EDITION 22

THREATSPLOIT ADVERSARY REPORT

JUNE 2020

Follow us!

www.briskinfosec.com

INTRODUCTION

Quite a lot of changes are implemented post COVID-19 and now we are right now in a New Normal, where we follow certain rules and are restricted from several things just to be safe. But this is actually tough for few of us and mainly for organizations. Several organizations are currently in a critical situation with so many questions in mind and unable to predict the future, they are still doubtful in making their next move. Organizations are not clear on how they would run their business? How to handle this situation? etc., According to them Work from home has been their new normal, which is the best option picked by various organizations. Even though the decision sounds good, handling a work from home scenario is quite risky.

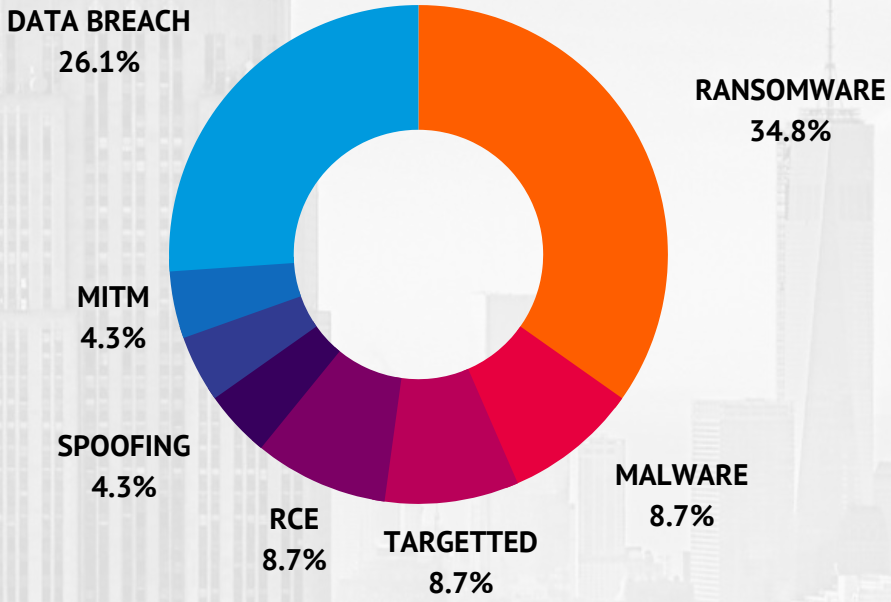
An organization must be watchful in order to save their data from the hands of several Hackers. Various Cybersecurity issues would arise at this point. According to a Check Point Software & Dimensional Research survey, 71% of IT and security professionals globally report an increase in security threats since the beginning of the pandemic. Check our Threatsploit Report for the month of April 2020 to know more about the threats that took place during this Covid-19 situation.

In certain cases most of the companies will not be aware for weeks or months that they are a victim of a cyberattack. Organizations plan to run their business and they concentrate more on customers and the projects they handle but they fail to strengthen the data security. As a result of the sudden lockdown employees were also requested to work from their personal devices which have no corporate security.

Even some confidential data and meetings will not have privacy as they use software to discuss them. These kind of small errors finally end up in creating a big loss to the company. The companies should take essential steps to stay away from cybersecurity risks. Security issues could make a company to lose their reputation in the industry and also among the customers; they lose their data and at times a huge amount of money also. To give you all an idea regarding these kinds of threats we have created this report that covers a brief about the current threats few organizations are facing.

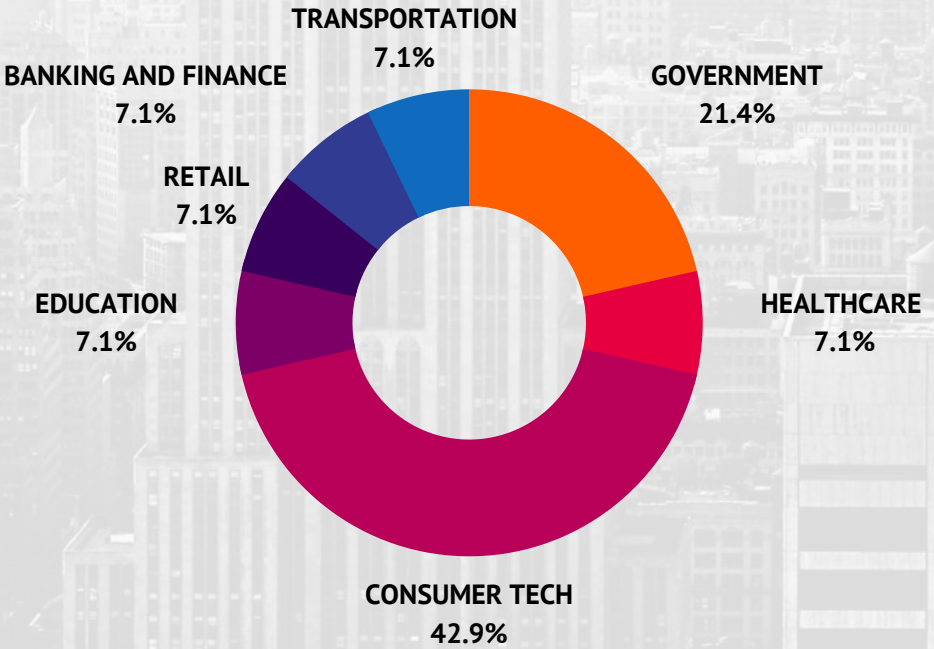
TYPES OF ATTACK VECTORS

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



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 has been hit the most.



GOVERNMENT

- Elexon Hit by Cyber Attack
- Second Texas Government Attack
- Taiwan’s major oil refineries hit by Malware
- Texas Court Slammed by ransomware attack
- N.J. town’s website knocked offline.
- Israeli sites defaced with code seeking permission to access users' webcams

HEALTHCARE

- Europe’s Largest Private Hospital Operator Hit by Ransomware
- Health Giant hit by Ransomware attack

CONSUMER TECH

- Thousands of data Centers affected by Critical SaltStack RCE Bug
- Users' Data Exposed via Misconfigured Firebase Databases
- Taiwan’s major oil refineries hit by Malware
- Biggest online retailers in Brazil suffers Data Breach
- New Bluetooth Vulnerability
- Thousands of QNAP devices vulnerable to remote takeover attacks
- Truecaller data breach
- Security flaws seen in Aarogya Setu
- Office 365 phishing uses Supreme Court theme and working CAPTCHA
- Satellite Hacking: Encryption in Space is Hard
- Docker Desktop Community and Enterprise finally held back from vulnerability.
- Billions of Thai internet records leaks

EDUCATION

- EduCBA unveils Data Breach after a Hack
- 25 million user records Leaked by a Top-rated app

RETAIL

- Ransomware Attack Hits A-List Celeb Law Firm
- Web hosting provider faces security lapse

BANKING AND FINANCE

- Biggest European bank leaks sensitive data on their website
- Banco BCR card data was exposed

TRANSPORTATION

- Biggest European bank leaks sensitive data on their website
- Banco BCR card data was exposed

Elexon Hit by Cyber Attack

Elexon was affected by a cyber attack that crippled its email server. It identified the root cause of the incident, and was working to restore its internal network and employee laptops. Experts believe that it could be ransomware, considering its impact, which caused employees to lose access to the company's email server. According to threat intelligence , Elexon had been running an outdated version of Pulse Secure, an enterprise-level SSL VPN server that lets employees access internal networks across the internet.

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of maintaince

TYPE OF LOSS
Reputation/Data

Second Texas Government Attack

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Unknown

TYPE OF LOSS
Reputation/Data

Texas' transportation agency network faced a ransomware attack, the second attack for the state government. Its website features were unavailable due to technical difficulties, but there was no clear information regarding the affected functions. Hackers use ransomware to invade computer systems and encrypt files in an effort to extort payments to unlock them

Taiwan's major oil refineries hit by Malware

Taiwan's CPC Corporation and its rival, Formosa Petrochemical Corporation (FPCC) were targeted by cyber-attackers, with disruption trickling down the supply chain to impact customers at gas stations. CPC's ransomware attack prompted the closure of IT and computer systems and prevented gas stations in the country from accessing the digital platforms used to manage revenue records. IT systems were immediately closed in every division to investigate the issue.

ATTACK TYPE
Malware

CAUSE OF ISSUE
Lack of awarness

TYPE OF LOSS
Reputation/Data

Texas Court Slammed by ransomware attack

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

Texas revealed a ransomware attack launched against its court system but insists no ransom will be paid. The malware made its way through the OCA's branch network, and as soon as the ransomware was spotted, linked servers and websites were disabled in an attempt at damage limitation.

GOVERNMENT

N.J. town's website knocked offline.

Bernards Township's computers were breached by a ransomware attack where its website went offline. "We continue to dedicate all available resources to recovering from this event and will provide necessary updates as they are received," Mayor Jim Baldassare. The township is working with a third-party computer forensics specialists to investigate the breach, he added.

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Unauthorized access

TYPE OF LOSS
Reputation/Data

Israeli sites defaced with code seeking permission to access users' webcams

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Existing Vulnerability

TYPE OF LOSS
Reputation/Data

Thousands of Israeli websites were defaced to show an anti-Israeli message and with malicious code seeking permission to access visitors' webcams. Most of the websites were hosted on uPress, where the hackers exploited vulnerability in a WordPress plugin to plant the defacement message on Israeli sites hosted on its platform. Efforts were underway to restore all affected sites.

HEALTHCARE

Europe's Largest Private Hospital Operator Hit by Ransomware

Fresenius has been hit in a ransomware cyber attack on its technology systems. The Snake ransomware affected every part of the company's operations around the globe. The assault on Fresenius comes amid increasingly targeted attacks against healthcare providers on the front lines of responding to the COVID-19 pandemic.

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Security loopholes

TYPE OF LOSS
Reputation/Data

Health Giant hit by Ransomware attack

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation

Magellan Health recently hit by the ransomware attack resulted in a temporary systems outage and the exfiltration of certain confidential company and personal information. The company investigated the incident with forensic experts and also notified their customers and their employees.

Thousands of data Centers affected by Critical SaltStack RCE Bug

Two severe security flaws were detected in the open-source SaltStack Salt configuration framework that could allow an adversary to execute arbitrary code on remote servers deployed in data centers and cloud environments. It's highly recommended that Salt users update the software packages to the latest version.

ATTACK TYPE
RCE

CAUSE OF ISSUE
Security flaw

TYPE OF LOSS
Reputation/Data

Users' Data Exposed via Misconfigured Firebase Databases

ATTACK TYPE
Data Breach

CAUSE OF ISSUE
Security Misconfiguration

TYPE OF LOSS
Reputation/Data

More than 4,000 Android apps that use Google's cloud-hosted Firebase databases 'unknowingly' leaked sensitive information on their users. The researchers also warned that the misconfigurations are likely to impact iOS and web apps as well. Exposed databases using known Firebase's REST API that's used to access data stored on unprotected instances, retrieved in JSON format

Taiwan's major oil refineries hit by Malware

Taiwan's CPC Corporation and its rival, Formosa Petrochemical Corporation (FPCC) were targeted by cyber-attackers, with disruption trickling down the supply chain to impact customers at gas stations. CPC's ransomware attack prompted the closure of IT and computer systems and prevented gas stations in the country from accessing the digital platforms used to manage revenue records. IT systems were immediately closed in every division to investigate the issue

ATTACK TYPE
Malware

CAUSE OF ISSUE
Poor security pratice

TYPE OF LOSS
Reputation/Data

Biggest online retailers in Brazil suffers Data Breach

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

Natura left its 250,000 customers' personal information and payment details public without knowledge. In addition to Natura&Co customers, a third-party company named Wirecard also was affected since the information about customer payments was public for at least two weeks. Nearly 40,000 customers of Moip also got their account details publicly exposed. Access tokens without any security protocols were left exposed to Wirecard accounts too.

New Bluetooth Vulnerability

Academics from EPFL unveiled security vulnerability in Bluetooth that potentially allow an attacker to spoof a remotely paired device, exposing over a billion of modern devices to hackers. The attacks, dubbed BIAS, concern Bluetooth Classic, which supports Basic Rate (BR) and Enhanced Data Rate (EDR) for wireless data transfer between devices.

ATTACK TYPE
Spoofing

CAUSE OF ISSUE
Security vulnerability

TYPE OF LOSS
None

Thousands of QNAP devices vulnerable to remote takeover attacks

ATTACK TYPE
RCE

CAUSE OF ISSUE
Root Privileges

TYPE OF LOSS
None

Three vulnerabilities in the firmware of QNAP network-attached storage (NAS) devices were released. Thee bugs reside in Photo Station, a photo album app that comes preinstalled with all recent versions of QNAP NAS systems. Since the Photo Station app runs with root privileges, attackers can exploit the three bugs to take full control over QNAP devices.

Truecaller data breach

Personal data of millions of Truecaller users, including Indians, has been leaked online and it is available on sale on dark web. But Truecaller denied all reports of a data breach and said the data is safe and that there is no record of the sensitive user information, including the financial data being extracted from its database

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Unknown

TYPE OF LOSS
Reputation/Data

Security flaws seen in Aarogya Setu

ATTACK TYPE
Data leak

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

An ethical hacker alleged that security flaws in Aarogya Setu application enabled him to see that five people at the Prime Minister's Office (PMO) and two people at the Indian Army headquarters were unwell. But the Aarogya Setu team said no personal information of any user had been proven to be at risk and this was just an alert from the Ethical hacker.

Office 365 phishing uses Supreme Court theme and working CAPTCHA

Hackers tried to bypass security controls in Office 365 and added a CAPTCHA page in the chain of redirects that ends on a phishing template for login credentials and also nt them an email purporting to be from the Supreme Court and claiming to deliver a subpoena for a hearing. To stay away from this users are advised take a closer look at the phrasing and grammar mistakes in the text.

ATTACK TYPE
Phishing

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

Satellite Hacking: Encryption in Space is Hard

An Oxford University-based security researcher used £270 of home television equipment to capture terabytes of real-world satellite traffic — including sensitive data from "some of the world's largest organisations." Further details will be announced by the researcher at the Black Hat event.

ATTACK TYPE
MITM

CAUSE OF ISSUE
Poor security pratice

TYPE OF LOSS
Reputation/Data

Docker Desktop Community and Enterprise finally held back from vulnerability.

Severe privilege escalation vulnerability was patched in the Windows Docker Desktop Service. Finally Docker released a new version with a patch for the vulnerability, involving the use of the SecurityIdentification impersonation level when connecting to the named pipes of spawned child processes.

ATTACK TYPE
Privilege escalation

CAUSE OF ISSUE
Security vulnerability

TYPE OF LOSS
None

Billions of Thai internet records leaks

Thailand's AIS pulled a database offline that was spilling billions of real-time internet records on millions of Thai internet users. Researchers found a database, containing DNS queries and Netflow data, on the internet without a password with access to this database, anyone could "quickly paint a picture" about what an internet user does in real-time.

ATTACK TYPE
Data leak

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

EDUCATION

EduCBA unveils Data Breach after a Hack

Online education site EduCBA started notifying customers that they are resetting their passwords after suffering a data breach. The customers are intimated strongly advised to change the passwords to a strong and unique one as well. The data breach notification doesn't include technical details about the attack, it only states that email, name, password, courses visited, etc may have been compromised

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of maintenance

TYPE OF LOSS
Reputation/Data

25 million user records Leaked by a Top-rated app

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

Mathway the most highly rated and popular apps on Android and iOS suffered a data breach of its own. A database belonging to this app was discovered for sale on a Dark Web marketplace, and the files involved include email addresses and passwords. Customers are advised to change their passwords to be safe. According to Mathway's statement, the passwords themselves were not acquired, but cryptographically protected versions of the passwords.

RETAIL

Ransomware Attack Hits A-List Celeb Law Firm

Grubman Shire Meiselas & Sacks that works with several A-list celebrities was hit by REvil ransomware attack. Hackers threatened to release the 756 gigabytes of data allegedly stolen, including non-disclosure agreements, client contracts and personal correspondence.Information allegedly stolen includes clients' phone numbers, email addresses, personal correspondence, contracts, and non-disclosure agreements made with ad and modeling firms.

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

Web hosting provider faces security lapse

ATTACK TYPE
Data leaks

CAUSE OF ISSUE
Lack of security

TYPE OF LOSS
Reputation/Data

Digital Ocean notified few customers about a security lapse that exposed some of their account details. The security leak occurred due to an internal Digital Ocean document that was mistakenly left accessible online and was accessed at least 15 times. Exposed personal details which includes email addresses, user's bandwith usage, comunication notes and the amount of money the customer paid during calendar year 2018

Banco BCR card data was exposed

The Maze ransomware gang posted payment card data stolen during a breach at Banco de Costa Rica.The crew gained access to BCR servers in February, encrypting data and stealing approximately four million unique payment card numbers. The gang intends to release the stolen data in drip feed fashion, putting pressure on the bank to pay up a ransom demand.

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Unauthorized access

TYPE OF LOSS

Reputation/Data

Biggest European bank leaks sensitive data on their website

ATTACK TYPE

Security misconfiguration

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation/Data

Santander's Belgian branch had a misconfiguration in its blog domain, allowing its files to be indexed. The researchers saw sensitive information, including an SQL dump and JSON file that can be used by hackers to potentially phish Santander's bank customers and informed them, and the company finally fixed the issue.

EasyJet affected by a massive data breach

EasyJet fell as victim to a cyber-attack, exposing email addresses and travel details of around 9 million of its customers. As a precautionary measure recommended by the ICO, the airline started contacting their affected customers to advise them to be "extra vigilant, particularly if they receive unsolicited communications."

ATTACK TYPE

Data breach

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation/Data

CONCLUSION

According to an article, if work from home is the new normal, it's time to take a long-term look at the situation and acknowledge some of those risks that are inherent in not having people in the same building under the same corporate security umbrella are going to be on going and need to be accounted for. We keep reading and listening a lot about the on going cybersecurity issues at this Covid-19 situation.

- *Are ready to face those issues? Do we have a recovery plan?*
- *Are we away from those hackers?*
- *How do I save my organization as my employees are working from different locations?*

Relax!! If you're having these questions and even more doubts regarding cyber threats we are there to help you. We assure that we will help you to keep your data safe and also give you clear information on your company's current status and what steps to be taken to stay away from any kind of cyber attack.

REFERENCES

- https://www.computing.co.uk/news/4015282/uk-electricity-middleman-elexon-hit-cyber-attack
- https://www.usnews.com/news/politics/articles/2020-05-17/transportation-agency-hacked-in-2nd-texas-government-attack
- https://www.zdnet.com/article/texas-courts-slammed-by-ransomware-attack/
- https://portswigger.net/daily-swig/taiwans-major-oil-refineries-struck-by-malware-causing-chaos-at-gas-stations
- https://krebsonsecurity.com/2020/05/europes-largest-private-hospital-operator-fresenius-hit-by-ransomware/
- https://threatpost.com/revil-ransomware-attack-celeb-law-firm/155676/
- https://www.bleepingcomputer.com/news/security/healthcare-giant-magellan-health-hit-by-ransomware-attack/
- https://www.msn.com/en-us/news/us/n-j-town-s-computers-target-of-ransomware-attack-mayor-says-town-s-website-knocked-offline/ar-BB146k6F?ocid=hplocalnews&srcref=rss
- https://thehackernews.com/2020/05/saltstack-rce-vulnerability.html
- https://thehackernews.com/2020/05/saltstack-rce-exploit.html
- https://www.zdnet.com/article/digital-ocean-says-it-exposed-customer-data-after-it-left-an-internal-doc-online/
- https://thehackernews.com/2020/05/android-firebase-database-security.html
- https://www.2-spyware.com/natura-cosmetics-data-breach-a-quarter-of-a-million-customers-exposed
- https://thehackernews.com/2020/05/easyjet-data-breach-hacking.html
- https://thehackernews.com/2020/05/hacking-bluetooth-vulnerability.html
- https://www.bleepingcomputer.com/news/security/online-education-site-educba-discloses-data-breach-after-hack/
- https://techcrunch.com/2020/05/24/thai-billions-internet-records-leak/
- https://www.zdnet.com/article/privilege-escalation-vulnerability-patched-in-docker-desktop-for-windows/?&web_view=true
- https://www.komando.com/news/leaks-25-million-user-records/739833/
- https://www.cbronline.com/news/satellite-hacking?&web_view=true
- https://www.indiatoday.in/technology/news/story/personal-data-of-millions-of-truecaller-users-available-on-dark-web-1531969-2019-05-22
- https://www.finextra.com/newsarticle/35891/maze-ransomware-gang-leak-banco-bcr-card-data
- https://cybernews.com/security/one-of-biggest-european-banks-leaking-sensitive-data-on-website/
- https://www.zdnet.com/article/thousands-of-israeli-sites-defaced-with-code-seeking-permission-to-access-users-webcams/?&web_view=true
- https://www.zdnet.com/article/hundreds-of-thousands-of-qnap-devices-vulnerable-to-remote-takeover-attacks/
- https://www.thehindu.com/news/national/ethical-hacker-robert-baptiste-elliot-alderson-sees-security-flaws-in-aarogya-setu/article31515292.ece
- https://www.bleepingcomputer.com/news/security/office-365-phishing-uses-supreme-court-theme-and-working-captcha/?&web_view=true

YOU MAY ALSO BE INTERESTED IN OUR PREVIOUS WORKS

FEEL FREE TO REACH US FOR ALL YOUR CYBERSECURITY ASSESSMENT

contact@briskinfosec.com | www.briskinfosec.com

Affiliated by

Awards

10 MOST PROMISING CYBERSECURITY SOLUTION PROVIDER 2019

THE LEADERS GLOBE
THE MOST POWERFUL CYBER SECURITY SOLUTION PROVIDER