BRISKINFOSEC

THREATSPLOIT ADVERSARY REPORT

AUG 2021| EDITION- 36

3RD YEAR CELEBRATION
THANK YOU FOR YOUR SUPPORT

BRISK INFOSEC
CYBER TRUST & ASSURANCE

INTRODUCTION

We are proud to celebrate the Third Anniversary of the Threatsploit Adversary Report by Briskinfosec Technology.

Threatsploit began as an initiative to raise cyber-security awareness among professionals from various industries. Threatsploit Adversary Report has acquired recognition among the IT community over time and effort. We would like to thank everyone for their unwavering support and encouragement, which has inspired us to create more high-quality material each month.

Welcome to the Threatsploit Report of August 2021 covering some of the important cybersecurity events, incidents and exploits that occurred this month. This month, the cybersecurity sector witnessed a massive rise in ransomware and data breach attacks across geographies. Besides, many other attack types were seen spiking during these recent months.

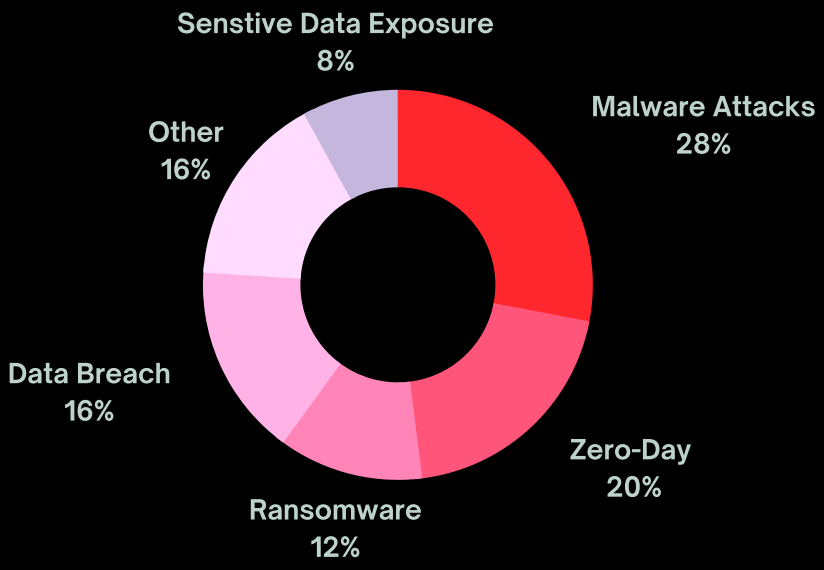
The primary reason is and has always been the same....

"Employees and stakeholders have limited or no perception or understanding of threats and misplaced understanding of massive cyber threats or consequences".

Since the time Work From Home (WFH) has become the new normal, security incidents has peaked with more and more issues relating to VPNs and other remote connecting mediums. WFH option has further limited the ability of IT functions to apply software patches for both old and new critical vulnerabilities, exposing the information assets for hackers to exploit and compromise. Let us walk you through some of the important security incidents that happened this month.

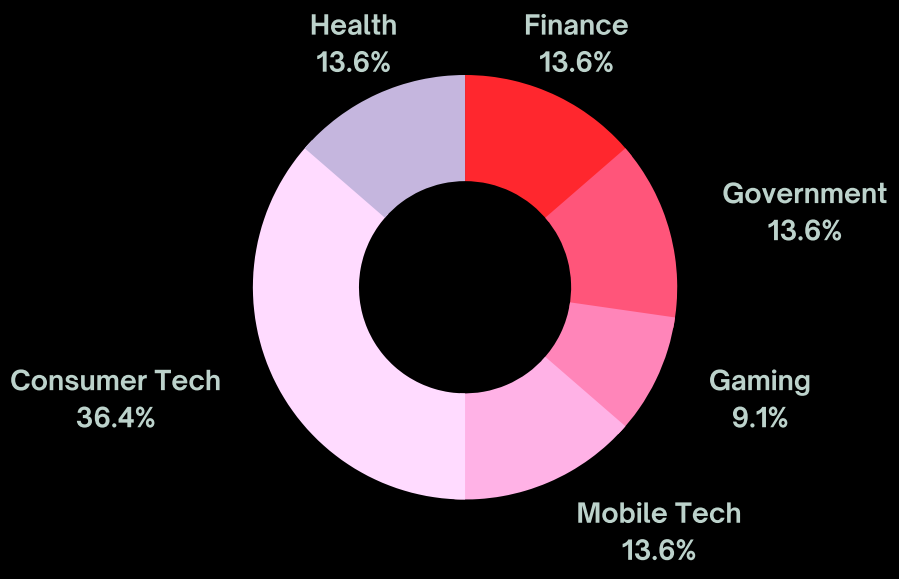
TYPES OF ATTACK VECTORS

The pie-chart indicates the percentage of malicious cyber-attacks that exploited the information infrastructure and compromised the security mechanisms across organisations from various business verticals.



SECTORS AFFECTED BY ATTACKS

The pie-chart indicates the percentage of malicious cyber-attacks that exploited the information infrastructure and compromised the security mechanisms across organisations from various business verticals.



CONTENTS

LATEST THREAT ENTRIES

CONSUMER TECH

- Hackers sending fake copyright complaint notice with malware to Facebook users: Expert
- Update Your Chrome Browser to Patch New Zero-Day Bug Exploited in the Wild
- Threat actors scrape 600 million LinkedIn profiles and are selling the data online – again
- Microsoft warns over this unusual malware that targets Windows and Linux
- There are new unpatched bugs in Windows Print Spooler
- Vulnerability in Schneider Electric PLCs allows for undetectable remote takeover
- Researchers find new attack vector against Kubernetes clusters via misconfigured Argo Workflows instances
- SonicWall releases urgent notice about 'imminent' ransomware targeting firmware

FINANCE

- Insurance giant CNA reports data breach after a ransomware attack
- Coinbase Users Face Ongoing Phishing Attacks
- Morgan Stanley Hit by Third-Party Vendor That was Using the Accellion FTA Service

GOVERNMENT

- Malware-infected documents discovered on the Kazakhstan government's portal
- Hackers use new malware to target Indian government officials, according to SideCopy.
- The White House has announced the formation of a ransomware task force, and one option is to hack back.

GAMING

- Malware Detection Increased due to Discord CDN and API Abuses
- Pirated Games Spreading Cryptojacking Malware

CONTENTS

HEALTH

MOBILE

TOOL OF THE DAY

CYBERMONDAY

BLOG OF THE MONTH

CONSUMER TECH

Hackers sending fake copyright complaint notice with malware to Facebook users: Expert

Cybercriminals are sending out fake copyright complaint notifications to Facebook users with malicious links that can harm computers, a security researcher warned about the incident. Criminals have created several pages in the name of Copyright Constraints Page 2021. The warning message for users claims to be from Facebook Security Team. The criminals are tagging politicians including Members of Parliament, MLAs, government officials, and celebrities.

Attack Type
Malware Attack & Social Engineering
Cause of Issue
Lack Of Security Awareness
Type of Loss
Facebook Account & System Compromise
References
https://rb.gy/yfs2qf

Update Your Chrome Browser to Patch New Zero-Day Bug Exploited in the Wild

Google has pushed out a new security update to Chrome browser for Windows, Mac, and Linux with multiple fixes, including a zero-day that it says is being exploited in the wild. The latest patch resolves a total of eight issues, one of which concerns a type confusion issue in its V8 open-source and JavaScript engine (CVE-2021-30563). The search giant credited an anonymous researcher for reporting the flaw on July 12.

Attack Type
Zero Day Vulnerability
Cause of Issue
Lack Of Security Awareness
Type of Loss
Data Theft
References
https://rb.gy/afdea

Threat actors scrape 600 million LinkedIn profiles and are selling the data online – again

LinkedIn appears to have experienced a massive data scrape for the third time in four months. Once again, an archive of data collected from hundreds of millions of LinkedIn user profiles surfaced on a hacker forum. The social media platform is refusing to treat malicious scraping as a security problem. It says it will not allow new victims to be affected by the hack attacks.

Attack Type
Sensitive Data Exposure
Cause of Issue
Lack Of Data Protection
Type of Loss
Profile Data
References
https://rb.gy/bh7xsi

Microsoft warns over this unusual malware that targets Windows and Linux

Microsoft is warning customers about the LemonDuck crypto mining malware which is targeting both Windows and Linux systems. The group was discovered to be using Exchange bugs to mine for cryptocurrency in May, two years after it first emerged. It is taking advantage of high-profile security bugs by exploiting older vulnerabilities during periods where security teams are focussed on patching critical flaws, and even removing rival malware.

Attack Type
Malware Attack
Cause of Issue
Lack Of Malware Protection
Type of Loss
System Compromise
References
https://rb.gy/zrsx86

There are new unpatched bugs in Windows Print Spooler

Security researchers have unearthed new elevation of privilege (EoP) bugs in Windows Print Spooler, one of the oldest Windows components. One bug can be exploited by an attacker to elevate privilege to SYSTEM level (then run arbitrary code with those privileges) The other is a signature-check bypass that also allows EoP, by exploiting certain aspects of the Point and Print capability.

Attack Type
Zero Day Vulnerability
Cause of Issue
Lack Of Security Patches
Type of Loss
System Compromise Via Privilege Escalation
References
https://rb.gy/z320hh

Vulnerability in Schneider Electric PLCs allows for undetectable remote takeover

Attack Type
Zero Day Vulnerability
Cause of Issue
Lack Of Security Patches
Type of Loss
System Compromise
References
https://rb.gy/kid3tc

A vulnerability in Schneider Electric's Modicon programmable logic controllers could allow a remote attacker to gain total and undetectable control over the chips. The vulnerability affects Modicon chips M340, M580 and other models from the Modicon series. Once leaked, attackers can use the stolen hash to take over the secure connection that UMAS establishes between the PLC and its managing workstation. Reconfiguration, in turn, allows the attacker to perform remote code execution attacks, including installation of malware.

Researchers find new attack vector against Kubernetes clusters via misconfigured Argo Workflows instances

Security researchers have found that cybercriminals are going after a new attack vector against Kubernetes clusters via misconfigured Argo Workflows instances. Attackers have been detected dropping crypto-miners like the Kannix/ Monero-miner through this attack vector. Security researchers said the attacks were concerning because there are hundreds of misconfigured deployments. Exposed instances can contain sensitive information such as code and credentials.

Attack Type
Security Misconfiguration
Cause of Issue
Lack Of Patch Management
Type of Loss
Sensitive Instance Data
References
https://rb.gy/5svn2n

SonicWall releases urgent notice about 'imminent' ransomware targeting firmware

Attack Type
Malware Attack (Ransomware)
Cause of Issue
Lack Of Malware Protection.
Type of Loss
Data Encrypted
References
https://rb.gy/htvdt9

Networking device maker SonicWall warns of "imminent ransomware campaign" using stolen credentials. The threat is targeting Secure Mobile Access (SMA) 100 series and Secure Remote Access products running unpatched and end-of-life 8.x firmware. SonicWall urged its users to update to the latest available SRA and SMA firmware, explaining that those who don't are "at imminent risk of a targeted ransomware attack"

FINANCE

Insurance giant CNA reports data breach after ransomware attack

CNA Financial Corporation, a leading US-based insurance company, is notifying customers of a data breach following a Phoenix CryptoLocker ransomware attack that hit its systems in March. "The investigation revealed that the threat actor accessed certain CNA systems at various times from March 5, 2021 to March 21, 2021," CNA said in breach notification letters mailed to affected customers today. "During this time period, the threat actor copied a limited amount information before deploying the ransomware." The data breach reported by CNA affected 75,349 individuals, according to breach information filed with the office of Maine's Attorney General. After reviewing the files stolen during the attack, CNA discovered that they contained customers' personal information such as names and Social Security numbers.

Attack Type
Malware Attack (Ransomware)
Cause of Issue
Lack of Malware Protection
Type of Loss
Data Breach
References
https://rb.gy/yuoyhl

Coinbase Users Face Ongoing Phishing Attacks

Coinbase is the largest exchange in the U.S., and researchers have detected numerous phishing campaigns against Coinbase users. Researchers at anti-phishing firm INKY have discovered dozens of current phishing campaigns targeting Coinbase users. This campaign uses a well-written and presented email supporting the Coinbase logo. There is little in the content to indicate a scam – no spelling errors or typos, and it uses acceptable style and grammar.

Attack Type
Social Enginnering (Phishing)
Cause of Issue
Lack Of Security
Type of Loss
PII Data
References
https://rb.gy/xm607t

Morgan Stanley Hit by Third-Party Vendor That was Using the Accellion FTA Service

Morgan Stanley has told the Attorney General of New Hampshire that the personal information of some of its clients was compromised by a third-party vendor using the Accellion FTA service. Names, residences, birth dates, Social Security numbers, and corporate company names were among the data obtained from the stolen documents. Despite the fact that the stolen files were encrypted, Morgan Stanley claims that the attacker was able to access the decryption key during the security event due to the vulnerability.

Attack Type
Zero-day Vulnerability
Cause of Issue
Improper Patch Management
Type of Loss
PII Data
References
https://rb.gy/xm607t

GOVERNMENT

Malware-infected documents discovered on the Kazakhstan government's portal

The official website of the Kazakhstan government has hosted documents infected with malware for more than five months, since January this year.In a report published last week, T&T Security and Zerde Holding, two local security firms, said they identified at least two documents uploaded on the government's legal and budget-related sections that were installing a version of the Razy malware on users' systems. The two files were made available via eGov.kz, the Kazakhstan government official portal, where citizens can register to file taxes, interact with various government agencies, and download official documents.

Attack Type
Malware Attack
Cause of Issue
Lack Of
Malware Protection
Type of Loss
Reputation &
Data Loss
References
https://rb.gy/a0jjuz

Hackers use new malware to target Indian government officials: SideCopy.

A cyber-espionage group has been observed increasingly targeting Indian government personnel, researchers say. The goal is to steal access credentials from Indian government employees with a focus on espionage, they say. As many as four new custom remote access trojans (RATs) have been deployed, signalling a "boost in their development operations" Targeting tactics and themes observed in campaigns indicate a high degree of similarity to the Transparent Tribe APT (aka APT36)

Attack Type
Trojan
Cause of Issue
Lack Of
Malware Protection.
Type of Loss
Sensitive Data,
System Compromise
References
https://rb.gy/xm607t

The White House has announced the formation of a ransomware task force, and one option is to hack back

The Biden administration is unleashing a range of options to stem the growing ransomware threat, a senior administration official said — including offering rewards as high as $10 million for help identifying the perpetrators. Other options on the table include launching disruptive cyberattacks on hacker gangs, as well as developing partnerships with businesses to speed up the sharing of information about ransomware infections. The White House has formed a previously unannounced cross-government task force to coordinate a series of defensive and offensive measures against ransomware, as POLITICO first reported Wednesday. The actions follow a series of high-profile hacks that have underscored how cybersecurity weaknesses can wreak havoc on American society.

Attack Type
Ransomware
Cause of Issue
Unknown
Type of Loss
Unknown
References
https://rb.gy/1x2pum

GAMING

Malware Detection Increased due to Discord CDN and API Abuses

Researchers have observed a huge increase in the number of Discord malware detections in comparison to last year. A recent report claims that malware incidents have increased 140 times from the last year due to CDN and API abuse. Researchers observers a spike in infostealers and RATs targeting Discord. The attackers behind these operations have used social engineering tricks to propagate credential-stealing malware. The Discord credentials collected from the victims are then used to target other users. In addition to this, the research team has discovered outdated malware—hosted on the Discord CDN—such as spyware and fake app info stealers as well. Researchers had detected more than 4,700 active URLs delivering the malicious Windows .exe.

Attack Type
Malware Attack
Cause of Issue
Lack Of
Malware Protection
Type of Loss
System And Data
Compromise
References
https://rb.gy/163qa2

Pirated Games Spreading Cryptojacking Malware

A new Monero cryptojacking malware has been discovered spreading via cracked versions of well-known online games. According to researchers, the threat is identified as Crackonosh. In the case of Crackonosh, the ultimate goal is to install the coin miner XMRig to mine Monero cryptocurrency from within the cracked software downloaded to the infected device. So far, attackers behind this recent campaign have mined 9000 XMR (more than $2 million) in total. Additionally, the malware is spreading fast, infecting 222,000 unique devices in more than a dozen countries since last December. As of May, it is still getting about 1,000 hits in a single day. Moreover, the most targeted countries are the Philippines with 18,448 victims, followed by Brazil (16,584), India (13,779), Poland (12,727), the U.S. (11,856); and the U.K (8,946).

Attack Type
Malware Attack
Cause of Issue
Lack Of Malware
Protection.
Type of Loss
System Compromise
References
https://rb.gy/28q4ot

HEALTH

UC San Diego Health discloses data breach after phishing attack

UC San Diego Health, the academic health system of the University of California, San Diego, has disclosed a data breach after the compromise of some employees' email accounts. UC San Diego Health discovered unauthorized access to some of its employees' email accounts on April 8, after being initially alerted to suspicious activity on March 12. The attackers may have accessed or acquired the personal information of patients, employees, and students between December 2, 2020, and April 8, 2021, after breaching the email accounts in a phishing attack. There is no "no evidence that other UC San Diego Health systems were impacted, nor do we have any evidence at this time that the information has been misused," the academic health system explained.

Attack Type
Data Breach & Phishing
Cause of Issue
Lack Of Data Protection
Type of Loss
PII Data
References
https://rb.gy/njeiac

US medical imaging center reports possible data breach after emails 'accessed'

A data breach at a US medical imaging center has potentially exposed the private medical information of patients. Express MRI, based in Georgia, Atlanta, revealed that some personal data may have been accessed in a breach dating back to July 10, 2020, during which unauthorized emails were sent from an Express MRI email account. It was originally believed that no medical data was exposed. However a second investigation, which concluded last month, found that while there was "no conclusive evidence" any particular patient information was actually accessed, read, or exported.

Attack Type
Data Breach
Cause of Issue
Lack Of Data Protection
Type of Loss
Email And PII Data
References
https://rb.gy/xm607t

Data breach at third-party provider exposes medical information of US healthcare patients

A data breach at a third-party provider has potentially exposed the private medical information of patients at Northwestern Memorial HealthCare (NMHC) providers. Unknown actors gained unauthorized access to a database owned by Elekta, which provides a cloud-based platform that handles legally-required cancer reporting to the State of Illinois. In a security advisory, the healthcare provider, based in Chicago, said that the attackers made a copy of the datasets, which include patient names, dates of birth, Social Security numbers, health insurance information, and medical record numbers. The database also contained clinical information related to cancer treatment, including medical histories, physician names, dates of service, treatment plans, diagnoses, and/or prescription information.

Attack Type
Data Breach
Cause of Issue
Lack Of Data Protection
Type of Loss
Data Exposure
References
https://rb.gy/detsq3

MOBILE TECH

Turns Out That Low-Risk iOS Wi-Fi Naming Bug Can Hack iPhones Remotely

The Wi-Fi network name bug that was found to completely disable an iPhone's networking functionality had remote code execution capabilities and was silently fixed by Apple earlier this year, according to new research. The denial-of-service vulnerability, which came to light last month, stemmed from the way iOS handled string formats associated with the SSID input, triggering a crash on any up-to-date iPhone that connected to wireless access points with percent symbols in their names such as "%p%s%s%s%s%n." While the issue is remediable by resetting the network settings (Settings > General > Reset > Reset Network Settings), Apple is expected to push a patch for the bug in its iOS 14.7 update, which is currently available to developers and public beta testers.

Attack Type
Zero Day Vulnerability
Cause of Issue
Lack Of Security Patches
Type of Loss
System Compromise
References
https://rb.gy/yuoyhl

Uber found to have interfered with privacy of over 1 million Australians

Attack Type
Data Privacy Violation
Cause of Issue
Lack Of Data Protection
Type of Loss
PII Data
References
https://rb.gy/zzqqv3

The Office of the Australian Information Commissioner (OAIC) has handed down its determination that Uber interfered with the privacy of over 1 million Australians in 2016. The personal data of an estimated 1.2 million Australian customers and drivers were accessed from a breach in October and November 2016. It came to light in late 2017 that hackers had stolen data pertaining to 57 million Uber riders worldwide, as well as data on more than 600,000 drivers. Instead of notifying those impacted, Uber concealed the breach for more than a year and paid a hacker to keep it under wraps.

Malicious Android App Posed As QR Scanner To Launch Joker Malware That Steals SMS Data

Researchers uncovered a new wave of Android malware campaign " Joker" which posed as a QR scanner to target Android users. Joker malware carries functionalities of both Spyware and Trojan capabilities, and quite sophisticated remain undetected through the traditional malware analysis methods. Attackers adapt the traditional evasion technique of Dynamic Code Loading (DCL) and reflection that helps attackers to drop the malicious file on the victim's device. Once the file gets installed and launched by the victim, the malicious app establishes a connection to the Command and control server drops a trojan.

Attack Type
Malware Attack
Cause of Issue
Lack Of Application Security
Type of Loss
User's Sms Data
References
https://rb.gy/mfypii

Signal fixes bug that sent random images to wrong contacts

Signal has fixed a serious bug in its Android app that, in some cases, sent random unintended pictures to contacts without an obvious explanation. Although the issue was reported in December 2020, given the difficulty of reproducing the bug, it isn't until this month that a fix was rolled out to the Android users of the end-to-end encrypted messaging app. When sending an image using the Signal Android app to one of your contacts, the contact would occasionally receive not just the selected image, but additionally a few random, unintended images, that the sender had never sent out.

Attack Type
Application Vulnerability
Cause of Issue
Lack Of Secure Coding
Type of Loss
Reputation Loss
References
https://rb.gy/kxhkqq

Mint Mobile data breach allows hackers to port phone numbers

US-based telecommunication company Mint Mobile has revealed the company became a victim of a data breach that allowed several phone numbers to be ported out to another carrier, along with possible access to subscriber data. An email sent on Saturday to affected customers by Mint Mobile disclosed there was a breach of the carrier's systems. The company also admits the attacker may have gained access to some account information, including names, numbers, email addresses, passwords and account numbers.

Attack Type
Data Breach
Cause of Issue
Lack Of Data Protection
Type of Loss
Data Loss
References
https://rb.gy/gamyzr

Clubhouse may be leaking data to Chinese govt: Stanford report

As invite-only audio chat app Clubhouse becomes popular globally including in India, researchers at Stanford University in the US have warned that the app may be leaking users' audio data to the Chinese government. The Stanford Internet Observatory (SIO) has confirmed that Agora, a Shanghai-based provider of real-time engagement software, supplies back-end infrastructure to the Clubhouse app. The users' metadata is sent over the internet in plaintext (not encrypted), meaning that any third-party with access to a user's network traffic can access it.

Attack Type
Sensitive Data Exposure
Cause of Issue
Lack Of Data Protection
Type of Loss
Profile Data
References
https://rb.gy/ybq9qb

TOOLS OF THE MONTH

WASCAN

WAScan is designed to find various vulnerabilities using the "black-box" method, which means it won't study the source code of web applications but will work like a fuzzier, scanning the pages of the deployed web application, extracting links and forms and attacking the scripts, sending payloads and looking for error messages,..etc.

Read More:
https://www.briskinfosec.com/tooloftheday/toolofthedaydetail/WaScan-web-application-fingerprint-Scanner

WAFW00F

WAFW00F identifies and fingerprints Web Application Firewall (WAF) products. WAFW00F sends a normal HTTP request and analyses the response; this identifies a number of WAF solutions.

Read More:
https://www.briskinfosec.com/tooloftheday/toolofthedaydetail/WafW00f-Tool-to-Fingerprint-and-identify-Web-Application-Firewall

LEGION

Legion is one of the most famous open-source network penetration testing frameworks, which can execute vulnerabilities assessment tasks, to identify online devices in a network, collect nifty information of targeted devices, and expose the attacks against targeted devices.

Read More:
https://www.briskinfosec.com/tooloftheday/toolofthedaydetail/Legion-to-Discover-Reconnaissance-and-exploitation-of-infra-systems

CYBERMONDAY

Cyber Attack Happens Every 39 Seconds

For those who still feel that deploying a firewall or anti-virus in their firm is more than enough to prevent cyberattacks, consider this stunning fact: according to Google's survey, a new and continually developing cyber attack emerges every half-minute.

Cybersecurity is not an easy problem to solve for any business. Just when one challenge has been met, another variable appears

The majority of corporations are well aware of the shortcomings in the security procedures in place. Hackers focus on chaining many medium level vulnerabilities in order to exploit a high/critical level vulnerability. Cybercrime is a major threat to corporate security, according to cybersecurity experts.

What is the purpose of a Cybersecurity Audit?

A cybersecurity audit acts as a 'checklist' to confirm that the policies established by a cybersecurity team are still in existence and that control structures are in place to apply them.

BLOG OF THE MONTH

CLOUD SECURITY AND THE BEST WAYS TO SECURE IT FROM BREACHES

Each and every day, at least 100 organizations from somewhere on this earth face threats in their cloud environment. There isn't just one gateway for security vulnerabilities to strike your cloud environment. There are countless ways for attacks to slump your cloud security and cause data breaches. Hence, a proper security assessment of your cloud environment must be done regularly to stay protected against cyber threats and breaches.

Read More about Jerry Louis's Insight on Cloud Security: https://www.briskinfosec.com/blogs/blogsdetail/Cloud-Security-And-The-Best-Ways-To-Secure-It-From-Breaches-

CONCLUSION

According to an article, online threats has risen by as much as six times their usual levels recently as the Covid 19 pandemic provided greater scope for cyber attacks. All the attacks mentioned above - their types, the financial and reputation impacts they have caused to organizations, the loopholes that paved way for such attacks invariably causing disaster to organizations - are just like a drop in an ocean. There are more unreported than that meets the eye. Millions of organizations and individuals have clicked those links and have fallen victims to these baits of hackers. The most obvious reason being ‘lack of awareness. Well, as the saying goes,

"Prevention is better than Cure" - be it COVID-19 or Cyber threats.

Briskinfosec is ready to help you in your journey to protect your information infrastructure and assets. We assure you that we will help you to keep your data safe and also give you clear information on your company’s current status and what are the steps needed to be taken to stay away from any kind of cyber attack.

We appreciate your ongoing support in our efforts to help Briskinfosec's Threatsploit Report succeed.

CONTACT US FOR ALL YOUR CYBERSECURITY NEEDS

Briskinfosec
Technology and
Consulting Pvt
LtdChennai, india.
Ph - +91 860 863 4123

www.briskinfosec.com.com
contact@briskinfosec.com