NOVEMBER 2018

THREATSPLOIT ADVERSARY REPORT

WWW.BRISKINFOSEC.COM

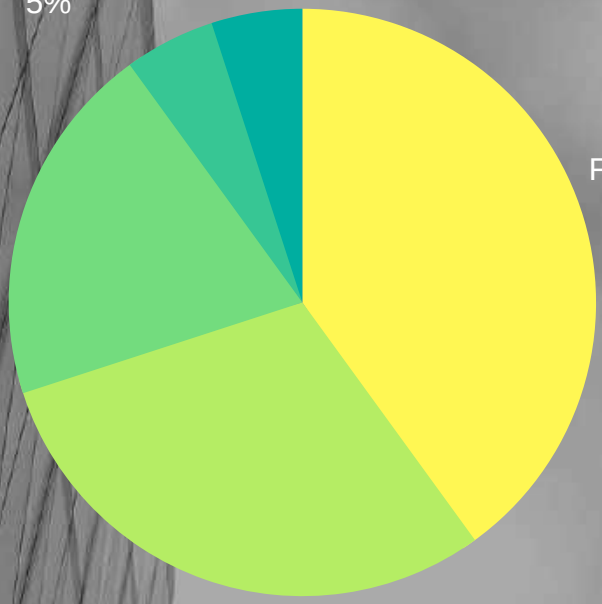
Threatsploit report is a comprehensive report about various cyber attack activities.

Briskinfosec has established its fame by serving all its esteemed clients excellently both in the Asia – pacific region as well in the other parts of the Globe. These days the word “Hacks” and “Hackers” are the most feared words by every organization due to the undeniable fact that every security framework and tool which was considered to be the best has pathetically relinquished to the Hackers test. As technology is making lives easier on one side, there is also another side of the story which isn’t acknowledged by many such as the stealthy digital hacks, data compromises, identity masquerading which still persist in various sectors such as health sector, energy companies, software companies, banking authorities and others, perhaps the initiation of various wakefulness measures.

The above consolidated Threatsploit report is an intensified and extended work of Briskinfosec which illustrates the compromised status of many organization due to proper security vendor being devoid. Hence, a proper security vendor needs to monitor your organization for anomalous detection and breach prevention.

MONTHLY STATISTICS 2018

FINANCIAL ANALYSIS FOR OCTOBER 2018



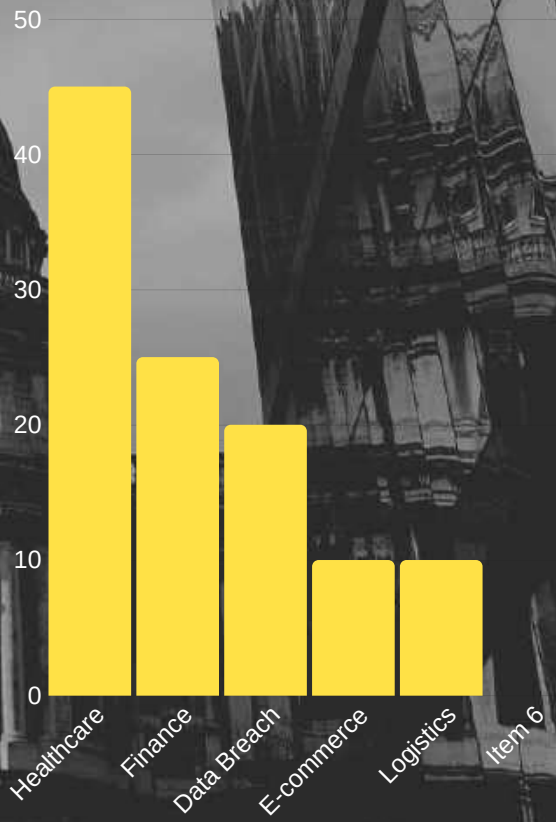
40%

Cyber attacks against financial industries are becoming more frequent, sophisticated and more widespread

REPUTATION ANALYSIS FOR OCTOBER 2018

45%

Healthcare Experiences Twice the Number of Cyber Attacks As Other Industries



HEALTHCARE

- Criminals Hijacked Records of 75,000 Users From Healthcare.Gov
- Unauthorised Access Attempts Detected on Singapore's HealthHub Portal
- Misconfigured Database Breaches Thousands of MedCall Advisors Patient Files
- Two Phishing Attacks on Minnesota DHS Breach 21,000 Patient Records
- Phishing Attack Breaches Insurance Data of 37,000 Patients for 1 Month
- 3 Phishing Hacks Breach 20,000 Catawba Valley Patient Records

FINANCE

- Tesco Bank Hit With $21.3 Million Fine Over Debit Card Fraud
- North Korean Hackers Tied to $100 Million in SWIFT Fraud
- Bupa Fined $228,000 After Stolen Data Surfaces on Dark Web
- South Korean Gov't Investigating Bithumb Security Breach, World's Largest Exchange

CRYPTOCURRENCY

- Connecticut City Pays Ransom After Crypto-Locking Attack
- Cryptocurrency Exchanges Lost $882 Million to Hackers

E-COMMERCE

- Magecart Card-Stealing Gang Hits "Shopper Approved' Plug-In

LOGISTICS

- Cathay Pacific Breach Hits Over 9 Million Customers

DATA BREACH

- Pocket iNet Leaves 73 GB of Sensitive Data Exposed
- Google Forced to Reveal Exposure of Private Data
- Water Utility Attacked
- Deadly Malware That Attacked Saudi Industrial Plant Came From Russia
- US Voter Records for Sale on Hacker Forum
- Nasty Linux Kernel Vulnerability Discovered, Mandatory Kernel Update Required

Healthcare-01

Criminals Hijacked Records of 75,000 Users from Healthcare.Gov

Presented on oct 2018, Repercussions-75k victims facing data breaches on center for medicare and medical services, website-www.healthcare.gov

An official post from an anonymous site confirmed that about 75,000 user's data from Healthcare.gov service was hijacked by an obscure group of cyber-criminals. "Obamacare" - An medical healthcare plan is a federally facilitated exchanges used by the healthcare agents and brokers which has been uploaded in the site.On Saturday, a peculiar framework was announced by the centers for medical and medicaid services (CMS) which provoked the executives to arouse a warning and for an investigation inception, after a strange system activity detection in the FFE, said by the CMS on October 13, 2018.The CMS said in a press release that the associated ones with the anomalous activity were deactivated and due to surplus caution, the direct enrollment pathway for the agents were disabled.Notions for replenishing and re-enabling FFE direct enrollment for agents and brokers within the week are in the process - says Government agency. Obamacare health care plans can still be enrolled by the U.S citizens through Healthcare.gov portal platform or the Marketplace Call Center.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Account Hijacked	Lack of Awareness	Reputation	USA

Healthcare-02

Unauthorised Access Attempts Detected on Singapore's HealthHub portal

Reported on oct 2018, Repercussions- 72 HealthHub accounts suspected hacked, website-www.healthhub.com

Singapore natives use HealthHub -An one stop portal and mobile application for accessing a wide range of health content, honours and E-services. On Sept 28th, Oct 3rd, Oct 8th and on Oct 9th, the agencies had detected the presence of more than usual attempted logins to the Healthhub portal through the usage of more than 27,000 unique ID's or email addresses with 98% of the email address proving irrelevant to the current HealthHub accounts and the persuaded log-in attempts garnering failure. The successfully logged 72 accounts were subsequently locked and the HPB had intimidated the account holders of suspicious activity detection and to verify and inform if any of them had made the attempts of their own. Within the next few moments, the HPB were informed about a call from a suspected user claiming that her email ID had gone haywire by a person whom without authentication had logged into a portal. The agency later announced that no sign or gesture of a breach in a HealthHub system was sensed.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Unauthorised access	weakness	Reputation	Singapore

Healthcare-03

Misconfigured Database Breaches Thousands of MedCall Advisors Patient Files

Presented on oct 2018, Repercussions-10000 files exposed in online on amazon s3 buckets,website-docs.aws.amazon.com

Security researcher Britton White intimidated Databreaches.net and discovered that North Carolina based tech vendor Medcall is disclosing protected patient data through Amazon S3 bucket 2 times in a month by leaving a storage bucket containing 10,000 files exposed in the internet available for downloading, deleting and for editing, with later confirming it. The databases which included few patient names, email and postal addresses, phone numbers, dates of birth and social security numbers with other files holding the records of patient evaluations and conversations with doctors, their medications, allergies and other brief personal data issues were listed on grayhatwarfare.com. An searchable tool, which overtly lists the current open Amazon S3 buckets. To intensify the shame, this isn't the 1st time this database is exposed. It's the2nd!!!

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Security Misconfigured	Lack of Awareness	Reputation	USA

Healthcare-04

Two Phishing Attacks on Minnesota DHS Breach 21,000 Patient Records

Reported on oct 2018, Impact - 21000 patients details leaked on Minnesota Department of Human Services, website-https://mn.gov/dhs/

Mail accounts of two DHS employees which comprised of names, addresses, telephone numbers, birth dates, social security numbers, educational records, medical information, employment and financial information, were confirmed to be breached by the investigation panel after the personnel's clicked on malicious links which were triumphantly conjured by the hackers through phishing. Ongoing investigation of other employees mail id's being compromised are yet to be disclosed by the Minnesota DHS, with contingencies oscillating towards the "YES" side. The IT department confirmed the breaches only on August with the incident happening at the time of 28th and 9th of June and July 2018, respectively. Post the discovery of phishing attacks, both accounts were secured for paving further access to other data's. Immediate actions for securing these accounts were facilitated with "Blanked out scenario" prevailing on the verdict of Data being viewed, downloaded or in being misused.

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

Healthcare-05

Phishing Attack Breaches Insurance Data of 37,000 Patients for 1 Month

Presented on oct 2018, Repercussions-37k patients detailed leaked on gold coast health plan , website-https://m.goldcoasthealthplan.org/

About 37,000 patients data's under the California-based Gold Coast Health Plan which included member names, health plan identification numbers, dates of medical services, dates of birth and medical procedures, were breached through a phishing attack which was executed by hackers when an email account of an employee was compromised from mid-June till August dawn. This information went inebriated in surface after being discovered by the Gold coast officials on Aug 8th, due to which unauthorized access was halted on the same day with law enforcement and cyber forensics being contacted for ulterior investigation. After scrutiny, it was revealed that hackers have illegitimately persuaded in transferring the funds of Gold coast health Plan into their account. After this official verdict, the victims were cautioned to monitor the medical bills on their on their credit reports for anomalous detection. Since then, hazards of phishing attacks have been imparted with heightened security monitoring kind of method being levied for obstruction of unauthorized access and for the enhancement of security perimeter.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Phishing Attack	Lack of Awareness	Reputation	California

Healthcare-06

3 Phishing Hacks Breach 20,000 Catawba Valley Patient Records

Reported on oct 2018, Repercussions-20k patients records exposed on Catawba valley, website-www.cvcc.edu

Officials discovered unauthorized access on an employee email account on Aug. 13 and immediately secured the account and launched an investigation with help from a third-party forensic firm. The investigation determined it was not one but two accounts hacked for more than a month between July 4 and August 17. The investigation found those email accounts included patient names, dates of birth, medical data and health insurance information, according to officials. Social security numbers were included for some patients. Catawba Valley began notifying patients on Oct. 12 and created a dedicated call center to handle patient questions about the breach. Officials are recommending patients review any statements they receive from their insurance carrier to make sure they're not billed for any services they didn't receive. The medical center has since hired security experts to improve employee education while bolstering email controls and upgrading its software and hardware controls,

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

FINANCE-01

Tesco Bank Hit With $21.3 Million Fine Over Debit Card Fraud

Presented on oct 2018, Repercussions-21.3 million fine on tesco bank website-www.tescobank.gov

Failing to proactively prevent the foreseeable online attacks of the hackers has resulted for the Scotland-based Tesco bank an whooping $21.3 million loss, fine by the U.K's financial conduct authority. The 48 hours attack that incurred in November 2016 paved gateway for hackers to steal $2.93 million, reports the financial conduct Authority (an independently operating financial regulatory body of the U.K government. It was pronounced by the FCA that Tesco bank violated the standards which the financial firms must follow (Principal 2). "Principal 2 requires a firm to conduct its business with due skill, care and diligence", it tells. Magecart another threatening group whom focus on payment card stealing have been tied to another series of online attacks."Shopper Approved" an e-commerce service based organization situated in Ogden, Utah that enables sites in gathering local, merchant and product reviews from customers is cited to be the latest victim of cyberattack which was later confirmed by them after acknowledging the confirmation of attack from Magecart through an security firm, pertaining to the incident. Additional security measures were also implemented to ensure that this doesn't exist.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Deficiencies in card	Targeted Attack	Financial	USA

FINANCE-02

North Korean Hackers Tied to $100 Million in SWIFT Fraud

Presented on oct 2018, Repercussions-$100 M on Swift spoofing .

More than $100 million during illegitimate transfers through SWIFT have been conjured and stealthily deceived due to the incessant hacking attacks by an anonymous gang of North Korean Hackers (APT38) on the banks in Asia and Africa- says an U.S cybersecurity firm. These APT38 hackers group are different from the from the North Korean Hackers groups known as Lazarus and Temp.Hermit. The attackers whom launch long, sustained and stealthy attacks against the locked targets are the ones referred to the APT designation. More than 16 hacking operations in 11 countries have been conducted by the APT38 hackers group, since 2014 with FireEye researches in a Wednesday blogpost indicating that the group is large progressing more prolific operations with magnanimous resources.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Swift Spoofing	Targeted Attack	Financial	USA

FINANCE-03

Bupa Fined $228,000 After Stolen Data Surfaces on Dark Web

Presented on oct 2018, Repercussions-Fined $228000 data surfaces ok darkweb, website-www.bupa.com

BUPA insurance services were levied with a hefty amount of ($228,000) by the U.K data protection regulator for preventing to stop an personnel from deceiving 547,000 customer records, which was later hosted on the dark web.The information Commisioner's Office infuriated against BUPA, slamming that they failed to secure the personnel's data's perhaps a time period of 3 months being granted, post the havoc. U.K's information Commisioner Elizabeth Denham found that the extracted records from Bupa's customer relationship management system "Dubbed Swan", contained almost a whopping magnitude of 1.5 million records which included names, birth names, nationalities, policy-related data that includes email address, phone address, phone numbers and fax numbers with no medical data being pilfered. Also, it was figured out that the inadequacies around SWAN were "ultimate approach based" rather than the prospect of arising with notions and remediation's from specific incidents at that time itself without procrastination. According to the ICO's penalty notice, "Bupa Insurance services is gigantic, well-resourced and an experienced data controller". In 1988, the ICO found that Bupa violated the elements of the U.K Data Protection Act.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Data Theft	Targeted Attack	Reputation	USA

FINANCE-04

South Korean Gov't Investigating Bithumb Security Breach, World's Largest Cryptocurrency Exchange

Presented on oct 2018, Repercussions-crytocurrency exchanges data leaked,

According to reports, funds of Bithumb users were not stolen during the hacking attack. But, sensitive personal and financial information of at least 30,000 users has been leaked. The Seoul Central Prosecutor's Office for Advanced Criminal Investigation led by supervisor inspector Shin Bongsu, revealed that hackers targeted Bithumb employees with phishing emails, sending malware to the computers used by employees within the Bithumb headquarters. By using the emails of employees, the hackers were able to extract personal information of over 30,000 users.The Seoul Metropolitan Police Agency's Department of Cybercrime, told reporters that several Bithumb users notified the agency of suspicious transactions and bank account activities. Some users claimed that the personal information that was leaked during the security breach involved banking information, which allowed hackers to withdraw money from the bank accounts of Bithumb users. In the next few days, Bithumb will collaborate with government agencies and the South Korean police to investigate the security breach, and implement necessary security measures to prevent such attacks in the future.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Data Theft	Targeted Attack	Reputation	USA

CRYPTO-01

Connecticut City Pays Ransom After Crypto-Locking Attack

Presented on oct 2018, Repercussions-paid huge amount for ransom.

23 servers in Connecticut have brutally gone haywire due to a storming catastrophic ransomware attack, incurred during the time line of 2.49 A.M to 3.16 A.M on Oct 16th Tuesday dawn, reports the city of West-Haven. The city later emerged with a positivity note stating that the attack has been contained by evening 5.30 on 17th Oct. The mayor alongside the local and national authorities were instantly informed about this ransomware by the city's IT manager, David W. Richards, after its discovery.During the investigation phase, the West Haven police were assisted by "MS-ISAC", a division of the U.S department homeland security as well the DHS information sharing and analysis center for improving cybersecurity on various scales. They determined that the attack has thrived from the outskirts of U.S, announced during Thursday by the West Haven mayor Nancy R. Rossi.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Ransomware Attack	Targeted Attack	Reputation	USA

CRYPTO-02

Cryptocurrency Exchanges Lost $882 Million to Hackers

Presented on oct 2018, Repercussions-$882 M lost on exchange of cryptocurrency

As per the reports of Moscow based cybersecurity firm group-IB analysis, $882 million damages have been inflicted over two years during the exchange of cryptocurrency. The tally is likely to proliferate in the upcoming years due to the extravagant quantity of attention drawn towards cryptocurrency exchanges as well the initial coin offerings from various veteran Russian hacking groups such as Cobalt, Silence, MoneyTaker and the Lazarus group from North Korea. The number of targeted attacks on crypto exchanges will be elevated by 2019 with cryptocurrency exchanges showing certainty in being the latest target for most aggressive hacker groups usually attacking banks, writes GROUP-IB.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Not Published	lack of awareness	Reputation	USA

E-COMMERCE-01

Magecart Card-Stealing Gang Hits “Shopper Approved' Plug-In

Presented on oct 2018, Repercussions-62 Million fine on tesco bank website-www.healthcare.gov

“Shopper Approved”- an ecommerce service based company that enables sites to gather local, merchant and product reviews, located in Ogden, Utah is cited as the latest scapegoat to in the hackers abattoir. Magecart attack was confirmed by “Shopper Approved” saying it first acknowledged about the potential incident from the security firm RISKIQ, on the 17th of September. "Fortunately, we were able to quickly detect and secure the code related to the incident. We also put additional security measures in place to help ensure that this doesn't happen again," Scott Brandley, CEO of Shopper Approved, says in a security alert on the company's website. "After a thorough investigation, we were able to determine that only a very small percentage of our clients were involved and we have already reached out to those clients directly in an effort to help them remediate any issues."

ATTACK TYPE
Ransomware Attack

CAUSE OF ISSUE
Targeted Attack

TYPE OF LOSS
Reputation

COUNTRY
USA

LOGISTICS-01

Cathay Pacific Breach Hits Over 9 Million Customers

Presented on oct 2018, Repercussions-9 million customers personal details exposed on Cathay Pacific Airways, website- www.cathaypacific.com

Airline Cathay pacific is the newest acclaimed brand to suffer a catastrophic data breach, after unleashing the startling fact that the data’s of 9.4 million passengers might be stolen.
On Wednesday the firm claimed that they figured out the unauthorized access to the IT systems sustaining a wide range of sensitive personal information, both for its customers as well of its business unit Hong Kong Dragon Airlines.The various personal data’s that got affected were passenger name, nationality, date of birth, phone number, email, address, passport number, Hong Kong identity card number, frequent flyer program membership number, customer service remarks and historic travel information.However, the number of expired card numbers were 403 and the number of credit card numbers with no of CVV exposed in the breach was 27. There’s no other info available on how the incident may have occurred, but the airline is atrophied by apathy and chilled in giving a reply by saying “there’s no evidence of data being misused at this point”. “We apologize for any tragic repercussions this data security event may cause our passengers. We responded instantly to contain the event, set up a thorough investigation with the assistance of a leading cybersecurity firm for further strengthening our IT security measures,” said CEO, Rupert Hogg.

ATTACK TYPE
Unauthorised Access

CAUSE OF ISSUE
Targeted Attack

TYPE OF LOSS
Reputation

COUNTRY
Hong Kong

Data Breach-01

Pocket iNet Leaves 73 GB of Sensitive Data Exposed

Presented on oct 2018, Repercussions-73 GB of Sensitive Data Exposed on pocket Inet,website-www.pocketinet.com

An internet provider from Washington state, Pocket iNet, kept an AWS S3 server exposed online without a password, according to the UpGuard. The UpGuard cyber-risk team brough forth that the exposed information included 73 gigabytes of downloadable data, which comprises of passwords and other sensitive files, ranging from the spreadsheets to pictures and diagrams.Upguard also discovered, expedited and reported the exposed bucket, named pinapp2, on October 11, 2018, though Pocket iNet was basically unable to confirm the exposure. After a week's time, according to an UpGuard blog post, the exposure was secure.The exposure was finally secured on October 19th, preventing the exploitation of this data from any future malicious activity."Not all of the contents were able to be downloaded, with the bucket itself being exposed. However, a folder named tech, which contained sensitive information, was downloadable within the bucket. Pocket iNet's AWS misconfiguration also exposed several lists of plain-text passwords to multiple devices and services that belong to its employees. Included in the list of plain-text passwords were firewalls, core routers, switches, servers and wireless access points.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Security Misconfiguration	Targeted Attack	Reputation	USA

DATA BREACH-02

Google Forced to Reveal Exposure of Private Data

Presented on oct 2018, Repercussions-Private data exposed .

A storming catastrophe was reported by google, "An API bug in Google+ exposed the personal details of about 500,000 accounts". Later it was believed that the stolen data weren't misused just like "Calm after Storm". Ben smith- A google guy and an engineering vice-president has said that the patched bug by google wasn't disclosed publicly fearing that it would be accorded to regulatory scrutiny and the organizations reputational hazard, due to the request on behalf of the privacy and data protection office perhaps being compelled to reveal after The Wall Street Journal on Monday. Especially in this era of heightened sensitivity over data leaks and increasing questions about whether massive technology firms that gather, store and sell personal data are being both proactive and transparent in how they handle and safeguard the data.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Security Misconfiguration	Lack of awareness	Reputation	USA

Data Breach-03

Water Utility Attacked

Presented on oct 2018, Repercussions-Malware affected the utility on www.wuc.bw.

News[WU1] of the online attack against West Haven follows Onslow Water and Sewer Authority in Jacksonville, North Carolina, reporting that it was hit by an attack that began on Oct. 4, when Emotet malware infected its systems. The authority is a public, non-profit entity that provides water and sewer services to the unincorporated areas of the county as well as most local municipalities, serving more a population of more than 100,000. Officials say the attackers appeared to deliberately target the authority with a two-stage attack after last month's Hurricane Florence. The systems in [WU1]West Haven were again hit by another malware called as E motet with the attack initiating on Oct 4th which was followed by the On slow water and the sewer authority in Jacksonville, North Carolina. The unincorporated areas of the county as well as most local municipalities are being provided with water and sewer services by an authority that is non-private and non-profit entity, helping a population of more than 100,000. The authority was deliberately targeted by the attackers with a two- stage attack after last month's Hurricane Florence, report officials.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Ransomware Attack	Targeted Attack	Reputation	USA

DATA BREACH-04

Deadly Malware That Attacked Saudi Industrial Plant Came From Russia

Presented on oct 2018, Repercussions-hacker attacked industrial plant .

Critical industrial systems were targeted by hackers through a Russian government link for a certainty of a nefarious cyberattack at a Saudi petrochemical plant which was a part of global operation to destroy computers. A blog post published on Tuesday, aroused a feeling of suspicion that they have supreme confidence that a Moscow government's indigenous research facility being built with some of the malware is used in the attack, which temporarily halted operations at the plant. FireEye researchers said that "During the attack, the malware triggered a safety system that terminated the operations. If this was prevented, the attackers would have set off a potentially deadly chain of events and government involvement"-said Hulquist.

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

DATA BREACH-05

US Voter Records for Sale on Hacker Forum

Presented on oct 2018, Repercussions-US voter records leaked for sale in Hackers Forum.

An unlawful offering of a batch of U.S voter registration records appeared for online sale from 20 states which highlights the lax controls often being induced to voter records.The sinful trading of data's via web forum was detected and reported by two security companies Anomali labs and Intel 471. The data's that are least protected are the ones that contain the sensitive personal information which if obtained at the wrong hands might really cause unimaginable mayhem's. Aetna Hit With More Penalties for two breaches."On Oct. 4, the Department of Defense identified a breach of personally identifiable information of DoD personnel which was identified by the department of defense on Oct 4th that required congressional notification. Lt. Col. Joseph Buccino, a Pentagon spokesman, tells Information Security Media Group,"The department is progressing to accumulate more information about the incident, which involves the possible compromise of personally identifiable information (PII) of DoD personnel, maintained by a single commercial vendor that facilitated travel management services to the department.

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Data Theft	Targeted Attack	Reputation	USA

DATA BREACH-06

Nasty Linux Kernel Vulnerability Discovered, Mandatory Kernel Update Required

Presented on oct 2018, Repercussions-US voter records leaked for sale in Hackers Forum.

Jann Horn, a cybersecurity researcher exposed the unfixed vulnerability in Linux version since 3.16 to 4.18 which was under the Project Zero program. Now known as CVE-2018-17182, it is a cache invalidation bug that affects the memory management Linux module. The attacker can gain root access in the Linux-based computer by successful exploitation. Horn said that "While the bug itself is in code that is reachable even from relatively strongly sandboxed contexts, this blogpost only describes a way to exploit it in environments that use Linux kernels that haven't been configured for increased security (specifically, Ubuntu 18.04 with kernel linux-image-4.15.0-34-generic at version 4.15.0-34.37). The underprivileged user, using CVE-2018-17182 can be altering of memory and creating of an artificial denial of service attack can be done by the underprivileged user using CVE-2018-17182. The exploit was described by Horn as "Consumes an hour to run before popping a root shell." Various distinct patched versions such as 4.18.9, 4.14.71, 4.9.128, and 4.4.157

ATTACK TYPE	CAUSE OF ISSUE	TYPE OF LOSS	COUNTRY
Data Theft	Targeted Attack	Reputation	USA

CONCLUSION

The above consolidated threatsploit report is an intensified work of Briskinfosec. It urges the people in each and every corner of this globe to understand the urge of needing a proper cyber security facility with all the security features contained in it for maintaining the company's reputation.

"Thinking about a new beginning in the past is of no use. But, we all should think about having a best security in the present for a glorious future".

Yearning for top notch security?

We will make it to happen!

REFERENCE LINK

- https://www.healthcare-informatics.com/news-item/cybersecurity/health-data-breach-healthcaregov-portal-impacts-75k-people
- https://www.moh.gov.sg/content/moh_web/home/pressRoom/pressRoomItemRelease/2018/singhealth-s-it-system-target-of-cyberattack.html
- https://www.healthcareitnews.com/news/update-misconfigured-database-breaches-thousands-medcall-advisors-patient-files
- https://www.hipaajournal.com/minnesota-dhs-21000-patients-phishing-attack/
- https://mattheneus-healthcare.com/2018/10/09/phishing-attack-breaches-insurance-data-of-37000-patients-for-1-month
- https://www.opsfolio.com/newscenter/3-phishing-hacks-breach-20000-catawba-valley-patient-records/
- https://www.ft.com/content/4517f4cc-c028-11e8-95b1-d36dfef1b89a
- https://www.bankinfosecurity.com/north-korean-hackers-tied-to-100-million-in-swift-fraud-a-11579
- https://www.next-it.net/bupa-fined-228000-after-stolen-data-surfaces-on-dark-web
- https://www.cnbc.com/2018/06/19/south-korea-crypto-exchange-bithumb-says-it-was-hacked-coins-stolen.html
- https://www.courant.com/breaking-news/hc-br-west-haven-cyber-attack-ransomware20181019-story.html
- https://www.hackbusters.com/news/stories/3859064-cryptocurrency-exchanges-lost-882-million-to-hackers
- http://hexanika.com/feed-items/magecart-card-stealing-gang-hits-shopper-approved-plug-in-2/
- https://www.itpro.co.uk/data-breaches/32212/cathay-pacific-data-breach-hits-94-million-customers
- https://latesthackingnews.com/2018/10/26/pocket-inet-isp-exposed-73gb-of-sensitive-data-on-misconfigured-s3-bucket/
- https://www.huffingtonpost.in/2018/10/09/google-exposed-the-data-of-500-000-google-plus-users-and-didn-t-disclose-this-for-months_a_23554882/
- https://www.thestate.com/news/business/national-business/article220064300.html
- https://www.washingtonpost.com/world/national-security/potentially-deadly-malware-used-in-saudi-industrial-hack-likely-came-from-russia-researchers-say/
- https://www.forbes.com/sites/leemathews/2018/10/16/millions-of-voter-records-are-for-sale-on-hacker-forums/#7bed63fc24a7

This adversary research report is proudly presented by

BRISKINFOSEC TECHNOLOGY AND CONSULTING PVT LTD

Feel free to reach us for all your cybersecurity needs
contact@briskinfosec.com | www.briskinfosec.com
|USA|INDIA|UK