of two or more county's. These messages are being treated with the highest level of classification with strong encryption standards embedded in it and can only be unlocked by the receiving party.
Area 1 Security found indications that Beijing-sponsored hackers are behind the breached diplomatic cables, with the earliest copies were three years ago, in 2015. The COREU Network is EU's link for the rest of twenty-eight European Union-member states. Three organs of the European Union are cited as follows:
The main users of the mentioned network
The European Commission
The Council of the European Union and the European External Action Service

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

TECHNOLOGY

Massive Data Breach Hit Caribou Coffee, All Customers Transacted From Aug 28 to Dec 3 Affected

Presented on December2018-Repercussions that hit caribou-coffee,All customers transacted from Aug 28 to Dec 3.

Caribou Coffee, a U.S based Coffeehouse chain with 603 branches, publicly made disclosure that thousands of their customer records from at least 219 branches in Minnesota were affected by a data breach. The security breach happened for three-month straight before it was discovered, according to their official disclosure document. Unauthorized access to their servers was detected and all their customers who transacted with them between August 28th to Dec 3rd had their credit card number, full name, and other personal information extracted.
"On November 28, 2018, we identified unusual activity on our network through our information security monitoring processes. Upon identifying this issue, we began working with Mandiant, a leading cybersecurity firm, to understand the scope of the incident and determine whether there had been any unauthorized access. On November 30, 2018, Mandiant reported that it detected unauthorized access to our point of sale systems, exposing some of our customers' data. Mandiant worked with us to contain the breach and ensure that the unauthorized access was stopped immediately

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

CONCLUSION

A perfect security quality is like the “Crave for escaping from the hack Grave”. Cyber breaches had, are, and will continue to still persist. This is due to pathetic fact that cybersecurity isn’t still taken seriously. Even after acknowledging the fact of top firms being hacked, still there is a complacency feeling among small and mid-sized firms as ”Our data’s are secured as they are hosted on Cloud, OEM’s, Amazon and on other such reputed platforms”.

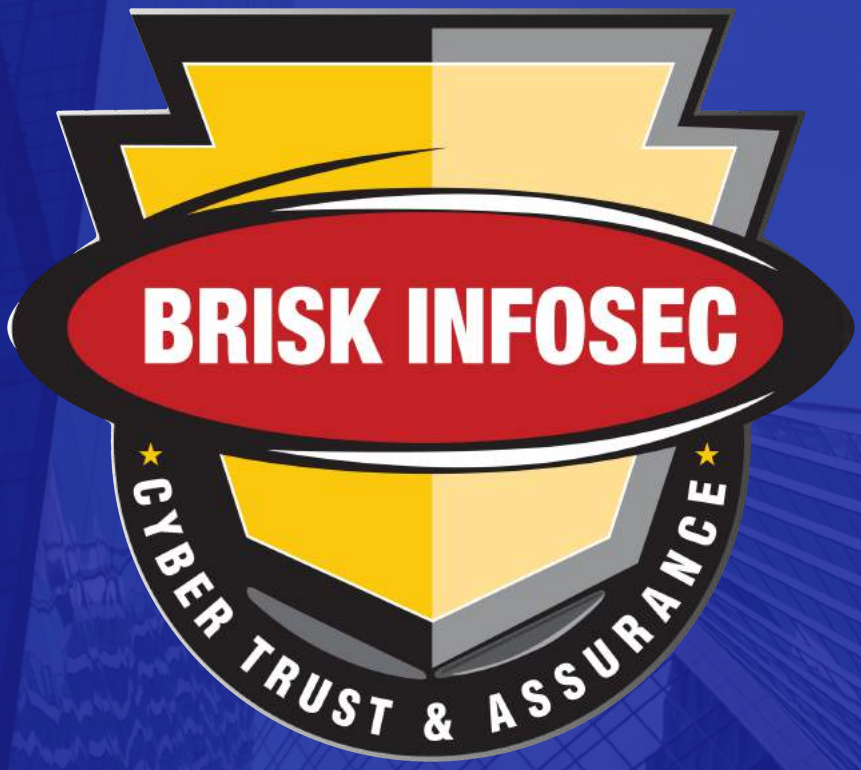
Honestly this isn’t sufficient to ensure CIA to the fullest. Apart from this, a proper security scanning is required. For this, you need to find a competent and dedicated cybersecurity vendor. If you want to hire a dexterous cybersecurity firm, you can have a profound and relaxed breath as you have approached the right place, who can make your security standards “strong enough to meet the cyber requirements”. Our dedication in proving our worth to all our esteemed clients is so high and that’s the reason why our consistency never dies. To know more about us

“Just get with us now in touch

It will for sure, mean you so much”.

Reference Links

https://healthitsecurity.com/news/email-error-lack-of-encryption-breaches-nebraska-patient-data
https://www.helpnetsecurity.com/2018/12/11/healthcare-databases-are-exposed-online/
https://healthitsecurity.com/news/third-party-vendor-hack-breaches-48000-baylor-frisco-patients
https://www.baltimoresun.com/news/maryland/education/higher-ed/bs-md-umms-hack-20181210-story.html
https://healthitsecurity.com/news/ocr-fines-colorado-provider-111000-for-hipaa-violations
https://healthitsecurity.com/news/dod-health-agency-security-flaws-put-patient-data-at-risk-oig-finds
https://www.healthcareitnews.com/news/14-million-patient-records-breached-unitypoint-health-phishing-attack
https://healthitsecurity.com/news/20000-patients-impacted-by-ransomware-attack-on-illinois-specialist
https://healthitsecurity.com/news/ocr-fines-florida-physicians-group-500000-for-hipaa-failures
https://healthitsecurity.com/news/ransomware-attack-impacts-ehr-of-rhode-island-provider
https://professionalhackers.in/new-shamoon-malware-variant-targets-italian-oil-and-gas-company/
https://professionalhackers.in/new-ransomware-spreading-rapidly-in-china-infected-over-100000-pcs/
https://www.telegraph.co.uk/technology/2018/11/30/private-data-500-million-marriott-guests-exposed-massive-breach/
https://thehackernews.com/2018/11/dell-data-breach-hacking.html
https://www.theverge.com/2018/12/3/18124849/quora-100-million-user-hack-name-email-messages
https://nypost.com/2018/12/03/youtube-star-pewdiepies-fans-hacked-50000-printers/
https://www.tripwire.com/state-of-security/featured/iranian-hackers-samsam-ransomware/
https://professionalhackers.in/uber-fined-1-1-million-by-uk-and-dutch-regulators-over-2016-data-breach/
https://professionalhackers.in/critical-sqlite-flaw-leaves-millions-of-apps-vulnerable-to-hackers/
https://m.dailyhunt.in/news/india/english/deccan+chronicle-epaper-deccanch/china+hacked+hpe+ibm+and+then+attacked+clients+sources-newsid-104457927
https://www.csoonline.com/article/3329296/security/twitter-bug-may-have-been-exploited-by-state-sponsored-hackers.html
https://www.financialexpress.com/industry/technology/cybersecurity-menace-nasa-confirms-data-breach-that-compromised-personal-data-of-employees/1418635/
https://www.cbc.ca/news/canada/new-brunswick/saint-john-malicious-activity-parking-payment-system-1.4962275
https://hackercombat.com/shamoon-malware-from-2016-2017-evolved-with-file-wiping-capability-targets-middle-east-countries/
https://www.worldwebsitedesign.com/more-than-19000-orange-modems-have-wi-fi-credentials/
https://hackercombat.com/european-unions-coreu-network-hacked-confidential-diplomatic-cables-stolen/
https://www.bizjournals.com/twincities/news/2018/12/20/caribou-coffee-warns-of-data-breach-at-265-stores.html
https://hackercombat.com/bjc-healthcare-another-healthcare-provider-becomes-a-malware-victim/
https://www.livemint.com/Companies/Gz4GNmtpRfe5a2oipJqXgL/Facebook-shares-take-historic-plunge-as-data-scandals-finall.html
https://www.bbc.com/news/technology-46552339



THREATSPLOIT ADVERSARY REPORT JANUARY 2019

www.briskinfosec.com