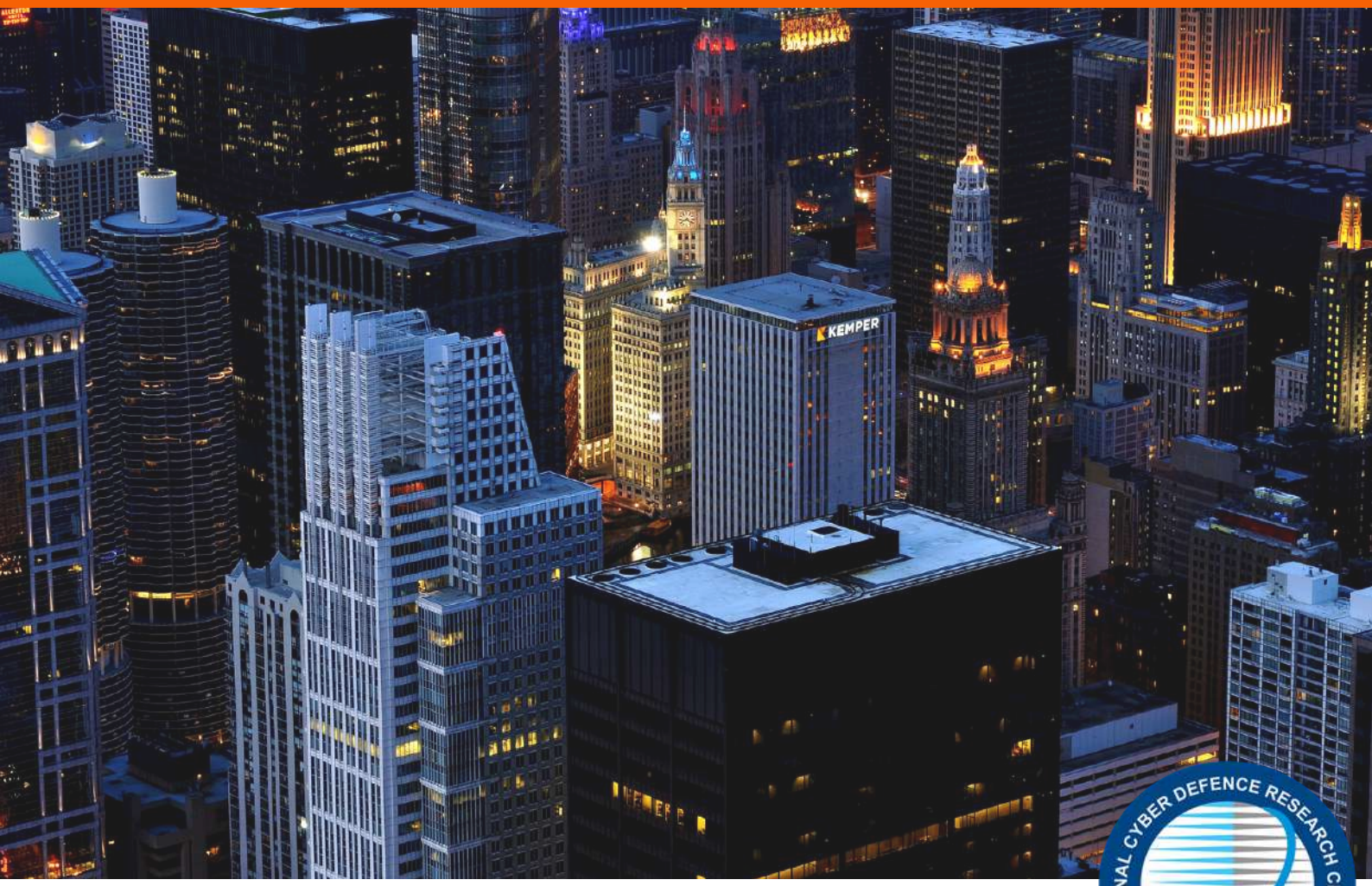
FEB 2020 | EDITION 18

THREATSPLOIT ADVERSARY REPORT



INTRODUCTION

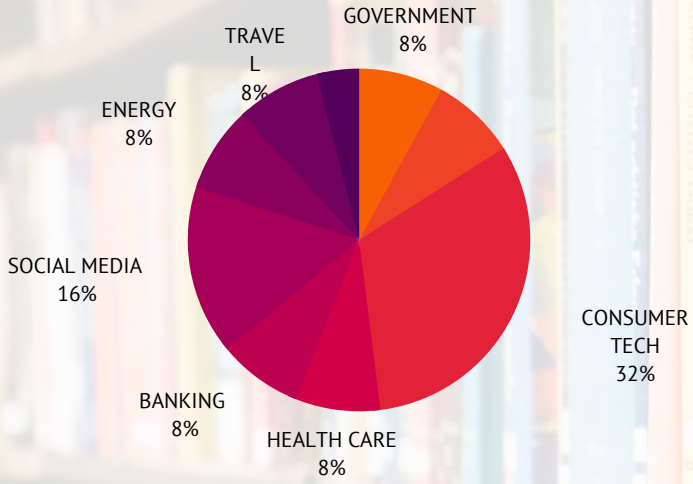
Welcome to the World of Threatsploit Adersary report which contains the global occurrence of most significant and awful cyberattacks identified by Briskinfosec during the month of January 2020.

Some of the cyberattacks include data breach in banks, Government organization etc. Almost all Sectors have been targeted. Inspite of strong Security implementation in many company has suffered a data breach., About 2,50,000 malware's and countless number of cyberattacks originate each and every day, worldwide.

There are many eye-opening incident in this report. Just read over to know it.

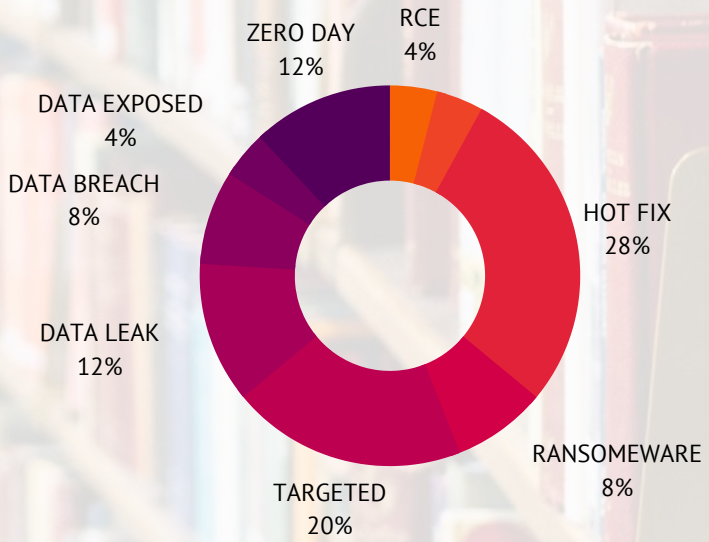
TYPES OF ATTACK VECTORS

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



SECTORS AFFECTED BY ATTACKS

The below Pie-chart shows the percentage of distinctive sectors that've fallen as victims to the horrendous cyber threats. From it, it's evident that the Consumer Technology and Retail has been hit the most.



Many cyberattacks initiate from various sectors. But, a majority of them seemed to have originated from consumer technology sector, holding about 32%. To prevent these, it's evident that top-notch reliable security is mandatory.

32%

consumer Tech

CONSUMER TECHNOLOGY

- Critical 0-day exploit found in Mozilla firefox.
- Massive number of cable modems are vulnerable to RCE(Cable Haunt).
- Researchers found 8 Critical Risks in Android VoIP components.
- Hacker leaks passwords for more than 500,000 servers, routers, and IoT devices.
- Cisco Patched Critical Bug In Firepower Management Center.
- Microsoft disclosed details of security breach that contains roughly 250 million entries. (Data breach).
- Microsoft January 2020 Patch Tuesday fixes 49 security bugs.
- Hackers exploited a zero day in trend micro antivirus.

HEALTH CARE

- MDhex Vulnerabilities Discovered In GE Healthcare Medical Device.
- LabCorp security lapse exposed thousands of medical documents.

RETAIL

- School Management Software Firm Active Network Reveals Data Breach.
- Payment processor leaked 6 million transaction details online.

BANKING

- MageCart attack hunts the Australia bush fire donors.
- P&N Bank data breach may have impacted 100,000 West Australians.

ENERGY

- Cyber-Attack on US Water Company Causes Network Outage.
- Israel says it thwarted serious cyber attack on power station.

SOCIALMEDIA

- Twitter and Facebook accounts for 15 NFL teams hacked.
- Kuwait news agency says its Twitter was hacked.
- TIkTok vulnerability.
- camero, Filecrypt, callcam SideWinder group Apps removed form play store.

GOVERNMENT

- Dozens of United Nations Servers Hacked.
- US government agency website hacked by group claiming to be from Iran..

TRAVEL

- Travelex hack: how a cyber attack by Sodinokibi ransomware hit the travel money firm – and what it means for you.
- Bay Area Library System Suffers Ransomware Attack.

TELECOMMUNICATION

- ACT Fibernet fixes bug in its Wi-Fi router settings

Critical 0-day exploit found in Mozilla firefox

A critical exploit has been discovered in Mozilla Firefox on versions before 72.0. This flaw is considered as "type confusion vulnerability" that occurs in Just-in-time (JIT) compiler of the Mozilla's JavaScript Spider Monkey engine. It was reported by cybersecurity researchers at Qihoo 360 ATA, who has also not yet released any information about their investigation and research. In simple, a type confusion vulnerability arises when the code doesn't verify what objects it is passed to and blindly uses it without checking it's type which allows the attackers to crash the application. Mozilla released update for both firefox and firefox ESR.

ATTACK TYPE
Zero day

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

Massive number of cable modems are vulnerable to RCE(Cable Haunt).

ATTACK TYPE
RCE

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

Cable modems using broadcom chips are vulnerable to a new vulnerability called as Cable Haunt. A group of Danish security. researchers revealed this vulnerability affects numerous devices, at least over 200 million devices in Europe alone. They have tested this vulnerability on a few modems listed, including Netgear, Sagemcom, COMPAL modems, and a Technicolor modem. The researchers proves that the attacker could able to claim access of the device by visiting the malicious url. Impact of this would be the attacker will gain access to the local network, intercept private messages, reroute traffic, or set up botnets.

Android's VoIP Components 8 Critical Risks in

Chinese researchers recently revealed 8 critical risks in Android's voice-over-internet-protocol (VoIP) components. They are Unauthorized Call Transfer, VoIP Call Bomb, Remote Denial of Service (DoS) in Telephony, Remote Code Execution (RCE), Remote DoS in Bluetooth, Data Leak and Permanent DoS, Caller ID Spoofing. These issues may leads to private data loses for telecom industry and users. Later Google has fixed these vulnerabilities.

ATTACK TYPE
Zero day

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

Hacker leaks passwords for more than 500,000 servers, routers, and IoT devices

ATTACK TYPE
Data leak

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

A Hacker exposed a Massive list of sensitive Data consists of the telnet devices of 500,000 servers approximately including the home routers and IOT devices. It was exposed on the popular hacking forum which includes IP address of each device with It's passwords for remote access.

CONSUMER TECHNOLOGY

Cisco Patched Critical Bug In Firepower Management Center

ATTACK TYPE
Hot fix

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

Cisco has fixed a critical security Flaw in its FMC. This vulnerability existed in the web-based interface of the tool. This bug could allow remote code execution with admin privileges on the device while bypassing authentication. Cisco have released a fix for the bug in Cisco FMC software releases. Cisco also patched other bugs in different products including 7 high and 18 medium severity vulnerabilities.

Microsoft disclosed details of security breach that contains roughly 250 million entries. (Data breach)

ATTACK TYPE
Security breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

Microsoft shared details of the latest breach which involved roughly 250 million entries from the support case analytics database. Eventually microsoft fixed the breach on New year's eve.Bob Diachenko, a security researcher spotted the security breach and alerted Microsoft of the issue. Huge records in the leaked database contained readable data on customers, including their email addresses, IP addresses, Locations, Descriptions of CSS claims and cases, Microsoft support agent emails, Case numbers, resolutions, and remarks, Internal notes marked as confidential.

Microsoft January 2020 Patch Tuesday fixes 49 security bugs

ATTACK TYPE
Hot fix

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

Microsoft has released January 2020 patch for windows server 2016 and 2012 which has 8 critical vulnerabilities among 49 vulnerabilities fixed by this update. Some of the noted bugs are CryotAPI, used for fake file signature and launch man-in-the-middle attack, and Remote Desktop Gateway, Used to attack vulnerable windows servers by initiating an RDP connection.

Hackers exploited a zero day in trend micro antivirus

ATTACK TYPE
Zero day

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

Researchers from Trend Micro found zero-days in major android apps. The malicious android apps are camero, filecrypt and callcam. These android apps are found in official google play store. They are believed to be linked to Sidewinder APT, a notorious hacking group. Later these are apps were removed from Google play store.

HEALTHCARE

MDhex Vulnerabilities Discovered In GE Healthcare Medical Device

ATTACK TYPE
Hot fix

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

Critical vulnerabilities are found in GE health care CARESCAPE patient monitoring devices. It also includes the SSH vulnerability exposing private keys (CVE-2020-6961) a SMB vulnerability allowing remote connection to read/write files on the system (CVE-2020-6963), MultiMouse / Kavoom KM vulnerability allowing remote control (CVE-2020-6964), vulnerability in VNC software allowing remote control (CVE-2020-6966), and deprecated Webmin version triggering numerous bugs (CVE-2020-6962). Finally, the vendors patched the flaws

LabCorp security lapse exposed thousands of medical documents

ATTACK TYPE
Data Exposed

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

A security venerability in the LabCorp website has exposed thousands of medical records such as test results containing sensitive health information. The unprotected web address which leads leakage of patient files, it was cached by google. The patient files include health information, name, date of birth and social security numbers, which can be downloaded as a document. The bug has been fixed by Labcorp.

REAIL

School Management Software Firm Active Network Reveals Data Breach

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

School Management Software firm Blue bear was suffered from a data breach. The attack lasted for over a month. The breach might have exposed sensitive information of customers usernames, passwords, payment card data, credit/debit numbers including date of expiration and security codes.

Payment processor leaked 6 million transaction details online.

ATTACK TYPE
Data leak

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Data

A security researcher found a data leak in a major payment system called Cornerstone, which provides payment system to many organisation's . The data was availabel online for more than 6 years from 2013. The data consits of transaction details of all the payee personal information including card type, the last four digits of the card number and its expiry date. The data can be viewed by anyone without any authentication and data was not encrypted. Later the conerstone placed some security measure in locking down the sensitive URls.

MageCart attack hunts the Australia bush fire donors.

ATTACK TYPE
Hot fix

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

Security researchers from the Malwarebytes labs has detected the Australia bush fire donation website hits by Magecart attack. The researchers found a legitimate donation collection website for the Australia bushfire under a credit-card skimming attack. They noticed a malicious skimmer â€˜ATMZOWâ€™ script running on the checkout page of the website. The script collects credit card or payment details of the victim and transfers it to another site. The researchers also found out that the same script runs on 39 different sites.

BANKING

P&N Bank data breach may have impacted 100,000 West Australians

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

P&N Bank in Western Australia had faced a serious data breach. In the cyberattack ,hackers have stolen personal information and sensitive customer account details of 100,000 customers. The attack took place by targeting the hosting provider when the bank was performing a server upgrade. The bank announced that it has fixed the flaw and recovered from the cyber-attack.

ENERGY

Cyber-Attack on US Water Company Causes Network Outage

ATTACK TYPE
Data leaked

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

Greenville water company in South Carolina was attacked. Attackers infiltrated the online payment system, the company reveals that 500,000 customers were affected and the company claimed that it does not store any card details of the customers. Greenville later revealed that it has been recovered from the cyber-attack and now it took preventive measures to avoid the attack in future

Israel says it thwarted serious cyber attack on power station.

ATTACK TYPE
Targeted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

Israel hampered a major cyber attack on one of its power stations. Attackers tried to control and immobilize a power station in Tel Aviv. It is to believe that Palestine, Lebanon, Iran, and Hezbollah may behind this attack. The company is also launching a sequence of products called Sophic which aimed to provide an additional layer of cybersecurity for critical infrastructure.

SOCIALMEDIA

Twitter and Facebook accounts for 15 NFL teams hacked

OurMine a sphosticated hacking group hacked twitter, Instagram and facebook account of 15 NFL teams. The teams include the San Francisco 49ers and Kansas City Chiefs. OurMine said that the internet security is low and had to be improved and some of the accounts had their profile pictures or headers changed or deleted. Twitter confirmed the accounts were hacked by a third-party platform. NFL is locked their accounts and workin gon to ge the accounts back..

ATTACK TYPE
Targeted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

Kuwait news agency says its Twitter was hacked

Kuwait government news agency KUNA had been hacked and used to spread false information in Twitter about US troops saying â€œU.S. military forces in Kuwait would be withdrawn imminently from the camp in kuwait in three daysâ€.Tareq al-Muzarem, head of Kuwaitâ€™s government communication office, confirmed the breach on their official Twitter account

ATTACK TYPE
Targeted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

TIkTok vulnerability

A Security researcher found a vulnerability in the TikTok video-sharing app, this vulnerability leads to SMS link spoofing, open redirection, and cross-site scripting. The attacker can modify the userâ€™s videos and view private information such as address and email. ByteDance immediately patched this vulnerability and released an update on official app stores.

ATTACK TYPE
Hot fix

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

camero, Filecrypt, callcam SideWinder group Apps removed form play store

Researchers from Trend Micro found zero-days in major android apps. The malicious Android apps are camero, filecrypt and callcam. These android apps are found in the official google play store. They are believed to be linked to Sidewinder APT, a notorious hacking group. Later these are apps were removed from Google play store.

ATTACK TYPE
Hot fix

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

GOVERNMENT

Dozens of United Nations Servers Hacked

ATTACK TYPE
Targeted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

Sophisticated hackers hacked U.N offices in Geneva and Vienna. It is to be noted that the hackers left no trace. The extent of the damage is still unknown. Dozens of servers were compromised, which collects sensitive data. The active directory component- where all users permissions are managed- was also compromised.

US government agency website hacked by group claiming to be from Iran

ATTACK TYPE
Targeted

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

Federal Depository Library Program(FDLP), the U.S Government website was defaced by Iranian hackers. Hackers defaced website referring to drone strike which killed Qassem Soleimani and Iranian General. Hackers posted a picture of President Donald Trump being punched in the face and bleeding from the mouth and also Hackers left the message â€œThis is an only a small part of Iranâ€™s cyber ability! Weâ€™re always readyâ€¦ To be continued ...â€ with Iranian flag and then the site was removed by Government.

TRAVEL

Travelex hack: how a cyber attack by Sodinokibi ransomware hit the travel money firm – and what it means for you

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Data

Travelex a Money exchanging website was attacked by ransomware group "Sodinokibi" on New Year's eve. Attackers are demanding 6 million USD for 5GB customer data which includes social security numbers, date of birth and payment card information. The attackers threatened to double the payment in case of a delay. Travelex took the system and website offline and it provides a refund to customers. The company started to work offline for more than 2 weeks still the company has not recovered from the breach.

EDUCATION

Bay Area Library System Suffers Ransomware Attack

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Data

Contra Costa Country library system had suffered a ransomware attack. The infection results in a serious network disruption at all their 26 branches showing that â€œour network is currently down and patrons cannot login at this time.â€ Librarian assured that no patrons personal data is compromised and it is taking all possible steps to protect the public. All affected servers are taken offline and some servers are recovered, and will opened soon.

TELECOMMUNICATITOTN

ACT Fibernet fixes bug in its Wi-Fi router settings

Security researcher Karan Saini found a vulnerability in Atria Convergence Technologies wifi routers, that default credentials are not changed by the users for more than 52,000 ACT provided devices, this leads to login credentials and personal information sniffing and monitoring the internet activity of the users. ACT provided the fix for this problem on 9th Jan 2020 for their customer's devices.

ATTACK TYPE

Hot fix

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation/Data

CONCLUSION

These are some of the major cyber attacks, But this is not all! We have just mentioned only a few attacks.Many people say that Corona virus spreads faster, but

can you guess what spreads faster?

Ransomware

There is a huge increase in Ransomware, Data-breach and Data leaks. There is no exception that only mid tier companies or companies with poor security will get easily affected even Top tier Companies such **Travelex** has suffered major Ransomware attack, and Even Amazon has suffered data leak exposing customer data.

This proves that no company is hack proof. In order to protect the data from cyber attacks many companies are Spending millions to protect the data and A proper cyber awareness to employees will prevent a few.....

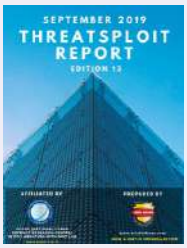
Trust me mates, we aren't lying!

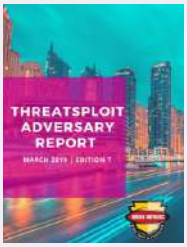
If you truly want to stay secured from all these, reaching out a trustworthy and exquisite cybersecurity firm is mandatory. It's the only best chance you're left to take to remain safe against cyberattacks. To know further, reach us out anytime

REFERENCES

- https://thehackernews.com/2020/01/hack-tiktok-account.html
- https://thehackernews.com/2020/01/android-zero-day-malware-apps.html
- https://www.zdnet.com/article/mozilla-patches-firefox-zero-day-reported-by-qihoo-360/
- https://latesthackingnews.com/2020/01/13/cable-haunt-vulnerability-haunts-cable-modems-using-broadcom-chips/
- https://cyware.com/news/researchers-find-8-critical-risks-in-androids-voip-components-e79d1198
- https://latesthackingnews.com/2020/01/16/microsoft-patch-tuesday-january-updates-address-49-vulnerabilities
- https://www.zdnet.com/article/hacker-leaks-passwords-for-more-than-500000-servers-routers-and-iot-devices/
- https://msrc-blog.microsoft.com/2020/01/22/access-misconfiguration-for-customer-support-database/
- https://siliconangle.com/2020/01/23/2000-wordpress-sites-hacked-new-scam-campaign/
- https://edgy.app/vulnerabilities-wordpress-plugins-place-400000-sites-at-risk?order=desc
- https://latesthackingnews.com/2020/01/27/cisco-patched-critical-bug-in-firepower-management-center
- https://threatpost.com/ring-sharing-user-data-facebook-data-miners/152300/
- https://www.intel.com/content/www/us/en/security-center/default.html
- https://latesthackingnews.com/2020/01/28/hackers-exploited-trend-micro-antivirus-zero-day-in-mitsubishi-electric-hack/
- https://newsjunky.in/an-adult-sexting-site-exposed-thousands-of-models-passports-and-drivers-licenses/
- https://flipboard.com/@TechCrunch/an-adult-sexting-site-exposed-thousands-of-models-passports-and-driver-licenses/f-a55fe3f4ba%2Ftechcrunch.com
- https://latesthackingnews.com/2020/01/27/mdhex-vulnerabilities-discovered-in-ge-healthcare-medical-devices/
- https://techcrunch.com/2020/01/28/labcorp-website-bug-medical-data-exposed/
- https://latesthackingnews.com/2020/01/06/school-management-software-firm-active-network-reveals-data-breach/
- https://techcrunch.com/2020/01/28/cornerstone-payments-credit-cards/
- https://tech.economictimes.indiatimes.com/news/internet/act-fibernet-fixes-bug-in-its-wi-fi-router-settings/73180221
- https://www.bleepingcomputer.com/news/security/australia-bushfire-donors-affected-by-credit-card-skimming-attack/
- https://www.zdnet.com/article/wawa-card-breach-may-rank-as-one-of-the-biggest-of-all-times/
- https://securityaffairs.co/wordpress/96435/data-breach/pn-bank-data-breach.html
- https://www.theguardian.com/world/2020/jan/05/us-government-agency-website-hacked-by-group-claiming-to-be-from-iran
- https://time.com/5773654/united-nations-server-hacked/
- https://www.infosecurity-magazine.com/news/uk-gov-database-leak/
- https://www.bbc.com/news/technology-51275786
- https://www.theverge.com/2020/1/8/21057228/kuwait-news-agency-twitter-hack-iran
- https://www.greenvilleonline.com/story/news/2020/01/23/greenville-waters-main-phone-line-down-water-safety-not-affected/4551641002/
- https://www.infosecurity-magazine.com/news/cyber-attack-on-greenvillewater/
- https://www.reuters.com/article/us-israel-cyber-powerstation/israel-says-it-thwarted-serious-cyber-attack-on-power-station-idUSKBN1ZS1SU
- https://inews.co.uk/inews-lifestyle/travel/travelex-hack-cyber-attack-ransomware-sodinokibi-travel-money-uk-firm-data-breach-explained-1358454

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