THREATSPLOIT ADVERSARY REPORT

MARCH 2020 | EDITION 19

BRISK INFOSEC

CYBER TRUST & ASSURANCE

www.briskinfosec.com

INTRODUCTION

Welcome to the world of our Threatsploit Adversary Report which contains a cluster of threats that several industries came across during the month of February 2020. Cybersecurity issues are becoming a day-to-day struggle for businesses.

Through our **Threatsploit Adversary Report** we make you aware of various threats that we come across in a single document. This explains the unexpected hack faced by the companies and the way they handled it. But several companies still struggle to come out of those threats. Over time these attacks have evolved stronger and more menacing, haunting and taunting security professionals, giving them nightmarish experience.

According to a research by Security Intelligence the average cost of a data breach is $3.92 million as of 2019.

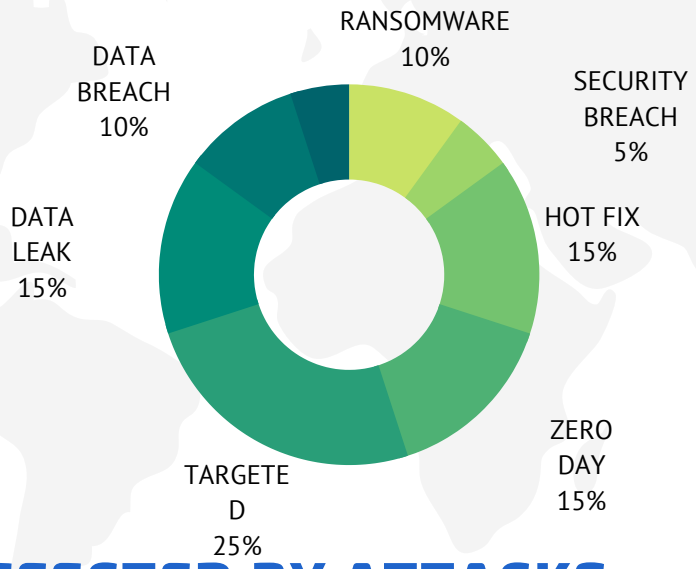
A recent security research also suggests that most companies have unprotected data and poor cybersecurity practices in place, which ends up in data loss.

To overcome this issue, it's imperative that companies make cybersecurity awareness, prevention and security as an important factor in their business.

In order to give you a clear idea on the recent threats we have compiled the following list of threats, we hope this would help you to be aware of the current insecurity status and come out with the best security option for your company data.

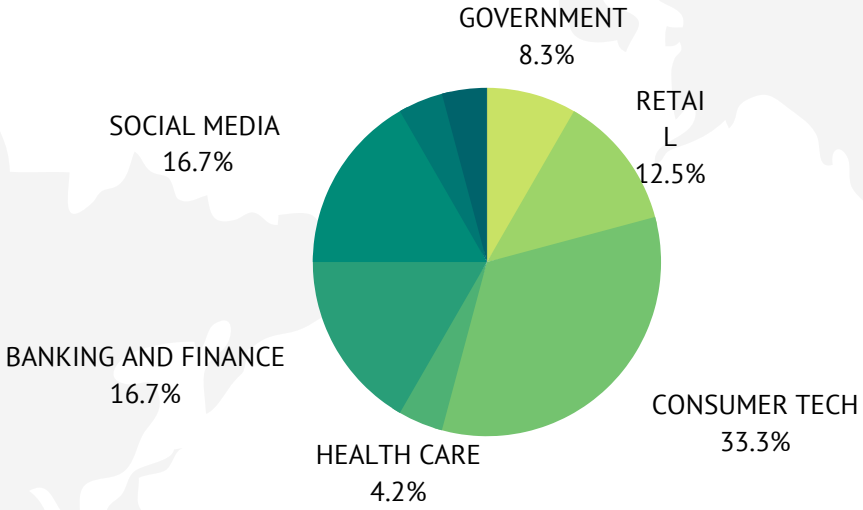
TYPES OF ATTACK VECTORS

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



SECTORS AFFECTED BY ATTACKS

The below Pie-chart 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 Retail has been hit the most.



Many cyberattacks initiate from various sectors. But, a majority of them seemed to have originated from consumer technology sector, holding about 55%. To prevent these, it's evident that top-notch reliable security is mandatory.

55%

consumer Tech

CONSUMER TECHNOLOGY

- Google had a Security Gap! Hacker created a virtual traffic jam on Google Maps.
- Tracker SA's Systems experienced "technical difficulties"
- Avon Lake's email blast system was hacked through Constant Contact
- Cisco's software-license management tool faces a critical bug
- Samsung experiences data leak
- Active Exploits Hit Vulnerable WordPress ThemeGrill Plugin
- Google patches Chrome zero-day under active attacks
- Windows 10 KB4532693 Update Bug Reportedly Deletes User Files

BANKING AND FINANCE

- Cisco Patched Critical Bug In Firepower Management Center
- Nedbank's telemarketing company experienced a Cyber Breaching
- Hackers exploited vulnerability in the official IOTA wallet app
- NDMC Employees Bank Accounts Illegally Hacked

SOCIALMEDIA

- Facebook and its messaging app's official Twitter Account was Hacked
- Twitter Faced a huge hit by OurMine for the second Time
- Ninja's Twitter Account Hacked
- WhatsApp Telegram Group Invite Links Exposed

RETAIL

- Slickwraps's customer trust was 'violated' in data breach
- US Consumers Exposed in Privacy Snafu
- Hacked Pokémon Received Through Trades Are Crashing Sword & Shield

HEALTHCARE

- Plastic surgery images and invoices leak from unsecured database

GOVERNMENT

- DOD DISA disclosed Data Breach
- UK: Redcar cyber-attack

OIL AND GAS

- Employee's Email Address was hacked

EDUCATION

- Confederation College aspects a Malware Incident

CONSUMER TECHNOLOGY

Google had a Security Gap! Hacker created a virtual traffic jam on Google Maps.

ATTACK TYPE
Security Gap

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

Nevertheless even Google had the Security Gap. It was hacked by a German artist Simon Weckert just by transporting 99 second hand smartphones in a handcart which generated virtual traffic jam in Google Maps. As a result, Google Maps started showing virtual traffic jams in the online navigational tool. As usual Google Maps' servers interpreted the situation as traffic congestion, and began showing this to others on the street. This, in turn, prompted drivers to turn away and avoid streets where there was actually no traffic.

Tracker SA's Systems experienced "technical difficulties"

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

Stolen vehicle recovery company, Tracker SA is working with local and third party experts to recover and restore some of its systems that were affected by a ransomware attack. According to the company's CEO Wayne de Nobrega, the attack has encrypted information on some systems." He also said that the recovery process is good and he added that there is no indication that any customer data has been compromised or accessed.

Avon Lake's email blast system was hacked through Constant Contact

ATTACK TYPE
Social Engg

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

The City of Avon Lake's email blast system was hacked by accessing the password which they use for Constant Contact, a national online marketing company. The emails arrived to the city residents' personal accounts from the online marketing company, stating that the recipients owed money to the city. Steve Presley the city's Finance Director said, he believes that it's not the fault of Constant Contact and they will work together and change all passwords making it harder for the hackers to get in.

Cisco's software-license management tool faces a critical bug

ATTACK TYPE
Hot fix

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

Cisco disclosed a critical flaw in its Cisco Smart Software Manager On-Prem product. The bug could allow a remote attacker to access a sensitive part of the system with a highly privileged account. According to Cisco, SSM On-Prem systems are only vulnerable if the high availability (HA) feature has been enabled. They urged their customers

CONSUMER TECHNOLOGY

Samsung experiences data leak

Samsung's customers found other users's login details was being shown to them in their "Find my Mobile" push notification while trying to change their passwords. Then over on Twitter, they asserted that this morning's push notification was a "message sent unintentionally during internal test". A Samsung rep said referring to the data breach on its UK customer account pages: "Less than 150 customers were affected, and we are contacting them directly.

ATTACK TYPE
Data leak

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

Active Exploits Hit Vulnerable WordPress ThemeGrill Plugin

ATTACK TYPE
zero day

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

Websites using a vulnerable version of the WordPress plugin, ThemeGrill Demo Importer, were being targeted by attackers. According to WebARX researchers, "This is a serious vulnerability and can cause a significant amount of damage," Researchers are urging users to update as soon as possible after discovering attackers are actively exploiting a flaw in the plugin

Google patches Chrome zero-day under active attacks

Google released a Chrome update to address three security bugs, including a zero-day vulnerability that is being actively exploited in the wild. The update is available for Windows, Mac, and Linux users, but not Chrome OS, iOS, and Android. The zero-day is tracked under the identifier of CVE-2020-6418, and is described only as a "type confusion in V8."

ATTACK TYPE
Zero day

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

Windows 10 KB4532693 Update Bug Reportedly Deletes User Files

ATTACK TYPE
Hot fix

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

The users are reporting that the new Windows 10 KB4532693 cumulative update is deleting their files. If the user's data gets missed they should first open the C:\users folder and see if any folders are ending with a .bak or .000 extension, if these folders exist, one of them is probably the users original profile, if data exists then the user should backup the data, and finally should restart the profile for Windows 10 a few times and see if your profile is restored. If not, then uninstall the KB4532693 update using the instructions.

Cisco Patched Critical Bug In Firepower Management Center

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

Altsbit an Italian crypto exchange platform's crypto exchange is been hacked and almost all funds are gone. Their hot wallet is totally emptied, fortunately a good part of the coins were kept on cold storage, these coins will be returned to the users of Altsbit, they will be distributed among all users of the platform each coin will have its calculation based on the percentage that was saved during the attack.

Nedbank's telemarketing company experienced a Cyber Breaching

ATTACK TYPE
Security breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

A South African financial services group Nedbank is investigating a cyber hacking in one of its service providers, Computer Facilities. Once the bank was aware of the cyber breaching it urgently contacted the service provider and leading forensic experts to conduct an extensive investigation and it disconnected Computer Facilities' systems from the internet. The bank's CEO Mike Brown said, "We take our responsibility to protect our client information seriously and our immediate focus has been on securing all Nedbank client data at Computer Facilities, which we have done."

Hackers exploited vulnerability in the official IOTA wallet app

ATTACK TYPE
Hot fix

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

IOTA Foundation, shut down its entire network after hackers exploited vulnerability in the official IOTA wallet app to steal user funds. They used an exploit in "a third-party integration" of Trinity, a mobile and desktop wallet app developed by the IOTA Foundation. So the foundation is working on an update for the Trinity wallet apps to patch the vulnerability exploited in the hack. In the meantime, IOTA members recommend that users don't open their wallets until the update is released and installed on their devices.

NDMC Employees Bank Accounts Illegally Hacked

ATTACK TYPE
Social Engg

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

The New Delhi Municipal Corporation (NDMC) alleged that lakhs of rupees were siphoned off from bank accounts of its 200 members using forged ATM cards, most of which belonged to SBI. The NDMC Employees Association noted that the forgery has possibly been done by "cloning of ATM cards."

Facebook and its messaging app's official Twitter Account was Hacked

Even Facebook has to face the 'Hack,' an hacking group 'hacked the social media giant's Twitter account in February 2020 and it also hacked Messenger's Twitter Id which is an add on pressure to Facebook. Once Twitter came to know about the vandalism they locked the compromised accounts and stated that they were working closely with their partners at Facebook to restore them.

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

Twitter Faced a huge hit by OurMine for the second Time

In the same month Twitter once again experienced the same distress from the OurMine company. The infamous hacker collective hacked the official Twitter accounts of FC Barcelona, the Olympics and the International Olympic Committee (IOC) via a third-party platform. As soon as Twitter became aware of the issue it took action and locked the accounts.

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

Ninja's Twitter Account Hacked

Tyler "Ninja" Blevins' Twitter account was the latest high profile account to get taken over by hackers. The attacker even tried to extort Ninja's wife and business partner, Jessica Blevins. The hacker tried to use opportunity to rack up followers, start a beef with Fortnite star Tfue and complain when an account was inevitably suspended. Besides deleting the tweets, Ninja posted a video blasting an "irrelevant" person for grasping in vain for popularity.

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

WhatsApp Telegram Group Invite Links Exposed

Researcher Jordan Wildon discovered that many search engines have indexed various messenger apps' group invite links. With the search engines showing up WhatsApp and Telegram group invite links publicly. This includes visibility of the links on all major search engines such as Google, Yahoo, Bing, and Yandex. This flaw not only ruined the privacy of private WhatsApp and Telegram groups but also made many illegal groups publicly accessible.

ATTACK TYPE
Data exposed

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

Slickwraps's customer trust was 'violated' in data breach

Slickwraps revealed a data breach impacting over 850,000 user accounts, admitting its mistake in permitting customer records to become public. The company said that an "attacker emailed customers connected to the breach," and it was also made aware of the breach via a post on Twitter. CEO Jonathan Endicott said, "We are deeply sorry for this over'sight…We promise to learn from this mistake and will make improvements going forward."

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

RETAIL

US Consumers Exposed in Privacy Snafu

ATTACK TYPE
Data exposed

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

Security researchers discovered a publicly exposed cloud database containing personal data and behavioural profiles on 120 million Americans. Security company UpGuard found the misconfigured Amazon S3 bucket eventually, tracing it back to market analysis company Tetrad. While the source of every data point is not clear, the end result is a collection of data that provides detailed information about Americans. The data, which appears to have gone from clients to Tetrad, varies by the type of business and their methods for data collection.

Hacked Pokémon Received Through Trades Are Crashing Sword & Shield

Pokémon Sword and Shield's surprise trade feature is currently causing players' systems to crash and is even having some long-term effects regarding online play. Trainers have been reporting instances of Pokémon received via Surprise Trades crashing their games. The Pokémon responsible for the problems are malicious ones that have been added by hackers.

ATTACK TYPE
Malware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

Plastic surgery images and invoices leak from unsecured database

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

VPNMentor's research team recently discovered a breached database belonging to plastic surgery technology company NextMotion. The compromised database contained 100,000s of profile images of patients, uploaded via NextMotion's proprietary software. This breach made NextMotion, its clients, and their patients incredibly vulnerable and represented a significant lapse in the company's data privacy policies.

HEALTHCARE

GOVERNMENT

DOD DISA disclosed Data Breach

The Defense Information Systems Agency (DISA) was hit by a data breach few months ago that may have compromised the personally identifiable information (PII) of thousands of military staff and civilian personnel. DISA sent letters to possible victims earlier in February 2020 to warn of a "data breach" involving a system run by the agency. According to the spokesperson, "DISA has conducted a thorough investigation of this incident and taken appropriate measures to secure the network."

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

UK: Redcar cyber-attack

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

Systems at Redcar and Cleveland Council have been down after the ransomware attack. Council leader Mary Lanigan said, "Our absolute priority since the first day of the attack has been to protect our front-line services…Significant progress has been made...all front-line services have continued, payments continue to be processed as normal, and there is no evidence so far to suggest any personal information has been removed from our servers."

OIL AND GAS

Employee's Email Address was hacked

An unknown person hacked the email address of an employee of Saibaba Petroleum Company, duping the dealer of Rs 5.48 lakh by accessing the firm's bank details from the office computer system. The fraud came to light when the audit team of the company noticed a discrepancy in the accounts payment. Taking cognisance of the employee's complaint, police booked unknown persons under Indian Penal Code sections 420 and 468 for fraud and forgery along with various sections of the Information Technology Act.

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Data

EDUCATION

Confederation College aspects a Malware Incident

ATTACK TYPE
Malware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Data

Confederation College IT systems were shut down by a malware incident but they said that until then there was no evidence of any personal information to be removed from its systems. But they also intimated that if the college learns that personal information was removed from its servers, it will notify all affected individuals. The college informed that the IT services should be restored within the week.

CONCLUSION

We hope the above given threats would be an eye opener for you to run your business in the most secured way.

According to a research by Accenture, 68% of business leaders feel their cybersecurity risks are increasing. So in order to stay away from these kinds of loss and threats people would spend a lot of money in finding best security professionals to keep their data secured.

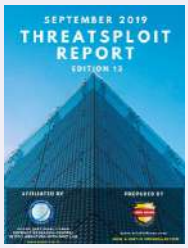
They would also spend money a lot in purchasing top se curity tools. But apart from this the employees should be given a proper awareness. This would reduce the causes for social engineering and phishing attack. They should also be aware about the types of calls and methods the intruders would use to deceive and exploit information from them.

Reach us out to know more about those information and we are here to keep your data secure too.

REFERENCES

- https://www.bbc.com/news/technology-51424352
- https://www.financialexpress.com/industry/technology/twitter-says-facebook-messenger-accounts-hacked/1860642/lite/
- http://www.simonweckert.com/googlemapshacks.html
- https://www.hindustantimes.com/tech/this-user-hacked-google-maps-traffic-flow-in-an-entire-area-with-99-smartphones/story-HdfSksLkoIEe355BIJ7VIO.html
- https://www.wired.com/story/99-phones-fake-google-maps-traffic-jam/
- https://www.dispatchlive.co.za/news/2020-02-02-tracker-sas-systems-hacked/
- https://www.timeslive.co.za/news/south-africa/2020-02-02-tracker-sas-systems-hacked/
- https://bitcoinist.com/altsbit-crypto-exchange-gets-hacked-almost-all-funds-have-gone/
- https://altsbit.com/order?url=dp-btc
- https://www.welivesecurity.com/2020/02/17/fcbarcelona-twitter-account-hacked-again/
- https://www.deccanherald.com/national/north-and-central/bank-accounts-of-over-200-new-delhi-municipal-council-employees-hacked-money-siphoned-off-804929.html
- https://www.indiatoday.in/india/story/bank-accounts-hacked-lakhs-rupees-siphoned-off-ndmc-employees-association-1646645-2020-02-15
- https://www.zdnet.com/article/nedbank-says-1-7-million-customers-impacted-by-breach-at-third-party-provider/
- http://www.irishnews.com/news/northernirelandnews/2020/02/07/news/translink-it-systems-targeted-in-suspected-ransomware-cyber-attack-1836604/
- https://www.cleveland.com/community/2020/02/avon-lake-email-blasts-get-hacked-through-constant-contact.html
- https://en.secnews.gr/210136/confederation-college-dechtike-epithesi-malware/
- https://www.cbc.ca/news/canada/thunder-bay/confederation-college-malware-incident-1.5449400
- https://ahmedabadmirror.indiatimes.com/ahmedabad/crime/company-email-account-hacked-rs-5-5-lakh-lost/articleshow/74216097.cms
- https://indianexpress.com/article/cities/ahmedabad/employees-computer-hacked-petroleum-dealer-duped-of-rs-5-48-lakh-6276552/
- https://coingape.com/iota-network-has-been-hacked-and-funds-stolen-again/
- https://www.zdnet.com/article/iota-cryptocurrency-shuts-down-entire-network-after-wallet-hack/
- https://thehackernews.com/2020/02/cisco-cdp-vulnerabilities.html
- https://www.zdnet.com/article/cisco-critical-bug-static-password-in-smart-software-manager-patch-now-says-cisco/
- https://www.msspalert.com/cybersecurity-markets/americas/dod-agency-data-breach/
- https://techcrunch.com/2020/02/20/defense-agency-disa-breach/
- https://www.infosecurity-magazine.com/news/120-million-us-consumers-exposed/
- https://www.upguard.com/breaches/tetrad-breach-120-million-households
- https://www.zdnet.com/article/slickwraps-says-customer-trust-was-violated-in-avoidable-data-breach/
- https://www.engadget.com/2020/02/22/ninja-twitter-account-hijacked/
- https://gadgets.ndtv.com/games/news/ninja-twitter-hacked-fortnite-star-mixer-streamer-2184661
- https://www.theregister.co.uk/2020/02/20/samsung_push_notification_1_1_personal_data/
- https://www.theregister.co.uk/2020/02/24/samsung_data_breach_find_my_mobile/
- https://threatpost.com/active-exploits-hit-vulnerable-wordpress-themegrill-plugin/152947/
- https://www.thegamer.com/hacked-pokemon-received-in-trades-crashing-sword-shield/
- https://www.zdnet.com/article/google-patches-chrome-zero-day-under-active-attacks/
- https://www.teiss.co.uk/redcar-ransomware-council-reveal-the-nature-of-recent-cyber-attack/
- https://www.bleepingcomputer.com/news/microsoft/windows-10-kb4532693-update-bug-reportedly-deletes-user-files/
- https://www.vpnmentor.com/blog/report-nextmotion-leak/

YOU MAY ALSO BE INTERESTED IN 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