EDITION 14

THREATSPLOIT

ADVERSARY REPORT

OCTOBER 2019

AFFILIATED BY

NCDRC (NATIONAL CYBER DEFENCE RESEARCH CENTRE)
IN COLLABORATION WITH BINT LABS

www.ncdrc.res.in

PREPARED BY

BRISK INFOSEC

www.briskinfosec.com

NOW, A CERT-IN EMPANELLED FIRM

HAPPY CYBER SECURITY AWARENESS MONTH

Our Special Thanks to
Digi Safe Nations (DSN)

www.briskinfosec.com

INTRODUCTION

COMPROMISED - Earlier, this was a word that was considered positive during instances of a fight. For example, when two fought, one would compromise at some point of time which would pacify the other and sooner or later, both would become good to each other forgiving the rift that existed between them. But now, the word "compromise" has become the most petrifying word, especially in information security sector. Every day, we as a cybersecurity organization come across the word 'Compromised' very often, with disasters and losses accompanying it. Glimpsing at a few instances,

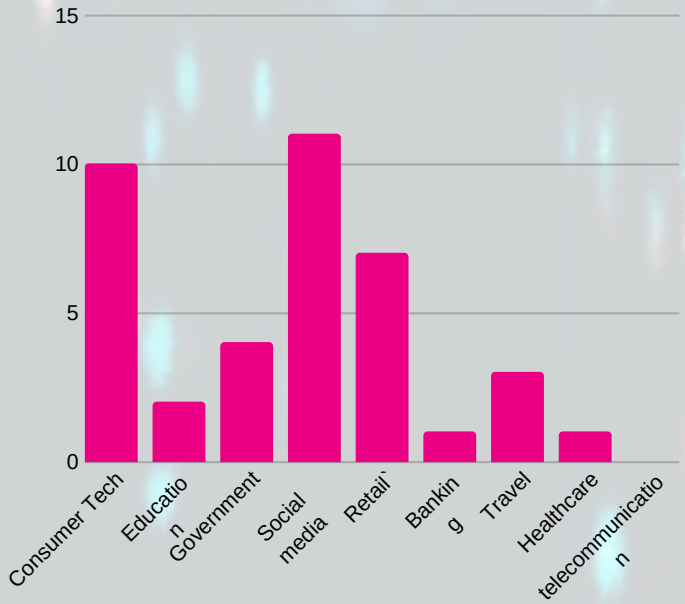
- **Deloitte**, One of the world's greatest accountancy firm, got millions of its customers data **compromised**.
- **Tesco** bank in USA got 2.93 million records of its customers breached and **compromised.**
- "**Capital one**" - A globally renowned bank got millions of its customers data **compromised**, becoming the biggest data breach in the banking history.
- **Just Dial** got the personal information of over 100 million users **compromised** due to a data breach.
- **Canva**, a popular Australian designing software company got 139 million users data **compromised**.
- **Instagram** exposed the private data of over 49 million customers and they were **compromised**.
- Last month, **Bulgaria** faced the biggest data breach in its history, resulting in the 5.1 million data of its citizens being **compromised**.
- On this month, **Ecuador** faced a historic data breach with 20+ citizen's data being **compromised**.

To know more on this month's worldwide cyber attacks and its impacts, just check over.

STATISTICS

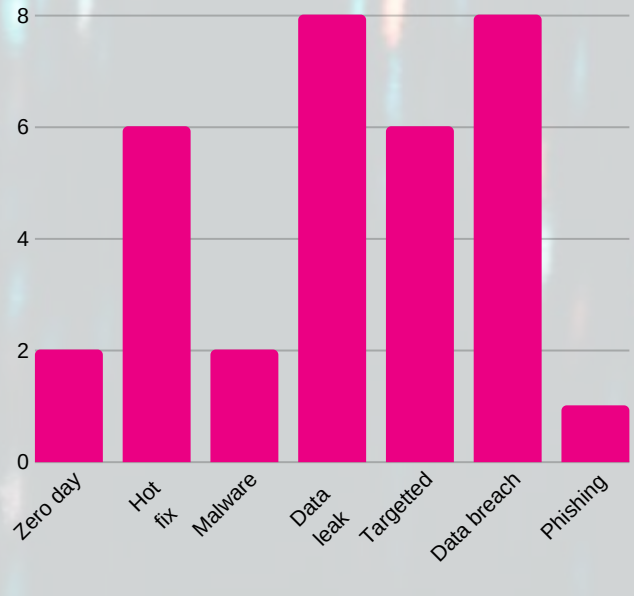
SECTORS AFFECTED BY ATTACKS

Below, there's Bar-chart that shows the percentage of distinctive sectors that've fallen as victims to the horrendous cyber threats. From it, it's evident that the Consumer Technology and social media has been hit the most.



TYPES OF ATTACK VECTORS

Below, there's a Bar-chart that indicates the percentage of nefarious cyber attacks that have broken the security mechanisms of distinct organizations.



1 Consumer Technology

- Researcher Drops phpMyAdmin Zero-Day Affecting All Versions.
- A major flaw in iOS 13.
- Microsoft Updates Patch 4 Critical Flaws In Windows RDP Client.
- Multiple Vulnerabilities in D-Link, Comba Routers, Warns Trustwave.
- Google removes two Chrome ad blocker extensions caught 'cookie stuffing'.
- Misconfigured Google Calendars leaking private information of thousands of users.
- Facebook Patches "Memory Disclosure Using JPEG Images" Flaws in HHVM Servers.
- Flaws discovered in popular router and NAS brands.
- Flaws in Over Half a Million GPS Trackers Expose Children Location Data.
- Update Google Chrome Browser to Patch New Critical Security Flaws.

2 Education

- DeLand High's Twitter really 'hacked?'
- Criminal investigation launched following college cyber attack.

3 Government

- This is undeniably the biggest data breach in Ecuador's history.
- Radio Pakistan's official website hacked.
- Taiwan People's Party website hacked in cyberattack.
- Palm Bay residents warned after utility bill pay portal hacked.

4 Social media

- WhatsApp 'Delete for Everyone' Doesn't Delete Media Files Sent to iPhone User.
- Several YouTube channels 'hacked', attackers breach data.
- Finance Minister's Facebook ID hacked.
- Stewie's Steam account hacked during CSGO Berlin Major playoffs.
- Magecart card-skimming attack hit hotel chains across 14 countries.
- Mattress Company Leaks Data Records of 387K Customers.
- Data Leak Hits 2.5 Million Customers of Cosmetics Giant Yves Rocher.
- Flight booking site Option Way exposed personal info on customers.
- Thermostat at 90 and a mysterious voice: Smart house hacked in Wis.
- Hacked Seattle road sign says 'Impeach the Bastard'.
- MongoDB server leaks 11 million user records from e-marketing service.

5 Retail

- Magecart card-skimming attack hit hotel chains across 14 countries
- Mattress Company Leaks Data Records of 387K Customers
- Data Leak Hits 2.5 Million Customers of Cosmetics Giant Yves Rocher
- Flight booking site Option Way exposed personal info on customers
- Thermostat at 90 and a mysterious voice: Smart house hacked in Wisconsin
- Hacked Seattle road sign says 'Impeach the Bastard'
- MongoDB server leaks 11 million user records from e-marketing service

6 Banking

- Scotiabank exposed source code and credentials on GitHub repositories

7 Travel

- Has Bolt Nigeria (Taxify) Been Hacked? Bolt Says No But Users Are Panicking After Strange Multiple Debits
- City of Ames parking ticket payment website hacked
- Malindo Air says data leak caused by ex-staffers at contractor firm

8 Healthcare

- Carle Foundation Hospital fell victim to a data breach

9 Telecommunication

- A Massive 1.7 Terabytes of Russian Telco Information Was Exposed

Researcher Drops phpMyAdmin Zero-Day Affecting All Versions

ATTACK TYPE
Zero day

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

phpMyAdmin is a free and open source administration tool that's used to manage CMS. Of late, a security researcher and tester, Manual Garcia, identified a vulnerability (CVE-2019-12922) in it. This medium rated vulnerability is said to be a part of CSRF (Cross Site Request Forgery) alias XSRF. This vulnerability deceives users into executing malicious actions and makes them delete their phpMyAdmin databases. As a remedy, Garcia suggests to "implement in each call, the validation of token variable" and also to check before clicking links.

A major flaw in iOS 13

ATTACK TYPE
Hot fix

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
GLOBAL

If you're an Apple user with iOS 13 version in it, then ensure you don't give your phone to anyone else. This is because of a flaw in it which allows hackers to bypass Apple's faceID and then gain access into the phone and compromise it. Ironically, this flaw was already reported to Apple in July by Jose Rodriguez, a security enthusiast, but Apple never took this seriously despite Jose showcasing POC's and giving clear analysis on this issue. This made Jose to leak this issue in public. After becoming public, Apple then decided to patch this and release a secured updated version 13.1. However, if Jose hadn't leaked this publicly, Apple wouldn't have taken this seriously either.

Microsoft Updates Patch for 4 Critical Flaws In Windows RDP Client

ATTACK TYPE
Hot fix

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
GLOBAL

Microsoft has newly released a patch update for September 2019. The update patched 79 security vulnerabilities. Amongst those, 61 were rated as important vulnerability, 17 were rated as critical vulnerability and one as moderate vulnerability. These patched vulnerabilities include RDP vulnerabilities, privilege escalation flaws and Remote Code Execution (RCE). Users are urged to update to the latest security patches ASAP, if they want to stay away from these vulnerabilities.

Multiple Vulnerabilities in D-Link, Comba Routers, Warns Trustwave

ATTACK TYPE
Hot fix

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
GLOBAL

Trustwave security researcher, Simon kenin, discovered 5 serious credentials exposing security flaws, 2 in D-Link routers and 3 in Comba routers. The critical vulnerabilities in these routers were so dangerous which could easily allow 3rd parties to compromise the user credentials. With regards to this, Simon had reached out both these companies and urged them to patch this issue ASAP. After repeated reach outs, D-Link patched it whereas Comba routers haven't patched yet.

Google removes two Chrome ad blocker extensions caught 'cookie stuffing'

ATTACK TYPE
Malware

CAUSE OF ISSUE
Security Misconfiguration

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

Google has removed two adblocker extensions from its Web store. What they are? Well, the first one is 'Adblock' that's offered by Adblock.Inc while the other is 'uBlock' that's offered by Charlie lee. Why were they removed? Well, these two adblockers tried to deceive users by impersonating as other reputable adblockers. They were also identified to have done cookie stuffing (a technique for gaining more data about user through extensions). Who discovered this? It's Andrey Meshkov, Co-founder and CTO of AdGuard found out the malicious activities in these.

Misconfigured Google Calendars leaking private information of thousands of users

ATTACK TYPE
Data leak

CAUSE OF ISSUE
Security misconfiguration

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

Recently, there's a talk that Google Calendar has been leaking massive private information of users. When a calendar invitation is sent to a user, a pop-up notification appears. The threat actors can perceive this and craft a malicious link and send it. Those links can redirect them towards a place, where financial and other critical credentials can be stolen. Initially, Google misjudged about this as a scam but now has started to look over this seriously.

Facebook Patches "Memory Disclosure Using JPEG Images" Flaws in HHVM Servers

ATTACK TYPE
Hot fix

CAUSE OF ISSUE
Security flaws

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Two high severity vulnerabilities (CVE-2019-11925 and CVE-2019-11926) were identified in Facebook that could give attackers remote access or launch DOS attacks. These can be done by just uploading a malicious JPEG file. These two vulnerabilities in FB were said to be residing in HHVM (Hip Hop Virtual Machine) – a open source virtual machine for executing programs written in PHP and hack programming languages. These vulnerabilities affect all versions, from 3.30.9 to 4.20.1. However, FB had patched this issue by releasing the latest version and users are urged to update to it, for staying away from these threats.

Flaws discovered in popular router and NAS brands

ATTACK TYPE
Zero day

CAUSE OF ISSUE
Security flaws

TYPE OF LOSS
Reputation

COUNTRY
GLOBAL

Security researchers have discovered 125 classified security vulnerabilities in 13 different routers that have the capacity to affect millions of users. It's said that each of these routers have at least one web application vulnerability in each, which when remotely exploited could give admin access of the users to the perpetrators. The vulnerabilities in these are many, ranging from injection attacks to Buffer overflow. This serious issue was reported to the respected companies. Few took this and started amendment measures while few haven't even responded yet.

CONSUMER TECHNOLOGY

Flaws in Over Half a Million GPS Trackers Expose Children Location Data

ATTACK TYPE
Data leak

CAUSE OF ISSUE
Development flaws

TYPE OF LOSS
Reputation/Data

COUNTRY
CHINA

29 different models GPS trackers from the Chinese company Shenzhen i365 have been discovered with serious security vulnerabilities. About 600,000 GPS tracking devices were found to expose user's details. It's said that the vulnerabilities were in the cloud environment, the JSON requests were in unencrypted format and communications happened through HTTP and not through HTTPS. Despite being made from China, this GPS is used by millions of people in Europe and other foreign lands. The security researchers reported this issue to the company but there's no response from them yet.

Update Google Chrome Browser to Patch New Critical Security Flaws

ATTACK TYPE
Hot fix

CAUSE OF ISSUE
Avoiding updation

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

Google's existing version has been discovered with 1 critical and 3 high risk security vulnerabilities. These when exploited could yield intruders remote access through which malicious arbitrary codes could be launched, thus redirecting them to rogue pages and compromising their data. This issue was identified by Man Yue Mo from Semmle, to whom Google rewarded about $40,000. Further, as a good news, Google has patched these vulnerabilities and had launched an updated version, 77.0.3865.90. To stay safe from these vulnerabilities, users are urged to update to this latest version ASAP.

EDUCATION

DeLand High's Twitter really 'hacked?'

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Improper Maintenance

TYPE OF LOSS
Reputation/Data

COUNTRY
Deland/Florida

A picture of a nude breast woman was seen in a school's twitter account at Deland. It's said that the woman had done this to irritate her ex-boyfriend and called this as her 'power move'. She also posted that her lone nipple has single handedly shook the notoriety of florida. Regarding this, the school principal Melissa said, our twitter account has been hacked. However, the post was removed within 15 minutes. Official investigation on how this hack happened is underway.

Criminal investigation launched following college cyber attack

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Improper DB Maintenance

TYPE OF LOSS
Reputation

COUNTRY
WILTSHIRE (UK)

Cyber criminals have hacked the personal data and breached the bank details of students and staff at Swindon College in Wiltshire. This is the latest computer crime to affect an education institution on Sept 12th. The college officials have issued a statement, "Our college people data are breached and are at risk. However, this issue is being reported to the National cybercrime agency and an official investigation is underway. Also, College people are given some precautions to remain safe and avoid further disasters.

This is undeniably the biggest data breach in Ecuador's history

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Unsecured server usage

TYPE OF LOSS
Reputation/Data

COUNTRY
ECUADOR

G. William Roberto, the General Manager of an IT Consulting firm Novaestrat, has been arrested for being the cause of Ecuador's biggest data breach. Wondering what? Well, he has exposed the personal details of 20+ million Ecuador citizens (almost the entire population) on an unsecured Elasticsearch server. This contained about 18 GB cache of data from distinct sources. However, the incident was notified to Ecuadorian's CERT who then took the server offline. The authorities have said that needed steps are being taken for overall security betterment.

Radio Pakistan's official website hacked

ATTACK TYPE
Security breach

CAUSE OF ISSUE
Fragile website security

TYPE OF LOSS
Reputation/Data

COUNTRY
PAKISTAN

The official website of Pakistan's radio broadcasting has been hacked and shut down. The cybercriminal group behind this is identified as 'Crash Rulers'. On its homepage, there was also a sarcastic message posted like "Hello Admin, you are very secured; Appreciated your security; We got an eye on you; Expect us; Pakistan zindabad!" However, the website was brought back to normal after some time.

Taiwan People's Party website hacked in a cyberattack

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Fragile website security

TYPE OF LOSS
Reputation/Data

COUNTRY
TAIWAN

The official website of Taiwan's People Party (TPP) got hacked after intruders compromised the website's registration system. Intruders did this by targeting and successfully exploiting the SMS verification mechanism. Since then, the website's owner, Mayor Ko Wen-je, has forfeited using the existing cloud services. Also, individuals are asked to register as 'friends of the party' rather than joining it. This is said to be done to avoid debate and bring in improvements for the betterment of Taiwan. However, official investigation on who's behind this hiccup is still underway and nothing good has popped up yet.

Palm Bay residents warned after utility bill pay portal hacked

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Unsecured server

TYPE OF LOSS
Reputation

COUNTRY
USA

Palm Bay customers who are using computers or mobiles to pay their water bills are being warned of a data breach. Customers using this service from July 27th to Sept 5th, got their banking information exposed due to which they are vulnerable. SunGuard alias Central-Square, the company that powers the water bills website says, like Palm Bay, eight cities were hacked and 8500 customers were prone to cyberattacks. However, the company's spokesperson cautioned customers to monitor their credit cards for suspicious checks and if found, urged them to report immediately.

SOCIAL MEDIA

WhatsApp 'Delete for Everyone' Doesn't Delete Media Files Sent to iPhone User

ATTACK TYPE
Hot fix

CAUSE OF ISSUE
App development issues

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

If you thought that the "Delete for Everyone" feature in WhatsApp truly deletes the ones you'd wanted, then you've highly mistaken my friend. The discoverer of this privacy issue Mr. Shitesh Sachan, a security consultant says that WhatsApp in iOS isn't designed to delete the received files and whereas against an Android user, WhatsApp deletes the sent media files from the recipient's device gallery as well. Moreover, this feature in WhatsApp is only available for 1 hour, 8 minutes and 16 seconds. However, a spokesperson from WhatsApp said, betterment work on this feature is ongoing.

Several YouTube channels 'hacked', attackers breach data

ATTACK TYPE
Security breach

CAUSE OF ISSUE
Clicking malicious links

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

Some of the familiar YouTube accounts like Built, Troy Sowers, MaxChekVids and Musafir have been breached. All these accounts aren't now available in YouTube. The major cause for these hacks is due to coordinated phishing links. The phishing links redirected them towards malicious sites, where credentials could be hijacked. Few of the hacked channels tried certain strategies like changing passwords, signing out from the existing accounts and creating a new one but none of these worked. More shockingly, Ryan Scott, owner of PURE Function channel said he used 2FA and still got hacked. However, Google hasn't commented anything about this yet.

Finance Minister's Facebook ID hacked

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
BANGLADESH

The official facebook ID of Bangladeshi's Finance Minister Mr. AHM Mustafa Kamal Mahmood Hossain has been recently hacked. With regards to this, all the known people have been requested not to respond to any requests, messages or unwanted posts that crops up from that ID, said the Finance Ministry on a press release. Required actions to set this right are being taken and it's hoped that the problem will be resolved soon. However, an official investigation is about to be started on this.

Stewie's Steam account hacked during CSGO Berlin Major playoffs

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
USA

Stewie's Steam account has been hacked during the eve of CSGO BERLIN play offs. On September 6th at 5.10 P.M, Stewie tweeted that someone hacked his steam account and he is unable to do anything. He was uncertain if he touched something or clicked on some malicious links. What's more surprising is the fact that his account got hacked despite using 2FA (Two Factor Authentication). However, after some time, his account became normal and he was able to use it.

Magecart card-skimming attack hit hotel chains across 14 countries

ATTACK TYPE
Malicious Input

CAUSE OF ISSUE
Lack of input validation

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

Magecard based attacks haven't halted yet. During this month, hotels booking websites have become the recent victims of it. Two hotel booking websites that were owned by separate chains, were affected by injecting malicious Java scripts. However, some security voids are said to be the reasons for these attacks in hotels. First one: hotels didn't ask for CVV/CVC while the other, due to the hosting of payment information in unreliable domains. Regarding this, a swift response from the victims is anticipated soon.

RETAIL

Mattress Company Leaks Data Records of 387K Customers

ATTACK TYPE
Data exposed

CAUSE OF ISSUE
Weak password's usage

TYPE OF LOSS
Reputation/Data

COUNTRY
MILWAUKEE (US)

Jeremiah Fowler, an active security researcher discovered an unprotected database on Sept 5th that was named as "Customers." Digging deeper, he found out that the exposed online database was of a mattress company named Verlo, from Milwaukee. Further, it was also revealed that the DB contained 387K data on Verlo's customers. The comprised data included names, numbers, addresses and much more. The main cause for this is because of storing data without strong passwords. However, Fowler had notified the company on this issue.

Data Leak Hits 2.5 Million Customers of Cosmetics Giant Yves Rocher

ATTACK TYPE
Data leak

CAUSE OF ISSUE
Unsecured Database

TYPE OF LOSS
Reputation/Data

COUNTRY
CANADA

Aliznet is a popular French retail consultancy with many aristocratic firms being its clients. But of late, VPN mentor security researchers discovered that Aliznet has exposed 2.5 million data of one it's client, Yves Rocher from Canada (a cosmetic giant firm). The exposed client data included names, numbers, addresses and much more. Apropos to it, over 6 million customer data were also found exposed containing info like transactions, store locations, billings history and much more. Also, an API vulnerability allowing to access an app built for Yves employees was also accessible. Without a doubt, this is a huge setback for Yves Rocher.

Flight booking site Option Way exposed personal info on customers

ATTACK TYPE
Data exposed

CAUSE OF ISSUE
Weak passwords usage

TYPE OF LOSS
Reputation

COUNTRY
FRANCE

Option Way, a flight booking site had exposed about 100 GB of customers information, discovered the VPN Mentor security researchers Noam Rotem and Ran Locar. The exposed information contained the PII of customers and even their credit card details, which could be accessed and compromised by intruders easily. The primary cause for this data exposure is due the usage of weak passwords by the company. Further, this breach is regarded as a 'goldmine for hackers' as massive data was very easily accessible.

Thermostat at 90 and a mysterious voice: Smart house hacked in Wisconsin

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Using Compromised pwd

TYPE OF LOSS
None

COUNTRY
WISCONSIN (USA)

A couple had complained that some anonymous hacker had hacked their home's smart system. They reported that hackers controlled their thermostat and an indoor camera on their Google's nest system. When the couple came home, they identified that thermostat's temperature kept on rising and a voice from kitchen's camera played out vulgar things. The couple even changed the password but nothing good was reaped. Henceforth, they'd decided to report to the internet provider. It seems that the couple used a compromised password and that's the reason for these happenings. Further, they cautioned fellow people about this and urged them to implement 2FA (Two Factor Authentication). However, an official investigation is ongoing about who are the one's behind this.

RETAIL

Hacked Seattle road sign says 'Impeach the Bastard'

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Improper security practice

TYPE OF LOSS
Reputation/Data

COUNTRY
SEATTLE

At Seattle, someone broke into an electronic roadwork sign and replaced the normal traffic suggestion with a political message that read "Impeach the bastard." This is referenced towards to the US president Mr. Donald Trump. The Seattle Department of Transportation (SDOT) informed this to the National Barricade Contractor. When they dug deep, they identified that a hacker had gained access into the sign's controls and had manipulated the content. However, the SDOT swore to improve their security measures and prevent such issues in the times ahead.

MongoDB server leaks 11 million user records from e-marketing service

ATTACK TYPE
Data leaks

CAUSE OF ISSUE
Unsecured server usage

TYPE OF LOSS
Reputation/Data

COUNTRY
CALIFORNIA

Bob Diachenko, a security researcher discovered an unsecured Mongo server that'd exposed the personal details of about 11 million customers. The unsecured server is identified to be from a Californian based email marketing firm. The exposed data contained 43.5 GB of dataset comprising information of customer's names, email addresses, physical addresses, DNS details and much more. To revive the data, hackers demanded 0.4 BTC and swore to then delete the backup data. Also, an official investigation is underway over this issue.

BANKING

Scotiabank exposed source code and credentials on GitHub repositories

ATTACK TYPE
Data exposed

CAUSE OF ISSUE
Flawed security practices

TYPE OF LOSS
Reputation/Data

COUNTRY
CANADA

Canadian banking giant, Scotiabank, serving over 25 million employees has exposed many of its critical information over GitHub repositories like internal source code, login credentials and access keys. However, the company's spokesperson said that the leaked information causes no harm to our customers, our employees and partners. Further, Scotiabank's technical team are working hard to remove all the exposed information ASAP.

Has Bolt Nigeria (Taxify) Been Hacked? Bolt Says No But Users Are Panicking After Strange Multiple Debits

ATTACK TYPE
Data breach

CAUSE OF ISSUE
App flaw

TYPE OF LOSS
Reputation/Data

COUNTRY
NIGERIA

Popular cab app, Bolt that's earlier named as Taxify, has been facing a setback with it's services, of late in Nigeria. There's a strange activity ongoing like the users of Bolt are still being debited of the rides they've taken and paid in the past. After cybercrime department stepped in, it was identified that Bolt app has been hacked, thus causing hiccups and palpitations to the Nigerian users. However, users are urged to delink their bank accounts from Bolt app. Also, Bolt swore that that're working hard to solve this issue ASAP and declared to assist the victims of this.

TRAVEL

City of Ames parking ticket payment website hacked

ATTACK TYPE
Data leak

CAUSE OF ISSUE
Weak 'cloud' usage

TYPE OF LOSS
Reputation/Data

COUNTRY
LOWA

The City of Ames in Lowa, had fallen to cyberattacks once again. The first time was on Nov 2018 when 4600 customers got their details compromised. Now, it's happened on Sept 12th and about 1500 citizens who paid their parking tickets online got their information stolen due to storing it a weak cloud environment. However, the city's spokeswoman Susan had asked the customers who paid from July 30th to Sept 12th to monitor their banking transactions. Further, she'd said that work is underway for better security implementations.

Malindo Air says data leak caused by ex-staffers at contractor firm

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Ex-employees Threat

TYPE OF LOSS
Reputation/Data

COUNTRY
MALAYSIA

Malaysia's Malindo air confirmed that 46 million passenger's personal details were exposed online. This breach was first notified to the company by Kaspersky. While investigating deeper, it was identified that two ex-employees from their e-commerce service provider 'GoQuo' in India have improperly accessed and stole customers personal data. The exposed data were also of the customers from the Thai's Lion air. However, it's glad that the airline company had contained this issue and have also informed the police in India and Malaysia as well.

HEALTHCARE

Carle Foundation Hospital fell victim to a data breach

ATTACK TYPE
Phishing

CAUSE OF ISSUE
Unauthorized access

TYPE OF LOSS
Reputation

COUNTRY
USA

Carle foundation hospital recently fell victim to data breach. Carle's team identified that an unauthorized party had gained access to three of their physician email accounts. With the help of a proper cybersecurity firm, they identified that some of their patient's information were contained in the email accounts. The attack type is identified as phishing. Regarding the intruder, there's no information yet.

TELECOMMUNICATION

A Massive 1.7 Terabytes of Russian Telco Information Was Exposed

A mindboggling amount of 1.7 Terabytes of data has been exposed from an unprotected Rsync server in Russia. The exposed information contained the telecommunication installations of the Russian federation like the SORM (monitoring and blocking traffic) instructions, details about the FSB data, power stations, admin credentials, backups and much more. Almost all Russian telco firms are affected due to this, with Nokia and Mobile Tele systems being the most affected. This happened on Sept 9th and was contained by Sept 13th. Quantity of data compromise remains unknown but this is undeniably, one of the worst security disasters in Russian history.

ATTACK TYPE

Data breach

CAUSE OF ISSUE

Unprotected server usage

TYPE OF LOSS

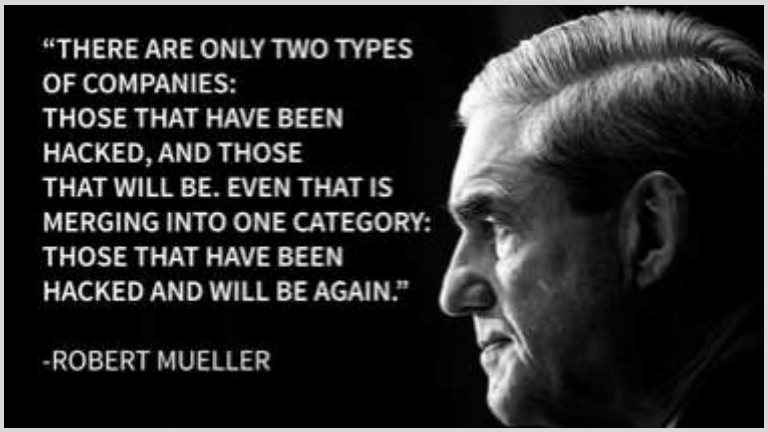
Reputation/Data

COUNTRY

RUSSIA

EDUCATION

CONCLUSION

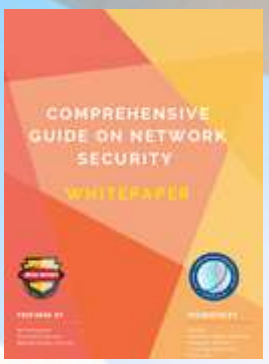


Well, as per the words of this legend, data breaches and data compromises seem inevitable. Both these words are roaring endlessly in this entire digital cosmos. Despite all the stunning technological inventions and promising security advancements, cyber breaches still keep rising. There's a cybersecurity saying that 2FA and storing data in cloud environment with strong passwords, secures you from cyber threats. But now, even they've become outdated as hackings are happening despite implementing them. All the best security tools seem to provide relief from hackings but they're neither a permanent relief nor trustworthy. All these at one point of time fail. Then, what's the state and fate of our digital data? Well, the ultimate hope that would help is the firewall named 'Human firewall'. It's none other than our own intelligence. It's our proper instincts before thinking while clicking the links that come for us. For doing and being right in these, a proper cybersecurity training and an effective security service providing company needs to be approached. Just reach us out anytime. We'll discuss further and accomplish the deed of 'staying secured' against cyber threats triumphantly together.

REFERENCES

- https://thehackernews.com/2019/09/phpmyadmin-csrf-exploit.html
- https://www.forbes.com/sites/tjmccue/2019/09/21/read-this-and-double-check-your-google-calendar-settings/#6f5e829c7f0c
- https://thehackernews.com/2019/09/microsoft-windows-update.html
- https://www.silicon.co.uk/security/security-management/vulnerabilities-d-link-comba-routers-trustwave-286393
- https://www.zdnet.com/article/google-removes-two-chrome-ad-blocker-extensions-caught-cookie-stuffing/
- https://timesofindia.indiatimes.com/gadgets-news/dont-hand-your-iphone-to-anyone-if-you-have-just-upgraded-to-ios-3/articleshow/71218726.cms
- https://thehackernews.com/2019/09/facebook-hhvm-vulnerability.html
- https://www.techradar.com/in/news/flaws-discovered-in-popular-router-and-nas-brands
- https://www.techradar.com/in/news/popular-gps-trackers-found-to-have-major-security-flaws
- https://thehackernews.com/2019/09/google-chrome-update.html
- https://www.news-journalonline.com/news/20190912/nude-photo-retweet-was-deland-highs-twitter-really-hacked
- https://feweek.co.uk/2019/09/17/criminal-investigation-launched-following-college-cyber-attack/
- http://www.fox35orlando.com/news/palm-bay-residents-warned-after-utility-bill-pay-portal-hacked
- https://thehackernews.com/2019/09/ecuador-data-breach.html
- http://www.kashmirtimes.com/newsdet.aspx?q=94470
- https://www.taiwannews.com.tw/en/news/3777591
- https://thehackernews.com/2019/09/whatsapp-delete-for-everyone-privacy.html
- https://timesofindia.indiatimes.com/gadgets-news/several-youtube-channels-hacked-attackers-breach-two-factor-authentication-security-as-well/articleshow/71297499.cms
- https://www.dhakatribune.com/bangladesh/2019/09/15/finance-minister-s-facebook-id-hacked
- https://www.talkesport.com/news/stewies-steam-account-hacked-during-csgo-berlin-major-playoffs/
- https://www.zdnet.com/article/magecart-strikes-again-hotel-booking-websites-come-under-fire/
- https://threatpost.com/mattress-company-leaks-data-records-of-387k-customers/148530/
- https://www.infosecurity-magazine.com/news/data-leak-affects-25m-customers/
- https://www.scmagazine.com/home/security-news/flight-booking-site-option-way-exposed-personal-info-on-customers/
- https://www.wave3.com/2019/09/25/milwaukee-couples-smart-house-hacked-thermostat-set-voice-speaks-camera/
- https://q13fox.com/2019/09/25/hacked-seattle-road-sign-says-impeach-the-bastard/
- https://www.zdnet.com/article/mongodb-server-leaks-11-million-user-records-from-e-marketing-service/
- https://www.scmagazine.com/home/security-news/data-breach/report-scotiabank-exposed-source-code-and-credentials-on-github-rhttps://weetracker.com/2019/09/25/has-bolt-taxify-been-hacked-in-nigeria/
- https://whoradio.iheart.com/content/2019-09-25-city-of-ames-parking-ticket-payment-website-hacked/
- https://in.reuters.com/article/us-lionair-leak/malindo-air-says-data-leak-caused-by-ex-staffers-at-contractor-firm-idINKBN1W80DTepositories/
- https://weetracker.com/2019/09/25/has-bolt-taxify-been-hacked-in-nigeria/
- https://whoradio.iheart.com/content/2019-09-25-city-of-ames-parking-ticket-payment-website-hacked/
- https://in.reuters.com/article/us-lionair-leak/malindo-air-says-data-leak-caused-by-ex-staffers-at-contractor-firm-idINKBN1W80DT
- https://www.securitymagazine.com/articles/90921-carle-foundation-hospital-suffers-data-breach-due-to-phishing-attack
- https://www.technadu.com/1-7-terabytes-russian-telco-information-exposed/80476/

YOU MAY BE INTERESTED IN OUR WHITEPAPERS



YOU MAY ALSO BE INTERESTED IN OUR PREVIOUS WORKS

REFERENCES ABOUT BRISKINFOSEC

CASE STUDIES
CASE STUDIES

SOLUTIONS

SERVICES

RESEARCH

COMPLIANCES

BLOGS

FEEL FREE TO REACH US FOR ALL
YOUR CYBERSECURITY NEEDS

contact@briskinfosec.com | www.briskinfosec.com