THREATSPLOIT

ADVERSARY REPORT

EDITION 12

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

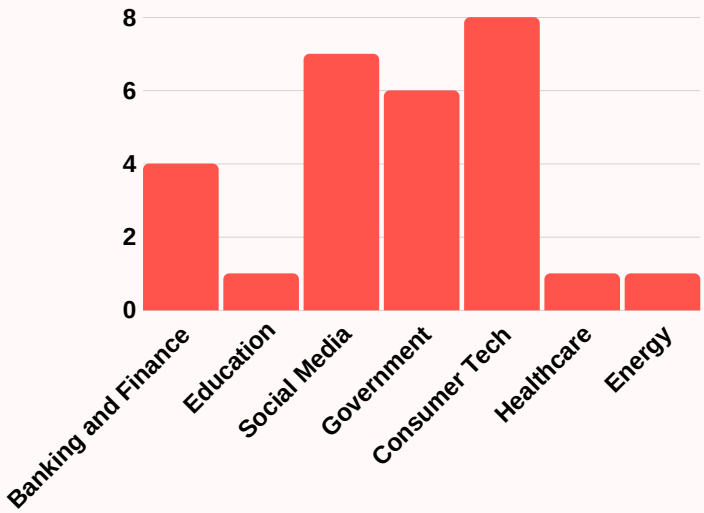
INTRODUCTION

To indicate a volcanic eruption, a single spark of fire is more than enough. Nothing more is needed than that. Similarly, with regards to cybersecurity, about 2,50,000 malwares and countless number of cyberattacks originate each and every day, worldwide.

To tell about all of them in one single report is near to impossible. But, the best collection of such notorious ones is more than enough to indicate about how terrifying the entire stuff would be. Below is the collection of the most significant cyberattacks that’ve happened globally during the month of July. Just scroll down to read them all.

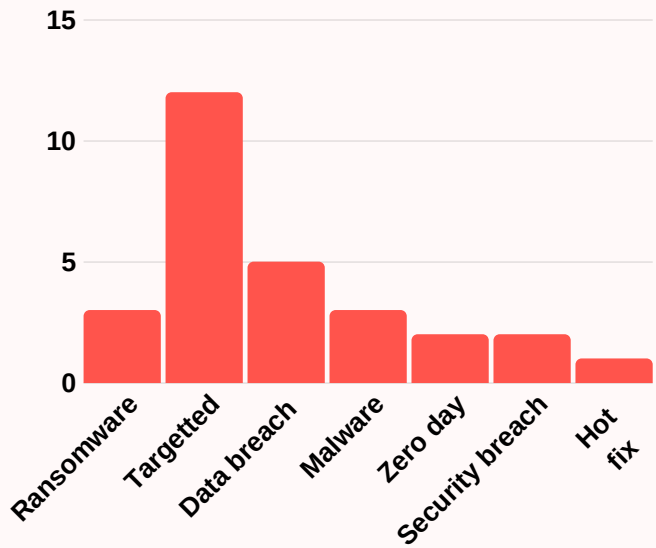
Sectors affected by Attacks

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



Types of Attack Vectors

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



1 Government

- LaPorte County to pay ransom after computer servers hacked
- Metropolitan Police website hacked with bizarre tweets and emails posted
- Russia's secret intelligence agency hacked: 'largest data breach in its history'
- National Security, Immigration websites shut down after 'hack'
- Randolph county government site hacked
- LAPD Data Breach Exposes 2,500 Officer Records

2 Education

- Monroe College hacked, $2 million in Bitcoin demanded as ransom

3 HEALTHCARE

- Clinical Pathology Laboratories alerts 2.2 million patients of data breach

4 BANKING AND FINANCE

- Bitpoint Exchange Hacked for $32 Million in Cryptocurrency
- Philadelphia Federal Credit Union confirms security breach
- Stock Trader Robinhood Stored Passwords in Plaintext
- Woman Arrested in Massive Capital One Data Breach

5 CONSUMER TECHNOLOGY

- Canonical GitHub account hacked, Ubuntu source code safe
- Users of 7-Eleven's mobile payment service lose total of ¥55 million after 900 accounts hacked
- Pale Moon's Archive Server hacked and is used to spread malware
- Security flaw on Zoom app could allow Mac webcams to be hacked
- How I Could Have Hacked Any Instagram Account
- Serious Remote Code Execution Flaw Affects ProFTPD Powered FTP Servers
- Deliveroo Accounts Are Being Hacked And Sold For Just $6
- An exposed password let a hacker access internal Comodo files

6

Social Media

- Bharat Director Ali Abbas Zafar's Instagram and Twitter Accounts Hacked
- Amrita Rao's social media account hacked
- S'pore's Young Lions Instagram account hacked, name changed to "OSAMA"
- Hackers Take Over Virgil Abloh's Instagram & Try to Scam Followers With Sneakers
- Jessica Alba's Twitter Account Is Hacked By Hateful Racist
- Ninja's Instagram Account Was Hacked
- Juice Wrld's Twitter Hacked, Verification Lost

LaPorte County to pay ransom after computer servers hacked

Hackers have proved their mettle in La Porte County. In July 2019, the county's computer servers were affected badly by a virus. The remedy for it is believed to cost more than $132,000, or 10.5 bitcoin. Hence, the county decided to pay a ransom after the FBI determined that its "keys" weren't able to unlock the data. The county's insurance agent will cover $100,000 of the ransom. However, there's no proof about the compromise of any personal information yet.

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Metropolitan Police website hacked with bizarre tweets and emails posted

ATTACK TYPE
Targeted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
UNITED KINGDOM

A series of tweets were launched from Scotland's Metropolitan Police Force that has more than million followers, with rapper 'Digga D' as well in it. Regarding to this, the Scotland Police Force had admitted that some unauthorized access was evident. But, the tweets were later deleted which contained expletive contents. The force revealed that they've made changes to their access arrangements. An official investigation is ongoing to fix this issue.

GOVERNMENT

Russia's Secret Intelligence Agency Hacked: 'Largest Data Breach In Its History'

FSB (Russia's Federal Security Service) - Russia's primary security agency has been hit by a devastating data breach that'd stolen over 7.5 terabytes of data. The leaked data comprised of several highly confidential files like FSB's secret projects, scarping plan of social media's, Nautilus-S (Tor's de-anonymization project) and many more. The cause for this calamity is due to **0v1ru$**. This data calamity is cited to be the biggest data breach in Russian history. What's more shocking is that, FSB hasn't come forward with anything about this yet.

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
RUSSIA

National Security, Immigration websites shut down after 'hack'

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
USA

The official websites of National Security Ministry and the Immigration Division had been hacked. National Security Minister, Stuart Young, notified that both the websites have been shut down. The cause behind this is under investigation. However, Young confirmed that, there's no need to ponder about this too much as there isn't any real damage that's happened because of this hack.

GOVERNMENT

Randolph County government site hacked

The website of Randolph's County Government had been hacked. The homepage had an expletive political statement on it, says the manager, Hal Johnson. The hacker group responsible for this is identified as "Vanda the God." They're a Brazilian hacking group, who've hacked over 50 governments and organizations. However, within 7 hours, the website was brought back to normal state through valiant team efforts from their Government's security team. Since then, security mechanisms were strengthened further to remain secure in the future.

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

LAPD Data Breach Exposes 2,500 Officer Records

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

The Los Angeles Police Department (LAPD) is investigating about a data breach that'd leaked the personal information of about 2500 officers and also the records of 17,500 potential police candidates. The exposed data encompassed the names, email's, social security numbers and much more of police officers and candidates. However, the department had notified the victimized people on this one and swore to strengthen the security defenses. But, the hackers responsible for this remain unidentified yet!

EDUCATION

Monroe College hacked, $2 million in Bitcoin demanded as ransom

Monroe college in Fordham recently fell as a victim to hacking. The attack identified as Ransomware, had encrypted many important data files of the college. To regain normal state, hackers demanded $2 million in bitcoin. This matter is now being investigated by the New York Police Department (NYPD). However, the college officials have notified about this blow to their students through Facebook. A result for this is bound to be expected soon!

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Clinical Pathology Laboratories alerts 2.2 million patients of data breach

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
USA

Clinical Pathology laboratories in America was cautioned by the American Medical Collection Agency (AMCA) that about 2.2 million patients Personal Health Information (PHI) had been exposed. The cause for this humongous data leak is due a data breach that'd happened on 5th July 2019. The exposed data contains names, addresses, phone numbers, credit card information and many more. Moreover, even other lab testing companies like Quest diagnostics and LabCorp were also affected.

HEALTHCARE

Bitpoint Exchange Hacked for $32 Million in Cryptocurrency

Bitpoint – A Japanese cryptocurrency exchange company had lost a whopping sum of $32 million due to a hack that commenced on 11th July 2019. With regards to this, the company said the hackers had stolen funds from both of its "hot" and "cold" wallet, indicating that the exchange network was fully compromised. The company claims that they've detected thefts even from other cryptocurrencies like Bitcoin cash, Litecoin, Ripple and Ethereal. Finally, the company had notified the law enforcements about it.

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
JAPAN

Philadelphia Federal Credit Union confirms security breach

ATTACK TYPE
Security breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
PHILADELPHIA

On July 8th 2019, the credit card of Philadelphia Federal Credit union users had been hacked. Every time when the hack commenced, around $200 to $500 dollars were stolen. This'd happened in many ATM's of South Philly at PNC bank, Wells Fargo and at the Bank of America in Cherry Hill. Pertaining to this, PFCU officials said, "We've notified all our customers and have issued new debit cards, providing money they've lost. Further, we're working hard to figure out the suspects behind this."

Stock Trader Robinhood Stored Passwords in Plaintext

Robinhood – An investment and stock trading app was identified to have stored passwords and other user details in plain text. They were informed about this by an anonymous source through mail. Regarding this, even they'd agreed about this issue. They've sent an email to all their users notifying them about this fact. Moreover, they'd also swore to take this matter seriously and are on the distance to fix this problem ASAP.

ATTACK TYPE
Improper way of Data storage

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Woman Arrested in Massive Capital One Data Breach

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
USA

Page A. Thompson, a 33 year old woman, had been arrested for accessing tens of millions of Capital One credit card applications. This woman from Seattle had done this by bypassing a misconfigured firewall. Apropos to it, she'd posted these data on public GitHub which resulted in her arrest. This breach caused by her had affected nearly 100 million in U.S and 6 million in Canada. Regarding to this, Richard D. Fairbank, Chairman and CEO of Capital one says, "I deeply apologise for what'd happened. Also, I swear to set things absolutely right in time."

Canonical GitHub account hacked, Ubuntu source code safe

ATTACK TYPE
Data comprimization

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
UNITED KINGDOM

Canonical limited, the organization behind the Ubuntu Linux distribution, had been hacked once again on 6th July 2019. The Ubuntu security team confirmed that, "The canonical accounts on GitHub were compromised due to which unknown repositories creation (about 11) and other strange activities started happening. Further, the Launchpad infrastructure (building and the maintenance place of Ubuntu) was also isolated from the GitHub. An investigation is underway to fix this issue. But, the hacker group behind this remain unidentified yet!"

Users of 7-Eleven's mobile payment service lose total of ¥55 million after 900 accounts hacked

ATTACK TYPE
Malicious Access

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

900 users of 7-Eleven mobile payment service have lost about $510,000 due to some malicious access into their accounts. The problem began when the operator of Seven & I Holdings Co., unleashed the 7pay (payment app) across 20,000 stores at haste. However, Tsuyoshi Kobayashi, the president of Seven pay Co, notified all of its customers during a press conference in Tokyo that, "The company complies to compensate the losses faced by our users. An investigation is underway to fix this issue."

Pale Moon's Archive Server hacked and is used to spread malware

ATTACK TYPE
Malware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

On July 9th 2019, Pale Moon company suffered a data breach that affected its archive server. Also, a malware began to spread. Upon detection on the very next day, they've shut down the server instantly in order to prevent the malware's surge. According to the sources, this breach had affected all the archived exe.files of Pale Moon 27.6.2 as well its previous versions. The patch for the above problem is to be provided yet. However, this hasn't destroyed the functioning of Pale Moon's prime functions.

Security flaw on Zoom app could allow Mac webcams to be hacked

ATTACK TYPE
Zero day

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
GLOBAL

Jonathan Leitschuh, a software engineer, discovered an important vulnerability in Zoom app for Apple Mac computers. Mr. Jonathan further stated that, this vulnerability doesn't get removed just by uninstalling the app. But, if this remains unpatched, it could spy on people through their webcams, stealthily. In a Medium post, Mr. Jonathan says, about 4 million webcams and 750,000 companies are vulnerable to this threat. This issue was reported to Zoom but a proper patch hasn't been released from them yet!

How I Could Have Hacked Any Instagram Account

Lakshman Muthiyah, a young Indian Intelligent man has found a vulnerability in Instagram which presented him a bounty of $30,000. Somewhere, he'd read that Instagram and Facebook are impossible to be hacked. He defied and tested it. He tried to find a vulnerability in both, but ended up successful in Instagram. He showcased the POC's to the Instagram officials and urged them to fix the issue in it. Instagram fixed it and thanked him!

ATTACK TYPE
Security misconfiguration

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
INDIA

Serious Remote Code Execution Flaw Affects ProFTPD Powered FTP Servers

ATTACK TYPE
Zero day

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

A German based security researcher named '**Tobias Madel**' has discovered a critical vulnerability in FTP server that's currently being used by millions of servers globally. The vulnerable software is named as ProFTPD, that's used along with SourceForge, Samba and Slackware, as well with Debian. This malicious software enables users to repeat information from one place to another server. Finally, steps are being taken to fix this issue ASAP.

Deliveroo Accounts Are Being Hacked And Sold For Just $6

The user accounts of Deliveroo (An online food delivery company) had been hacked. It seems like either their passwords were stolen from a dark web dealer for just $5.99 nor through deceiving phishing links. The victims are facing strange activities like unordered orders made in their names and much more. But, there isn't any breach occurrence detected on Deliveroo's internal systems. However, the company said they're working relentlessly to fix this issue.

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

An exposed password let a hacker access internal Comodo files

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
USA

Jelle Ursem, a Netherlands based security researcher, has discovered a security loophole in Comodo company (former SSL certificates issuer). An email address and password of Comodo was exposed over the public GitHub repository. An unidentified hacker had utilized this email id and password, and had procured access to the company's internal files, documents and many more. Ursem notified comodo about this issue. The account was soon locked down and the situation was brought back to normal.

Bharat Director Ali Abbas Zafar's Instagram and Twitter Accounts Hacked

Ali Abbas Zafar - One of the Bollywood's most talented director, the person who gave blockbusters like Sultan, Tiger Zinda Hai and Bharat, starring Bollywood's king Salman Khan, recently fell a victim to cyberattacks. Investigation reveals that random pictures and messages were sent from his Instagram and Twitter accounts to random people. However, the ace director cautioned 'Hack Alert' to his people and promised to notify them when things are settled.

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
INDIA

Amrita Rao's social media account hacked

Bollywood actress, Amrita rao's twitter account was hacked in July. Regarding this, she said "The link appeared to be from a top TV channel and they'd wanted to write an article about me. When I further went the distance, my password was asked and I'd entered it. But shockingly, nothing seemed to appear. Hence, I've decided to report this incident to twitter officials and to the cybercrime department. Investigation is underway to remedy this situation."

ATTACK TYPE
Targeted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
INDIA

S'pore's Young Lions Instagram account hacked, name changed to "OSAMA"

The Instagram account of Singapore's young Lions football (managed by the Football Association of Singapore (FAS)) club was hacked on July 2nd 2019. Apropos to that, the profile name was altered as OSAMA and the website link was replaced with the link of the hacking group as handle@1peprs. By 3rd July 2019, the entire account was missing on Instagram. Investigation is ongoing to find the cyber rogues and in fixing this issue ASAP.

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
SINGAPORE

Hackers Take Over Virgil Abloh's Instagram & Try to Scam Followers With Sneakers

Virgil Abloh, a well renowned designing and DJ icon, recently fell as a victim to cyberattacks. The 38 year old's Instagram account was hacked. The intruders posted 2 suspicious stories in a ploy to deceive 4.2 million followers and reap financial awards. Post acknowledgement, Abloh notified in an hour to his fans about his Instagram hack. Sooner, he also informed that the situation has been contained.

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
USA

Jessica Alba's Twitter Account Is Hacked By Hateful Racist

Jessica Alba – A 38 year old businesswoman and also a Hollywood actress recently fell as a victim to hacking. Yes, her account had been hacked by a racist on a night, who'd sent a series of hateful messages to her account. Those messages remained active for hours. Somehow, they were taken down quickly. By the time when twitter users are awake, its hoped that this would be solved. However, Jessica hasn't commented anything on this yet!

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

SOCIAL MEDIA

Ninja's Instagram Account Was Hacked

ATTACK TYPE
Malware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
GLOBAL

Tyler 'Ninja' Blevins – one of the best streamers in gaming had fallen as a prey to hacking. On 25th July 2019, an image was visible on its Instagram page which swore to give away thousands of iPhone Xs', V-Bucks and much more. Instead, when clicked, the links on it led to some malicious sites which is believed to contain malware. Sooner, the wife of the streamer Jessica Blevins, notified that the account was back to normal. Efforts to trace down the perpetrator are in progress.

Juice Wrld's Twitter Hacked, Verification Lost

Juice wrld- A popular Chicago rapper, had of late been a victim of cyber hacking. He had lost his twitter account verification status due to hacking. His compromised account was seen with tweets that lashed out at the U.S government and showing abhorrence towards many such stuffs. Due to this, the 20 year old has hit the flash news since this incident occurrence.

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

COUNTRY
USA

Ransomware Attack Cripples Power Company's Entire Network

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

COUNTRY
SOUTH AFRICA

A ransomware attack had been launched from Johannesburg. It'd struck the South African electric utility city power and had crippled it's systems, database and applications. This attack even prevented few users from purchasing electricity units. However, the city power company informed that, "Remediation work is ongoing to fix this issue ASAP. Till now, most of the haywire apps and systems have been contained. They've consoled their customers saying none of their details were compromised. Also, they'd owed their deep apologies".

ENERGY

CONCLUSION

- There's a hacking attempt for every half-a-minute.
- About 4 million data records are being tampered/manipulated every day globally.
- Most of the cyberattacks happen due to lack of human awareness.

Well, all these statistics to be acknowledged is truly shocking. The prime reason is, many people still believe that firewall, antivirus and other basic security mechanisms are more than sufficient to stay secured. But, they don't realize that technological evolution parallelly leads to the evolution of hacking and cyberthreats. The best way to remain secured from all these attacks is to stay coherent with the daily happenings of cybersecurity.

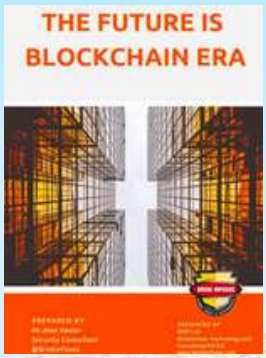
Trust me mate.

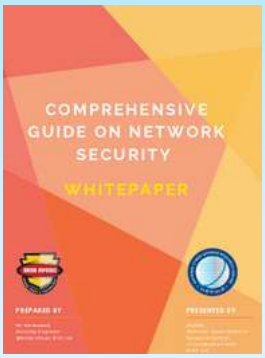
Cybersecurity is a field that has plenty of scope, both in the present and future. But, higher the value, higher is the threat around it. Hence, to remain secure, a proper cybersecurity organization needs to be approached. Briskinfosec secures your data and systems with its finest cybersecurity services and advance cyber training that makes your organization highly resilient against cyber threats. To know further, reach us out anytime. We're always at your service.

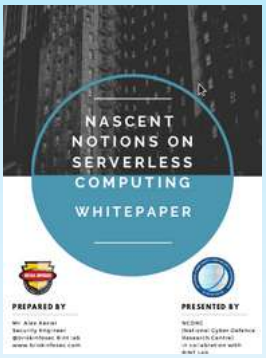
REFERENCES

- https://www.wndu.com/content/news/LaPorte-County-to-pay-ransom-after-computer-servers-hacked-512666481.html
- https://www.bbc.com/news/uk-england-london-49054332
- https://www.forbes.com/sites/zakdoffman/2019/07/20/russian-intelligence-has-been-hacked-with-social-media-and-tor-projects-exposed/#30a01ed16b11
- http://www.looptt.com/content/national-security-immigration-websites-shut-down-after-hack
- https://myfox8.com/2019/07/30/randolph-county-government-website-taken-over-by-hackers/
- https://www.databreachtoday.com/report-lapd-data-breach-exposes-2500-officer-records-a-12856
- https://www.nydailynews.com/new-york/nyc-crime/ny-monroe-college-hacked-bitcoin-20190711-uhmv5a4mz5gxja6od7lme37h7e-story.html
- https://www.beckershospitalreview.com/cybersecurity/clinical-pathology-laboratories-alerts-2-2-million-patients-of-data-breach.html
- https://www.zdnet.com/article/bitpoint-cryptocurrency-exchange-hacked-for-32-million/
- https://6abc.com/400-philadelphia-federal-credit-union-customers-hacked/5384088/
- https://www.macobserver.com/news/robinhood-plaintext-passwords/
- https://www.databreachtoday.com/woman-arrested-in-massive-capital-one-data-breach-a-12852
- https://www.zdnet.com/article/canonical-github-account-hacked-ubuntu-source-code-safe/
- https://www.japantimes.co.jp/news/2019/07/04/business/corporate-business/users-7-elevens-mobile-payment-service-lose-total-%C2%A555-million-900-accounts-hacked/#.XSwENJzhXeQ
- https://www.ghacks.net/2019/07/11/pale-moons-archive-server-hacked-and-used-to-spread-malware/
- https://www.independent.co.uk/life-style/gadgets-and-tech/news/webcam-hack-zoom-app-mac-apple-spy-macbook-a8997141.html
- https://thezerohack.com/hack-any-instagram?fbclid=IwAR3TzNlVuFmzHDmczDPXSIhFeZjO37bIRvEZXVfUIKhmO8TEZjTOjEnjmVk#articlescroll
- https://www.malaysiainternet.my/2019/07/serious-remote-code-execution-flaw-affects-proftpd-powered-ftp-servers/
- https://techcrunch.com/2019/07/27/comodo-password-access-data/
- https://www.news18.com/news/movies/bharat-director-ali-abbas-zafars-instagram-and-twitter-accounts-hacked-2234871.html
- https://timesofindia.indiatimes.com/entertainment/hindi/bollywood/news/amrita-raos-social-media-account-hacked/articleshow/70194589.cms
- https://mothership.sg/2019/07/young-lions-football-instagram-hack/
- https://www.highsnobiety.com/p/virgil-abloh-instagram-hack/
- https://heavy.com/news/2019/07/jessica-alba-twitter-hacked/
- https://dotesports.com/news/ninjas-instagram-account-has-been-hacked
- https://www.xxlmag.com/news/2019/07/juice-wrld-twitter-hacked/

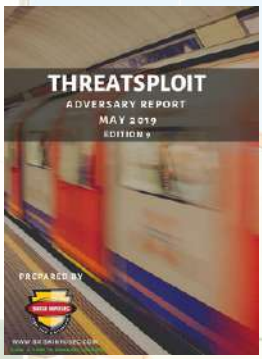
YOU MAY BE INTERESTED IN OUR WHITEPAPERS







YOU MAY ALSO BE INTERESTED IN OUR PREVIOUS WORKS



REFERENCES ABOUT BRISKINFOSEC

CASE STUDIES

SOLUTIONS

SERVICES

RESEARCH

COMPLIANCES

BLOGS

FEEL FREE TO REACH US FOR ALL YOUR CYBERSECURITY NEEDS

contact@briskinfosec.com | www.briskinfosec.com