THREATSPLOIT

ADVERSARY REPORT

MAY 2019

EDITION 9

PREPARED BY

BRISK INFOSEC

CYBER TRUST & ASSURANCE

WWW.BRISKINFOSEC.COM

NOW, A CERT-IN EMPANELLED FIRM

INTRODUCTION

Before thriving into the world of Threatsploit, Briskinfosec, takes this opportunity to wish all the readers, a belated happy "International Workers' Day".

Can you count the droplets of water pouring from the upper atmosphere as rain?
Can you count the number of stars twinkling in the sky?

Obviously, the answer is No. Of course, it would be great if you were able to, but the immeasurable quantity makes it impossible to be done by a normal human being. Similarly, the amount of cyberattacks cropping up in various parts of the cosmos seems too much to be kept a note of. Hence, we took up that challenge and have collected the most notorious and significant global cyberattacks that've occurred in the month of May 2019.

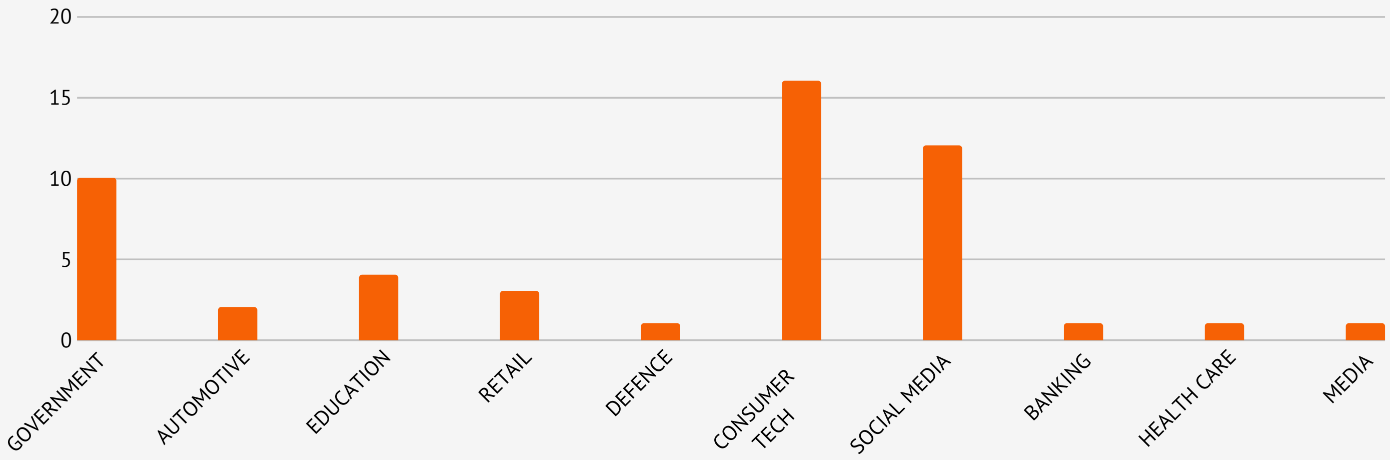
During this process, we've figured out an increase in the number of cyberattacks when compared to previous months. All these attack breakouts were gathered from Russia, India, China, U.S.A, Japan, China, and much more. Moreover, even the most complex security problems faced by companies are explained in a lucid manner that you'll understand at ease.

Many cyberattacks initiate from various sectors. But, a majority of them seemed to have originated from consumer technology sector, holding about 32%. To prevent these, it's evident that top-notch reliable security is mandatory.

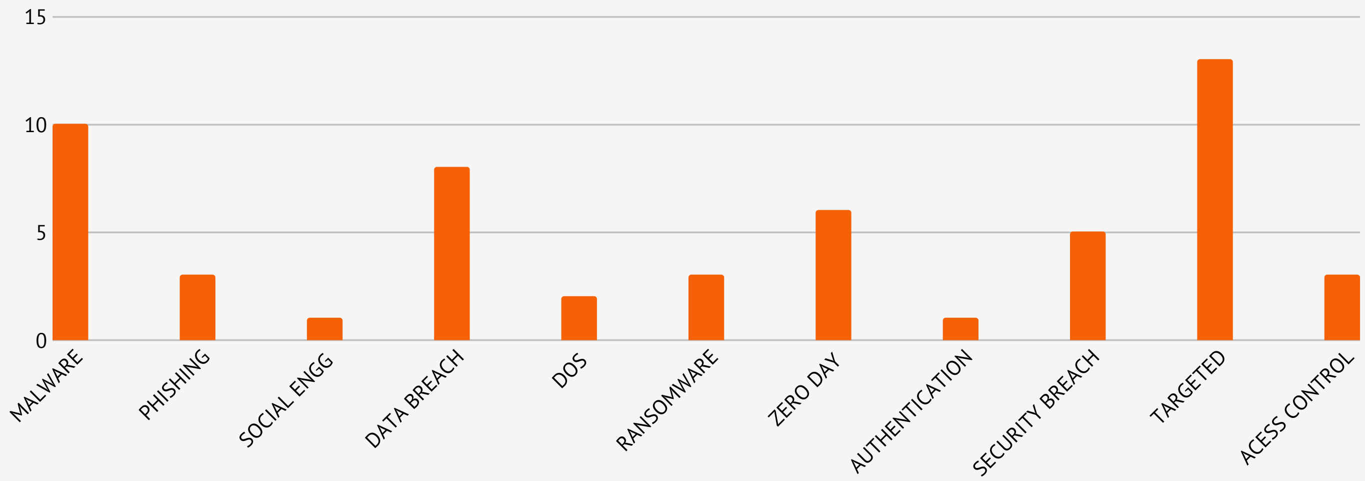
32%

Consumer Technology

SECTORS AFFECTED BY ATTACKS



TYPE OF ATTACKS



GOVERNMENT

- Russian hackers are targeting European embassies, according to report
- Malware-packing Chinese lady who hacked her way into Trump's Florida Mar-a-Lago now faces federal charges
- Ryuk malware hacked a county government website. It's been down for 6 days
- Massive American presidential election hack confirmed
- Hacker Exposes Confidential Files, Correspondence from Mexican Embassy in Guatemala
- Website of PetroBangla gets hacked twice within 2 Days
- Former Likud minister Gideon Sa'ar's phone hacked — report
- Hacker group posts hundreds of law officer records
- DoS attack against election results portal under investigation in Finland
- Toyota and Lexus Dealerships Hacked, Millions Left Vulnerable

AUTOMOTIVE

- Hackers Steal More Than 100 Mercedes-Benz Cars in Chicago by Hacking Car2Go Car-Sharing App
- Tesla Autopilot 'Hacked'

EDUCATION

- Matsya University's website gets hacked
- ExtremismJammu varsity website hacked after Kerala students 'beaten up, called beef eaters'
- Georgia Tech Data Breach Leaves 1.3M Exposed
- Security breach shuts down network for Woodruff Arts Center, High Museum

RETAIL

- Bodybuilding.com discloses security breach
- Hungry Hackers Use McDonald's App to Steal $1,500 in Fast Food
- Chipotle customers say their accounts are being hacked

DEFENCE

- AFP database hacked, missions of 20,000 personnel exposed

CONSUMER TECHNOLOGY

- Microsoft Finds Backdoor in Huawei Laptops That Could Give Hackers Access
- Zero-day XML External Entity (XXE) Injection Vulnerability in Internet Explorer Can Let Attackers Steal Files, System Info
- These Developers Hacked Knuckles & Vive Controllers to Play MIDI
- Hacked Lime scooters play offensive voice messages
- Mailgun hacked part of massive attack on WordPress sites
- JustDial data breach puts over 100 million users' personal information at risk
- Docker Hub hack exposed data of 190,000 users

- Oracle Patches 3-Year-Old Java Deserialization Flaw in April Update
- Beware! Google Chrome address bar can reportedly be used to launch a phishing attack
- Kaspersky Labs Discovers 'Previously Unknown Vulnerability' in Microsoft Windows
- Dragonblood vulnerabilities found in WPA3 WiFi authentication standard
- Qualcomm Patches Critical Security Flaw That Affects 46 Chipsets, but Millions of Devices Still Vulnerable
- Patched Apache flaw is a serious threat for web hosting providers
- Xiaomi devices came with vulnerability baked into its pre-installed security app
- Wipro data breach, Nasscom monitoring cyber threats to IT industry
- A Weather Channel knocked off air by 'malicious software attack'

SOCIAL MEDIA

- Official Fortnite Twitter account has been hacked
- France's 'Secure' Telegram Replacement Hacked in an Hour
- Bachelor' alum Amanda Stanton said a hacker leaked nude photos
- Trevor Lawrence's Instagram Has Been Hacked
- Hackers demand that Soulja Boy pays to get his Instagram back
- WWE Star Lana's Snapchat Reportedly Hacked With Sex Tape
- Justin Fields, Jake Fromm's Instagram accounts hacked
- Over 540 million Facebook records found on exposed AWS servers
- French Footballer Kylian Mbappe's Twitter Hacked, Asks for Bitcoin (BTC)
- Dr DisRespect Twitter and Twitch Channels Were Hacked Today
- Swedish Social Democrats' Twitter account hacked
- Facebook now says millions of Instagram passwords were stored in plain text

BANKING

- City of Tallahassee direct deposit payroll system hacked; attack marks second hack in a month

HEALTH CARE

- Hackers Can Use DICOM Bug to Hide Malware in Medical Images

MEDIA

- 2 Million Credit Cards Exposed After Hack of Buca di Beppo, Planet Hollywood and Others

Russian hackers are targeting European embassies, according to report

Many European embassies and government officials fell into the phishing trap of hackers by inadvertently clicking the malicious link which appeared to be from official United States department document, says a new report from Check Point Research. Once the link was clicked, the intruders seized control of the system by activating an installed software termed as 'TeamViewer', a popular remote access service.

ATTACK TYPE
Phishing

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Malware-packing Chinese lady who hacked her way into Trump's Florida Mar-a-Lago now faces federal charges

ATTACK TYPE
Social engineering

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Yujing Zhang, a 32 year old Chinese woman, hacked her way into Donald Trump’s private club, Mar-A-Lago, and deceived the secret service agents through social engineering techniques. The insider agents believed that she would be a daughter of a member, but doubts aroused when she told to the receptionist that she is here to attend an evening meeting today. However, the bitter truth was no such meeting was scheduled on this evening. She eventually stumbled and started to blabber. Evidently, then she got caught and was convicted to federal charges.

Ryuk malware hacked a county government website. It's been down for 6 days

The imperial county government website in El Centro has been down for six days. According to The Times, a ransomware named as ‘Ryuk’ had infiltrated the network systems and demands ransom in bitcoin to seek manumission. Forensic investigation is going on to figure out the attack’s origin. Further, staff members are using Gmail accounts and other communicating mediums to caution public about this threat.

ATTACK TYPE
Malware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Massive American presidential election hack confirmed

ATTACK TYPE
Authentication

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Berkeley high school in California conducted its very first student election council. Not e-voting software, but emails were used by students for submitting their votes. Around 2400 students have casted their votes and all of them seem to have appeared from a single computer. Yes! Here’s where suspicion aroused and it was later detected that 2 students have somehow gained access to the database and were the reason behind this incident.

Hacker Exposes Confidential Files, Correspondence from Mexican Embassy in Guatemala

After expressing grievance over the ignorance shown by the Mexican officials despite showcasing all their sensitive document leakage through bug bounty efforts, the hacker, identified as @0x55, decided to spill all these data trove publicly over the internet. The data trove with over 5000 confidential documents contained information about the Mexican embassy people in Guatemala like their visa data, credit cards, personal information, and much more. This hack's cause was due to a vulnerable server in Guatemala.

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

ATTACK TYPE
Targeted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
BANGLADESH

Website of PetroBangla gets hacked twice within 2 Days

On April 7th 2019, the oil, gas, and mineral corporation of Bangladesh's official website named PetroBangla, was hacked. The suspects identified themselves 'N33LOB33'. Tariqul Islam Khan, the public relation wing manager of PetroBangla, told that the server was shut down after the website hack. Around 9.30 AM, the website became normal. However, 7 hours and 30 minutes post that, the website got hacked again.

Former Likud minister Gideon Sa'ar's phone hacked

Gideon Sa'ar, senior Likud party member, got his cell phone hacked, reports the kan public broadcaster on an April Sunday. Also, the mobile of Blue and White party leader, Benny Gantz, was hacked. Sources regarding who hacked the phone and who's behind it remain mysterious. Gantz has said that the primary connotation behind this hack was politically driven.

ATTACK TYPE
Malware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
ISRAEL

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Hacker group posts hundreds of law officer records

On a Saturday dawn of 2019 April, an anonymous hacker group have posted the personal information of over 1400 police officers, federal agents, employees of FBI, secret service specialists, and sheriff's from North Carolina and Florida. The FBI national academy associates have cited 3 affected culprits to have used a malicious 3rd party software, and they're believed to be the cause for this breach. However, the federals confirmed that the database is safe.

GOVERNMENT

DoS attack against election results portal under investigation in Finland

This time, the election result portal of Finland has been struck by a DOS attack. This attack has disrupted the election portal services, says Arto Jaaskelainen, the head of electoral administration at the Ministry of Justice. However, the National Bureau of Investigation confirms that the election results would face null problems as the attack wasn't on casting or counting of votes. Till now, the question of "who are the actual suspects", remains still mysterious and unfigured.

ATTACK TYPE
DoS

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
FINLAND

Toyota and Lexus Dealerships Hacked, Millions Left Vulnerable

About 3.1 million items of Toyota and Lexus customer data have been breached due an attack on leadership in Japan. An unauthorized access has struck the network on 21st March, but was tragically identified only after a month (someday in April). Toyota announced that the names, birth dates, and customers data could've been compromised but not the credit card details. Toyota told that they are going to launch an investigation on this ASAP.

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
JAPAN

AUTOMOTIVE

Hackers Steal More Than 100 Mercedes-Benz Cars in Chicago by Hacking Car2Go Car-Sharing App

Car2Go, alias, Share Now (BMW and Daimler-backed car sharing program) recently got hacked and is missing nearly 100 to 200 high end sophisticated cars, says CBS Chicago reporter, Brad Edwards. All the hijacked cars were recently recovered by the Chicago police department. Police have suspected around 12 people as the possible culprits involved in this heist.

ATTACK TYPE
Security breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Tesla Autopilot 'Hacked'

Keen Lab, a cybersecurity research firm told to a research paper on Saturday that they've successfully gained the steering control of an Autopilot (self-driving) Tesla car. Repeated attempts were made to perplex and blur the path of Autopilot. With regards to Keen's findings, Tesla said that they weren't representing real world issues and hence, there isn't any necessity to worry about it. Also, a representative from Tesla told, "Keen's findings are loftily appreciated but wouldn't yield him any bounty".

ATTACK TYPE
Access control

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
USA

Matsya University's website gets hacked

The website of Matsya University in Rajasthan has been hacked on a Tuesday morning. A hacker group called as "Black Scorpions" had told that they're the ones as the reason for this hack. The hackers are believed to be from Pakistan. They've posted a message in the main page telling "Pakistan Zindabad". Further, they've also posted, "The atrocities against minorities must be stopped and Kashmiris must be given proper rights".

ATTACK TYPE
Targeted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
INDIA

Extremism Jammu varsity website hacked after Kerala students 'beaten up, called beef eaters'

ATTACK TYPE
Targeted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
INDIA

The website of varsity was hacked by a group called as "Kerala Cyber Warriors", after two Kerala students were allegedly beaten up in the central university of Jammu, reports the Indian Express. This incident commenced on April 15th and the two were beaten on the grounds for eating beef, obviously getting labelled as "traitors". Kerala Cyber Warriors seem to have hacked the website in order to seek justice for those two Kerala victims whom were mercilessly mauled by those "ABVP-RSS" activists in Jammu.

Georgia Tech Data Breach Leaves 1.3M Exposed

The personal information of about 1.3 million people from The Georgia Institute of Technology comprising of students, staffs, students applicants and many more have been compromised on 14th April 2019, confirms the institute. The cause of this behemoth disaster is cited to be the usage of an unsecured database which was accessed by an external entity. The Institute's cybersecurity team conducted an intense research on this issue. However, this vulnerability was finally patched but the hacker is unknown.

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Security breach shuts down the network for Woodruff Arts Center, High Museum

ATTACK TYPE
Security breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
ATLANDA

A malicious third party has affected the networks of Woodruff Arts center and has crippled the center's operation and systems. Apropos of that, The Alliance Theatre, The Atlanta Symphony Orchestra, and the High Museum of Art were also affected by the breach. There wasn't any risk on personal and financial data. The center upon acknowledging this incident, instantly initiated measures along with a forensic firm to secure the systems and also in enhancing the security measures.

Bodybuilding.com discloses security breach

India's largest online store, Bodybuilding.com, got all its IT systems crippled due to a security breach, caused due to 'clicking the phishing' link by its employees on July 2018. The hackers accessed the company's network in February 2019. Neither, the staff of that company nor the forensic veterans are sure about customers data manipulation. However, the company has alerted people over this issue and has cautioned them to be aware of such.

ATTACK TYPE
Phishing

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
INDIA

RETAIL

ATTACK TYPE
Malware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

Hungry Hackers Use McDonald's App to Steal $1,500 in Fast Food

On one morning, Patrick O' Rourke, decided to drink coffee just like everyone else. Instead of travelling distances, he decided to order through McDonald's app, coffee with two sugar and two milk. All of a shock, he nearly found about $2000 CAD to be defrauded from his bank account. After a quick google search, he figured out that many Canadians including him, have suffered from such similar issues of deceptive transactions, in Montreal. However, the hack is speculated to have happened, due to fragile password usage.

Chipotle customers say their accounts are being hacked

Chitpotle's most loyal customers have been victims to cyberattacks, over a week. Burrito fans have said on twitter that they've been seeing strange deeds ongoing in their accounts. According to reports on Reddit and Twitter, hackers compromised credit card information and illicitly ordered and procured free foods. As a response to all these incidents, the company's representative announced through a mail that "They're toiling hard to sort out this threat ASAP".

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

DEFENSE

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
PHILIPPINES

AFP database hacked, missions of 20,000 personnel exposed

A local hacker group has successfully breached the database of the Armed Forces of Philippines (AFP) and have exposed the personal information, missions, absent records and much more of over 20,000 personnel's. All these data were procured during a mission of three day international hacking. The hackers have been identified as Pinoy LulzSec group, and they've also compromised the database of technological university of Philippines.

Microsoft Finds Backdoor in Huawei Laptops That Could Give Hackers Access

A backdoor vulnerability in the kernel (core of OS) of certain Huawei laptop models (Matebook) which gave access to unprivileged users for seizing data was finally identified, announced the researchers at Microsoft. This vulnerability was a resemblance to a malware, DoublePulsar. Microsoft instantly reported this issue to Huawei, and Huawei issued patches on April 9th. But, due to this black mark, many countries revealed that they wouldn't use Huawei Network devices as they were petrified due to security concerns.

ATTACK TYPE
Malware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
CHINA

ATTACK TYPE
Zero day

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Zero-day XML External Entity (XXE) Injection Vulnerability in Internet Explorer Can Let Attackers Steal Files, System Info

A Zero-day extensible MarkUp Language (XML) external entity injection vulnerability (XXE) in Microsoft's Internet Explorer was recently discovered, says the security researcher, John Page. For this vulnerability to be exploited, a malicious XML file must be inflicted into the user's HTML (Hyper Text Transfer Protocol) server. If exploited, the perpetrator can gain foothold on the victims data. John Page had reported this issue to Microsoft and they haven't released any patches yet.

These Developers Hacked Knuckles & Vive Controllers to Play MIDI

With regards to the future VR headsets, some dexterous developers had spent some time to launch Valve Index Controllers and MIDI files. In 2016, developer Brian Lindenhof, first built a VR controller using built-in haptic actuators. Lindenhof is known for his work on Climbey, the VR climbing game that pits you against difficult obstacles courses.

ATTACK TYPE
Security breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

ATTACK TYPE
Access control

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
USA

Hacked Lime scooters play offensive voice messages

Around 8 Lime company's electric scooters have been stolen from the streets of Brisbane after thugs changed the audio files on scooters to display profane sayings. Mr. Nelson Savanh, Lime's Queensland public affairs manager said that extensive work is going to see if any other scooters are pilfered. The company is anxiously awaiting for the verdict from Brisbane City Council regarding the scooter trial.

Mailgun hacked part of massive attack on WordPress sites

Mailgun WordPress, a popular email automation and email delivery site has been breached on 10th April 2019 by some indistinct online weasels. There is a vulnerable area in many WordPress called as Yuzo-related posts, containing XSS (Cross site scripting). It is mostly through this loophole, intruders are gaining access to the systems. At this moment, there's a constant attack persuasion on all websites, using this WordPress platform.

ATTACK TYPE
Malware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
INDIA

JustDial data breach puts over 100 million users' personal information at risk

A recent cyber breach in Just Dial Company has exposed the sensitive data of over 100 million users which contained information about their names, email addresses, mobile numbers, date of birth and much more. This data breach was first discovered by Rajshekhar Rajaharia, who stated that 70% of data belonged to users whom had accessed Just Dial's customer care number "88888-88888". Nevertheless, the company is still unable to fix this issue despite being notified by Rajshekhar.

Docker Hub hack exposed data of 190,000 users

On 25th April 2019, Docker hub, the official repository for Docker container images has confirmed a security breach incident had happened with the data of over 190,000 being left exposed. Reports suggest that the hacker could've accessed Docker hub's user names, hashed passwords, GitHub and Bitbucket account logins, and much more. The company has alerted the users about this and as a pivotal part of remediation, has urged users to reset passwords and to review their GitHub and Bitbucket accounts.

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

ATTACK TYPE
Access control

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
USA

Oracle Patches 3-Year-Old Java Deserialization Flaw in April Update

During the quarter of 2019, precisely on 17th April 2019, a critical patch update was launched by Oracle which fixed almost 297 vulnerabilities across its software portfolio. However, there was a deserialization Java flaw that had been secretly lurking in 19 products of Oracle. This vulnerability was successfully patched in the recently released update. Security veterans continue to emphasize on the mandatory fact that both old and new flaws must be immediately patched.

Beware! Google Chrome address bar can reportedly be used to launch a phishing attack

An ardent developer, James Fisher, discovered a vulnerability in Chrome's address bar that could land them in a fake site and exploit their data. When Android users use chrome in mobile and as they scroll downwards, the URL bar vanishes. Intruders can use this vulnerability to display a fake URL address bar named "Inception bar". Also, this attack can blind you from seeing the original address bar when scrolled up. To detect this fake address bar, lock the phone and then unlock it. The real address bar will appear over the unreal one.

ATTACK TYPE
Malware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Kaspersky Labs Discovers 'Previously Unknown Vulnerability' in Microsoft Windows

ATTACK TYPE
Zero day

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

An unknown vulnerability in Microsoft windows which was successfully exploited by an anonymous hacker group was detected by Kaspersky labs. The hackers installed a backdoor through an essential element of Windows OS and primarily targeted to seize the system's Kernel (core of the system). This isn't the first but fifth time a vulnerability in windows has been detected in recent months. Just like a silver line amidst dark clouds, the vulnerability got finally patched on 10th April 2019.

Dragonblood vulnerabilities found in WPA3 WiFi authentication standard

WiFi alliance's WiFi WPA3 security and authentication standard was identified with Dragonblood vulnerabilities. Thoughts could arouse, what's there to worry about?
Well, Dragonblood vulnerabilities comprise of 5 vulnerabilities like DoS vulnerability, two downgrade vulnerabilities, and two side channel information leaks. If these get exploited, could allow intruders to tamper the WiFi network passwords as well compromise the encrypted network traffic. The company insists to update software's to thwart such attacks

ATTACK TYPE
Zero day

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

Qualcomm Patches Critical Security Flaw That Affects 46 Chipsets, but Millions of Devices Still Vulnerable

ATTACK TYPE
Zero day

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
USA

A security bug (CVE-2018-11976) that could give attackers root access to devices has been identified in Qualcomm's chipsets. This flaw was discovered by Keegan Ryan. It is identified that this flaw affects 46 Qualcomm chipsets which are lately being used in many smartphones, tablets, laptops, and smartphones. Qualcomm classified this vulnerability as critical. Finally, this bug was later patched.

CONSUMER TECHNOLOGY

Patched Apache flaw is a serious threat for web hosting providers

Organizations using Apache web servers are insisted to implement the recent security update, in order to fix a privilege escalation flaw (CVE-2019-0211) which could permit unprivileged web host users to execute code with root privileges. In more simple words, could yield the complete access about the system to the intruder. This vulnerability was discovered by a security researcher, Charles Fol, and it is said to affect the HTTP apache server on Unix systems.

ATTACK TYPE
Zero day

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

ATTACK TYPE
Zero day

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
CHINA

Xiaomi devices came with vulnerability baked into its pre-installed security app

One of the largest Chinese mobile company, Xiaomi (3rd in the world) was recently identified with a vulnerability in its pre-installed apps, unveils the Israel cybersecurity researchers from Check Point Software technologies. The app named as Guard provider was initially meant to prevent malicious activities, instead, exposed the users to attacks. Due to this insecured nature, the intruders could attempt many attacks. However, Check Point reported this to Xiaomi and it has been successfully fixed, confirmed the Israelite firm.

Wipro data breach, Nasscom monitoring cyber threats to IT industry

A recent phishing attack has crippled the IT systems of Wipro and almost a dozen of clients have been affected, says investigative journalist Brian krebs. Not just Wipro, even Infosys, Cognizant, and Capgemini have been affected, says Nasscom. With regards to this, Wipro said to CNBC-TV18 "We've detected an abnormal activity in our network and since then, we've been working with multiple security partners to resolve this issue".

ATTACK TYPE
Phishing

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
INDIA

TELECOMMUNICATION

ATTACK TYPE
Malware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
USA

A Weather Channel knocked off air by 'malicious software attack'

A weather channel network has been crippled due to a malicious attack on its software, says anchor, Jim Cantore. The network's morning show "AMHQ", which must kick-start at 6 A.M wasn't telecasted. Instead, it went on air at 7:39 A.M and at 7:43 A.M, the anchors announced the reasons for this inconvenience. The network head said that the federal law enforcement is seriously investigating about this issue.

Official Fortnite Twitter account has been hacked

On 3rd April 2019, the official twitter of Fortnite got hacked and epic games hasn't released a single note about this. The cause for this hack points towards a suspicious employee of the same community. This hack happened despite the patch being already released for a fixed vulnerability. Countless number of interesting tweets started brewing, since the hack, and the site leaking the tweets is said to be 'Tweetdeck'. The hacker is suspected to be a 'Call of Duty' player, and stringent action will be taken when the culprit gets caught, says epic games.

ATTACK TYPE
Targeted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

France's 'Secure' Telegram Replacement Hacked in an Hour

ATTACK TYPE
Targeted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
FRANCE

French government recently launched a messaging app called as Tchap, citing it to be more secure than telegram. However, French security researcher Elliot Alderson, alias Robert Baptiste, downloaded this app from google play store and identified an email validation error, through which an intruder could access to messaging groups. The patch to fix this vulnerability was issued around 13:00 CET. Baptiste says, this attempt looks similar to that of Patanjali whom launched kimbho app as a better one over WhatsApp, which later proved as a security nightmare.

Bachelor' alum Amanda Stanton said a hacker leaked nude photos

Amanda Stanton, a woman from film limelight, said that she was the latest victim to an online privacy breach as her nude photo after her recent breast implantation has been leaked on the internet. Stanton has informed about this entire saga to her fans. Further, she also notified the forensic officials about this hack incident.

ATTACK TYPE
Security breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Trevor Lawrence's Instagram Has Been Hacked

ATTACK TYPE
Targeted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
USA

Another familiar college athlete, Trevor Lawrence, fell as the recent prey to cyberattacks. Yes, his Instagram account has been hacked. He isn't the first one to be affected by online privacy as Jake Fromm from Georgia and Justin fields from Ohio have also been affected in the earlier 2019, due to similar online privacy. Fortunately, Lawrence was able to regain his account control after two hours.

Hackers demand that Soulja Boy pays to get his Instagram back

The Instagram account of a popular rapper named Soulja Boy, with whopping followers of more than 5.9 million, has been hacked on 15th April 2019. The anonymous hacker is identified as a female who has appeared on the rapper's livestream and demanded a colossal payment of over $1000 in order to regain the normal state of his Instagram account. Nevertheless, someone from his team has come forth to handle and resolve this issue.

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

WWE Star Lana's Snapchat Reportedly Hacked With Sex Tape

ATTACK TYPE
Targeted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
FRANCE

An unidentified hacker has targeted and hacked the snapchat account of a woman from WWE (World Wrestling Entertainment) named Lana. Apropos of this, the hacker has also released a sex video of this 34 year old WWE woman. Also, the short video of her was deleted after being showed up on "SmackDown Live". However, sources close to her say that the woman in that sex video wasn't her at all.

Justin Fields, Jake Fromm's Instagram accounts hacked

Ohio state quarterback Justin Fields and Jake Fromm of Georgia got their personal Instagram accounts hacked. Three messages within five hours were posted all of a sudden, and made them acknowledge the online threat. Fromm has an avid fan following of over 3 lakhs and Fromm over 1.5 lakhs. Most significantly, both have been targeted on the same day. This issue is reported to the Ohio's state offence and they've started the investigation.

ATTACK TYPE
Security breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Over 540 million Facebook records found on exposed AWS servers

ATTACK TYPE
Targeted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
USA

Two third party companies have collected over 540 million Facebook records from two Amazon cloud servers, finds data breach hunters. The first server (AWS), containing over 146 GB data belonged to a Mexico based online media platform while the second AWS server stored 22,000 passwords and much more. The first server obviously had more quantity of exposed data than the second, and hence consumed more time to secure it.

French Footballer Kylian Mbappe's Twitter Hacked, Asks for Bitcoin (BTC)

Another well-known football celebrity named Kylian Mbappe's has fallen as a prey to social media piracy. Yes, the international French football player's twitter account was hacked on 10th April 2019. The hacker demanded a ransom of 200 Euro in Bitcoin and this was asked through direct message.

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
FRANCE

Dr DisRespect Twitter and Twitch Channels Were Hacked Today

ATTACK TYPE
Targeted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

One of the most popular content writer named, "Dr Disrespect", got his Twitter channel and Twitch account hacked on 16th April 2019. This famous gaming personality enjoys a massive fan base following. After hackers gained access to his twitter account, they altered the channel's name to 'scrimakagrahamclark' and posted indistinct and obscene contents on the page. However, the twitter account became normal after a few days. But, the hacker still remains unidentified.

Swedish Social Democrats' Twitter account hacked

On 15th April 2019, a Monday dawn, the official twitter account of Sweden's ruling social democratic party account got hacked. About 20 false posts have cropped up and few among them were like "Steven lofven, the PM, would resign his job", "Cannabis has been legalized" and "Bitcoin has replaced Sweden's official currency". The hack posts have also abused Muslims with words "One like equals one dead Muslim". Somehow, the party was able to regain their account control, but the mastermind behind this hack still remains unidentified.

ATTACK TYPE
Targeted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
SWEDEN

Facebook now says millions of Instagram passwords were stored in plain text

ATTACK TYPE
Targeted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
USA

Millions of passwords of Instagram users were stored in plain text and hackers could've possibly compromised the security of these accounts, reveals the report on Krebson Security. With regards to this, earlier Facebook announced that only tens of thousand's user accounts have been tampered. But, now agrees that over millions of user data have been compromised. The cause for this security outbreak is cited to be the usage of weak database. As a caution, Facebook has started alerting customers about this issue.

BANKING

City of Tallahassee direct deposit payroll system hacked; attack marks second hack in a month

200 employees of Tallahassee city didn't get their paychecks as they were subjected to a cyberattack that disrupted the direct deposits. Law enforcement and technology staffs were working to contain the situation. Alison Faris, the spokeswomen said, "People are working hard to retrieve back the pay checks". This isn't the first but second time the city of Tallahassee has become a victim to cyberattacks.

ATTACK TYPE

Malware

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation/Data

COUNTRY

USA

HEALTHCARE

Hackers Can Use DICOM Bug to Hide Malware in Medical Images

Markel Picado Ortiz, a cybersecurity engineer, discovered on 18th April 2019, a vulnerability in the DICOM image format. It was a 30 year old standard used to exchange and accumulate the medical images. It was through this flaw, hackers have been planting malicious codes and corrupting the patient's data. Ortiz explained that through this, other malware and multi-stage attacks can also be launched. However to execute this, attackers must have valid directory credentials or permissions. Remediation work is being done to sort out this issue.

ATTACK TYPE

Malware

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation/Data

COUNTRY

USA

MEDIA

2 Million Credit Cards Exposed After Hack of Buca di Beppo, Planet Hollywood and Others

From May 23rd 2018 to March 18th 2019, somewhere in between this timeline, a hacking incident has commenced that compromised the credit cards of nearly 2 million users of a restaurant company called as Earl Enterprises. Forensic investigation reveals that the attack was identified as a malware which was successfully installed on the point-of-sale systems. Customers can check the online tool at Earl Enterprises and figure out if they've been hacked. However, the company announced that they're working hard to resolve this issue.

ATTACK TYPE

Targeted

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation/Data

COUNTRY

SWEDEN

REFERENCES

- https://www.business-standard.com/article/news-ians/russian-hackers-targeting-european-embassies-report-119042300478_1.html
- https://boingboing.net/2019/04/03/malware-packing-chinese-lady-w.html
- https://www.latimes.com/local/lanow/la-me-imperial-county-website-down-20190418-story.html
- https://www.forbes.com/sites/leemathews/2019/04/14/even-student-council-elections-are-being-hacked-now/#53f27aef5b98
- https://www.spamfighter.com/News-22160-Website-of-PetroBangla-gets-hacked-twice-within-2-Days.html
- https://securityboulevard.com/2019/04/hacker-exposes-confidential-files-correspondence-from-mexican-embassy-in-guatemala
- https://www.timesofisrael.com/former-likud-minister-gideon-saars-phone-hacked-report/
- https://www.nbcnews.com/tech/security/hacker-group-posts-hundreds-law-officer-records-n994231
- http://www.helsinkitimes.fi/finland/finland-news/domestic/16333-dos-attack-against-election-results-portal-under-investigation-in-finland.html
- https://www.thedrive.com/news/27524/over-100-mercedes-benz-vehicles-stolen-following-criminal-hack-of-car-sharing-app-report
- https://securitytoday.com/articles/2019/04/02/toyota-and-lexus-dealerships-hacked-millions-left-vulnerable.aspx
- https://www.sciencealert.com/experiment-steers-tesla-autopilot-into-oncoming-traffic-with-just-3-stickers-on-the-road
- https://www.timesnownews.com/india/article/alwar-raj-rishi-bhartrihari-matsya-university-website-hacked-black-scorpians-pakistan-zindabad-alwar-university-news-rajasthan-news/393281
- https://freepresskashmir.com/2019/04/17/jammu-varsity-website-hacked-after-kerala-students-beaten-up-called-beef-eaters/
- https://www.pymnts.com/news/security-and-risk/2019/georgia-tech-data-breach-personal-info/
- https://www.wsbtv.com/news/local/atlanta/security-breach-shuts-down-network-for-woodruff-arts-center-high-museum/943823423
- https://filipinotimes.net/news/2019/04/03/afp-database-hacked-missions-20000-personnel-exposed/
- https://www.today.com/food/chipotle-has-been-receiving-dozens-hacker-complaints-t152535
- https://mobilesyrup.com/2019/04/23/mcdonalds-mobile-app-defrauded-2000-dollars/
- https://www.zdnet.com/article/bodybuilding-com-discloses-security-breach/
- https://gadgets.ndtv.com/laptops/news/huawei-matebook-pcmanager-security-flaw-nsa-microsoft-defender-2017801
- https://www.cso.com.au/vendor_blog/2/trendlabs-malware-blog/21925/zero-day-xml-external-entity-xxe-injectionvulnerability-in-internet-explorer-can-let-attackers-steal-files-system-info/
- https://www.roadtovr.com/developers-hacked-knuckles-vive-controllers-play-midi-file-music/
- https://www.brisbanetimes.com.au/national/queensland/hacked-lime-scooters-play-offensive-voice-messages-20190423-p51ghx.html
- https://koddos.net/blog/hacked-mailgun-wordpress-site-falls-under-hackers-attack/
- https://www.grahamcluley.com/docker-security-breach-exposes-data-of-190000-users/
- https://www.timesnownews.com/technology-science/article/justdial-data-breach-puts-over-100-million-users-personal-information-at-risk-all-details-here/402785
- https://www.eweek.com/security/oracle-patches-3-year-old-java-deserialization-flaw-in-april-update
- https://www.usatoday.com/story/money/2019/04/29/google-chrome-address-bar-flaw-can-used-launch-phishing-attacks/3614140002/
- https://www.infosecurity-magazine.com/news/kaspersky-labs-discovers-unknown/
- https://medium.com/cyber-journal/dragonblood-vulnerabilities-found-in-wpa3-wifi-authentication-standard-cc32ca00b2e5
- https://gadgets.ndtv.com/mobiles/news/qualcomm-chipsets-critical-security-flaw-patched-android-april-2019-update-2029115
- https://www.helpnetsecurity.com/2019/04/03/apache-web-server-cve-2019-0211/
- https://www.timesofisrael.com/check-point-researchers-find-security-breach-in-xiaomi-phone-app/
- https://www.cnbctv18.com/information-technology/in-the-wake-of-wipro-data-breach-nasscom-monitoring-cyber-threats-to-it-industry-3035901.htm
- https://fortniteintel.com/official-fortnite-twitter-account-has-been-hacked/15266/
- https://threatpost.com/frances-secure-telegram-messaging-hacked/144010/
- https://www.thisisinsider.com/bachelor-amanda-stanton-said-a-hacker-leaked-nude-photos-2019-4
- https://campussports.net/2019/04/04/trevor-lawrences-instagram-has-been-hacked/
- https://revolt.tv/stories/2019/04/16/soulja-boy-instagram-hacked-0700ca17ae
- https://www.totalprosports.com/2019/04/18/wwe-star-lanas-snapchat-reportedly-hacked-with-sex-tape-pics-video/
- Justin Fields, Jake Fromm's Instagram accounts hacked
- https://www.zdnet.com/article/over-540-million-facebook-records-found-on-exposed-aws-servers/
- https://beincrypto.com/french-footballer-kylian-mbappes-twitter-hacked-asks-for-bitcoin-btc/
- https://www.twingalaxies.com/feed_details.php/5018/dr-disrespect-twitter-and-twitch-channels-were-hacked-today/6
- https://www.bbc.com/news/world-europe-47935251
- https://indianexpress.com/article/technology/social/facebook-now-says-million-of-instagram-passwords-were-stored-in-plain-text-5683490/
- https://gizmodo.com/2-million-credit-cards-exposed-after-hack-of-buca-di-be-1833710618
- https://hitinfrastructure.com/news/dicom-standard-flaw-could-compromise-medical-device-security

CONCLUSION

May 2019 was another baffling and defying month to both cybersecurity organizations and professionals. The above security breach reports provides ample evidence that the need to adapt towards more effective and contemporary security devices/services is always a mandatory one.

Apropos of that, Briskinfosec recommends certain necessities to maintain firm security defences. They are:

1. Proper user awareness
2. Scrutinized assets management
3. Competent Vulnerability and Patch management services
4. Two-Factor Authentication
5. Implementation and usage of strong passwords
6. Have a secure vision beyond the threats of Malware
7. Reach out a competent cybersecurity firm – Briskinfosec!

REFERENCES ABOUT BRISKINFOSEC

CASE STUDIES

SOLUTIONS

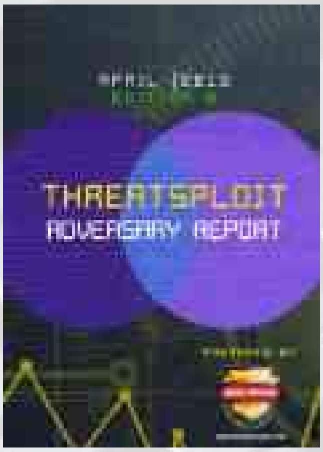
SERVICES

RESEARCH

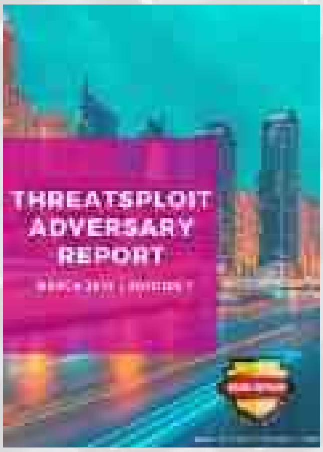
COMPLIANCES

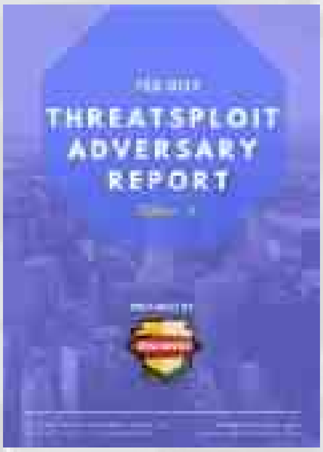
BLOGS

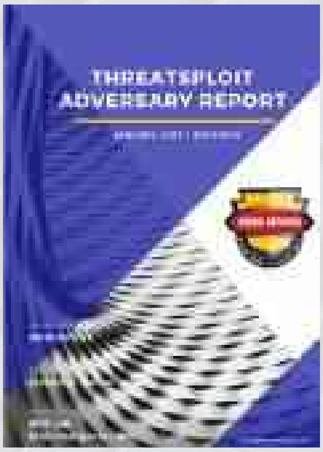
YOU MAY BE INTERESTED ON OUR PREVIOUS WORKS


APRIL 2019

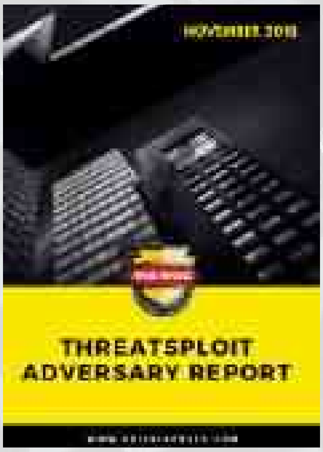
THREATSPLOIT ADVERSARY REPORT


THREATSPLOIT ADVERSARY REPORT


THREATSPLOIT ADVERSARY REPORT


THREATSPLOIT ADVERSARY REPORT

THREATSPLOIT ADVERSARY REPORT


NOVEMBER 2018

THREATSPLOIT ADVERSARY REPORT

THREATSPLOIT ADVERSARY REPORT FOR SEP 2018

AUG 2018

THREATSPLOIT ADVERSARY REPORT

“WE EXIST HERE TO ELIMINATE THE CYBER THREATS RATHER THAN TO JUST PARTICIPATE IN THE BATTLE AGAINST THEM.”

BRISK INFOSEC

CYBER TRUST & ASSURANCE

WWW.BRISKINFOSEC.COM