THREATSPLOIT

ADVERSARY REPORT

JUNE 2019

EDITION 10

PREPARED BY

BRISK INFOSEC

CYBER TRUST & ASSURANCE

WWW.BRISKINFOSEC.COM

CERT-IN EMPANELLED CYBERSECURTY FIRM

INTRODUCTION

Welcome to the world of Threatsploit Adversary report which contains the global occurrence of the most significant and horrendous cyberattacks identified by Briskinfosec during the entire month of May 2019. This report evidently proves that in-spite of some strong security defenses used by organizations, they're still a victim to cyberattacks. Moreover, these cyberattacks absolutely show zero signs of reduction.

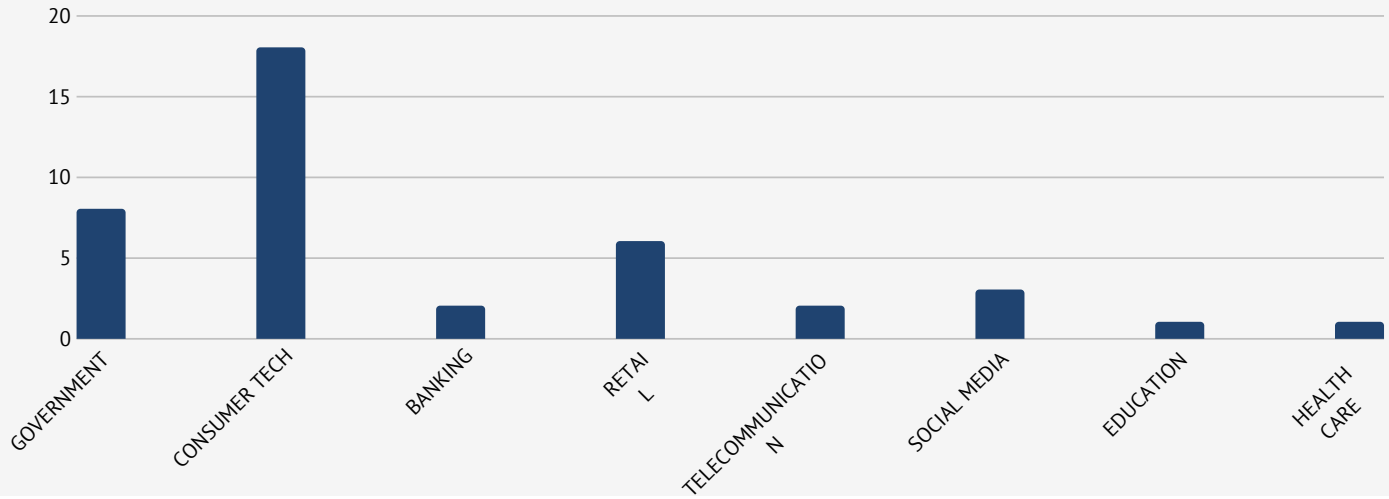
Over time, these attacks have evolved stronger and are more menacing, haunting and taunting security professionals, giving them nightmarish experiences. For instance, Apple's security is believed to be the earth's most formidable one, but itself was hacked. Similarly, there are many such eye-opening incidents in this report. Just read over to know it.

Many cyberattacks initiate from various sectors. But, a majority of them seemed to have originated from consumer technology sector, holding about 44%. To prevent these, it's evident that top-notch reliable security is mandatory.

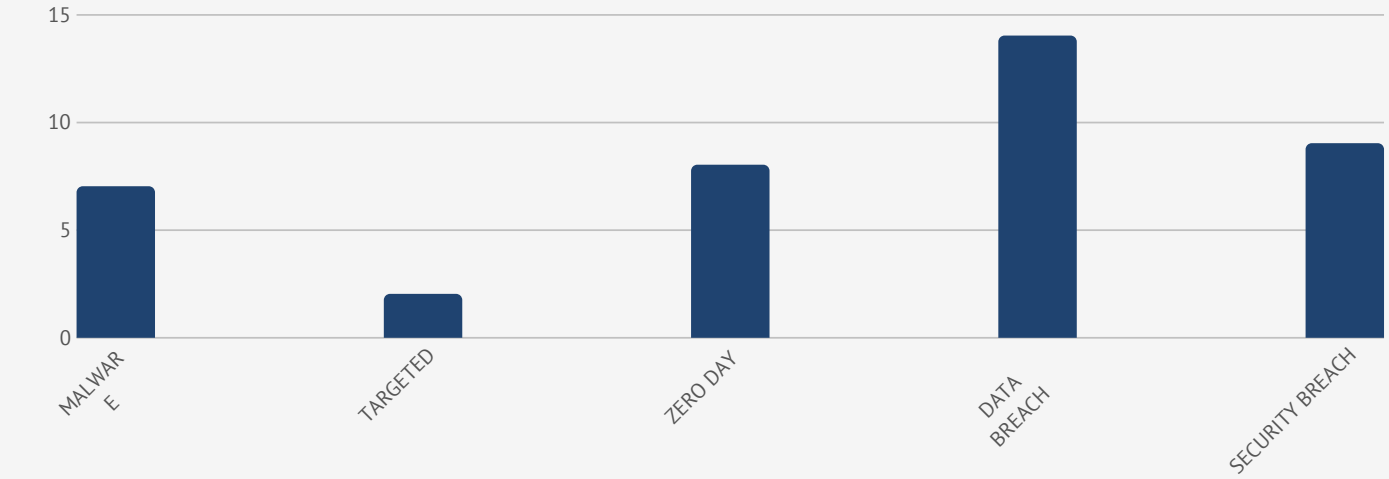
44%

Consumer Technology

SECTORS AFFECTED BY ATTACKS



TYPE OF ATTACKS



GOVERNMENT

- Delhi BJP's hacked website
- Massive Data Breach Exposes Russian Officials' Passports, Reports Say
- Andhra Pradesh agriculture ministry site exposed Aadhaar data of farmers
- Hackers breach US license plate scanning company
- Singapore Red Cross data breach
- British Transport Police website hacked
- Official website of TSSPDCL hacked
- Ransomware Cyberattacks Knock Baltimore's City Services Offline

CONSUMER TECHNOLOGY

- Joomla and WordPress Found Harboring Malicious Redirect Code
- Download Hijack Flaw Patched in Slack Patches for Windows
- White label SOS panic buttons can be hacked via SMS
- Australian tech unicorn Canva suffers security breach
- Wyzant online tutoring platform suffers data breach
- Crooks using hacked Microsoft email accounts to steal cryptocurrency
- Critical Remotely Exploitable Vulnerability Discovered in Oracle WebLogic Server
- Serious SQLite Remote Code Execution Vulnerability Discovered
- That WhatsApp bug exposes our vulnerability, too
- UC Browser for Android, Vulnerable to URL Spoofing Attacks
- MDS vulnerabilities lead Chrome OS 74 to disable hyper-threading
- Linksys Smart Wi-Fi Router Vulnerability Could Leak Sensitive Information To Hackers
- Thrangrycat flaw in millions of Cisco devices could enable 'Secure Boot' bypass
- Office 365 Accounts Compromised via ATO Attacks Used in BEC Scams
- Docker vulnerability could allow attackers to read-write on host–.patch in pipeline
- Teen hacked Apple twice hoping to get job but got caught by FBI and police

BANKING

- First American Financial Corp Leaked Hundreds of Millions of Title Insurance Records
- Software company Wolters Kluwer faced malware attack

RETAIL

- New Zealand's treasury website hacked Floyd's Coffee Shop
- Wi-Fi Passwords Hacked at Local Coffee Shop
- Airbnb user accounts allegedly hacked; previous bookings canceled and new bookings made
- Hackers accessed data from more than 460,000 accounts at Uniqlo's online store
- Have Three Major US Antivirus Companies Been Hacked?
- Hundreds of Orpak gas station systems can be easily hacked thanks to hardcoded passwords

TELECOMMUNICATION

- Econet Website Hacked
- TalkTalk data breach customer details found online

SOCIAL MEDIA

- Gigi Hadid's Twitter hacked, flooded with antisemitic content
- Account Hijacking Forum OGusers Hacked
- Instagram hacked leaving 49 MILLION exposed

EDUCATION

- Data breach at Augustana College

HEALTHCARE

- Auditor-General hacked into hospitals to expose online security flaws

GOVERNMENT

Delhi BJP's hacked website

Bharatiya Janata Party's Delhi wing website has been hacked. The hackers have replaced several pages of the website with Beef dishes recipes. Also, the party's history was altered as Beef History. However, other contents of the homepage remain unchanged. This hacking attack commenced when PM Modi and the new cabinet were taking oath at Rashtrapati Bhavan in New Delhi.

ATTACK TYPE
Security breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
INDIA

Massive Data Breach Exposes Russian Officials' Passports, Reports Say

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
UK

The passport data of 360,000 people, including those of former government officials, the deputy chairman of the state, former deputy prime minister and of many were posted online in a massive data leak, reports the RBC news website. The significant cause of this breach is cited as 'reluctance' towards security and being devoid of proper awareness towards it. The Russian government has imposed a fine of $1,150 dollar per individual, who've been identified guilty of the breach.

Andhra Pradesh agriculture ministry site exposed the Aadhaar data of farmers

French security researcher, Elliot Alderson, discovered the Aadhar numbers exposure of thousands of Andhra Pradesh farmers which comprised of their names, father's name, mobile numbers, village names, caste and much more. All these were accessible even through a simple online search. However, cybersecurity experts have said that proper awareness must be given to all people regarding such incidents.

ATTACK TYPE
Malware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Hackers breach US license plate scanning company

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

An intruder with the pseudo-name "Boris Bullet-Dodger", infiltrated the database of a license plate readers company for the U.S government. The hacker has leaked these information's in the dark web. The leaked information contained 65,000 file names comprising of local data, zip codes, government clients, dates, timestamps, image files, and other sensitive data. However, the company has notified about this breach to customers and an official investigation is going on.

CONSUMER TECHNOLOGY

Joomla and WordPress Found Harboring Malicious Redirect Code

The websites of Joomla and WordPress have been detected with a malicious script that redirects users towards a malicious site. Eugene Woznaik, a security researcher, identified a rogue hypertext access (.htaccess files) as the reason for this redirection. It is said that by planting corrupted index.php files, hackers were able to gain access and inject malicious redirects. However, this flaw was patched with the release of Apache 2.3.9 version.

ATTACK TYPE
Malware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

Download Hijack Flaw Patched in Slack Patches for Windows

ATTACK TYPE
Zero day

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Slack users are insisted to upgrade their applications to the latest version 3.4.0. This is due to a download hijack vulnerability discovered by Tenable security researcher David Wells in Slack Desktop version 3.3.7 that allowed intruders to alter the victim's file storage directory. This vulnerability has a CVSS rating of 5.5 (medium). However, this vulnerability was patched with the newly released version, 3.4.0.

White label SOS panic buttons can be hacked via SMS

A panic alarm kept for usage to at-least 10,000 senior people in UK can be remotely controlled by sending easy SMS queries, discovered the researchers at Fidus Information Security. As a remediation, Fidus said that using unique codes to be printed for making configuration changes would be good. Also, it had contacted suppliers to point out the device's risk which had resulted in some considering to recall them while others, jeopardized to respond.

ATTACK TYPE
Malware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
UK

Australian tech unicorn Canva suffers security breach

ATTACK TYPE
Data exposure

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
AUSTRALIA

A Sydney based company named, Canva, that provides graphic design service was hacked and nearly 139 million users were affected. The hacker behind this is identified with the pseudo name "GnosticPlayers." The deceived data were primarily customer usernames, real names, email addresses, city and country, google tokens, and much more. Finally, the exposed server was closed after Canva was acknowledged about this.

Wyzant online tutoring platform suffers data breach

The systems of Wyzant company has been detected with a data breach which compromised its user data that included Facebook profile information. The anonymous intruder was also able to gain access to few of the users Personally Identifiable Information (PII). The pilfered information may also encompass names, email addresses, ZIP codes and much more. However, the flaw has been finally patched with an investigation, still ongoing.

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Crooks using hacked Microsoft email accounts to steal cryptocurrency

ATTACK TYPE
Security breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Microsoft email accounts which were recently hijacked by cybercriminals are now used to steal cryptocurrency, reports Motherboard. One such victim, Jevon Ritmeester, claims to have lost more than one bitcoin with his account being compromised. Even Reddit users have claimed to have experienced the same thing. However, several victims have appealed to take legal action against Microsoft, warning them to compensate the financial losses.

Critical Remotely Exploitable Vulnerability Discovered in Oracle WebLogic Server

A security vulnerability, CVE-2019-2725, with a CVSS score of 9.3 out of 10 was discovered in Oracle's WebLogic Server (WLS). This flaw is highly exploited by many and is used to install ransomware, cryptocoin miners, and other hazardous software. To fix this issue, Oracle insists to apply the latest patch immediately. Apropos of that, blocking unwanted URL's and deleting WAR is highly recommended.

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Serious SQLite Remote Code Execution Vulnerability Discovered

ATTACK TYPE
Zero day

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
USA

A critical security flaw has been identified in SQLite by a security researcher, Cory Duplantis, from Cisco Talos, which if exploited could allow an intruder to execute remote code on the target system. This vulnerability has a CVE rating of 8.1 and a number CVE-2019-5018. However, this flaw was patched by the vendors with the release of a latest version 3.28.0.

That WhatsApp bug exposes our vulnerability, too

A horrendous vulnerability has been discovered in WhatsApp which could allow intruders to spy on the victim's data and ultimately compromise it. This vulnerability has been figured out as a Buffer Overflow vulnerability and is primarily said to damage the VOIP (Voice-Over-Internet-Protocol). No further details about this vulnerability is given. However, this vulnerability has been patched as of now.

ATTACK TYPE
Zero day

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

UC Browser for Android, Vulnerable to URL Spoofing Attacks

ATTACK TYPE
Zero day

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
CHINA

The newest versions of UC Browser and UC Browser Mini has exposed the data of over 600 million users leaving them susceptible to URL spoofing attacks, elucidates the security researcher Arif Khan, the first to find and report the flaw. Mr. Arif says, to avoid exposing users, the developers of these two apps should leave out UX "improvements" features and display the real domain in all cases, "if they can't write good regex or effectively secure this functionality."

MDS vulnerabilities lead Chrome OS 74 to disable hyper-threading

Microarchitectural Data Sampling (MDS) vulnerability, comprising of attacks like Fallout and Zombieload can be used to read sensitive data, website contents, passwords, credit card numbers, cookies and much more. However, this vulnerability was fixed after Google issued an update to chrome 74 OS and disabled Intel's Symmetric Multi-Threading (SMT). With Hyper-Threading disabled, Intel's CPU performance could be affected.

ATTACK TYPE
Zero day

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
USA

Linksys Smart Wi-Fi Router Vulnerability Could Leak Sensitive Information To Hackers

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
USA

Over 25,000 Linksys smart Wi-Fi routers are susceptible to the remote exploit of intruders, reports the security researcher of Bad Packets, Troy Mursch. Further analysis by him revealed that 25,617 routers were vulnerable with MAC addresses, device names, operating system types, WAN settings, firewall status, firmware settings, DDNS configurations. However, the vulnerability is still said to be active despite a patch being released by the company.

'Thrangrycat' flaw in millions of Cisco devices could enable 'Secure Boot' bypass

Countless Cisco devices used by corporates, governments, and military networks have been detected with a CVE-2019-1649 flaw in Secure Boot process which could allow unauthorized users to disable the critical functions of system. This vulnerability got a name as 'Thrangrycat', given by the researchers from Red Balloon. Ang Cui - founder and chief scientist of Red Balloon Security says, "Fixing this isn't easy. A firmware patch would help to a certain extent but isn't the complete cure."

ATTACK TYPE
Zero day

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
USA

Office 365 Accounts Compromised via ATO Attacks Used in BEC Scams

ATTACK TYPE
Security breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Office 365 accounts have been zeroed down and compromised by cybercriminals through Account Takeover (ATO) which cybercriminals in the future can leverage for other attack purposes, says Barracuda Networks. Attackers have used social engineering, phishing techniques and brute-force attacks to compromise Office 365 accounts. As a remediation measure, Barracuda suggests to use - 2FA, deploy ATO detection and protection solutions, and machine-learning based defense solutions.

Docker vulnerability could allow attackers to read-write on host – patch in pipeline

A new vulnerability in docker has been discovered by Aleksa Sarai, which could give intruders "arbitrary read-write access to the host filesystem with root privileges." With regards to this, he said that he has given his patches to the docker community and his disclosure was made with the adherence of docker's security system. However, Docker hasn't made any official statements yet.

ATTACK TYPE
Zero day

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
USA

Teen hacked Apple twice hoping to get a job but got caught by FBI and police

ATTACK TYPE
Security breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
USA

Apple has been hacked by a boy of 17, who did it with an intention of getting a job in there but instead became a victim of hacking charges. FBI discovered the incident and reported it to the Australian Federal Police (AFP). When investigated, the teen said that he did this only for a job but it ended up in a fiasco. However, the boy was found to be innocent and the magistrate didn't subject him to punishment.

IT services giant HCL left employee passwords, other sensitive data exposed online

HCL firm's data encompassing employee's data, customer details and passwords (in plain text) have been leaked publicly. This issue remained unacknowledged until UpGuard identified and brought it to their knowledge. They also identified various domains and subdomains that exposed company's records, amassing up to 364 and SAP codes of over 2800 employees. However, HCL analysts rectified this issue and said their data weren't any more visible publicly.

ATTACK TYPE
Malware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Google says it stored some G-Suite passwords in plain text for 14 years

ATTACK TYPE
Security breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

A bug on Google which had been furtively lurking in G-Suite for 14 years (since 2005) has been finally discovered on May 22nd 2019. This vulnerability (bug) in G-suite users has caused its user's passwords to remain in an unencrypted format. However, Google said that it has notified customers and reset passwords as precautionary measures. It also confirmed that there isn't any misuse on those exposed passwords and has apologized to all users.

First American Financial Corp Leaked Hundreds of Millions of Title Insurance Records

First American Financial, a real estate insurance company could've provided unauthorized access towards its customers financial information. According to The Wall Street Journal, the firm's application was identified with a flaw that was first detected by Brian Krebs, krebs security researcher. He said that the exposed information consisted of millions of bank account details, mortgage and tax record details, and other sensitive information. However, the company has hired a forensic company and has then blacklisted unknown users access.

ATTACK TYPE
Malware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Software company Wolters Kluwer faced malware attack

ATTACK TYPE
Malware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
NETHERLANDS

Wolters Kluwer, an accounting software company was hit by a dreadful cyberattack, terminating many services of the company. The attack has commenced on 7th May 2019 and has defaced the company's site for a very long time. After few days, Wolters Kluwer was able to restore its service to its products and is back online, finally.

New Zealand treasury website hacked Floyd's Coffee Shop

Hackers have somehow managed to infiltrate New Zealand's treasury website. Gabriel Makhlouf, Treasury's secretary, confirmed that an anonymous entity has made over 2000 attempts to compromise data, reports nzherald.co.nz. Forensic investigation is going on to identify whether the attempts originated from outside or inside the country. However, the convicts are speculated to be the country's opposition party, but they've denied it.

ATTACK TYPE
Security breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
NEW ZEALAND

Wi-Fi Passwords Hacked at Local Coffee Shop

Norton's Wi-Fi risk report says that 70% of hacking incidents commence when users connect to unsafe free Wi-Fi networks at restaurants, airports and coffee shops. Yes, one such coffee shop in Portland named Floyd coffee shop got its Wi-Fi network hacked. Intruders somehow got access to the Wi-Fi network in shop and have changed the passwords and gained access to the logged users in that network. Since then, Floyd coffee shop has strengthened its security defenses.

ATTACK TYPE
Targeted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

RETAIL

Airbnb user accounts allegedly hacked; previous bookings canceled and new bookings made

Thousands of Airbnb user accounts have been hacked and are being used for bookings, costing in thousands of dollars. Apropos of that, they've also been locked out of their accounts and are unable to reset their passwords. Few've even complained that their previous bookings have been annulled. As a remediation, every Airbnb user has been urged to look for any suspicious behavior in their accounts. If so, then they are insisted to report to the company ASAP.

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Hackers accessed data from more than 460,000 accounts at Uniqlo's online store

Fast Retailing, the Japanese firm behind Uniqlo retail chain, announced that more than 460,000 customers data on its online purchasing site was hacked on 10th May 2019, due to the illegitimate login of an unknown entity. Its said that customer names, addresses, contact details and credit card data were accessed. However, an investigation is being launched and the unknown intruder is to be found

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/data

COUNTRY
JAPAN

RETAIL

Have Three Major US Antivirus Companies Been Hacked?

New York based threat intelligence company – Advanced Intelligence LLC (AdvIntel) say that they have evidence of 3 US based antivirus companies being hacked by a Russian firm dubbed "Fxmsp", whom claim to be peddling their source codes, security plugins, and network access online for $300,000. After acknowledging this, the company had contacted the law enforcement. Still now, the names of those 3 companies remain unrevealed.

ATTACK TYPE
Security breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Hundreds of Orpak gas station systems can be easily hacked thanks to hardcoded passwords

ATTACK TYPE
Zero day

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
ISRAEL

Popular gas station Orpak's 'SiteOmat' systems have been detected with several security vulnerabilities, with simple skills enough to exploit them. The Cybersecurity and Infrastructure Security Agency (CISA), rated the vulnerability's severity as 9.8 out of 10. This software monitors the amount of fuel stored, it's temperature and pressure, and also processes the card payments. Most of the exposed systems are from U.S. However, CISA reported that this bug got fixed with the release of new software version – v6.4.414.139.

TELECOMMUNICATION

Econet Website Hacked

Econet company's official website was hacked after its product microsite was pulled and delinked from its homepage, whose content was still accessible everywhere online. This indicated that when someone searched for Econet on the internet, the delinked URL would still appear on Google searches, taking them to old unsecured microsite on the website. However, the company has rectified this issue by cleaning up the old indexes.

ATTACK TYPE
Malware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
SOUTH AFRICA

TalkTalk data breach customer details found online

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/data

COUNTRY
UK

An investigation confirmed that TalkTalk has failed in informing about the 2015 mega breach to nearly 4,545 customers, whose personal information has been compromised. Apropos of that, customer names, addresses, email addresses, dates of birth, customer numbers and mobile numbers have also been exposed online. However, the company has conveyed its sincere apologies and has sent notification to all the victims about the breach.

Gigi Hadid's Twitter hacked, flooded with antisemitic content

The twitter account of a 24 year old female model, Gigi Hadid, was hacked on Friday and was lashed by a series of racist and antisemitic remarks on her profile. This model enjoys a humongous fanbase of 9 million followers. However, her twitter account regained normality after 30 minutes, since the breach incident and Hadid thanked all her followers for supporting her.

ATTACK TYPE
Targeted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

SOCIAL MEDIA

Account Hijacking Forum OGusers Hacked

Ogusers[.]com – a well-known forum meant for hijacking online accounts and conducting SIM swapping attacks on the victim's phone itself was hacked on 12th May 2019, exposing the email addresses, hashed passwords, IP addresses, private messages and much more of over 113,000 users. Users after acknowledging their data breach, slammed this forum administrator nicknamed as ACE. However, its enchanting to see such bad guys getting a taste of their own activities.

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

Instagram hacked leaving 49 MILLION exposed

A humongous database hosted by Amazon web services, exposed the private data of millions of Instagram influencers, celebrities and of many. The cause of this breach is said to be the phones and email addresses of users that's left unprotected with passwords, indicating that anyone could espy the contents. This database has been left exposed for a couple of hours and a spokesperson has said, "The company is working intensely to resolve this issue ASAP."

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

EDUCATION

Data breach at Augustana College

One of the colleges in rock island, Augustana college, has been detected with a cyberattack after one of its server was identified with an unauthorized access. All college members have been notified to remain cautious as their social security members and dates of birth have been pilfered in this attack. The attack is identified as a ransomware. The director of public relations and social media, Mr. Ashleigh Johnston, says that more colleges are becoming a victim of ransomware and Augustana is just one among them.

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

HEALTHCARE

Auditor-General hacked into hospitals to expose online security flaws

The IT systems of one of the familiar hospitals in Victoria has been hacked by its auditor-general, Andrew Greaves, during an audit, who was then able to access many sensitive data of patients. This incident has brought into lights, the fragile security conditions that's prevailing among Victoria's health service providers. The major cause of this is identified to be the staff's, whom were easily susceptible to social engineering attacks. Mr. Greaves says, "All these health services need more focus on their data protection."

ATTACK TYPE

Security breach

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation/Data

COUNTRY

AUSTRALIA

REFERENCES

- https://www.nationalheraldindia.com/india/latest-news-breaking-news-live-updates-30th-may
- https://www.themoscowtimes.c/om2019/05/15/massive-data-breach-exposes-russian-officials-passports-reports-a65596
- https://tech.economictimes.indiatimes.com/news/internet/andhra-pradesh-agriculture-ministry-site-exposed-aadhaar-data-of-farmers/69545991
- https://www.scmagazine.com/home/security-news/data-breach/license-plate-reader-firm-breached-data-leaked/
- https://www.ibtimes.sg/after-singhealth-singapore-red-cross-data-breach-this-time-leaves-4000-people-affected-30860
- https://www.bbc.com/news/uk-england-48281494
- https://www.informationsecuritybuzz.com/expert-comments/british-transport-polices-website-has-been-hacked/
- https://www.thehansindia.com/news/cities/hyderabad/official-website-of-tsspdcl-hacked-526225
- https://www.npr.org/2019/05/21/725118702/ransomware-cyberattacks-on-baltimore-put-city-services-offline
- https://threatpost.com/joomla-and-wordpress-malicious-redirect-code/145068/
- https://www.infosecurity-magazine.com/news/download-hijack-flaw-patched-in/
- https://nakedsecurity.sophos.com/2019/05/14/white-label-sos-panic-buttons-can-be-hacked-via-sms/
- https://www.bleepingcomputer.com/news/security/office-365-accounts-compromised-via-ato-attacks-used-in-bec-scams/
- https://devclass.com/2019/05/29/docker-vulnerability-could-allow-attackers-to-read-write-on-host-patch-in-pipeline/
- https://www.zdnet.com/article/australian-tech-unicorn-canva-suffers-security-breach/
- https://mobilesyrup.com/2019/05/27/teenager-hacked-apple-to-get-job/
- https://www.zdnet.com/article/wyzant-online-tutoring-platform-suffers-data-breach/
- https://nakedsecurity.sophos.com/2019/05/01/criminals-used-hacked-microsoft-email-accounts-to-pilfer-cryptocurrency/
- https://www.infoq.com/news/2019/05/critical-remote-vuln-weblogic/
- https://latesthackingnews.com/2019/05/14/serious-sqlite-remote-code-execution-vulnerability-discovered/
- https://www.khaleejtimes.com/editorials-columns/that-whatsapp-bug-exposes-our-vulnerability-too-
- https://www.bleepingcomputer.com/news/security/uc-browser-for-android-vulnerable-to-url-spoofing-attacks/
- https://www.techrepublic.com/article/mds-vulnerabilities-lead-chrome-os-74-to-disable-hyper-threading/
- https://www.zdnet.com/article/over-2500-smart-linksys-routers-may-leak-owners-sensitive-data/
- https://www.scmagazine.com/home/security-news/thrangrycat-flaw-in-millions-of-cisco-devices-could-enable-secure-boot-bypass/
- https://www.pymnts.com/news/security-and-risk/2019/first-american-financial-consumer-data-breach/
- https://www.cnbc.com/2019/05/26/wolters-kluwer-baltimore-ransomware-attacks-have-big-ripple-effects.html
- https://www.business-standard.com/article/news-ians/new-zealand-treasury-website-hacked-on-eve-of-budget-119052900554_1.html
- https://cyberoregon.com/2019/05/22/wi-fi-passwords-hacked-at-local-coffee-shop-cybersecurity-expert-offers-tips/
- https://cyware.com/news/airbnb-user-accounts-allegedly-hacked-previous-bookings-canceled-and-new-bookings-made-04e3fe87
- https://www.cbronline.com/news/antivirus-companies-hacked
- https://techcrunch.com/2019/05/02/orpak-gas-station-password/
- https://www.techzim.co.zw/2019/05/press-release-our-website-is-safe-and-secure-econet/
- https://www.theinquirer.net/inquirer/news/3076181/talktalk-failed-to-inform-4-500-customers-about-2015-mega-breach
- https://www.dailydot.com/upstream/gigi-hadid-twitter-hacked/
- https://krebsonsecurity.com/2019/05/account-hijacking-forum-ogusers-hacked/
- https://www.cornwalllive.com/news/uk-world-news/instagram-hacked-leaving-49-million-2890179

CONCLUSION

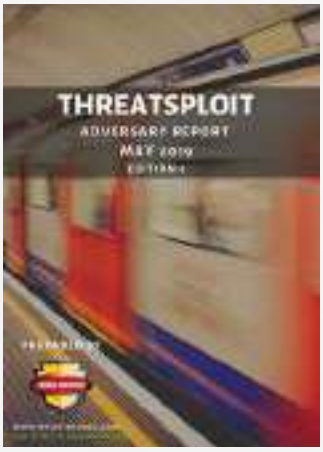
Everyone yearns for redemption after being hit by breaches. In a pursuit of that, they tend to increase the quality of their security defenses and hire top security professionals to keep their security environment secure. Apropos of that, they purchase top security tools, spend lavishly towards it, hoping automation would yield them absolute salvation against cyberthreats. All these are fine but above all, there is something that's more important. It's about cautioning us, humans.

Apart from the significance bestowed towards security tools, proper awareness towards employees must also be given. The reason is for almost many cyber attacks, there's at least a semi-cure. But for social engineering and phishing attacks, there's no other cure than proper human awareness. Staffs/employees should be educated about the types of calls and methods, intruders would use to deceive and exploit information from them. Ultimately, they should be trained in such a way that they remain secure on any occurrence of social engineering persuasions.

There's a saying, "The weakest link in cyberchain are humans." Hence, if they're made resilient, then they can face the worse of cyberattacks with a sense of hope.

You may ask, why worse? Well, the worst is yet to come!

YOU MAY BE INTERESTED ON OUR PREVIOUS WORKS



REFERENCES ABOUT BRISKINFOSEC

CASE STUDIES

SOLUTIONS

SERVICES

RESEARCH

COMPLIANCES

BLOGS

FEEL FREE TO REACH US FOR ALL YOUR CYBERSECURITY NEEDS

CONTACT@BRISKINFOSEC.COM | WWW.BRISKINFOSEC.COM