

EDITION 21

THREATS PLOIT ADVERSARY REPORT

MAY 2020

PREPARED BY : BRISKINFOSEC



INTRODUCTION

Security issue is been really a thriller to all industries where cyber criminals have been increased in huge numbers and it hits the business in unexpected ways and time. At times this security issue gives a big headache for companies and also to individuals, as their social media accounts are also been hacked and misused. Our April 2020's Threatsploit report contains most of the threats that have been affecting various industries during this COVID-19 situation. It has been a challenging situation for us to stay safe and also to keep our business safe at this moment because many companies adopt work-from-home policies in response to the COVID-19 pandemic.

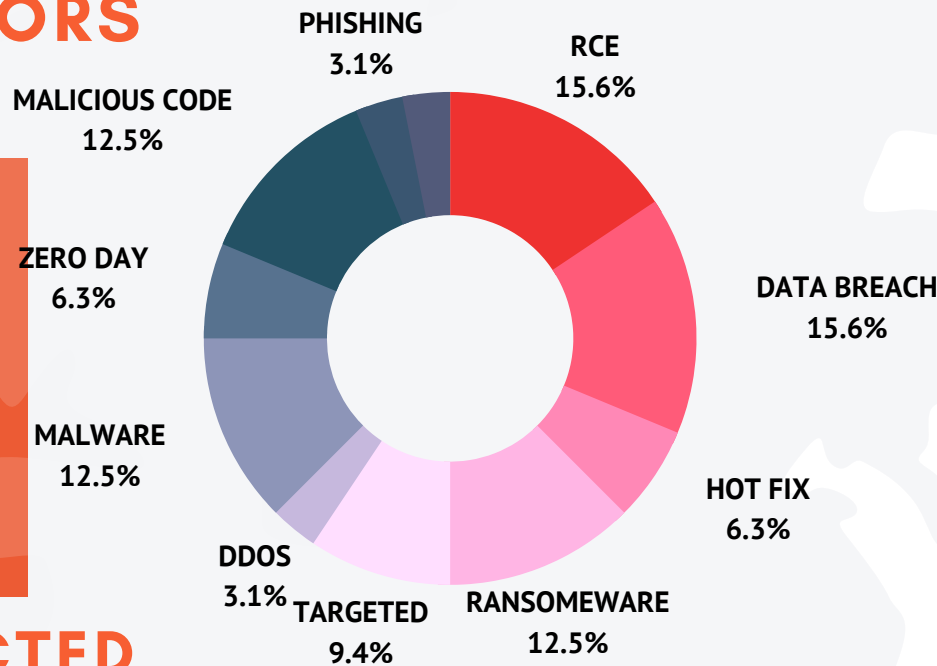
As many of us are settling into a routine of working from home we have to be more cautious in saving our business from the cyber criminals. Many of us have not applied the same security in our networks that would be in place in a corporate environment, or the employees would not be aware of the corporate security policies. So, these kind of flaws also would end up in security issues.

We have listed various threats that would make you aware and start taking steps in order to be away from those kinds of threats.

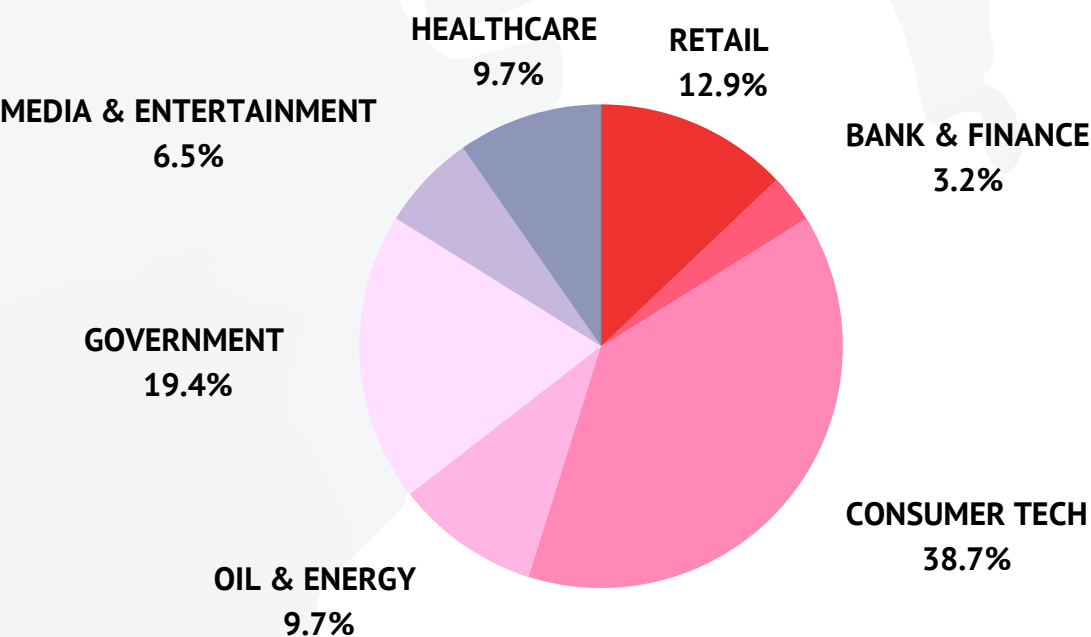


TYPES OF ATTACK VECTORS

The Pie-chart indicates the percentage of nefarious cyber attacks that have broken the security mechanisms of distinct organizations.



SECTORS AFFECTED BY ATTACKS



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

Many cyberattacks initiate from various sectors. But, a majority of them seemed to have originated from consumer technology sector, holding about 39%. To prevent these, it's evident that top-notch reliable security is mandatory.

39%

consumer Tech

GOVERNMENT

- San Francisco Airport faces Data Breach
- Italy's social security website Hacked
- Milwaukee election officials' video chat meeting hacked
- Email Addresses and Passwords for NIH, WHO, Gates Foundation employees reportedly spread online
- Cyber security Vulnerabilities found in FCC systems
- Mississippi mayor's online meeting hacked

OIL & ENERGY

- Remote Access Trojan (RAT) targets Azerbaijan energy companies
- Spearphishing campaigns target oil, gas companies with spyware
- EDP faces Ransomware Attacker

MEDIA & ENTERTAINMENT


- EA faces a Malicious Attack
- Microsoft Battles 4 Bugs Under Active Exploit
- Nintendo accounts Hacked

RETAIL

- Aptoid app store users' details leaked on hacking forum
- OGUUsers hacked for the second time in a year
- Website of PH magazine hacked
- Pay payments platform exposed millions of Credit Card Numbers

CONSUMER TECH

- Two Zoom Zero-Day Flaws Uncovered
- Malicious Typosquatted Libraries Found On RubyGems Repository
- New Google Chrome Extensions Caught Hijacking Cryptocurrency Wallets
- Cognizant hit by the Maze Ransomware attack
- Starbleed bug impacts FPGA chips
- Viewing a GIF in Microsoft Teams triggered account hijacking bug

- 
- Apple Patches Two IOS Zero-Days Abused For Years
 - Security Researcher disclosed 4 Zero-Day Bugs in IBM's Enterprise Security Software
 - Online auction of record-breaking whisky collection faced cyber-attack
 - SeaChange Hit by Sodinokibi Ransomware
 - Hackers Mount Zero-Day Attacks on Sophos Firewalls
 - Canadian accounting firm MNP faces cyberattack

BANKING AND FINANCE

- Canadian accounting firm MNP faces cyberattack

HEALTHCARE

- Hacker used stolen AD credentials to ransom hospitals
- Hartford HealthCare Hit by Data Breach
- Genetic Testing Lab hit by Data Breach

San Francisco Airport faces Data Breach

Malicious code was planted on San Francisco International Airport's (SFO) two sites – SFOConnect.com and SFOConstruction.com. The attackers inserted malicious computer code on these websites to steal some users' login credentials. SFO said that the users accessing these websites from outside the airport network through IE on a Windows-based device or a device not maintained by SFO have been affected.

ATTACK TYPE

Malware

CAUSE OF ISSUE

Poor Security Practice

TYPE OF LOSS

Reputation/Data

ATTACK TYPE

Malware

CAUSE OF ISSUE

Malicious Campaigns

TYPE OF LOSS

Reputation/Data

Italy's social security website Hacked

Computer hackers have attacked Italy's social security website, forcing it to shut down in early April 2020, just as people were starting to apply for coronavirus benefits, the head of the welfare agency said. Pasquale Tridico said his INPS agency had received some 339,000 applications for the 600 euro (\$655) so far, but that hackers had compromised access to the site.

Milwaukee election officials' video chat meeting hacked

The Milwaukee Board of Election Commissioners met virtually, on Zoom, to discuss their plans but hackers forced them out. They cancelled the meeting after unknown hackers took over the screen displaying religious video, disturbing pictures and words.

ATTACK TYPE

Targetted

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation

Email Addresses and Passwords for NIH, WHO, Gates Foundation employees reportedly spread online

Unknown activists posted nearly 25,000 email addresses and passwords allegedly belonging to the NIH, WHO, Gates Foundation and other groups working to combat the coronavirus pandemic. NIH said, "We are always working to ensure optimal cyber safety and security for NIH and take appropriate action to address threats or concerns." Gates Foundation is monitoring the situation in line with their data security practices.

ATTACK TYPE

Targetted

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation/Data

Cyber security Vulnerabilities found in FCC systems

The Government Accountability Office urged FCC to take steps to boost the security of its comment submission process following a review that revealed dozens of cyber vulnerabilities. The GAO undertook its review of the FCC's security for the ECFS following this incident after requests from numerous Democratic lawmakers.

ATTACK TYPE

*Security
Loophole*

CAUSE OF ISSUE

Lack of maintainances

TYPE OF LOSS

Reputation

ATTACK TYPE

*Unauthorized
access*

CAUSE OF ISSUE

Poor security practice

TYPE OF LOSS

Reputation/Data

Mississippi mayor's online meeting hacked

Moss Point Mayor Mario King's online meeting was hacked with vulgar and racist words and images because of his recent comments about the new coronavirus in his city. So, he said, "Future Zoom meetings for Moss Point will still be held online. He added that he will require a password for the online gatherings so if there are any more issues, the user's IP address can be obtained.

Remote Access Trojan (RAT) targets Azerbaijan energy companies

Remote Access Trojan (RAT) was discovered in a set of campaigns targeting the energy sector, with a slew of post-exploitation tools to log keystrokes, record footage from webcams and steal browser credentials. At that time, researchers said they aren't sure who is behind the malware, or how they are distributing it. However, the researchers guess that victims are tricked into downloading the document via email or a social media message.

ATTACK TYPE

Malware

CAUSE OF ISSUE

Unknown

TYPE OF LOSS

Reputation/Data

Spearphishing campaigns target oil, gas companies with spyware

Cyber criminals are targeting the oil and gas industry sector with highly targeted spear-phishing campaigns impersonating shipment companies and engineering contractors while attempting to infect their targets with Agent Tesla info-stealer malware payloads. It is also used for collecting system info, for stealing clipboard contents, as well as for killing malware analysis related processes and antivirus solutions.

ATTACK TYPE

Phishing

CAUSE OF ISSUE

Social engg

TYPE OF LOSS

Reputation/Data

EDP faces Ransomware Attacker

Using the Ragnar Locker ransomware attackers encrypted the systems of Portuguese multinational energy giant Energias de Portugal (EDP) and are now asking for a 1580 BTC ransom. During the attack, the ransomware operators claim to have stolen over 10 TB of sensitive company files and they are now threatening the company to leak all the stolen data unless the ransom is paid. An EDP spokesperson said that the attack did not impact the company's power supply service and critical infrastructure.

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Unauthorized access

TYPE OF LOSS

Reputation/Data

EA faces a Malicious Attack

ATTACK TYPE

DDoS

CAUSE OF ISSUE

Lack of awareness

TYPE OF LOSS

Reputation/Data

Electronic Arts had some issues with its online functionality after a malicious attack. The company's servers had been hit by a distributed denial of service (DDoS) attack which took them offline. Due to that the users have been unable to play games like FIFA 2020, Apex Legends and Battlefield, in addition to being stopped from logging into the company's Origin online service. "Something's up with our online services, but we're on it," EA said.

Microsoft Battles 4 Bugs Under Active Exploit

Microsoft released 113 vulnerabilities out of those, 19 are rated as critical, and 94 as important. Crucially, four of the vulnerabilities are being exploited in the wild; and two were previously disclosed. In all, the update includes patches for Microsoft Windows, Microsoft Edge, ChakraCore, IE, Microsoft Office and Microsoft Office Services and Web Apps, Windows Defender, Visual Studio, Microsoft Dynamics, and Microsoft Apps for Android and Mac.

ATTACK TYPE

Hot fix

CAUSE OF ISSUE

Security loopholes

TYPE OF LOSS

Reputation

ATTACK TYPE

unauthorized intrusion

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation

Nintendo accounts Hacked

Nintendo users have been increasingly reporting from mid of March that their accounts have been getting hacked and accessed from remote locations around the globe, with some users losing money as a result of the unauthorized intrusion. So, the users are advised to enable two-step verification (2SV), in order to prevent intrusions.

Aptoide app store users' details leaked on hacking forum

A hacker leaked the details of 20 million users of Aptoide, a third-party app store for Android applications, which the hacker said to have obtained following a hack that took place earlier in April 2020. The leaked details contain information on users who registered and used the Aptoide app store.

ATTACK TYPE

Data Breach

CAUSE OF ISSUE

Unauthorised access

TYPE OF LOSS

Reputation/Data

ATTACK TYPE

Security Breach

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation/Data

OGUsers hacked for the second time in a year

OGUsers disclosed a security breach, for the second time in the past year. "It appears that someone was able to breach the server through a shell in avatar uploading in the forum software and get access to our current database dating April 2, 2020," said Ace, the forum's administrator. The attacker is believed to have stolen the details of more than 200,000 users, the latest user counter listed on the forum.

Website of PH magazine hacked

The website of Philippine Graphic, was hacked with 'malicious redirect' in the mid of April 2020. All stories posted in the site once clicked, will redirect the viewer to a porn site. The editors and administrators of the Graphic website were unable to notice the hacking because they have been blocked from accessing the site. Meanwhile, PH started posting its stories in its Facebook page at that moment.

ATTACK TYPE

Malicious Redirect

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation

ATTACK TYPE

Data exposed

CAUSE OF ISSUE

Poor Security Practice

TYPE OF LOSS

Reputation/Data

Pay payments platform exposed millions of Credit Card Numbers

The startup left millions of credit card transaction records exposed for anyone to see on the Internet for nearly three weeks before securing it, and the database was pulled offline after Paay became aware of the issue. Paay co-founder Yitz Mendlowitz said, "An error was made that left that database exposed without a password."

Two Zoom Zero-Day Flaws Uncovered

According to researchers, two zero-day flaws have been uncovered in Zoom's macOS client version. The first flaw allows unprivileged attackers to gain root privileges. The second zero day flaw gives attackers Zoom's mic and camera access, allowing for a way to record Zoom meetings, or snoop in on victims' personal lives – sans a user access prompt.

ATTACK TYPE

Zero day

CAUSE OF ISSUE

Security loopholes

TYPE OF LOSS

Reputation/Data

ATTACK TYPE

*malicious
library*

CAUSE OF ISSUE

Malicious campaign

TYPE OF LOSS

Reputation/Data

Malicious Typosquatted Libraries Found On RubyGems Repository

Over 700 malicious gems packages written in Ruby programming language that supply chain attackers were caught recently distributing through the RubyGems repository. The malicious campaign leveraged the typosquatting technique where attackers uploaded intentionally misspelled legitimate packages in hopes that unwitting developers will mistype the name and unintentionally install the malicious library instead.

New Google Chrome Extensions Caught Hijacking Cryptocurrency Wallets

Google ousted 49 Chrome browser extensions from its Web Store that masqueraded as cryptocurrency wallets but contained malicious code to siphon off sensitive information and empty the digital currencies, the offending extensions were removed within 24 hours after they were reported to Google. The researchers theorize this could be either because the criminals are after high-value accounts only or that they have to manually sweep the accounts.

ATTACK TYPE

Malicious code

CAUSE OF ISSUE

Malicious extension

TYPE OF LOSS

Reputation/Data

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Unknown

TYPE OF LOSS

Reputation/Data

Cognizant hit by the Maze Ransomware attack

Cognizant said that its revenue could be impacted by the recent Maze ransomware attack. The attack disrupted internal Cognizant systems and affected clients leading the company to rope in law enforcement agencies and outside experts to contain the fallout. In an internal message to employees, Cognizant said, "Our security and IT teams are investigating and working to resolve the issues as quickly as possible."

Starbleed bug impacts FPGA chips

A team of academics discovered a new security bug that impacts Xilinx FPGA chipsets. Named Starbleed, which is different from previous exploits, allows attackers with both physical or remote access to extract and tamper with an FPGA's bitstream to reprogram the chip with malicious code.

ATTACK TYPE

Remote access

CAUSE OF ISSUE

Security bug

TYPE OF LOSS

Reputation/Data

ATTACK TYPE

Malicious code

CAUSE OF ISSUE

Security Vulnerability

TYPE OF LOSS

Reputation/Data

Viewing a GIF in Microsoft Teams triggered account hijacking bug

In end of April 2020, CyberArk researchers found a subdomain takeover vulnerability, combined with a malicious .GIF file, could be used to "scrape a user's data and ultimately take over an organization's entire roster of Teams accounts." Finally, Microsoft resolved the security problems in Microsoft Teams which could have attacked its user accounts.

Apple Patches Two iOS Zero-Days Abused For Years

In April 2020 researchers revealed two zero-day security vulnerabilities affecting Apple's stock Mail app on iOS devices they believe that both vulnerabilities have been actively exploited by an "advanced threat operator" since 2018. Hence, in mid of April Apple began making a patch available to mitigate the security flaws in its publicly available beta software.

ATTACK TYPE

Hot fix

CAUSE OF ISSUE

Zero day bug

TYPE OF LOSS

Reputation/Data

Security Researcher disclosed 4 Zero-Day Bugs in IBM's Enterprise Security Software

A cybersecurity researcher disclosed technical details and PoC for 4 unpatched zero-day vulnerabilities affecting IBM Data Risk Manager (IDRM), after the company refused to acknowledge the responsibly submitted disclosure. An IBM spokesperson said, "a process error resulted in an improper response to the researcher who reported this situation to IBM. We have been working on mitigation steps and they will be discussed in a security advisory to be issued."

ATTACK TYPE

zero day

CAUSE OF ISSUE

Security vulnerability

TYPE OF LOSS

Reputation

Online auction of record-breaking whisky collection faced cyber-attack

Online auction of rare whiskies has been postponed indefinitely after being targeted in a cyber-attack. In mid of April 2020, WhiskyAuctioneer.com experienced a targeted, technologically sophisticated, sustained and malicious attack on their website and databases. As a precaution, they have been in touch with their customers who may have been impacted by this.

ATTACK TYPE

Targetted

CAUSE OF ISSUE

Poor Security Practice

TYPE OF LOSS

Reputation/Data

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Poor Security Practice

TYPE OF LOSS

Reputation/Data

SeaChange Hit by Sodinokibi Ransomware

SeaChange International was the victim of the Sodinokibi Ransomware gang, where the ransomware operators posted images of SeaChange's data on the leak site; they have created a page to the company containing images of allegedly stolen documents. Sodinokibi operators threatened the company, saying they have 3 days to contact them.

Hackers Mount Zero-Day Attacks on Sophos Firewalls

An actively exploited vulnerability in Sophos' enterprise firewall was identified and promptly fixed. At the end of April 2020, an unnamed client alerted Sophos to a "suspicious field value visible in the management interface." A short investigation found the field value was not an error, but instead an actively exploited zero-day vulnerability.

ATTACK TYPE

Malware

CAUSE OF ISSUE

Malicious Campaigns

TYPE OF LOSS

Reputation/Data

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Lack of awarness

TYPE OF LOSS

Reputation/Data

Canadian accounting firm MNP faces cyberattack

Canadian accounting firm MNP forced a company-wide shutdown of their systems after getting hit with a cyberattack inorder to prevent the devices from being infected. At this time, MNP states that they are still investigating whether data has been stolen and ransomware operators have yet to claim credit for the attack.

ATTACK TYPE*RCE***CAUSE OF ISSUE***Known vulnerability***TYPE OF LOSS***Reputation/Data***Hacker used stolen AD credentials to ransom hospitals**

Hackers deployed ransomware on the systems of U.S. hospitals and government entities using stolen Active Directory credentials months after exploiting known remote code execution vulnerability in their Pulse Secure VPN servers. Even though the vulnerability was patched by Pulse Secure a year ago, the U.S. Cybersecurity and Infrastructure Security Agency warned organizations to patch their Pulse Secure VPN servers against on-going attacks, in January 2020.

Hartford HealthCare Hit by Data Breach

Hartford HealthCare warned their patients about a cybersecurity incident that took place between February 13 and 14 this year. According to the notification, attackers gained access to patients' personal information after compromising email accounts belonging to two of Hartford HealthCare's more than 30,000 employees. After suspicious activity was observed the HealthCare "immediately took steps to secure the accounts" and engaged a technology forensics firm to investigate the attack.

ATTACK TYPE*Data breach***CAUSE OF ISSUE***Lack of awareness***TYPE OF LOSS***Reputation/Data***Genetic Testing Lab hit by Data Breach**

Ambry Genetics reported an email hacking incident that may have exposed medical information on nearly 233,000 individuals. The company said its notifying customers because their personal information is being disclosed in the incident. They have taken steps designed to prevent this type of event from happening again, including through an ongoing effort to enhance their security measures and to provide additional training to employees.

ATTACK TYPE*Data breach***CAUSE OF ISSUE***Lack of awareness***TYPE OF LOSS***Reputation/Data*

CONCLUSION

As massive amount of work now happens online, cybersecurity is a growing issue. We have listed all these threats in order to give you awareness about various security issues mainly during this work from home situation. Organizations must give more importance in this where they have to keep their data safe. They must make their employees aware on all these issues and also contact the best security company to be away from these kind of issues.

We are available to give you more information on cyber threats and will also help you to keep your data safe.

Contact us for more information.

REFERENCES

- <https://economictimes.indiatimes.com/markets/stocks/earnings/maze-ransomware-attack-to-hit-cognizant-revenue/articleshow/75251293.cms>
- <https://www.bleepingcomputer.com/news/security/ragnarlocker-ransomware-hits-edp-energy-giant-asks-for-10m/>
- <https://www.bleepingcomputer.com/news/security/us-govt-hacker-used-stolen-ad-credentials-to-ransom-hospitals/>
- <https://www.zdnet.com/article/details-of-20-million-aptoide-app-store-users-leaked-on-hacking-forum/>
- <https://www.bleepingcomputer.com/news/security/leading-accounting-firm-mnp-hit-with-cyberattack/>
- <https://www.zdnet.com/article/details-of-20-million-aptoide-app-store-users-leaked-on-hacking-forum/>
- https://www.scmagazineuk.com/pulse-secure-customers-remain-vulnerable-even-vpn-patching/article/1680745?&web_view=true
- https://www.scmagazineuk.com/pulse-secure-customers-remain-vulnerable-even-vpn-patching/article/1680745?&web_view=true
- <https://www.jpost.com/breaking-news/italys-social-security-website-hit-by-hacker-attack-623191>
- <https://www.jpost.com/breaking-news/italys-social-security-website-hit-by-hacker-attack-623191>
- <https://www.pcgamesinsider.biz/news/70908/ea-servers-taken-out-by-ddos-attacks/>
- <https://threatpost.com/april-patch-tuesday-microsoft-active-exploit/154794/>
- <https://threatpost.com/two-zoom-zero-day-flaws-uncovered/154337/>
- <https://thehackernews.com/2020/04/rubygem-typosquatting-malware.html>
- <https://thehackernews.com/2020/04/chrome-cryptocurrency-extensions.html>
- <https://www.cbs58.com/news/milwaukee-election-officials-video-chat-meeting-hacked>
- <https://www.zdnet.com/article/hacking-forum-gets-hacked-for-the-second-time-in-a-year/>
- <https://www.zdnet.com/article/hacking-forum-gets-hacked-for-the-second-time-in-a-year/>
- <https://www.zdnet.com/article/nintendo-accounts-are-getting-hacked-and-used-to-buy-fortnite-currency/>
- <https://msbusiness.com/2020/04/mississippi-mayors-online-meeting-hacked-with-racial-slurs/>
- <https://www.zdnet.com/article/starbleed-bug-impacts-fpga-chips-used-in-data-centers-iot-devices-industrial-equipment/>
- <https://www.zdnet.com/article/this-is-how-viewing-a-gif-in-microsoft-teams-triggers-account-hijacking-bug/>
- <https://www.burhani.co/apple-patches-two-ios-zero-days-abused-for-years/>
- <https://threatpost.com/apple-patches-two-ios-zero-days-abused-for-years/155042/>
- <https://thehackernews.com/2020/04/ibm-data-risk-manager-vulnerabilities.html>
- <https://www.bleepingcomputer.com/news/security/spearphishing-campaigns-target-oil-gas-companies-with-spyware/>
- <https://www.itproportal.com/news/hackers-exploit-sophos-firewall-zero-day/>
- <https://covid19.inforisktoday.com/genetic-testing-lab-hack-affects-233000-a-14182>
- <https://www.indiatvnews.com/technology/news-paay-payments-platform-exposed-users-credit-card-details-see-what-happened-610622>
- <https://www.theguardian.com/technology/2020/apr/25/online-auction-of-record-breaking-whisky-collection-hit-by-cyber-attack>
- <https://www.theguardian.com/technology/2020/apr/25/online-auction-of-record-breaking-whisky-collection-hit-by-cyber-attack>
- <https://www.enigmasoftware.com/seachange-video-platform-hit-by-revil-sodinokibi-ransomware/>
- <https://www.washingtonpost.com/technology/2020/04/21/nearly-25000-email-addresses-passwords-allegedly-nih-who-gates-foundation-are-dumped-online/>
- <https://thehill.com/policy/cybersecurity/494554-federal-watchdog-finds-numerous-cybersecurity-vulnerabilities-in-fcc>

YOU MAY ALSO BE INTERESTED IN OUR PREVIOUS WORKS





FEEL FREE TO REACH US
FOR ALL YOUR
CYBERSECURITY NEEDS

contact@briskinfosec.com
www.briskinfosec.com

Affiliated by



Awards

