THREATSPLOIT
ADVERSARY REPORT

MAY 2021

BRISK INFOSEC
CYBER TRUST & ASSURANCE

EDITION 33

www.briskinfosec.com

INTRODUCTION

Welcome to the Threatsploit report of May 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.

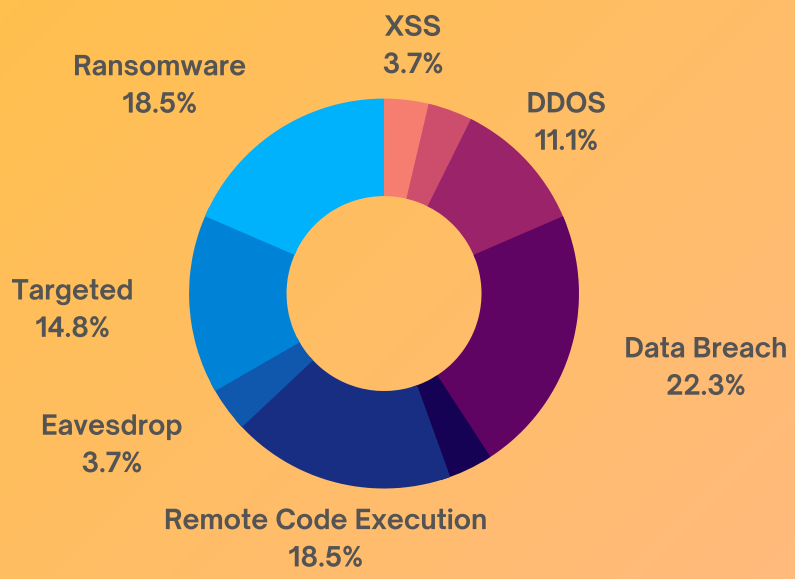
The primary reason is and has always been the same....

"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.

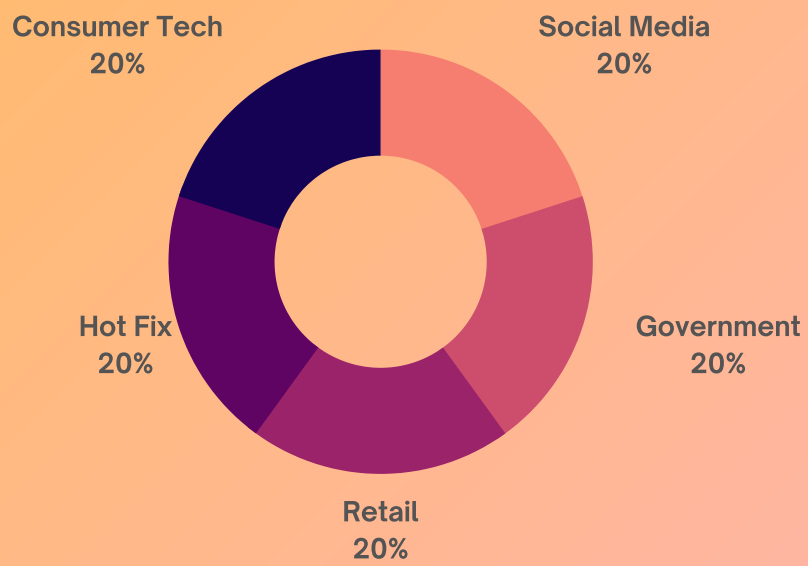
TYPE OF ATTACK VECTORS

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

This chart shows the percentage of Industry sectors that are victim of cyber threats. It is evident that the Consumer Technology has been hit the most



LATEST THREAT ENTRIES

CONSUMER TECH

- Cring Ransomware
- EtterSilent Hacking Tool
- Joker malware infects over 500,000 Huawei Android devices
- Hackers compromised APKPure client to distribute infected Apps
- Cracked copies of Microsoft Office and Adobe Photoshop steal your session cookies, browser history, crypto-coins
- Two million database servers are currently exposed across cloud providers
- Linux Kernel Bug Opens Door to Wider Cyberattacks
- Nvidia Warns: Severe Security Bugs in GPU Driver, vGPU Software
- Apple iOS 14.5 Patches 50 Security Vulnerabilities
- 3.2 Billion Leaked Passwords Contain 1.5 Million Records with Government Emails
- Hackers threaten to leak stolen Apple blueprints if $50 million ransom isn't paid
- F5 BIG-IP Found Vulnerable to Kerberos KDC Spoofing Vulnerability

SOCIAL

- Cybercriminals use Telegram Bots and Google Forms for Automated Phishing
- The credentials of 533 Facebook users have been a leak
- LinkedIn Data Leak: Hundreds of Thousands of Spam Emails Flood Users' Inboxes
- Apple Mail Zero-Click Security Vulnerability Allows Email Snooping
- WhatsApp Pink is malware spreading through group chats

RETAIL

- VISA: Hackers increasingly using web shells to steal credit cards
- Domino's India hacked? Credit data of 10L users on 'sale' for Rs 4 cr
- Zero-Day Exploits Hit SonicWall Enterprise Email Security Appliances

FINANCE

- Celsius Suffers Third-Party Data Breach, Customers Report Phishing Texts, Emails
- India's Data Breach Saga Continues; Country's Second Largest Stockbroker, Upstox, Hit!
- GitHub Infrastructure Used to Mine Cryptocurrency
- Phishing attacks target Chase Bank customers

EDUCATION

- PoC for Moodle flaw released
- University of Hertfordshire Suffers Cyber-Attack That Takes Down its Entire IT Network
- University of California victim of a nationwide hack attack

HOT FIX YOU SHOULD NOTICE

- VMware patches flaws

BRISKINFOSEC TOOL OF THE DAY

- Lynis
- Vulnscan
- Grapefruit
- Nikto
- Xspear
- Altair

CYBER MONDAY

- If you think technology can solve your security problems; then you don't understand the problems and the technology.
- What is the purpose of a Cybersecurity Audit?
- What is Cyber Resilience?

BLOGS OF THE MONTH

- Beware of NetWire RAT Malware spread via Microsoft Excel 4.0 Macro
- Layer Wise Analysis of Security in IoT
- Detection and Exploitation of XML External Entity Attack

CONSUMER TECH

Cring Ransomware

The ransomware, known as Cring, first appeared in January and exploits a vulnerability in Fortigate VPN servers. While Fortinet released a security patch to address the vulnerability, cyber criminals can still use the exploit against networks that have yet to implement the security update. Attackers can remotely access the username and password by manipulating unpatched VPN applications, enabling them to manually connect to the network.

Attack Type
Security Breach
Cause of Issue
Ransomware
Type of Loss
Reputation
References
https://rb.gy/q2ijpc

EtterSilent Hacking Tool

Attack Type
Security Breach
Cause of Issue
Lack of Security
Type of Loss
Reputation
References
https://rb.gy/jjehqs

According to the study, the document maker, known as EtterSilent, has been marketed in a Russian cybercrime forum and comes in two versions. One exploits a Microsoft Office vulnerability, CVE-2017-8570, and the other employs a malicious macro. As per the researchers, EtterSilent was used in a campaign last month that used another method named Bazar loader against targets, which can help attackers infect victims with other malware or ransomware.

Joker malware infects over 500,000 Huawei Android devices

More than 500,000 Huawei users have downloaded applications infected with Joker malware that subscribes to premium mobile services from the company's official Android store. In AppGallery, researchers discovered ten seemingly harmless apps that contained code for connecting to a malicious command and control server to receive configurations and additional components.

Attack Type
Malicious Mobile Applications
Cause of Issue
Malware Apps
Type of Loss
PII Data
References
https://rb.gy/iyzarh

Hackers compromised APKPure client to distribute infected Apps

Attack Type
Trojan
Cause of Issue
Malware
Type of Loss
Data
References
https://rb.gy/ozkyl0

APKPure, one of the most popular alternative app stores, was the target of a supply chain attack in which threat actors exploited client version 3.17.18 in order to distribute malware. The study of the client's code showed that the intruder altered it by inserting the Android. Malware named Triada. The Triada Trojan will penetrate all processes running on mobile devices and gain persistence, allowing threat actors to download, instal, and uninstall payloads without the users' permission.

Cracked copies of Microsoft Office and Adobe Photoshop steal your session cookies, browser history, crypto-coins

Bitdefender has issued an alert that pirated versions of Microsoft Office and Adobe Photoshop are stealing browser session cookies and Monero cryptocurrency wallets from tightwads who instal them. Bitdefender discovered that some versions of both suites were being spread with malware that stole browser session cookies (or, in the case of Firefox, the user's entire profile history), hijacked Monero cryptocurrency wallets, and exfiltrated other data via BitTorrent after first opening a backdoor and disabling the target machine's firewall.

Attack Type
Malware
Cause of Issue
Using Cracked Software
Type of Loss
Data
References
https://rb.gy/vxocpc

Two million database servers are currently exposed across cloud providers

Attack Type
Security Misconfiguration
Cause of Issue
Lack of Security Best Practices
Type of Loss
Full System/ Data Compromise
References
https://rb.gy/tqmdv9

Censys discovered more than 1.93 million databases on cloud servers that were exposed online without a firewall or other security safeguards, according to its study, which was published in April 2021. According to the security firm, threat actors may discover these databases and assault them with exploits for older vulnerabilities in order to gain access to their data. Furthermore, if the database was accidentally leaked, it is likely that it is also using a weak or no password, revealing its entire contents to everyone who discovers its IP address.

Linux Kernel Bug Opens Door to Wider Cyberattacks

An information-disclosure protection flaw in the Linux kernel has been discovered, which can be exploited to reveal information in compromised devices' kernel stack memory. According to Cisco Talos, which discovered the flaw, the bug (CVE-2020-28588) occurs in the /proc/pid/syscall functionality of 32-bit ARM devices running Linux. It is caused by an incorrect conversion of numeric values when reading the text. Attackers may generate 24 bytes of uninitialized stack memory with a few commands, which can be used to circumvent kernel address space layout randomization (KASLR).

Attack Type
Security Update Issue
Cause of Issue
Security Flaw
Type of Loss
Unknown
References
https://rb.gy/b2nbcr

Nvidia Warns: Severe Security Bugs in GPU Driver, vGPU Software

Attack Type
Cyber Security Research
Cause of Issue
CVE Finding
Type of Loss
Unknown
References
https://rb.gy/1twkwb

Nvidia has disclosed a collection of security flaws in its graphics processing unit (GPU) display driver that could expose gamers and others to privilege-escalation attacks, arbitrary code execution, denial of service (DoS), and information disclosure. Meanwhile, Nvidia's virtual GPU (vGPU) programme contains a number of flaws that could lead to a variety of similar attacks.

Apple iOS 14.5 Patches 50 Security Vulnerabilities

The fix, which is currently being rolled out through the iOS and iPadOS automatic-update mechanisms, provides protection against a WebKit vulnerability that Apple claims attackers might have exploited in the wild. The most critical of the 50 known vulnerabilities (CVE-2021-30661), according to Apple, is a use-after-free memory corruption bug in WebKit Storage. The iOS and iPadOS 14.5 updates also address a slew of high-risk "arbitrary code execution" flaws in a variety of mobile operating system components, including flaws in FontParser and ImageIO.

Attack Type
Cyber Security Research
Cause of Issue
Memory Corruption Bug
Type of Loss
Unknown
References
https://rb.gy/ddnrom

3.2 Billion Leaked Passwords Contain 1.5 Million Records with Government Emails

Attack Type
Data Leak
Cause of Issue
Security Breach
Type of Loss
Government Data, Personal Data
References
https://rb.gy/himkxv

In one of the biggest data dumps of breached usernames and passwords, 3.28 billion passwords linked to 2.18 billion unique email addresses were revealed. Furthermore, the leak contains 1,502,909 passwords associated with email addresses from government domains around the world, with the United States government alone accounting for 625,505 of the leaked passwords, followed by the United Kingdom (205,099), Australia (136,025), Brazil (68,535), and Canada (50,726). The results are based on an examination of a large 100GB data collection known as "COMB21" — aka Compilation of Several Breaches — that was made available for free in an online cybercrime forum earlier this February by combining data from numerous leaks in various companies and organisations that occurred over the years.

Hackers threaten to leak stolen Apple blueprints if $50 million ransom isn't paid

Quanta, a major Apple supplier, announced on Wednesday that it had been the victim of a ransomware attack by the REvil ransomware community, which is now demanding that the iPhone maker pay a $50 million ransom to prevent confidential data from being leaked on the dark web.

Attack Type
Ransomware
Cause of Issue
Security Breach
Type of Loss
Financial, Business Data
References
https://rb.gy/7k6q1x

3.2 Billion Leaked Passwords Contain 1.5 Million Records with Government Emails

Attack Type
Data Leak
Cause of Issue
Security Breach
Type of Loss
Government Data, Personal Data
References
https://rb.gy/himkxv

According to cybersecurity researchers, F5 Big-IP application delivery services are vulnerable to a new bypass vulnerability (CVE-2021-23008) in the Kerberos Key Distribution Center (KDC) defence function. The KDC Spoofing vulnerability enables an attacker to bypass security policies and gain unrestricted access to sensitive workloads by circumventing Kerberos authentication to Big-IP Access Policy Manager (APM).

SOCIAL

Cybercriminals use Telegram Bots and Google Forms for Automated Phishing

Threat actors are using Google Forms and Telegram as alternate methods to collect stolen data and begin using it right away. Furthermore, Telegram bots are used in automated phishing platforms available on the dark web. The admin panel manages the overall phishing assault as well as the related financial records.

Attack Type
Online Scams
Cause of Issue
Automated Phishing Attack
Type of Loss
Data
References
https://rb.gy/o6h9wz

The credentials of 533 Facebook users have been leaked

Attack Type
Data Breach
Cause of Issue
Unknown
Type of Loss
PII Data
References
https://rb.gy/kmfham

A user on a low-level hacking platform freely distributed the phone numbers and personal information of hundreds of millions of Facebook users online. The exposed data contains personal information from over 533 million Facebook users from 106 countries, including over 32 million records on US users, 11 million on UK users, and 6 million on Indian users. It contains their phone numbers, Facebook IDs, full names, addresses, birthdates, profiles, and, in some cases, email addresses.

LinkedIn Data Leak: Hundreds of Thousands of Spam Emails Flood Users' Inboxes

Users of the job-searching online service are being threatened with a slew of phishing emails and scams in an effort to hijack their accounts or promote bogus LinkedIn email leads. According to Bitdefender Antispam Lab telemetry, the impact of the LinkedIn data leak appears to have already manifested itself in the form of new spam campaigns targeting the inboxes of hundreds of thousands of users.

Attack Type
Phishing
Cause of Issue
Spam Mails
Type of Loss
Data
References
https://rb.gy/ixh0b0

Apple Mail Zero-Click Security Vulnerability Allows Email Snooping

Attack Type
Broken Access Control
Cause of Issue
Security Flaw
Type of Loss
Data
References
https://rb.gy/jk96id

A zero-click security flaw in Apple's macOS Mail will allow a cyberattacker to add or change any arbitrary file within Mail's sandbox environment, opening the door to a variety of attacks. Exploiting the bug could result in the unauthorised disclosure of sensitive information to a third party; the ability to alter a victim's Mail configuration, including mail redirects that allow the takeover of the victim's other accounts through password resets; and the ability to adjust the victim's configuration so that the attack can spread to correspondents in a worm-like fashion.

WhatsApp Pink is malware spreading through group chats

An odd baiting tactic has emerged, with WhatsApp users receiving links claiming to change the app's theme from its trademark green to pink. Simultaneously, it offers "new functions" that have yet to be defined. Cyber experts have advised users of the messaging app to avoid clicking on any such links. The worrying aspect is that the connection has been disguised as an official WhatsApp update, leaving people unaware of the sinister intent behind the link's distribution.

Attack Type
Phishing
Cause of Issue
Lack of Security
Type of Loss
Private Data
References
https://rb.gy/0zy0ez

RETAIL

VISA: Hackers increasingly using web shells to steal credit cards

Attack Type
RCE via Shell Upload
Cause of Issue
Malicious File Uploads
Type of Loss
Reputation
References
https://rb.gy/t4dqjf

Bitdefender has issued an alert that pirated versions of Microsoft Office and Adobe Photoshop are stealing browser session cookies and Monero cryptocurrency wallets from tightwads who instal them. Bitdefender discovered that some versions of both suites were being spread with malware that stole browser session cookies (or, in the case of Firefox, the user's entire profile history), hijacked Monero cryptocurrency wallets, and exfiltrated other data via BitTorrent after first opening a backdoor and disabling the target machine's firewall.

Domino's India hacked? Credit data of 10L users on 'sale' for Rs 4 cr

Bitdefender has issued an alert that pirated versions of Microsoft Office and Adobe Photoshop are stealing browser session cookies and Monero cryptocurrency wallets from tightwads who instal them. Bitdefender discovered that some versions of both suites were being spread with malware that stole browser session cookies (or, in the case of Firefox, the user's entire profile history), hijacked Monero cryptocurrency wallets, and exfiltrated other data via BitTorrent after first opening a backdoor and disabling the target machine's firewall.

Attack Type
Data Breach
Cause of Issue
Lack of Security
Type of Loss
PII Data, Financial Data
References
https://rb.gy/wbqzcr

Zero-Day Exploits Hit SonicWall Enterprise Email Security Appliances

Attack Type
Security Breach
Cause of Issue
Ransomware
Type of Loss
Reputation
References
https://bit.ly/3vIfvWn

SonicWall has patched three crucial security flaws in its hosted and on-premises email security (ES) product that is currently being actively exploited. The vulnerabilities were discovered and disclosed to SonicWall on March 26, 2021, by FireEye's Mandiant subsidiary, after the cybersecurity firm observed post-exploitation web shell behaviour on an internet-accessible device inside a customer's environment that had SonicWall's ES framework running on a Windows Server 2012 installation. On April 6, 2021, FireEye reported a third vulnerability (CVE-2021-20023) to SonicWall.

FINANCE

Celsius Suffers Third-Party Data Breach, Customers Report Phishing Texts, Emails

According to the study, the document maker, known as EtterSilent, has been marketed in a Russian cybercrime forum and comes in two versions. One exploits a Microsoft Office vulnerability, CVE-2017-8570, and the other employs a malicious macro. As per the researchers, EtterSilent was used in a campaign last month that used another method named Bazar loader against targets, which can help attackers infect victims with other malware or ransomware.

Attack Type
Security Breach
Cause of Issue
Spam Mails
Type of Loss
PII Data
References
https://rb.gy/eelzqk

India's Data Breach Saga Continues; Country's Second Largest Stockbroker, Upstox, Hit!

Attack Type
KYC Data Leak
Cause of Issue
Security Flaw
Type of Loss
PII Data
Financial Data
References
https://rb.gy/sviovh

Upstox, India's second-largest stockbroker, is said to have experienced a data breach that affected nearly 2.5 million of its users. The leak was discovered when the infamous threat group "ShinyHunters" sold the stolen data on the dark web. According to the information revealed, the following details were leaked: Full Names, Email Address, Date of Birth, PAN (Permanent Account Number), KYC information and so on.

GitHub Infrastructure Used to Mine Cryptocurrency

A series of malicious activities on software developers' repositories have been published, with the end goal of mining cryptocurrency. Threat actors appear to be targeting repositories with this function activated in order to add malicious GitHub Actions and fill Pull Requests that will later aid them in executing malicious attacker code.

Attack Type
Malicious Code Execution
Cause of Issue
Security Flaw
Type of Loss
Data
References
https://rb.gy/fu823z

Phishing attacks target Chase Bank customers

Attack Type
Social Engineering
Cause of Issue
Phishing Attack
Type of Loss
Unknown
References
https://rb.gy/vfsxqx

Armorblox found two email campaigns that impersonated Chase in an effort to steal login credentials. Armorblox, an email protection company, published a new study on Tuesday that examined two recent phishing campaigns targeted at Chase Bank customers and provided advice on how to defend yourself from such scams. The first advertisement purported to include a credit card receipt, while the second informed recipients that their account access had been limited due to suspicious behaviour. The target in both cases was the same: obtain your account credentials.

EDUCATION

PoC for Moodle flaw released

The Wizcase cyber research team, led by Ata Hakcil, discovered a security flaw in Moodle, an open-source learning platform. Anyone with an account on a given school's Moodle (with the TeX filter enabled) could then take over the accounts of students, professors, and even platform administrators.

Attack Type
User Account Takeover
Cause of Issue
Security Flaw
Type of Loss
Data Loss
References
https://rb.gy/5ae8et

University of Hertfordshire Suffers Cyber-Attack That Takes Down its Entire IT Network

Attack Type
Cyber Attack
Cause of Issue
Ransomware
Type of Loss
Reputation
References
https://rb.gy/hu4wqm

VMware has patched two vulnerabilities in its vRealize Operations (vROps) product. The bugs, CVE-2021-21975 and CVE-2021-21983, are related to server-side request forgery and an arbitrary file write problem. VMware has patched the bugs in all affected versions of vRealize Operation Manager, as well as Cloud Foundation and vRealize Suite Lifecycle Manager.

University of California victim of a nationwide hack attack

The University of California is advising its students and employees that a ransomware group might have stolen and released their personal information, as well as that of hundreds of other colleges, government agencies, and businesses around the country. According to the statement, the hacker or hackers have also been sending threatening mass emails threatening to publish data "in an effort to scare people into giving them money."

Attack Type
Security Breach
Cause of Issue
Ransomware
Type of Loss
PII Data, Financial Data
References
https://rb.gy/xoqdtf

HOT FIX YOU SHOULD LOOK

VMware patches flaws

Attack Type
Server Side Request Forgery (SSRF)
Cause of Issue
Security Flaw
Type of Loss
Reputation
References
https://rb.gy/1ikqtp

VMware has patched two vulnerabilities in its vRealize Operations (vROps) product. The bugs, CVE-2021-21975 and CVE-2021-21983, are related to server-side request forgery and an arbitrary file write problem. VMware has patched the bugs in all affected versions of vRealize Operation Manager, as well as Cloud Foundation and vRealize Suite Lifecycle Manager.

TOOL OF THE MONTH

Lynis

Lynis is a security auditing tool for systems based on UNIX like Linux, macOS, BSD, and others. It performs an in-depth security scan and runs on the system itself. The primary goal is to test security defences and provide tips for further system hardening. It will also scan for general system information, vulnerable software packages, and possible configuration issues. Lynis was commonly used by system administrators and auditors to assess the security defences of their systems.

Vulscan

Vulscan is a module that enhances nmap to a vulnerability scanner. The nmap option -sV enables version detection per service which is used to determine potential flaws according to the identified product. The data is looked up in an offline version of VulDB.

Grapefruit

Grapefruit is a runtime Application Instruments for iOS application and previously it was known by passionfruit. It is used in runtime analysis, which can able to get iOS app details like binary information,listing classes, methods, browsing application's files in real-time, etc..

Nikto

Nikto is an Open Source web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software.

Xspear

Xspear is a powerful XSS scanning and parameter analysis tool on ruby gems, capable of both static and dynamic XSS vulnerability analysis. Therefore, it has the ability to scan, detect and analyze potential XSS vulnerabilities on web applications.

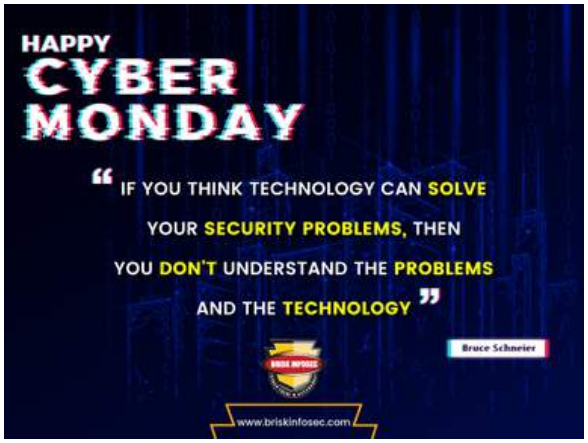
Altair

Altair is a Python-based tool that does not require any specific packages to be installed as a prerequisite. The SQLMAP and Lfier tools must be available at the disposal of the tool if the goal is to exploit the (LFI, SQL) vulnerabilities found during the scanning process.

CYBERMONDAY

If you think technology can solve your security problems; then you dont understand the problems and the technology.

Simply put, not all security problems are caused by technology. As a result, technology cannot solve the problems. There are several factors that contribute to the nature of a security issue. Some examples include human errors, negligence, complex coding, insider misuse, and so on. For all of these reasons, technology may be a band-aid rather than a panacea.



What is the purpose of a Cybersecurity Audit?

A cybersecurity audit serves as a 'checklist' to ensure that the policies stated by a cybersecurity team are currently in effect and that there are control structures in place to implement them.

What is Cyber Resilience?

Cyber resilience is an organization's ability to allow business acceleration (enterprise resiliency) by anticipating, reacting to, and recovering from cyber threats. A cyber-resilient organisation is capable of adapting to both known and unknown emergencies, threats, adversities, and challenge

BLOG OF THE MONTH

Beware of NetWire RAT Malware spread via Microsoft Excel 4.0 Macro

Microsoft Excel is one of the most commonly used office software in the world, and it is used to create and edit large spreadsheets. An application with this much popularity must be protected with the utmost care. NetWire Malware is a type of Remote Access Trojan (RAT) that can gain access to the target's machine registries, run infected scripts, delete data, and so on. The makers of NetWire Malware have been effective in spreading the malware using Microsoft Excel 4.0. This blog describes how NetWire Malware propagates through MS Excel and the impact it has.

Detection and Exploitation of XML External Entity Attack

An XML external entity injection (also known as XXE) web security vulnerability allows an attacker to interfere with an application's processing of XML data. An intruder can frequently view files on the filesystem of the application server and communicate with any back-end or external systems that the application can access. Depending on the application's behaviour, XXE can be manipulated using a variety of techniques. XML parsers are used to process inputs from the front-end application for the APIs in most web applications.

Layer Wise Analysis of Security in IOT

The Internet of Things (IOT) has spread its roots into many modern-day sectors such as smart cities, health, transportation, and so on. The risk of technology being vulnerable grows in direct proportion to its success. Sensors, as we all know, are highly vulnerable to security threats. This blog aims to discuss popular security issues and concerns in the Internet of Things.

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.

contact@briskinfosec.com | www.briskinfosec.com