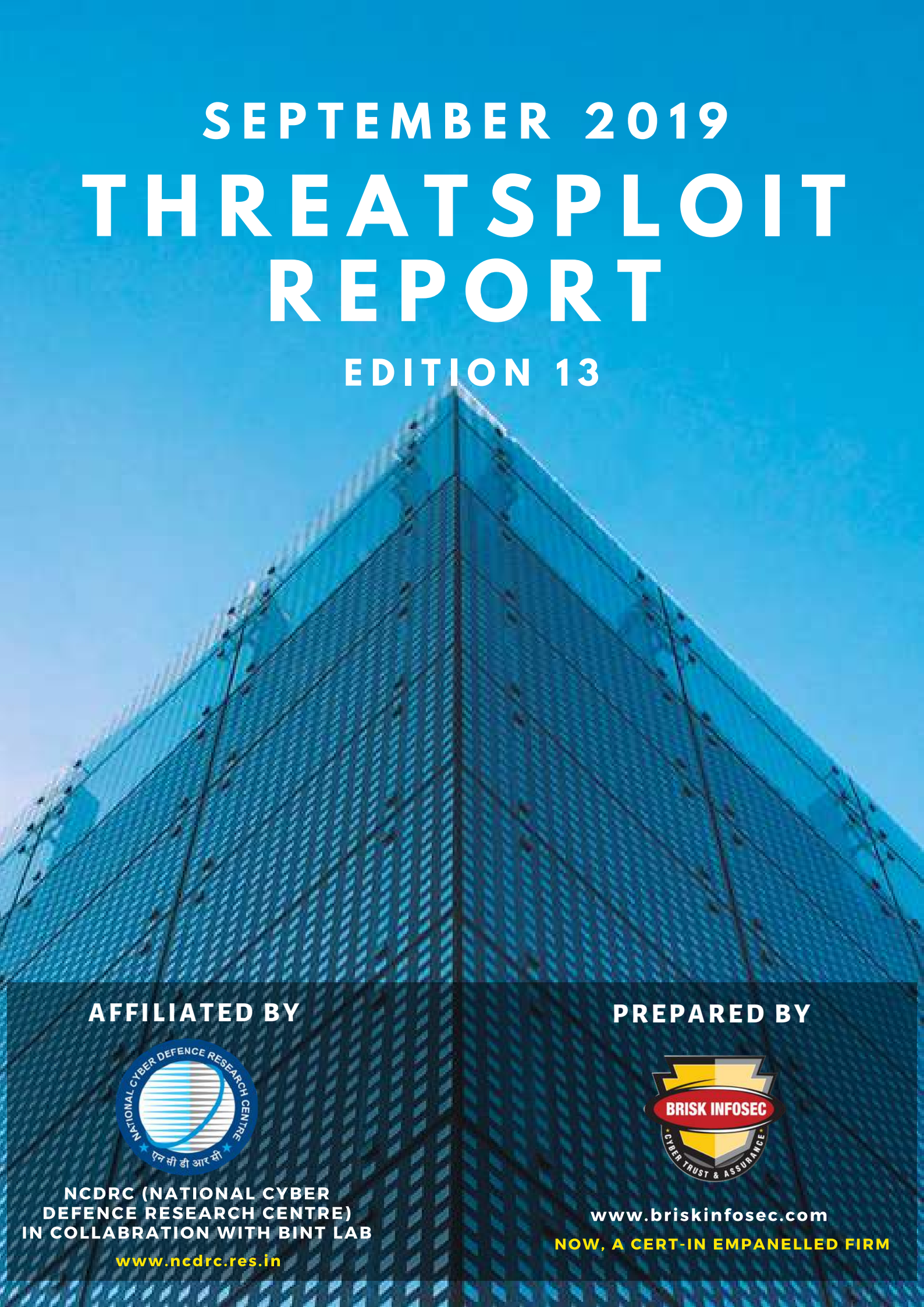


SEPTEMBER 2019

THREATSPLOIT REPORT

EDITION 13

AFFILIATED BY

NCDRC (NATIONAL CYBER DEFENCE RESEARCH CENTRE) IN COLLABRATION WITH BINT LAB

www.ncdrc.res.in

PREPARED BY

BRISK INFOSEC

CYBER TRUST & ASSURANCE

www.briskinfosec.com

NOW, A CERT-IN EMPANELLED FIRM

INTRODUCTION

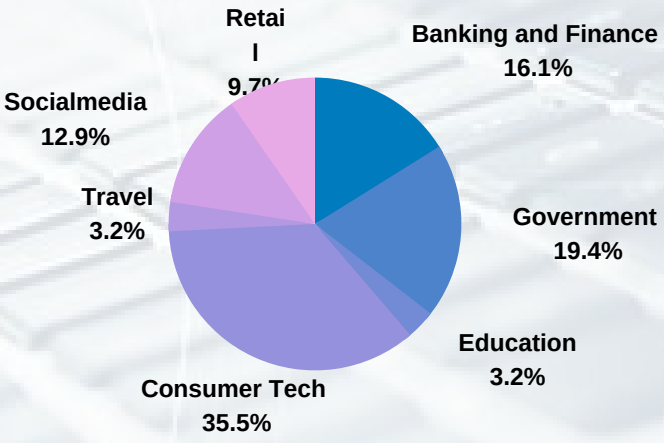
First and foremost, an earnest thanks to all of you from Briskinfosec! It's your continued support and significant feedback's that has helped us to accomplish and celebrate 1 year anniversary of our Threatsploit Reports. This new report containing the globally occurred cyberattacks on the month of August 2019, is the 13th edition. From the bottom of our hearts, once again, thank you for the continued support. Forever, we're grateful for it!

World has evolved; technology has evolved; people's lifestyle has evolved; their approach towards buying and paying for something has evolved (from analog to digital style). Alongside these, cyber threats have also evolved in a spectacular fashion. But, infinite human's attitude and approach towards cyber security hasn't evolved yet.

They're still comfortable in believing the outdated and sunk notion that a firewall, antivirus, an automated scan and one time security products purchase are more than enough to uphold their data security.
Also, these are the ones that organizations are still practicing to secure their data. That's why most of them have been in the hot news as one among the countless hacking victims. To know on how the cyberattacks have played out, the companies and nations affected and much more, just scroll down to check them out.

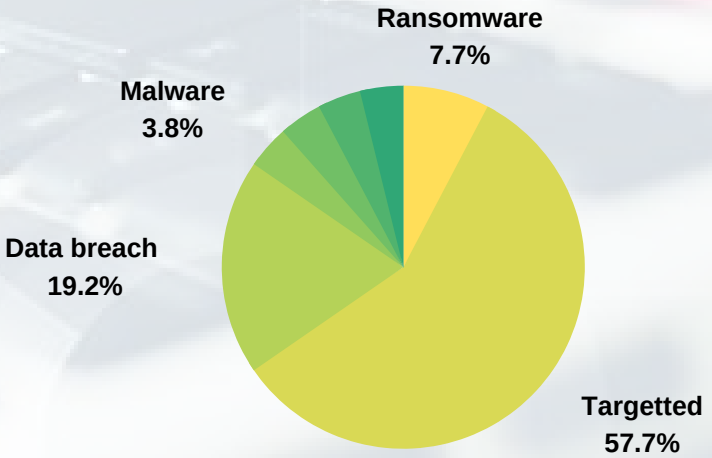
Sectors affected by Attacks

Below, there's Pie-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 has been hit the most.



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.



1 BANKING AND FINANCE

- European Central Bank Breach: ECB Confirms Hack And Shuts Down Website
- Westpac explains what to do if you've been caught up in a bank breach
- Mastercard says German Priceless Specials loyalty program breached
- Cyber Club Hacks Into First Microfinance Bank Of Pakistan Website, Posts Respect To Indian Bravehearts And Martyrs
- NASA Astronaut Accused Of Hacking Bank Account From Space

2 GOVERNMENT

- Murfreesboro water department website hacked
- Hacked Texas government agencies face $2.5 million ransom
- Charleston County suffers data breach impacting more than 800 employees
- Bihar Govt website hacked, hackers post message praising Pakistan
- City of Tyler website hacked by anti-government group
- Serious privacy breach at Ministry for Culture and Heritage

3 EDUCATION

- Amity University website hacked; Placement page asks for jobs at Porn sites

4 CONSUMER TECH

- Google Discloses 20-Year-Old Unpatched Flaw Affecting All Versions of Windows
- KDE Linux Desktops Are Vulnerable To Hack
- DSLR Cameras Can Be Infected With Ransomware
- KNOB Attack exploits Bluetooth spec flaw to spy on device connections
- Kern County suffers data breach compromising over 15000 employees' personal information
- WARNING — Malware Found in CamScanner Android App With 100+ Million Users
- Attackers are targeting vulnerable Fortigate and Pulse Secure SSL VPNs
- Two new Dragonblood vulnerabilities discovered in Wi-Fi WPA3 standard
- Newly discovered QualPwn vulnerability affects devices with Qualcomm chips
- Severe zero-day security flaw discovered in Steam
- Update your LibreOffice because 2 patches have been bypassed

5 TRAVEL

- Nigerian airline company, Aero Contractors website hacked by allegedly ISIS-tied group

6 SOCIALMEDIA

- BigJigglyPanda Twitter account hacked and compromised for over seven hours after another alleged AT&T error
- Curtis Pritchard's Instagram hacked
- Ellen DeGeneres Says Instagram Account Briefly Hacked Overnight With Phony Giveaways
- Shroud's Twitter account has been hacked

7 RETAIL

- Peripheral Maker Fanatec's Customer Database Was Hacked Last Week
- Hostinger Data Breach Affects Almost 14 Million Customers
- Biostar security software 'leaked a million fingerprints'

European Central Bank Breach: ECB Confirms Hack And Shuts Down Website

The European Central Bank on August 15th confirmed that, it's official website, Banks Integrated Reported Dictionary (BIRD), has been breached and few losses had occurred. This website gives details on the statistical and supervisory banking reports. The intruders had successfully breached it by launching a malware. This gave upsets to about 481 subscribers whose breached data included names, designations and email addresses. However, an official investigation is ongoing to fix this issue.

ATTACK TYPE
Malware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
GERMANY

Westpac explains what to do if you've been caught up in a bank breach

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
NEW SOUTH WALES

The security defenses of PayID, one of the popular payment service app has been breached and tens of thousands of customers personal and financial information are at risk. Phone numbers, account numbers and BSB's of them were accessed by scammers. The highlight here is, the impacted are from the biggest banks like the Commonwealth bank, National Australia bank, ANZ and Westpac. Regarding this, Westpac has stepped forward and cautioned all of its customers about this. They'd contacted the victims and assured that this will be sorted ASAP and there's no need to panic about it. Also, they've decided to pay 30,000 customers, each about $60 for being wrongly charged on their credit cards.

Mastercard says German Priceless Specials loyalty program breached

Priceless Specials, one of the German loyalty program partners of Mastercard Inc., has been breached and the personal information from the accounts of about 90,000 customers had been compromised. The incidents had predominantly attacked the German customers. The breached data encompassed names, payment card details, phone numbers, residential addresses and much more. Mastercard said, it's taking active steps to resolve this issue ASAP. As a first step, it has shut down the 'German Specials' program website.

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Cyber Club Hacks Into First Microfinance Bank Of Pakistan Website, Posts Respect To Indian Bravehearts And Martyrs

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
PAKISTAN

Pakistan's first Microfinance Bank had been hacked. The cyber criminals behind this are identified as Neo Hackers with a twitter name as NeOSec. Their website's homepage was seen with images paying tribute to Indian martyrs who died for upholding the safety of India. Further, there was also a message in it as, "First Microfinance Bank Of Pakistan Got Hacked, International Terrorist Day Jai Hind." However, the Pakistani bank hasn't commented anything on this yet!

BANKING AND FINANCE

NASA Astronaut Accused Of Hacking Bank Account From Space

Heard about hacking? Yes, you would've. Heard about hacking from space? If it sounds strange, won't be anymore. Anne Mclain, the NASA Astronaut who flew into space, had been accused of identity theft and hacking the bank account of her estranged spouse. With regards to the investigation, Anne adhered that she indeed checked out her spouse's bank details, just to check out the money maintained to take care of the kid they'd been raising together. But, she firmly denied any hacking attempts. However, an official investigation is still ongoing.

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Murfreesboro water department website hacked

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

The bill payment website of the water and sewage department of Murfreesboro City Government website was hacked. The compromised webpage contained an Iranian flag with a message, "Your hacked by Iranian hackers; we're closer to you; your identity and information is known to us." It seems that the hackers had procured access through some old flawed scripts. However, the company's spokesperson said they're working on fixing this issue. As of yet, the exact culprits remain unfound.

GOVERNMENT

Hacked Texas government agencies face $2.5 million ransom

Seems like a minimum of 22 cities and Governments in Texas have been coordinately affected by a ransomware attack. Not many details were revealed by the Government and officials due to confidentiality reasons. But, upsets have cropped up already from two cities, Borger and Keene. These places saw the sorrow scenes of citizens, being unable to access their birth/death certificates and pay their utility bills. Elliot Sprehe, a security researcher says that hints of the culprit point towards a single person and not a group. However, the FBI and Homeland Security Department are working on this intensely.

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Charleston County suffers data breach impacting more than 800 employees

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Data of 824 employees have been compromised in the country of Charleston, due to a human mistake. In depth analyses of the incident cites that a current employee from Human Resources has inadvertently shared a personal data list to a former employee, who seems to have misused it. The breached data comprised of names, birth dates, social security numbers, salaries and much more. However, as a precautionary, the county alerted the victims and 3 major US credit reporting agencies about this mishap. Further, the county said, a one year of free credit card monitoring services would be provided to the affected.

Bihar Govt website hacked, hackers post message praising Pakistan

The official website of Bihar's Education department had been hacked. The website's homepage was displayed with messages praising Pakistan and Islam like, "We love you Pakistan; no power is not enough to stop Muslims." The hacker behind this issue is identified to be from Turkey, with the name cited as Root Ayyildiz. Immediately upon acknowledging the concerned department, they made their site inaccessible and displayed HTTP error 503 message. However, the site hasn't been restored yet.

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
INDIA

GOVERNMENT

City of Tyler website hacked by anti-government group

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

The City of Tyler website in Texas, has registered its name newly in the victims list of cyberattacks. The website is said to redirect people to an image saying, "corruption turned political culture." It also wrote "#AntiGov", as the hacking group behind this is also said to be an anti-government group. However, the officials say that no payment data nor government services sites that host credit cards were compromised. For betterment, even the United States Secret Service has been called to aid in investigation.

Serious privacy breach at Ministry for Culture and Heritage

New Zealand's ministry for Culture and Heritage experienced a data breach of late. The personal and confidential information of many people were compromised. The compromised data included 228 passports of many countries, 55 driver licenses, 36 birth certificates and much more. This digital havoc happened due to a coding error and improperly uploading these details into the website which were found by 3rd parties, just by a simple google search. Chief Executive Ms. Cavanagh, apologized for this and said the people were contacted and offered replacement documents at zero cost. Also, the website was shut down.

ATTACK TYPE
Weaksecurity practice

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
NEW ZEALAND

EDUCATION

Amity University website hacked; Placement page asks for jobs at Porn sites

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
INDIA

www.amity.edu, the official website of Amity University got hacked. Hence, the university people had been informed to temporarily stop using the site. The hacking impact has made the placement page of university to claim $5000 from students in order to obtain jobs at highly reputed porn sites and in other firms like Bajaj, British airways, etc. What's more shocking is that, the college officials haven't commented anything on this yet.

Google Discloses 20-Year-Old Unpatched Flaw Affecting All Versions of Windows

A Google security researcher, Tavis Ormandy, has disclosed a high rating vulnerability that's left unpatched for a couple of decades. This vulnerability (CVE-2019-1162) has affected all the versions of Microsoft Windows, right from Windows XP to Windows 10. This vulnerability resides in MSCTF that allows client-server communication, as well, to do privilege escalation for applications. Further, Tavis POC's prove that there's no authentication in these interactions, due to which an intruder can easily compromise the session. Tavis reported to Microsoft, but they haven't commented anything on this yet!

ATTACK TYPE
Hot fix

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
None

COUNTRY
USA

KDE Linux Desktops Are Vulnerable To Hack

ATTACK TYPE
Hot fix

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

A security researcher, Dominic Penner, has discovered a vulnerability in KDE software. In twitter, he has uploaded the POC's and stated that this vulnerability affects all the KDE framework of versions below 5.60.0. KDE 4/5 Plasma desktops that's vulnerable to a command injection vulnerability existing in .desktop and .directory files. Penner also says that intruders can also drop shell commands and compromise the entire system. This issue has been reported but remains unpatched yet.

DSLR Cameras Can Be Infected With Ransomware

Eyal Itkin, a security researcher, articulated at DEFCON 2019 in Las Vegas that, even the photos of people in cameras aren't safe. He showcased that how simple it is for hackers to affect cameras by remotely planting a ransomware in it. The camera suspected was Canon EOS 80D, but in fact, it isn't the only one but many. The prime reason is, digital cameras can get connected to Wi-Fi. So, an illegitimate malicious update (a ransomware file) can be impersonated as a benign one, which people might believe and click it. To stay best secured, it's recommended to switch off Wi-Fi and Bluetooth while not in use.

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

KNOB Attack exploits Bluetooth spec flaw to spy on device connections

ATTACK TYPE
Hot fix

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
None

COUNTRY
GLOBAL

Three researchers named Daniele, Nils, and Kasper have discovered a flaw in Bluetooth that could aid intruders to perform MITM (Man-In-The-Middle) attacks. They said that the Key Negotiation of Bluetooth (KNOB) is broken. However, to fix this, Bluetooth SIG has updated the Bluetooth Core Specification to a minimum encryption key length of 7 octets for BR/EDR connections. Also, product developers are requested to do the same. Regarding the KNOB flaw, Google, Microsoft and Cisco have already patched this.

Kern County suffers data breach compromising over 15000 employees' personal information

Kern County witnessed a potential security breach in the systems of its third-party vendors which could affect the health benefits program of its employees. A spokesperson said that, "An official investigation is launched by the officials to check if data compromise had occurred." She also said if the investigation confirmed the data breach occurrence and the data compromise of people, free monitoring services would be provided surely.

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

WARNING — Malware Found in CamScanner Android App With 100+ Million Users

ATTACK TYPE
Malware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

CamScanner – It's one of the widely familiar PDF creator app with a whopping users of over 100 million people. Recently, it'd lost it's worth as it went haywire after being hit by a cyberattack. Yes, it'd been identified with a Trojan virus that allows remote actors to furtively install malicious codes and exploit data. The prime reason for this was due to the app Developers deal with an untrustworthy advertiser, says the Kaspersky researchers, as well the ones who discovered the flaw. Google has removed the app from Play Store. Users are also urged to uninstall it from their mobiles, if they're still using it.

Attackers are targeting vulnerable Fortigate and Pulse Secure SSL VPNs

Two vulnerabilities with details, CVE-2019-11510 and CVE-2018-13379, are used by attackers to exploit by sending specially crafted HTTPS request and download files from vulnerable servers. The former is a file reading vulnerability in Pulse Connect Secure while the latter is a path traversal flaw SSL VPN web portal. It's said that around 15,000 Pulse Secure VPN endpoints are vulnerable to CVE-2019-11510. Also, 2535 network providers were found to have vulnerable Pulse Secure VPN endpoints. To escape from this threat, users are urged to apply the patch fix ASAP

ATTACK TYPE
Hot fix

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

Two new Dragonblood vulnerabilities discovered in Wi-Fi WPA3 standard

ATTACK TYPE
Hot fix

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
None

COUNTRY
GLOBAL

Two security researchers, Mathy Vanhoef and Eyal Ronen, have discovered two Dragonblood vulnerabilities in WPA3 Wi-Fi standard. The first one was CVE-2019-13377 and the other was CVE-2019-13456. The former impacts the WPA3's Dragonfly handshake while the latter impacts the EAP-pwd and Free Radius framework that's used by the vendors for Wi-Fi connectivity. Further, these vulnerabilities can aid attackers to expose information from WPA3 cryptographic operations and even brute-force a Wi-Fi network's password. However, this issue was reported to the Wi-Fi alliance. They've said that they'll update it with proper patches and soon, WPA3.1 will have it's mark.

Newly discovered QualPwn vulnerability affects devices with Qualcomm chips

CVE-2019-10538 and CVE-2019-10540, these two vulnerabilities are collectively referred as QualPwn vulnerability. Both of these are Buffer Overflow vulnerabilities, with the former affecting Qualcomm WLAN component as well as the Android Kernel while the latter affects the Qualcomm WLAN component and the modem firmware. Unpatched phones that use Qualcomm Snapdragon 835 and 845 chips are vulnerable to QualPwn. This issue was addressed to them. Gladly, they were patched by the Qualcomm security team.

ATTACK TYPE
Hot fix

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

Severe zero-day security flaw discovered in Steam

ATTACK TYPE
Zero day

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

Steam is a digital distribution, management, and communication platform developed by Valve Corporation. It was recently discovered with a zero-day vulnerability by a researcher named Vasily kravets. This issue has exposed it's users blatantly to cyber threats. Vasily had reported this flaw to Valve but they'd ignored it then. But now, they've regretted over it saying our ignorance is something to be absolutely despised. They've also decided to look into this issue to fix it ASAP. But somewhere, this rectification deed seems to be a bit late.

CONSUMER TECH

Update your LibreOffice because 2 patches have been bypassed

If you use LibreOffice, it's high time to update it. The three vulnerabilities that were there in the previous versions are now resolved with the newly released version 6.2.6/6.3.0. The three vulnerabilities were named as CVE-2019-9850, CVE-2019-9851 and CVE-2019-9852. All of these had their unique ways of targeting and attacking the users. Hence, libre users are urged to update it ASAP in order to stay away from these threats.

ATTACK TYPE
Hot fix

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

Nigerian airline company, Aero Contractors website hacked by allegedly ISIS-tied group

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
None

COUNTRY
NIGERIAN

Aero Contractors, a Nigerian airline company got its website hacked. The hacking group behind this is identified as Moroccan Revolution Team (M.R.T). They're allegedly tied with ISIS. The hacked homepage of website was seen with an image of a dad carrying his killed son in the Syrian airstrike in 2016 with messages like, "Stop the war; M.R.T, I'm coming for you." Aero Contractors isn't the only one. Excluding this, 28 other websites were hacked on the same day. However, the company said that the issue has been resolved and there's no need for customers to panic.

TRAVEL

BigJigglyPanda Twitter account hacked and compromised for over seven hours after another alleged AT&T error

BigJigglyPanda, a popular video game streamer enjoying a massive 500,000 twitter followers got his twitter account hacked. The account was compromised for over 7 hours and hackers posted a series of threats and offensive tweets. Also, his twitter account's bio name was changed to #chuckling squad and was further linked to a Discord server. However, the hack tweets were removed. Now, the account is shrouded behind a "sensitive content" warning.

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Curtis Pritchard's Instagram hacked

Love Island's star, Curtis Pritchard of age 23, got his Instagram account hacked. The star dancer's account, who enjoy a humongous 1.5 million fan followers, was seen with scam advertisements like giving MacBooks, iPhones, Apple watches and Tesla cars for free. Thankfully, the issue was sorted within the next 24 hours and things went back to the normal state.

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Ellen DeGeneres Says Instagram Account Briefly Hacked Overnight With Phony Giveaways

Another popular show hosting personality, Ellen Degeneres got her Instagram account hacked. Her account was seen with pictures claiming to offer free Apple products, 30 Tesla model cars, 2000 iPhones, 1000 Mac books, 900 Apple watches alongside with Play stations and Xbox gift cards. This situation was soon brought back to normal. Ellen thanked the people who brought this to her notice.

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Shroud's Twitter account has been hacked

Popular streamer and a former professional Counter-Strike: Global Offensive player, Michael "Shroud" Grzesiek's twitter account had been hacked. The streamer has a huge fan base of 1.3 million followers. The intruder after gaining access has posted over 20 tweets that were of profanity and other inappropriate languages. Sooner, Shroud's Instagram account became normal. All the inappropriate tweets from the intruder was deleted.

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
CANADA

RETAIL

Peripheral Maker Fanatec's Customer Database Was Hacked Last Week

Fanatec, a company specialized in providing gaming equipment's, steering wheels, pedals and more sorts of these things, fell as a recent victim of hacking. The company's database was hacked and the Customers personal data were exposed over the internet. Regarding this, the company's CEO Thomas Jackermeier said, we've notified all the victims about this issue. For security reasons, we've reset all the passwords, as well, told to maintain this highly confidential as it would alert the hackers. This was informed to Customers through mail.

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
GERMANY

Hostinger Data Breach Affects Almost 14 Million Customers

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
INDIA

One of the highly reputed hosting providers, Hostinger, recently fell as a victim to hacking. Hostinger confirmed that a 3rd party had infiltrated into one of their servers and compromised about 14 million customers data that included user names, passwords, emails and addresses. The prime cause for this is cited to be the usage of weak passwords by customers. As a remedy, Hostinger has reset the login credentials of all its affected customers. They've also urged them to use strong passwords henceforth. From Hostinger side, they've decided to implement 2FA as a deed to improve security.

Biostar security software 'leaked a million fingerprints'

Biostar 2, a fingerprinting software that's being used globally by thousands of companies was created by a firm named Suprema. Unfortunately, of late, it has leaked 30 million records of its user's fingerprints and their other sensitive data. This was discovered by the security researchers working with VPN mentor company. They've also said that this humongous exposure can't be contained; even if contained, can't prevent catastrophe's from occurring as facial identities and fingerprints of a person are ever the same. But, Suprema retaliated back that further disasters could be stopped. However, the UK Commissioner's office had said that, they're going to start a legal investigation on this.

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
UNITED KINGDOM

Shroud's Twitter account has been hacked

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

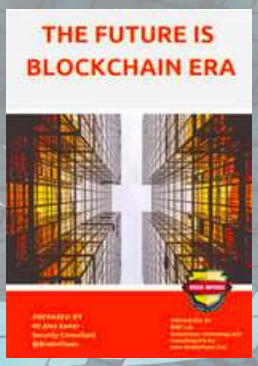
COUNTRY
CANADA

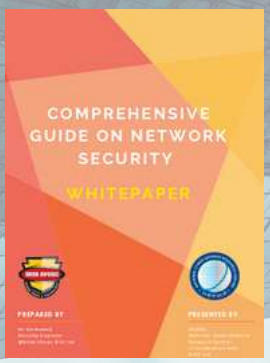
Popular streamer and a former professional Counter-Strike: Global Offensive player, Michael "Shroud" Grzesiek's twitter account had been hacked. The streamer has a huge fan base of 1.3 million followers. The intruder after gaining access has posted over 20 tweets that were of profanity and other inappropriate languages. Sooner, Shroud's Instagram account became normal. All the inappropriate tweets from the intruder was deleted.

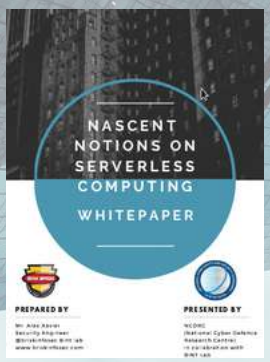
REFERENCES

- https://www.forbes.com/sites/daveywinder/2019/08/16/european-central-bank-breach-ecb-confirms-hack-and-shuts-down-website/#75ff00fe594b
- https://www.news.com.au/finance/business/banking/westpacs-payid-breach-sees-customers-banking-information-hacked/news-story/08c3fb5bad5ee01463233ed669b33013
- https://www.scmagazine.com/home/security-news/mastercard-says-german-priceless-specials-loyalty-program-breached/
- https://www.republicworld.com/technology-news/social-media-news/cyber-club-hacks-into-first-microfinance-bank-of-pakistan-website-posts-respect-to-indian-bravehearts-and-martyrs
- https://www.forbes.com/sites/daveywinder/2019/08/25/nasa-astronaut-accused-of-hacking-bank-account-from-space/#760b7ed954e9
- https://www.tennessean.com/story/news/2019/08/03/city-of-murfreesboro-website-hacked/1910207001/
- https://www.itpro.co.uk/security/34231/hacked-texas-government-agencies-face-25-million-ransom
- https://cyware.com/news/charleston-county-suffers-data-breach-impacting-more-than-800-employees-fe247096
- https://www.indiatoday.in/india/story/bihar-govt-website-hacked-hackers-post-message-praising-pak-1582104-2019-08-18
- https://www.easttexasmatters.com/news/top-stories/city-of-tyler-website-hacked-by-anti-government-group/
- https://www.rnz.co.nz/news/political/397437/serious-privacy-breach-at-ministry-for-culture-and-heritage
- https://techpoint.africa/2019/08/14/nigerian-airline-company-aero-contractors-website-hacked-by-alleged-isis-tied-group/
- https://thehackernews.com/2019/08/ctfmon-windows-vulnerabilities.html
- https://www.techworm.net/2019/08/kde-linux-desktop-vulnerable.html
- https://in.mashable.com/tech/5673/dslr-cameras-can-be-infected-with-ransomware-find-security-researchers
- https://searchsecurity.techtarget.com/news/252468914/KNOB-attack-puts-all-Bluetooth-devices-at-risk
- https://thehackernews.com/2019/08/android-camscanner-malware.html
- https://cyware.com/news/kern-county-suffers-data-breach-compromising-over-15000-employees-personal-information-ec5c2b67
- https://www.helpnetsecurity.com/2019/08/26/vulnerable-fortigate-pulse-secure-ssl-vpn/
- https://www.zdnet.com/article/new-dragonblood-vulnerabilities-found-in-wifi-wpa3-standard/
- https://cyware.com/news/newly-discovered-qualpwn-vulnerability-affects-devices-with-qualcomm-chips-2267ee9e
- https://www.game-debate.com/news/27521/severe-zero-day-security-flaw-discovered-in-steam
- https://securityaffairs.co/wordpress/89962/hacking/libreoffice-flaws.html
- https://techpoint.africa/2019/08/14/nigerian-airline-company-aero-contractors-website-hacked-by-alleged-isis-tied-group/
- https://reclaimthenet.org/bigjigglypanda-twitter-account-hacked/
- https://www.irishexaminer.com/breakingnews/entertainment/curtis-pritchards-instagram-hacked-943606.html
- https://deadline.com/2019/08/ellen-degeneres-instagram-hack-phony-giveaway-1202702631/
- https://dotesports.com/streaming/news/shrouds-twitter-account-has-been-hacked

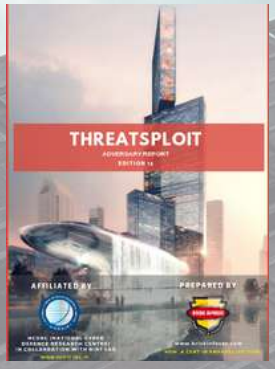
YOU MAY BE INTERESTED IN OUR WHITEPAPERS

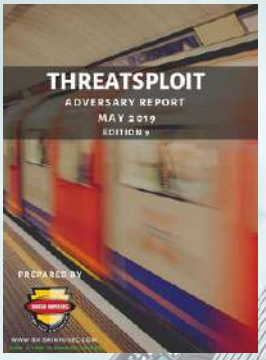






YOU MAY ALSO BE INTERESTED IN OUR PREVIOUS WORKS





REFERENCES ABOUT BRISKINFOSEC

CASE STUDIES

SOLUTIONS

SERVICES

RESEARCH

COMPLIANCES

BLOGS

CONCLUSION

After reading all these, what do you think? Do you think only this much cyberattacks have happened in August 2019 worldwide? If you think so, then you've highly mistaken my friend! All these that we've put in are just a teaser of cyberattacks which we've gathered from the planet earth. Honestly, there's many that're unsaid. While doing this, we wished you were here with us as there's so much that's left to say to you, with plenty of reasons, why. Primarily, we want to provide live practical demonstrations, so that you can have a clear understanding on how different notorious threat vectors can infiltrate stealthily into your security environment, how they can manipulate their identity and deceive you to click them (phishing), how to spot fileless attacks, how to spot Trojan's that affect and leave your systems without a trace, what're the security loopholes that should be amended and much more.

Trust me pals,

we aren't lying! If you truly want to stay secured from all these, reaching out a trustworthy and exquisite cybersecurity firm is mandatory. It's the only best chance you're left to take to remain safe against cyberattacks. To know further, reach us out anytime.

FEEL FREE TO REACH US FOR ALL YOUR CYBERSECURITY NEEDS

contact@briskinfosec.com | www.briskinfosec.com