THREATSPLOIT

JULY 2019

EDITION 11

PREPARED BY

WWW.BRISKINFOSEC.COM

This organization is empaneled by CERT-In for providing information security auditing service.

PREPARED BY

WWW.NCDRC.RES.IN.

NCDRC
(National Cyber Defence
Research Centre)
in collabration with
BINT Lab

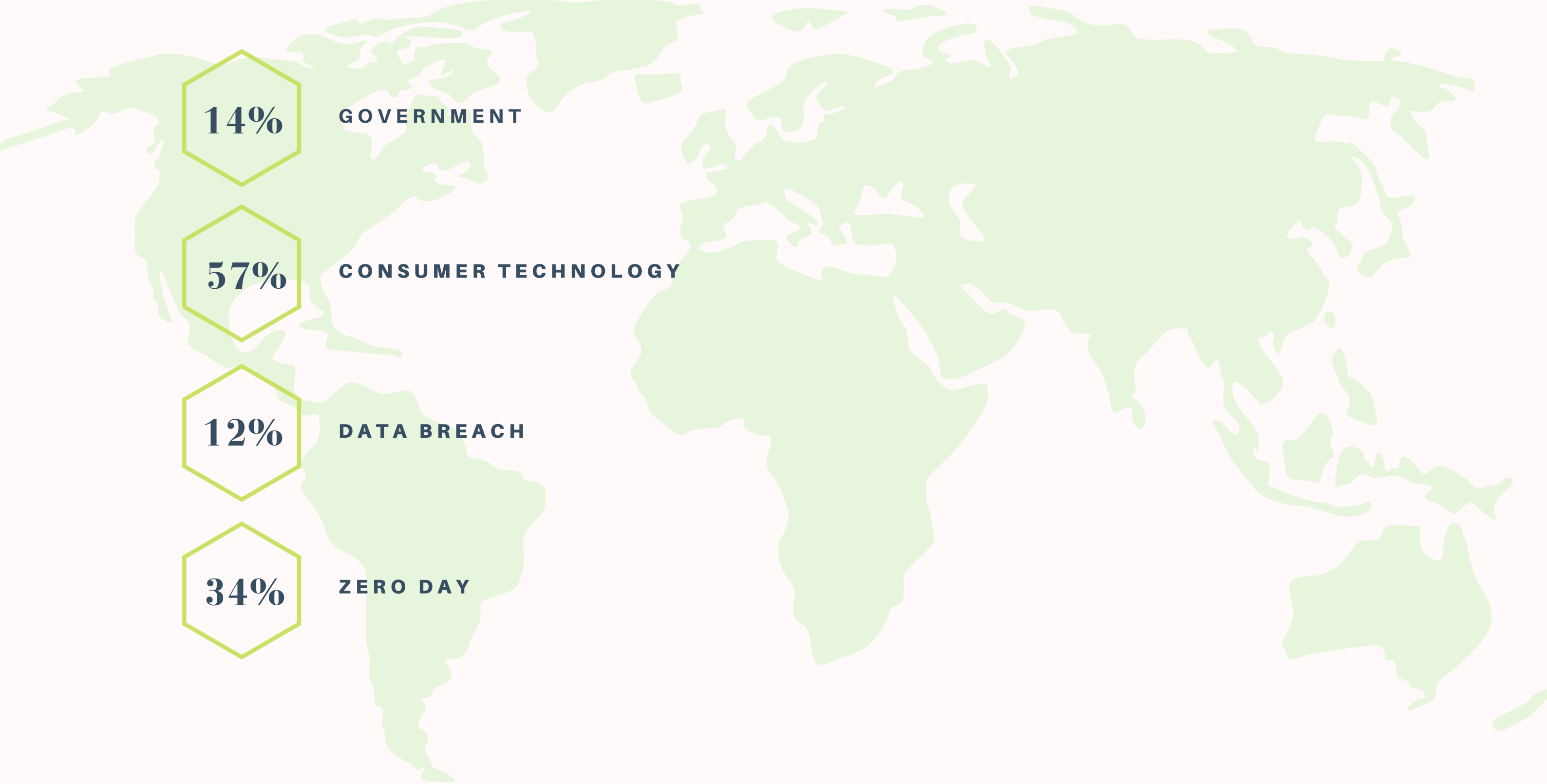
INTRODUCTION

Hi. If you've wanted to cherish some important and interesting happenings in the domain of cybersecurity, you can whistle as you've landed in the right place. Hearty welcome to our Threatsploit Adversary report which contains the collection of the globally happened cyberattacks, its impacts, the losses faced by companies and much more. My humble request to you is if you're a novice, basic ideas on some dreadful attacks are given.
Please have a walk-through:

Ransomware – An attack that encrypts data and demands ransom (money) to bring it back to normal.
Dos (Denial-of-Attacks) – Multiple requests from a single source to crash or deface a server/database.
DDoS (Distributed Denial-of-Service) – Multiple requests from multiple sources to crash or deface a server/database.
RCE – Remote Code Exploitation (An exploitation attack from somewhere done to access your system).

Phishing - A luring email/link sent with malicious intent in order to deceive and extract your data.
Zero-day exploit – An attack that's exploited immediately ever since it got deployed.

Over years, there have been massive occurrences of cyber attacks everywhere. Almost all sectors have joined the victim list of cyber breaches. Amongst them, few have been able to seek their redemption with the help of cybersecurity professionals. Many, still keep yearning with hope to get manumitted from breaches. Why and how do these happen? What's the cause for such security calamities. Just read through our report to acknowledge it!



14% GOVERNMENT

57% CONSUMER TECHNOLOGY

12% DATA BREACH

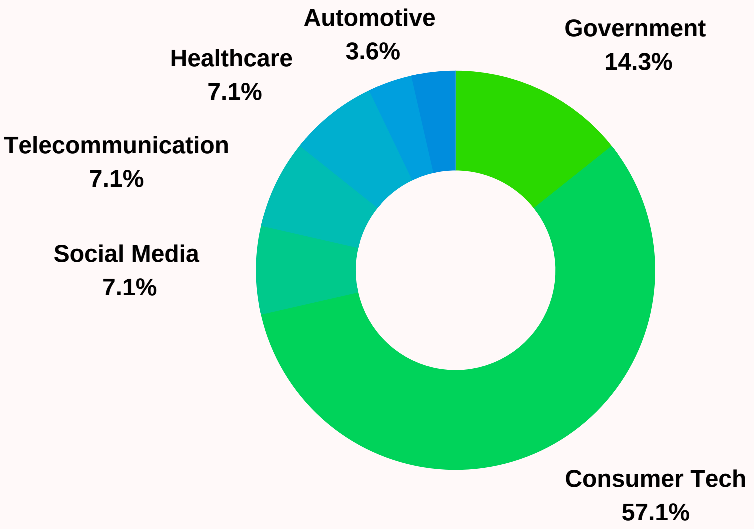
34% ZERO DAY

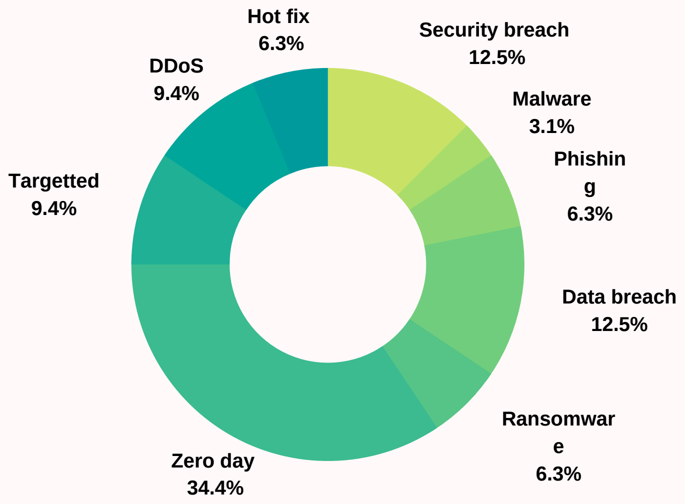
Sectors affected by Attacks

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 Consumer Technology has been hit the most.

Types of Attack Vectors

There's a pictorial representation below that indicates the percentage of nefarious cyber attacks that've broken organizations security mechanisms. Among all, Zero-day attack is the one that's occurred the most.





GOVERNMENT

- NASA Lab Hacked Using A $25 Raspberry Pi Computer
- IFMIS, JSC, NYS, Immigration Among 17 Government Websites Hacked
- Data Breach Probe Launched Into Potential Parliament hack
- Hit by Ransomware Attack, Florida City Agrees to Pay Hackers $600,000

CONSUMER TECHNOLOGY

- Dell Discovers Yet Another 'SupportAssist' Security Flaw
- New Vulnerabilities may let hackers remotely SACK Linux and FreeBSD System
- Mozilla Firefox 67.0.3 Patches actively exploited Zero-Day
- VLC Player gets Patched for Two High-Severity Bugs
- Oracle fixes Critical Bug in WebLogic Server Web Services
- Phishing Attack Exposes Data of 645,000 Oregon DHS Clients
- Microsoft Outlook for Android Open to XSS Attacks
- 'Emuparadise' gaming emulator website suffers data breach
- Ohio Provider Pays $75K Ransom After Serious Hack on IT System
- Microsoft's June 2019 Patch Tuesday fixes many of SandboxEscaper's zero-days
- Telegram Briefly Taken Offline in “Powerful” DDoS Attack
- Ubisoft Games Hit by Massive DDoS Attacks
- Remote attack flaw found in IPTV streaming service
- Remote Desktop Zero-Day Bug Allows Attackers to Hijack Sessions
- MacOS Zero-Day Allows Trusted Apps to Run Malicious Code
- Hackers use Firefox ‘Zero-day’ bug to attack against Coinbase employees
- EA Origin security flaw potentially exposed data of 300 million players
- TCS was hacked for its clients by China’s cyber spy campaign
- New Exploit for Microsoft Excel Power Query

DEFENCE

- Targeted strike on computer-controlled weapons of Iran

SOCIAL MEDIA

- Turkish group hacks Amitabh Bachchan's Twitter account
- Singer Adnan Sami's Twitter account hacked

TELECOMMUNICATION

- For two hours, a large chunk of European mobile traffic was rerouted through China
- Putin Q&A session call center hit by DDoS attack

HEALTHCARE

- Widely used medical infusion pump can be remotely hijacked
- AMCA data breach has now gone over the 20 million mark

AUTOMOTIVE

- Aircraft Parts Manufacturer halts operations after Ransomware Attack

BANKING AND FINANCE

- Almost 100,000 Australians' private details exposed in attack on Westpac's PayID

NASA Lab Hacked Using A $25 Raspberry Pi Computer

The Jet Propulsion Laboratory (JPL) of NASA had been hacked and about 500 MB of data was stolen from Major Mission Systems (MMS) as well from Deep Space Network (DSN). Upon investigation, it was identified that a tiny software device named 'Raspberry pi' was used to gain access, confirms the Federal report. The cause for this is said to be the failure in updating the inventory system. However, it's shocking to acknowledge that even one of the world's most renowned organization isn't escaping from cyber threats, due to fragile security prevalence. Finally, somehow the shortcomings were dealt.

ATTACK TYPE
Security breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

IFMIS, JSC, NYS, Immigration Among 17 Government Websites Hacked

ATTACK TYPE
Security breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
KENYA

Kurd Electronic Team, an Indonesian hacker group, have seized the systems of Integrated Financial Management and Information System (IFMIS) portal, and other governmental websites. The hacked websites were on servers powered by Unix based Free BSD operating system. However, the government was able to regain control of its systems and apologized to its people for such inadequate security practices.

Data breach probe launched into potential Parliament hack

Officials at the Houses of Parliament seemed disturbed after sensing a breach occurrence in its website. The cyber forensics were informed and they scrutinized the parliament's web page at the 'Palace of Westminster'. They identified that the confidential bills of Parliament were exposed and even the passwords to access it were available. Notably, these things shouldn't be meant for public viewing, but unfortunately were. A spokesperson said, intense investigation is ongoing to fix this flaw.

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
UK

Hit by Ransomware Attack, Florida City Agrees to Pay Hackers $600,000

ATTACK TYPE
Malware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Riviera beach, a small city in Miami, is now the recent victim of another grotesque ransomware attack. To regain normality, the hackers demanded 65 Bitcoin that sums up to $592,000. This attack happened on 29th May 2019 and became visible, after a police department employee inadvertently opened a corrupted email attachment. The city's spokeswoman, Rose Brown, informed the public that Rivera beach is intensely working with the law enforcement, to resolve this issue ASAP.

Dell Discovers Yet Another 'SupportAssist' Security Flaw

Dell's 'SupportAssist' troubleshooting PC utility was found to be vulnerable to attacks that could compromise all the Dell systems, as well allow both malware and rogue logged-in users. Dell has issued updated versions of the software and urged its customers to update the PC utility as soon as possible. Automatic updates are typically enabled by default but if that fails, users can download the latest versions of the software from Dell's website.

ATTACK TYPE
Zero day

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

New vulnerabilities may let hackers remotely SACK Linux and FreeBSD system

A Denial of Service flaw was found in the recent Linux kernels that can be exploited by remote attackers to trigger a kernel panic in vulnerable systems. Netflix Information Security Folk, Jonathan Looney, found three Linux vulnerabilities. To mitigate this, users should disable SACK processing on the system or block connections with a low MSS, using the filters. The second mitigation measure will only be effective when TCP probing is also disabled.

ATTACK TYPE
Zero day

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

Mozilla Firefox 67.0.3 Patches Actively Exploited Zero-Day

Mozilla released Firefox 67.0.3 and Firefox ESR 60.7.1 to patch an actively exploited and critical security vulnerability that could allow attackers to remotely execute arbitrary codes on machines running vulnerable Firefox versions. The Firefox and Firefox ESR Zero-day flaw that's fixed by Mozilla was also reported by Google Project Zero's Samuel Groß and the Coinbase Security team.

ATTACK TYPE
Zero day

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

VLC Player Gets Patched for Two High-Severity Bugs

Maintainers of the popular open-source VLC media player patched two high-severity bugs on a Friday of June. The flaws were an 'out-of-bound write' vulnerability and a 'stack-buffer-overflow' bug. Apropos of this, VideoLAN developers said the patches for other 33 bugs were also issued. The updated VLC 3.0.7 version, also included the patching of 21 medium security issues and 20 low security issues.

ATTACK TYPE
Zero day

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

CONSUMER TECHNOLOGY

Oracle Fixes Critical Bug in WebLogic Server Web Services

Oracle issued a patch for remote code vulnerability (CVE-2019-2729) that is being actively used in the attacks, says the researchers. This vulnerability was used to launch ransomware and mining attacks. This was first reported by Badcode, knownsec's 404 member. Two mitigation measures are instructed by researchers. They are:

- Delete "wls9_async_response.war" and "wls-wsat.war" then restart the WebLogic service
- Enforce access policy controls for URL access to the paths "/_async/*" and "/wls-wsat/*

ATTACK TYPE

Zero day

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation/Data

COUNTRY

USA

Phishing Attack Exposes Data of 645,000 Oregon DHS Clients

ATTACK TYPE

Phishing

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation/Data

COUNTRY

USA

The Department of Human Services (DHS) notified over half a million clients about their personal data leakage due a data breach. The breach was identified when 9 employees inadvertently opened a phishing email that gave intruders access to mailboxes. Password reset stopped the hacker from further accessing the compromised email accounts. Further, an investigation confirmed that no malware was planted on the computer network.

Microsoft Outlook for Android Open to XSS Attacks

Microsoft patched a vulnerability (CVE-2019-1105) in Microsoft Outlook for Android that stimulates XSS attacks. The software giant said it as a spoofing vulnerability that sends specially crafted emails to the targets. If the victim clicks the link, the malicious file gets over there. As a remediation, Microsoft urged its users to update its applications ASAP and also to verify, whether the URL seems legal or suspicious.

ATTACK TYPE

Spoofing vulnerability

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation/Data

COUNTRY

USA

Emuparadise gaming emulator website suffers data breach

ATTACK TYPE

Data breach

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation/Data

COUNTRY

GLOBAL

Emuparadise – a popular retro gaming website offering ROM's has become a victim of data breach by letting out 1.1 million user accounts. This was discovered by using a website, 'HaveIBeenPwned'. The compromised data included email addresses, IP addresses, usernames and hashed passwords using MD5 generator. It's said that Emuparadise's 'vBulletin forum' is the source of leak. As an awareness, cyber folks have advised to use unique set of password credentials while using every online account.

Ohio Provider Pays $75K Ransom After Serious Hack on IT System

On 14th June 2019, NEO Urology in Ohio, has been affected by a ransomware attack that crippled its IT systems and encrypted its data. The company reached out a forensic department and they've identified the attack to have risen from Russia. A ransom of $75,000 was paid to hackers for restoring their systems. To be mentioned, the hack was so intense that it consumed 3 days for the company to land in to the state of being normal.

ATTACK TYPE
Ransomware

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
USA

Microsoft's June 2019 Patch Tuesday fixes many of SandboxEscaper's zero-days

21 critical vulnerabilities amongst 88 other vulnerabilities have been patched by the King OS maker 'Microsoft' on June 2019. Apropos of that, 4 out of 5 zero-day exploits that were published online by an exploit seller named 'SandboxEscaper', were also patched. Apart from Windows and Office products, patches even for other significant flaws were launched. The most gracious factor overall was that, none of these exploits were exploited in the wild.

Telegram Briefly Taken Offline in a "Powerful" DDoS Attack

A predominantly used communicating medium, Telegram, has been hit by a severe DDoS (Distributed Denial of Service) attack. However, the company which enjoys a merit of having 200 million monthly users, swore to its customers that their data was secure. However, this problem was fixed and the service was back to being normal.

ATTACK TYPE
DDoS

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
RUSSIA

ATTACK TYPE
DDoS

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
FRANCE

Ubisoft Games Hit by Massive DDoS Attacks

Ubisoft, a gaming company has been struck by a series of Distributed Denial-of-Service (DDoS) attacks. This has scalped the server connectivity of a game named 'Phantom sight'. Its truly disappointing that many wouldn't be able to play the game until the prolongment of this adversity ends. The gang behind this breach remains still unknown. However, efforts are in underway to fix this issue.

CONSUMER TECHNOLOGY

Remote attack flaw found in IPTV streaming service

A critical remote execution flaw has been detected in one of the Ukrainian TV streaming device manufacturer, which when exploited, seizes the streaming flow and could make it go haywire. Infomir - Ukrainian IPTV (Internet Protocol Television), OTT - (Over The Top) and VOD – (Video on Demand), all these 3 streaming providers were the source of the flaw. All these required authentication to access but a logic problem removed its protection. Efforts are being invested to resolve this issue.

ATTACK TYPE

Zero day

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation/Data

COUNTRY

GLOBAL

Remote Desktop Zero-Day Bug Allows Attackers to Hijack Sessions

ATTACK TYPE

Zero day

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation/Data

COUNTRY

USA

A Zero-day vulnerability that could exploit Remote Desktop Services has been disclosed. Through this flaw, the lock screen of Windows machine could be bypassed despite the usage of 2FA. (Two Factor Authentication). This vulnerability is named as CVE-2019-9510 with an alias, Authentication bypass vulnerability. This was first discovered by Joe Tammariello, from Carnegie Mellon University. Also, Microsoft was informed about this issue.

MacOS Zero-Day Allows Trusted Apps to Run Malicious Code

MacOS researcher, Patrick Wardle, has identified zero-day flaw in Apple's Mojave operating system which allows hackers to run malicious codes on their systems. The main reason for this is Mojave applications verification mechanism was 100% improper. This attack also allows intruder to trigger synthetic mouse clicks on Mojave that could corrupt systems and disclose the GPS coordinates of a user's computer. However, Apple hasn't fixed this issue yet.

ATTACK TYPE

Zero day

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation/Data

COUNTRY

USA

Hackers use Firefox 'Zero-day' bug to attack against Coinbase employees

ATTACK TYPE

Zero day

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation/Data

COUNTRY

GLOBAL

Web browser company 'Mozilla' said that they've patched the Firefox vulnerability. Coinbase security researcher, Samuel D. Gross, discovered a Zero-day vulnerability in Firefox through which cyber attacks can be launched using JavaScript objects. Also, it can be exploited for launching UXSS (Universal cross-site scripting attacks). However, Mozilla has released its latest version and has urged its users to update it ASAP.

EA Origin security flaw potentially exposed data of 300 million players

Security researchers have identified a 'chain of vulnerabilities' that could possibly compromise the user accounts of Electronic Arts Origin, a Gaming Company. Security veterans have said that the cause for this attack is due to the security loophole that's present in the Origin's cloud environment. A sub-domain was possible to be inserted in that gap. However, the gaming company was able to provide a fix for this issue without much delay.

ATTACK TYPE

Data exposure

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation/Data

COUNTRY

USA

CONSUMER TECHNOLOGY

TCS was hacked for its clients by China's cyber spy campaign

ATTACK TYPE

Phishing

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation/Data

COUNTRY

INDIA

Tata Consultancy Services (TCS) recently became a victim of Chinese hacking campaign 'Operation Cloud Hopper'. However, TCS isn't the only victim. IBM, Hewlett Packard and many others have also been victim of this, for years without knowing it. In order to infiltrate the service provider's server, 'spear phishing emails' were used. Security experts traced the footholds of hackers and eliminated the malicious files one-by-one. But, the conspirators have re-arrived, in a stronger and spectacular fashion now.

New Exploit for Microsoft Excel Power Query

Mimecast Services security researchers have discovered a vulnerability in MS Excel, that can probably harm 120 million users. The vulnerability takes advantage of Power Query function in Excel, through which the data can be pulled. Also, the vulnerability can allow malwares to be infiltrated into the system. As a remedy, Microsoft urged it's users to disable DDE feature while it's dormant, for blocking 3rd party connections. However, a good thing is, this vulnerability hasn't been exploited in the wild.

ATTACK TYPE

Zero day

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation/Data

COUNTRY

USA

DEFENCE

Targeted strike on computer-controlled weapons of Iran

ATTACK TYPE

Security breach

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation/Data

COUNTRY

IRAN

The systems of Iran's 'Islamic Revolutionary Guard Corps' have been disabled by the offensive cyber strike of U.S, which has even been approved by the U.S President, Mr. Donald Trump. This attack was initially meant to be through missiles. Envisioning the physical annihilation, it was backtracked and done through cyber attacks. However, this is one such incident proving the undying bad blood that's flowing between the U.S and Iran.

SOCIALMEDIA

Turkish group hacks Amitabh Bachchan's Twitter account

Ayyildiz Tim, a hacker group with half Pakistan-Turkish descent have hacked the twitter account of Bollywood's greatest legend Mr. Amitabh Bachchan. They've altered various social media data of Mr. Amitabh. They've also issued a warning, stating that "The Muslims in India whom are tormented during Ramadan will soon be getting the taste of hell." Regarding this, the Mumbai police informed the cyber crime department and they've fixed this issue swiftly.

ATTACK TYPE

Media Target

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation/Data

COUNTRY

INDIA

Singer Adnan Sami's Twitter account hacked

Following the social media hack of Mr. Amitabh Bachchan, the next to fall on the victim list is the prominent singer, Mr. Adnan Sami. The singer's profile photo was replaced with the Prime Minister of Pakistan, Imran Khan. They've also changed the singer's bio and replaced it as 'Ayyildiz Tim Loves Pakistan.' However, the cyber crime department have caught sight of this issue and are working on it.

ATTACK TYPE

Media Target

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation/Data

COUNTRY

INDIA

TELECOMMUNICATION

For two hours, a large chunk of European mobile traffic was rerouted through China

On June 6th 2019, a massive chunk of European mobile traffic was rerouted through the infrastructure of 'China Telecom', the 3rd largest Chinese ISP provider. The cause of this incident is due to BGP (Border Gateway Protocol) route leak at Swiss data center that leaked over 70,000 routes from its internal routing table to the Chinese ISP. However, some safety measures were provided by the providers, in order to prevent collision of other networks.

ATTACK TYPE

Targeted

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation/Data

COUNTRY

EUROPEAN COUNTRIES

Putin Q&A session call center hit by DDoS attack

One of the Moscow's call center where it's honorable president Mr. Vladimur Putin, was having a live Q&A session was subjected to DDoS attacks. This attack has surged from Ukraine, says Margarita Simonyan (Sputnik and RT Editor-in-Chief). Finally, the attack has been nullified and the systems were back to being normal. Since then, security has become a prime concern for Russian Government.

ATTACK TYPE

DDoS

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation/Data

COUNTRY

RUSSIA

HEALTHCARE

Widely used medical infusion pump can be remotely hijacked

A workstation that's used hugely in many hospitals and other places to dock an infusion pump has been detected with security flaws through which exploitation and controlling can be done, says the security researchers at security firm 'CyberMDX'. By using this, the attackers could install malicious codes and even control the system operations. There are about 50 companies that use such devices. However, these aren't used in USA.

ATTACK TYPE
Zero day

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

AMCA data breach has now gone over the 20 million mark

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

American Medical Collective Agency (AMCA), a company that provides billing services to the US healthcare sector and other distinct customers, has shockingly exposed the personal and financial information of over 20 million Americans. The exposed data contained names, home addresses, bank account details and much more. This, in no way, is good for AMCA as lawsuits have been filled and a hard hitting penalty is bound to strike them from the courts.

AUTOMOTIVE

Aircraft Parts Manufacturer Halts Operations After Ransomware Attack

Asco - a Belgium company that's a significant supplier of parts to worldwide airline manufacturers has been shut down due to a notorious cyberattack. According to the company, the operations in Belgium, Germany, Canada and U.S have been scalped and more than 1400 employees became jobless. Rumors have been spreading like 'it's a kind of ransomware' but official statement by the company is yet to be made.

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
BELGIUM

BANKING AND FINANCE

Almost 100,000 Australians' private details exposed in attack on Westpac's PayID

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
AUSTRALIA

The private details of about 100,000 Australian bank customers have been exposed through a money transfer app named 'PayID'. The attack commenced in Westpac and has affected many banks over there. Cyber security professionals have issued a warning that stolen mobile numbers and other data could've been misused on a massive scale. However, the company's spokesman says, "Preventive measures are being taken to contain the incident."

REFERENCES

- https://fossbytes.com/nasa-lab-hacked-raspberry-pi/
- https://www.kahawatungu.com/2019/06/03/ifmis-jsc-nys-websites-hacked/
- https://gdpr.report/news/2019/06/18/parliament-hack/
- https://www.nytimes.com/2019/06/19/us/florida-riviera-beach-hacking-ransom.html
- https://www.tomshardware.com/news/dell-supportassist-cyber-security-flaw-pc,39700.html
- https://arstechnica.com/information-technology/2019/06/new-vulnerabilities-may-let-hackers-remotely-sack-linux-and-freebsd-systems/
- https://www.bleepingcomputer.com/news/security/mozilla-firefox-6703-patches-actively-exploited-zero-day/
- https://threatpost.com/vlc-player-gets-patched-for-two-high-severity-bugs/145518/
- https://www.bleepingcomputer.com/news/security/oracle-fixes-critical-bug-in-weblogic-server-web-services/
- https://www.bleepingcomputer.com/news/security/phishing-attack-exposes-data-of-645-000-oregon-dhs-clients/
- https://threatpost.com/microsoft-outlook-android-xss/145924/
- https://www.zdnet.com/article/emuparadise-gaming-rom-repository-suffers-data-breach/
- https://healthitsecurity.com/news/ohio-provider-pays-75k-ransom-after-serious-hack-on-it-system
- https://www.zdnet.com/article/microsofts-june-2019-patch-tuesday-fixes-many-of-sandboxescapers-zero-days/
- https://www.cbronline.com/news/telegram-down
- https://dotesports.com/rainbow-6/news/ubisoft-hit-with-string-of-ddos-attacks-just-as-r6s-operation-phantom-sight-goes-live
- https://www.zdnet.com/article/remote-attack-flaw-found-in-iptv-streaming-service/
- https://www.informationsecuritybuzz.com/expert-comments/expert-advice-on-attackers-bypassing-microsoft-rdp/
- https://threatpost.com/macos-zero-day-malicious-code/145259/
- https://www.cisomag.com/hackers-use-firefox-zero-day-bug-to-attack-against-coinbase-employees/
- https://www.businesstoday.in/technology/news/turkish-hacker-group-hacks-amitabh-bachchan-twitter-account-posts-anti-india-tweets/story/355080.html
- https://www.timesnownews.com/entertainment/news/people/article/after-amitabh-bachchan-singer-adnan-samis-twitter-account-hacked/434938
- https://www.zdnet.com/article/for-two-hours-a-large-chunk-of-european-mobile-traffic-was-rerouted-through-china/
- https://www.urdupoint.com/en/world/powerful-foreign-ddos-attack-hits-putin-qa-s-649693.html
- https://techcrunch.com/2019/06/13/alaris-infusion-pump-security-flaws/
- https://www.zdnet.com/article/medical-debt-collector-amca-files-for-bankruptcy-protection-after-data-breach/
- https://www.darkreading.com/attacks-breaches/cyberattack-hits-aircraft-parts-manufacturer/d/d-id/1334964
- https://www.smh.com.au/business/banking-and-finance/australians-private-details-exposed-in-attack-on-westpac-s-payid-20190603-p51u2u.html

CONCLUSION

Cyberattacks most notably Ransomware, Phishing, DoS, DDoS, Remote Code Exploitation and Zero-day exploit are being predominantly seen as the most daunting ones. 5 out of 6 cyberattacks are either one among these. In-order to stay resilient against the above and other related threats, newest defensive mechanisms are being deployed in the wild. Yet, these attacks only keep proliferating with time. More than 95% of people, till now, have an insignificant understanding of what cyber security actually is. They think it as a responsibility which once when given to the cyber security vendor, is no longer a concern to be thought about. But, this isn't true at all. It is and has ever been a shared responsibility.

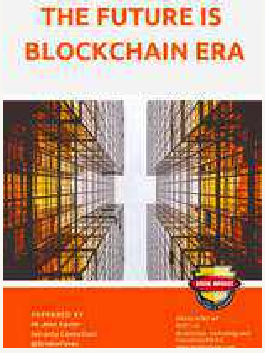
"APPLICATION SECURITY SHOULD BE A SHARED RESPONSIBILITY RATHER THAN CONSIDERING AS THE CLOUD'S RESPONSIBILITY"

Organizations vary considerably based on their maturity quotient, but also in the way they respond towards their cyber security concerns. Very few stay coherent with the daily happenings of cyber security and hence are able predestine the incoming attacks that are bound to strike their organizations. As a precautionary, they take up a proactive approach. While others, unafraid about the consequences of maintaining fragile security mechanisms, unfortunately when tarnished by cyber attacks, follow a reactive approach. However, we as a cyber security organization, would suggest a proactive approach. However, a proactive approach doesn't mean complete protection but it's a far better choice over reactive approach.

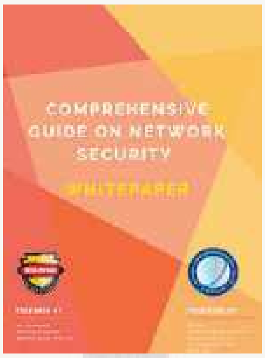
Most organisations require proper guidance from a competent cybersecurity organization to sort out the security issues in a swift and reliable manner. However, living in the midst of a money-driven world, it isn't easy to perceive sight of trusted organisations. Hence, reaching out to a genuine company is immeasurably important.

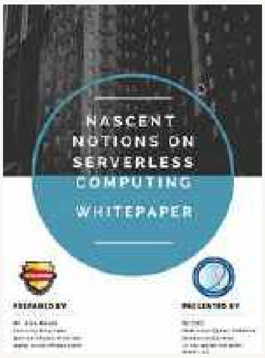
We, Briskinfosec, are a cybersecurity company that strives exclusively to fulfill the 360 degree cybersecurity requirements of people. We'll never take your needs for granted as we know the value of every data. All we want is to just provide you the best cybersecurity experience, thereby earning the name as your 'Cybersecurity favourite'. To know more, reach us out anytime over contact@briskinfosec.com.

YOU MAY BE INTERESTED ON OUR WHITEPAPERS

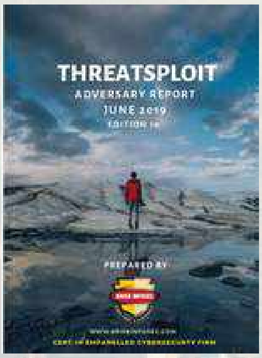

THE FUTURE IS BLOCKCHAIN ERA

BRISKINFOSEC PENTEST TOOLKIT WHITEPAPER

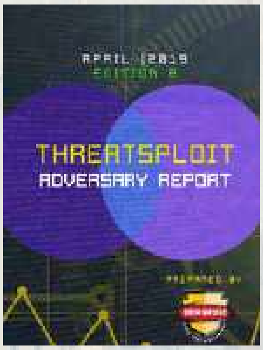

COMPREHENSIVE GUIDE ON NETWORK SECURITY WHITEPAPER


NASCENT NOTIONS ON SERVERLESS COMPUTING WHITEPAPER

YOU MAY ALSO BE INTERESTED ON OUR PREVIOUS WORKS

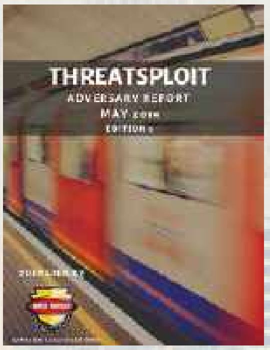

THREATSPLOIT ADVERSARY REPORT JUNE 2019

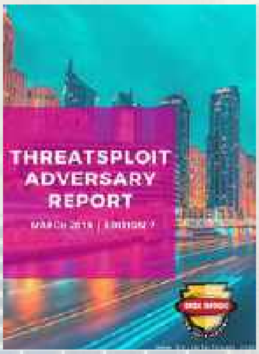
PREPARED BY


APRIL 2019 EDITION 8

THREATSPLOIT ADVERSARY REPORT

PREPARED BY


THREATSPLOIT ADVERSARY REPORT MAY 2019

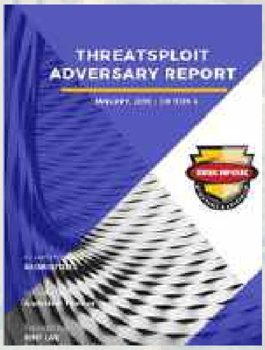

THREATSPLOIT ADVERSARY REPORT

MARCH 2019 | EDITION 7

FEB 2019

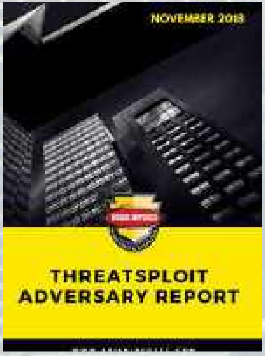
THREATSPLOIT ADVERSARY REPORT

PREPARED BY


THREATSPLOIT ADVERSARY REPORT

DECEMBER 2018

THREATSPLOIT ADVERSARY REPORT


NOVEMBER 2018

THREATSPLOIT ADVERSARY REPORT

REFERENCES ABOUT BRISKINFOSEC

CASE STUDIES

SOLUTIONS

SERVICES

RESEARCH

COMPLIANCES

BLOGS

BRISK INFOSEC

CYBER TRUST & ASSURANCE

FEEL FREE TO REACH US FOR ALL YOUR CYBERSECURITY NEEDS

contact@briskinfosec.com | www.briskinfosec.com