Edition-17

THREATSPLOIT ADVERSARY REPORT

January -2020

Wishing you a Happy New Year

www.briskinfosec.com

INTRODUCTION:

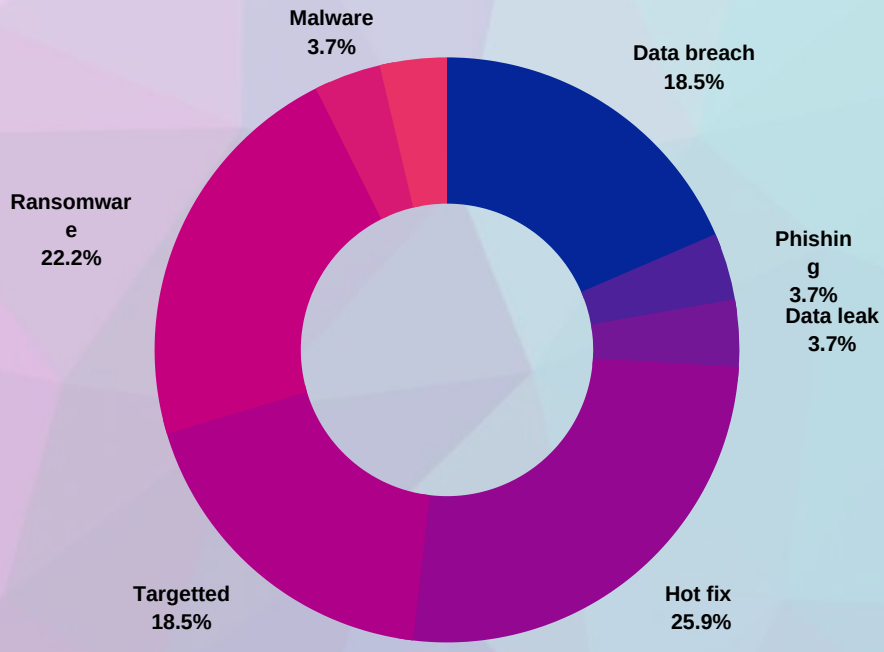
2019 has been a great year for Briskinfosec. Each month we're continually preparing a Threatsploit report consisting of major cyberattacks happening around the world. This new report containing the globally occurred cyberattacks in the month of December 2019.

This report contains a collection of major cyberattacks in Top Tier organisation such as Honda, Facebook and many of the Government organization are also been a victim of the cyber attacks

From the bottom of our hearts, once again, thank you for the continued support. Forever, we're grateful for it!

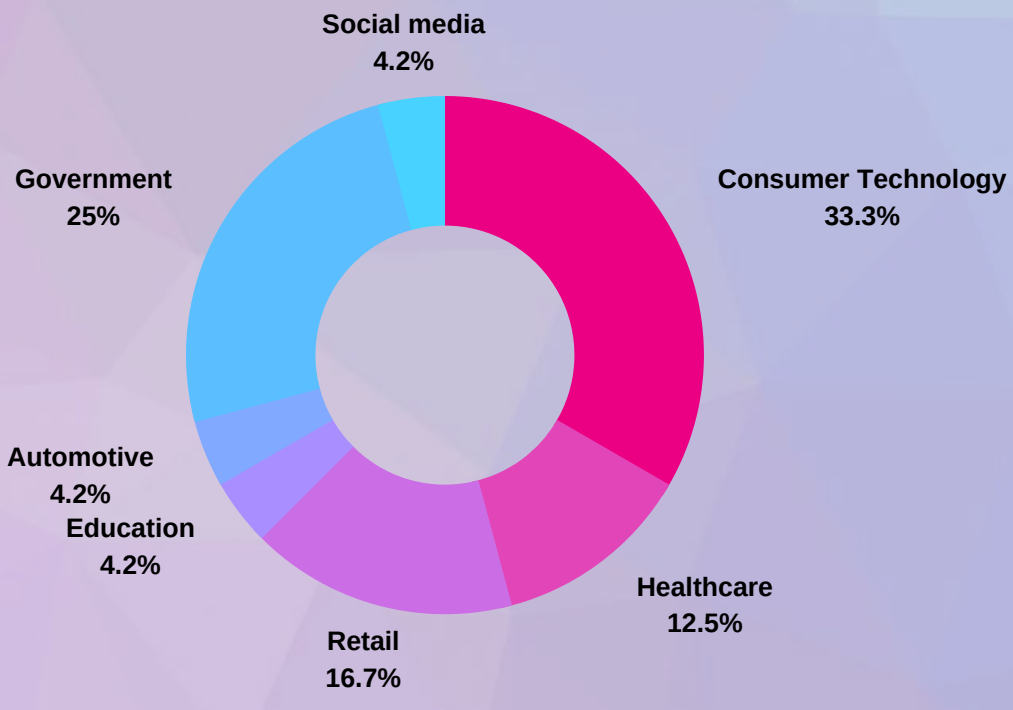
TYPES OF ATTACK VECTORS

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.



33%

consumer Tech

GOVERNMENT

- New Orleans government shut down by massive cyber attack
- Pensacola hit with cyber attack day after deadly naval base shooting
- St. Lucie County Sheriff's Office hit by cyber attack
- New Orleans Scrambles to Respond to Ransomware Attack
- Cyber-Attack Grounds Flights in Alaska - Infosecurity Magazine
- Data Leak Exposes Thousands of US Defense Contractor Staff

HEALTHCARE

- Life Labs pays hackers to recover data of 15 million customers
- New Orleans Scrambles to Respond to Ransomware Attack
- New Jersey hospital chain pays attackers to thwart ransomware incident

EDUCATION

- GU Website hacked, later restored

AUTOMOTIVE

- Honda exposes data of 26,000 customers in US

SOCIALMEDIA

- Over 267 million Facebook users had their details and profiles exposed publicly

RETAIL

- Love, Bonito confirms data breach on local and international customers
- Ransomware Attack Hits Data Center Provider CyrusOne
- 2.7 Billion Retail Customer Email Addresses Exposed Online
- Wawa Data Breach: Malware Stole Customer Payment Card Info

CONSUMER TECH

- Microsoft December 2019 Patch Tuesday plugs Windows zero-day
- Attackers Steal Credit Cards in Rooster Teeth Data Breach
- OpenBSD patches authentication bypass, privilege escalation vulnerabilities
- Drupal Warns Web Admins to Update CMS Sites to Patch a Critica Flaw
- Amazon Ring Leaks Thousands of Customer Data
  Critical Flaw in GoAhead Web Server Could Affect Wide Range of IoTDevice
- Security flaw in Airtel app exposes customers data, fixed now
- Citrix Vulnerability Could Affect 80,000 Companies

GOVERNMENT

New Orleans government shut down by massive cyber attack

New Orleans government computers were hacked due to a data breach. Flood of suspicious mails were sent due to ransomware and phishing attacks. The systems were shut down after 5 hours and the work were stalled. After, 3 hours, the works started to operate and officials started to re-operate.

ATTACK TYPE
Ransomware & Phishing

CAUSE OF ISSUE
Security flaws

TYPE OF LOSS
Reputation/Data

Pensacola hit with cyberattack day after deadly naval base shooting

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Security flaws

TYPE OF LOSS
Reputation/Data

Pensacola, a famous navel base has suffered a bit of cyberattack after a sudden shootout between ally troops and their groups. The cost of this is said to be the enemy troops cyber intelligence that lead this to roots. This investigation is ongoing and many information are going in the air but nothing got confirmed.

St. Lucie County Sheriff's Office hit by cyber attack

St. Lucie County sheriff's office in Dublin have been hit by a cyberattack that have halted the workings for a while. Forensic department were called and they're looking into it to the best they can to tell the one involving behind this. As a remediation, efforts are so much put in finding the causes behind this security disaster.

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Security flaw

TYPE OF LOSS
Reputation

New Orleans Scrambles to Respond to Ransomware Attack

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of awarness

TYPE OF LOSS
Reputation/Data

Nevada New Orleans county in United States has been hit by a Ransomware attack launched by hackers who targeting random targets. The systems were encrypted and officials work flow and business process were stopped. Investigation on who's doing and from where and caused are underway to be revealed.

GOVERNMENT

Cyber-Attack Grounds Flights in Alaska - Infosecurity Magazine

RavnAir Group was forced to ground flights on Saturday following a cyber-attack on the Alaskan company's computer network. The nature of the attack was not disclosed; however, the company did reveal that threat actors specifically targeted the small airline's turboprop-powered regional airliner, commonly known as the Dash 8. But, the airline had to disconnect its entire Dash 8 maintenance system and the back-up system.

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Security flaws

TYPE OF LOSS
Reputation

Data Leak Exposes Thousands of US Defense Contractor Staff

ATTACK TYPE
Data Leak

CAUSE OF ISSUE
Poor Security Pratice

TYPE OF LOSS
Reputation/Data

A digital consultancy of Boeing website has leaked names, phone numbers and email id of employees of more than 6000 Boeing staff. including the senior executives who worked on advance prototyping and sensitive technologies. CTO of Divycloud has said that the main reason of the data leakage is the mis configuration In cloud .

HEALTHCARE

LifeLabs pays hackers to recover data of 15 million customers

LifeLabs, leading diagnostic and therapy and research center in Canada at Quebec have been hit by a ransomware attack that encrypted their system data and corrupted their internal files and external workflow, making things bad and hard. As a fix, hackers demanded 15 million and Lifelabs paid it because they had.

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

New Orleans Scrambles to Respond to Ransomware Attack

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of awarness

TYPE OF LOSS
Reputation/Data

Hackensack Meridian Health hospital in New Jersey was hit by a ransomware on 1st week on December. Doctors and nurses were unable to use electronic records of the patients for non-urgent surgeries. The hospital paid huge amount to recover the system but the amount was covered by the insurance company. They is no indication that any users information are used or disclosed. the hackensack meridian gained the access of the system a week later after paying the ransom.

HEALTHCARE

New Jersey hospital chain pays attackers to thwart ransomware incident

Hackensack meridian hospital in NewJersey, United States, have been victimized by a ransomware that encrypted the patients details and other people. Actions are took by hospital to fix this issue quickly but couldn't. investigation is going still and the attacker and the hackers country are to be found.

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Poor Security Pratice

TYPE OF LOSS
Reputation/Data

EDUCATION

GU Website hacked, later restored

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Poor Security Pratice

TYPE OF LOSS
Reputation/Data

The official Gauhati University was hacked on dec 1 2019. Users said that on visiting the website could see a message flashing on the website along with a link popped up on the screen – Upcoming question papers leaked: Question Papers. When users clicked on the link, they were directed to a pornographic site. Hackers claimed that it to be hacked by Khanbaris. However, the authorities immediately consulted their IT teams without wasting any time further and restored the website sometime back

AUTOMOTIVE

Honda exposes data of 26,000 customers in US

Honda exposed important personal data of twenty six thousand people in the United states of America due to a data breach in their systems. The information is name, date of birth, county born, residence and much more. The affected customers are warned about their safety and are asked to make needed measures to secure from threats.

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

SOCIALMEDIA

Over 267 million Facebook users had their details and profiles exposed publicly

ATTACK TYPE
Data Exposed

CAUSE OF ISSUE
Lack of awarness

TYPE OF LOSS
Reputation/Data

An online database that had been widely unsecured exposed the names, Facebook ID, and phone numbers if millions if user information with many datas exposed online which could easily be compromised by hackers. The database was without even a password. The causer behind this cause is unchecked and traced.

Love, Bonito confirms data breach on local and international customers

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Poor Security

TYPE OF LOSS
Reputation/Data

Love and Bonito, two top marketing firms in Singapore have been listed as companies falling victims of data breach due to poor security features deployed in their infrastructure. Many important breached information were found and many details were openly exposed. They've cautioned customers who didn't get receive it very well at all.

Ransomware Attack Hits Data Center Provider CyrusOne

ATTACK TYPE
Ransomware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

Cyrus one, one of the top popular data center provider have been again hit by a ransomware. The 1st attack happened last year while the new is now. The attack has stopped the workings of people and organization's there with investigations looking for the causes to be proved and approved. Fixing attempts in going as soon as possible.

RETAIL

2.7 Billion Retail Custormer Email Addresses Exposed Online

ATTACK TYPE
Targetted

CAUSE OF ISSUE
Poor security process

TYPE OF LOSS
Reputation

Email addresses often get compromised like thousands. But, this time, billions of addresses were exposed, not just 1 billion but about 3 billion email addresses. These addresses are of people countries and of all young kids, men, women and overall coverage. Email users are told to change passwords before it's late.

Wawa Data Breach: Malware Stole Customer Payment Card Info

ATTACK TYPE
Malware

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

A data breach at Wawa at Crumlin city has went deep into the systems of the city over there and affected the payment card systems and its relations informations. The root for these issues is said to be a malware. This malware has affected about 850 places surrounding it like Dublin, Florida, Masidonia and much more. But, the forensic teams contained the situation and investigation is ongoing.

CONSUMER TECHNOLOGY

Researchers disclose DLL loading vulnerabilities in Autodesk, Trend Micro, Kaspersky software

ATTACK TYPE
Hot Fix

CAUSE OF ISSUE
Security flaw

TYPE OF LOSS
None

Safe breach labs identified 3 vulnerabilities CVE-2019-15628, the second vulnerability identified as CVE-2019-15689 and third CVE-2019-7365. All three vulnerabilities, if exploited, could cause damages. However, the vulnerabilities were identified and reported before they were executed users. Customers are told to update to the latest version for betterment.

Microsoft December 2019 Patch Tuesday plugs Windows zero-day

ATTACK TYPE
Hot fix

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation

Microsoft has released updates in the Windows operating system that has been exploited in the wild. An intruder who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights

Attackers Steal Credit Cards in Rooster Teeth Data Breach

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Malicious code

TYPE OF LOSS
Reputation

Rooster teeth productions has suffered a data breach that allowed hackers to sensitive information like payment card details, CVV numbers and much more. Malicious codes were injected which redirected users towards some wrong sites. Customers information many got stolen. The issue was identified and fixed on the same day.

OpenBSD patches authentication bypass, privilege escalation vulnerabilities

ATTACK TYPE
Hot fix

CAUSE OF ISSUE
Poor Security

TYPE OF LOSS
Reputation

OpenBSD, a publicly available and privately used OS has compromised by 4 damn vulnerabilities that gave access to sensitive information by giving remote access to the intruders and getting theirs done. This vulnerabilities were fixed in 40 hours, patched and remediated.

CONSUMER TECHNOLOGY

Drupal Warns Web Admins to Update CMS Sites to Patch a Critical Flaw

ATTACK TYPE
Hot Fix

CAUSE OF ISSUE
Security flaw

TYPE OF LOSS
Reputation

One of the worlds popular Content Management System named Drupal has some security flaws. Drupal admin has warned users to update its latest version 8.8.1. This version is the new version in the drupal heredity, having a patched critical vulnerability that's there in the initial versions. Users are told be update if they want security.

Amazon Ring Leaks Thousands of Customer Data

ATTACK TYPE
Data breach

CAUSE OF ISSUE
Lack of awareness

TYPE OF LOSS
Reputation/Data

The credentials and user data of 3,672 Ring camera owners were compromised and exposed log-in emails, passwords, time zones and the names people give to specific Ring cameras, which are often the same as camera locations, such as "bedroom" or "front door." Many more data are although exposed. An official investigation is ongoing to get origin clarity.

Critical Flaw in GoAhead Web Server Could Affect Wide Range of IoT Device

ATTACK TYPE
Hot fix

CAUSE OF ISSUE
lack of awareness

TYPE OF LOSS
Reputation

Cybersecurity researchers today uncovered details of two new vulnerabilities in the GoAhead web server software, a tiny application widely embedded in hundreds of millions of Internet-connected smart devices. The devices if hacked can trouble other devices and can cause problems. Effort is taken to patch it.

Security flaw in Airtel app exposes customers data, fixed now

ATTACK TYPE
Hot fix

CAUSE OF ISSUE
Security flaw

TYPE OF LOSS
Reputation

The airtel app has crtical vulnerability which can be used to get details of all the users i.e 325.5 million subscribers. it revealed information like Personal details , subscription information, device capability information for 4G, 3G & GPRS, network information, activation date, user type (prepaid or postpaid) And current IMEI number. The flaw was identified by indian cybersecurity research ahmed on dec 8 while testing its API, when the flaw was reported to Airtel, the airtel acknowledged the issue and fixed it.

CONSUMER TECHNOLOGY

Citrix Vulnerability Could Affect 80,000 Companies

A vulnerability is identified in enterprise software offerings from Citrix that potentially could put 80,000 companies in 158 countries at risk of a cyberattack. Citrix has issued patches to mitigate the risk, urging users to promptly apply them. The vulnerability could leave companies at risk of DDoS, phishing and cryptocurrency mining attacks, told the researchers to media.

ATTACK TYPE

Hot Fix

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation

CONCLUSION

These are some of the major cyber attacks, But this is not all! We have just mentioned only a few attacks.
Cyberattacks are becoming day to day struggle. There is a huge increase in data-breaches and ransomeware attacks. There is no exception that only mid tier companies or companies with poor security will get easily affected even Top tier Companies such

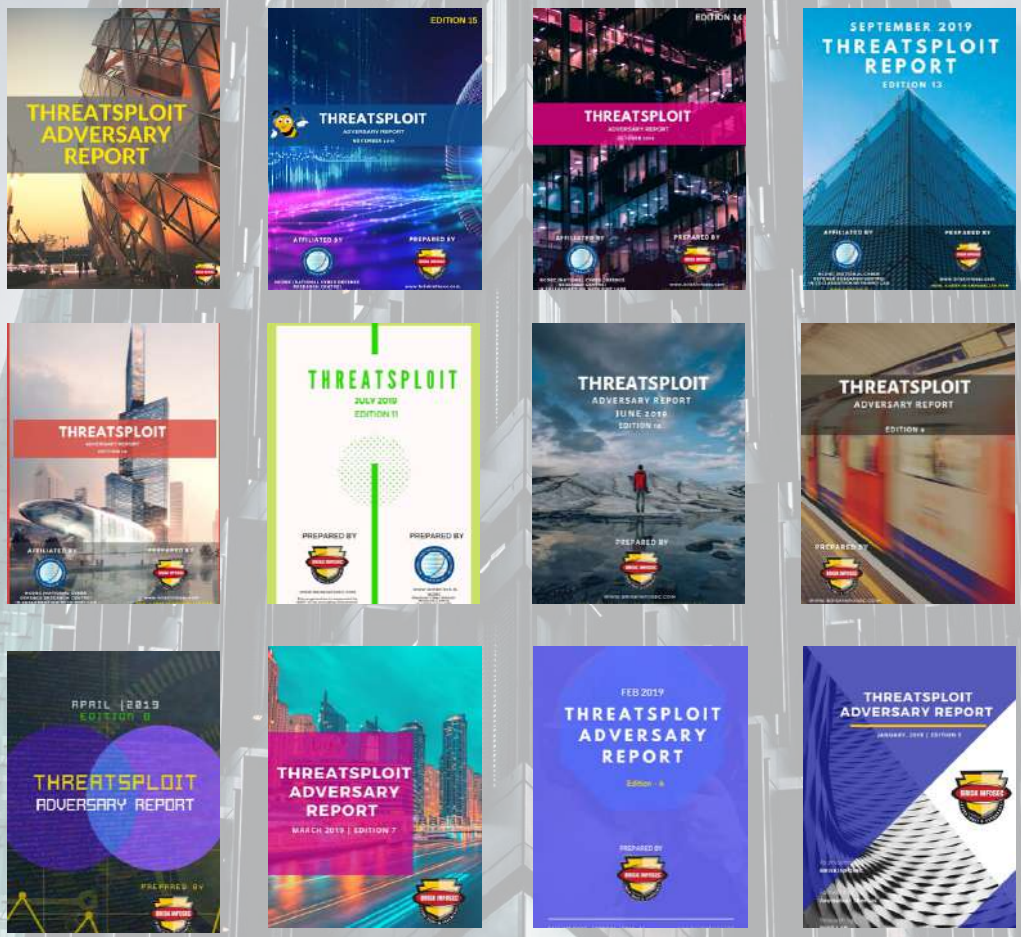
Honda has suffered major data-breach, and Even **Facebook** has suffered data leak exposing 2.7 million customer data. This proves that No company is hackproof.
In order to protect the data from cyber attacks many companies are Spending millions to protect the data, A proper cyber awarness to employees will prevent a few.....

Trust me mates,we aren't lying!
If you truly want to stay secured from all these, reaching out atrustworthy 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://www.newslivetv.com/guwahati/gu-website-hacked-later-restored/
- https://www.telegraph.co.uk/news/2019/12/15/new-orleans-government-shut-massive-cyber-attack/
- https://nypost.com/2019/12/09/pensacola-hit-with-cyberattack-day-after-deadly-naval-base-shooting/
- https://nypost.com/2019/12/08/second-victim-named-in-deadly-pensacola-shooting-was-also-a-navy-trainee/
- https://www.infosecurity-magazine.com/news/cloud-data-leak-thousands
- https://www.infosecurity-magazine.com/news/new-orleans-scrambles/
- https://cbs12.com/news/local/st-lucie-county-sheriffs-office-hit-by-cyber-attack
- https://www.infosecurity-magazine.com/news/cyberattack-grounds-flights-in/
- https://www.zdnet.com/article/researchers-disclose-bugs-in-autodesk-trend-micro-kaspersky-software/
- https://www.zdnet.com/article/microsoft-december-2019-patch-tuesday-plugs-windows-zero-day/
- https://economictimes.indiatimes.com/tech/internet/security-flaw-in-airtel-app-exposes-customers-data-fixed-now/articleshow/72421661.cms
- https://www.malcare.com/blog/critical-vulnerability-ultimate-addons-wpastra-elementor-beaver-builder/
- https://www.bleepingcomputer.com/news/security/attackers-steal-credit-cards-in-rooster-teeth-data-breach/
- https://thehackernews.com/2019/12/openbsd-authentication-vulnerability.html
- https://threatpost.com/amazon-blink-smart-camera-flaws/150962/
- https://thehackernews.com/2019/12/drupal-website-hacking.html
- https://www.securitymagazine.com/articles/91469-amazon-ring-leaks-thousands-o-customer-data
- https://thehackernews.com/2019/12/goahead-web-server-hacking.htmlCitrix Vulnerability Could Affect 80,000 CompCitrix Vulnerability Could Affect 80,000 Companies
- https://www.bankinfosecurity.com/citrix-vulnerability-puts-80000-companies-at-risk-report-a-13556
- https://techhq.com/2019/12/honda-exposes-data-of-26000-customers-in-us/
- https://themediahq.com/large-hospital-system-says-it-was-hit-by-a-ransomware-attack/
- https://www.cyberscoop.com/hackensack-meridian-health-ransomware-attack/
- https://www.zdnet.com/article/lifelabs-pays-hackers-to-recover-data-of-15-million-customers/
- https://www.marketing-interactive.com/love-bonito-confirms-data-breach-on-local-and-international-customers/
- https://threatpost.com/ransomware-data-center-cyrusone/150873/
- https://www.cisomag.com/2-7-billion-email-addresses-exposed-online/
- https://threatpost.com/wawa-data-breach-malware-stole-customer-payment-card-info/151337/
- https://www.businessinsider.in/tech/news/over-267-million-facebook-users-had-their-names-phone-numbers-and-profiles-exposed-thanks-to-a-public-database-researcher-says/articleshow/72892482.cms
- https://www.newslivetv.com/guwahati/gu-website-hacked-later-restored/ https://www.telegraph.co.uk/news/2019/12/15/new-orleans-government-shut-massive-cyber-attack/
- https://nypost.com/2019/12/09/pensacola-hit-with-cyberattack-day-after-deadly-naval-base-shooting/
- https://nypost.com/2019/12/08/second-victim-named-in-deadly-pensacola-shooting-was-also-a-navy-trainee/
- https://www.infosecurity-magazine.com/news/cloud-data-leak-thousands https://www.infosecurity-magazine.com/news/new-orleans-scrambles/
- https://cbs12.com/news/local/st-lucie-county-sheriffs-office-hit-by-cyber-attack
- https://www.infosecurity-magazine.com/news/cyberattack-grounds-flights-in/
- https://www.zdnet.com/article/researchers-disclose-bugs-in-autodesk-trend-micro-kaspersky-software/
- https://www.zdnet.com/article/microsoft-december-2019-patch-tuesday-plugs-windows-zero-day/
- https://economictimes.indiatimes.com/tech/internet/security-flaw-in-airtel-app-exposes-customers-data-fixed-now/articleshow/72421661.cms
- https://www.malcare.com/blog/critical-vulnerability-ultimate-addons-wpastra-elementor-beaver-builder/
- https://www.bleepingcomputer.com/news/security/attackers-steal-credit-cards-in-rooster-teeth-data-breach/
- https://thehackernews.com/2019/12/openbsd-authentication-vulnerability.html
- https://threatpost.com/amazon-blink-smart-camera-flaws/150962/
- https://thehackernews.com/2019/12/drupal-website-hacking.html
- https://www.securitymagazine.com/articles/91469-amazon-ring-leaks-thousands-o-customer-data
- https://thehackernews.com/2019/12/goahead-web-server-hacking.htmlCitrix Vulnerability Could Affect 80,000 CompCitrix Vulnerability Could Affect 80,000 Companies
- https://www.bankinfosecurity.com/citrix-vulnerability-puts-80000-companies-at-risk-report-a-13556https://techhq.com/2019/12/honda-exposes-data-of-26000-customers-in-us/
- https://themediahq.com/large-hospital-system-says-it-was-hit-by-a-ransomware-attack/
- https://www.cyberscoop.com/hackensack-meridian-health-ransomware-attack/
- https://www.zdnet.com/article/lifelabs-pays-hackers-to-recover-data-of-15-million-customers/
- https://www.marketing-interactive.com/love-bonito-confirms-data-breach-on-local-and-international-customers/
- https://threatpost.com/ransomware-data-center-cyrusone/150873/
- https://www.cisomag.com/2-7-billion-email-addresses-exposed-online/
- https://threatpost.com/wawa-data-breach-malware-stole-customer-payment-card-info/151337/

YOU MAY ALSO BE INTERESTED IN OUR PREVIOUS WORKS



REFERENCES ABOUT BRISKINFOSEC

CASE STUDIES

SOLUTIONS

SERVICES

RESEARCH

COMPLIANCES

BLOGS

contact@briskinfosec.com | www.briskinfosec.com