EDITION 28

DECEMBER

2020

THREATSPLOIT

ADVERSARY REPORT

PREPARED BY

Briskinfosec Technology

www.briskinfosec.com

INTRODUCTION

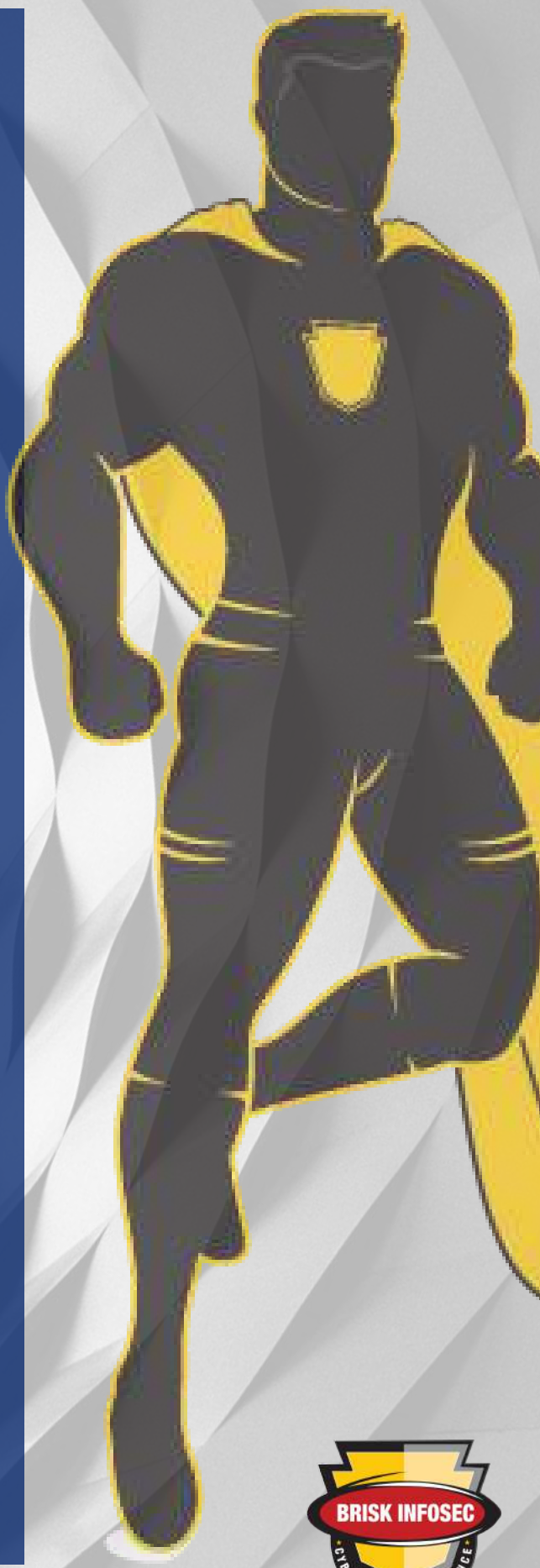
Welcome to the Threatsploit report of Decemeber 2020 covering some of the important cyber security events, incidents and exploits that occurred this month. This month, cyber security sector witnessed a massive rise in ransomware and data breach attacks across geographies. Besides, many other attack types 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".

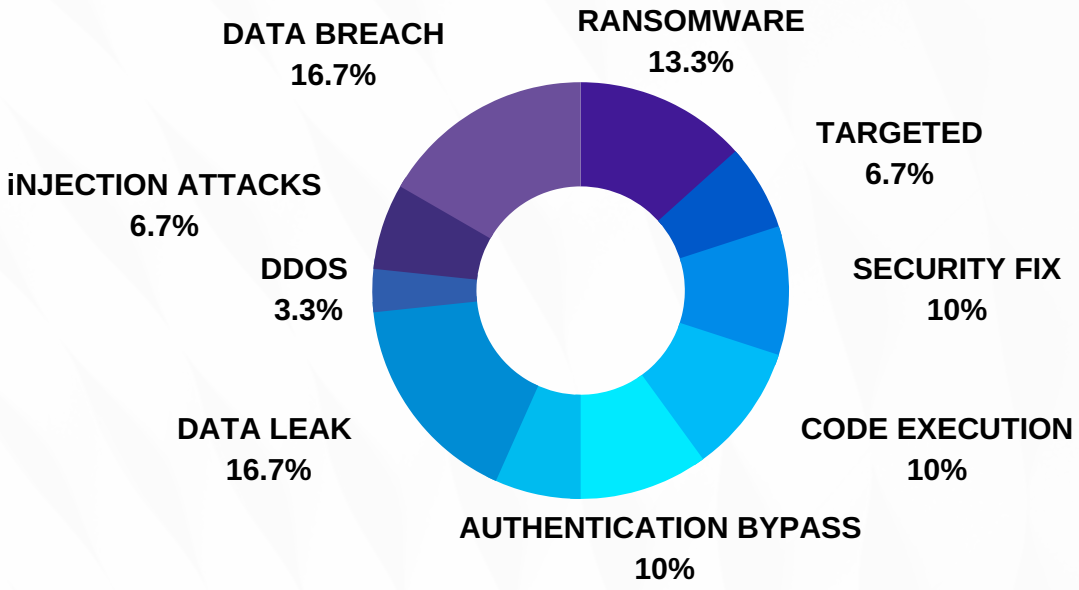
Since the time Work From Home (WFH) has become the new normal, security incidents has peaked with more and more issues relating to VPNs and other remote connecting mediums. WFH option has further limited the ability of IT functions to apply software patches for both old and new critical vulnerabilities,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

Let us walk you through some of the important security incidents that happened in the month of Decemeber 2020.



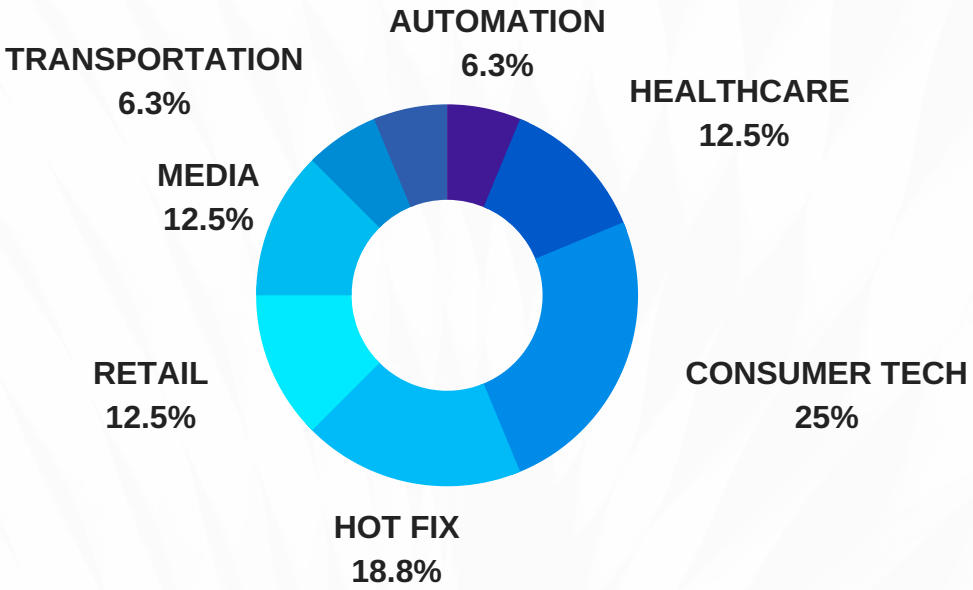
TYPES OF ATTACK VECTORS

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

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



Cyberattacks target every sector. But, a majority of them seemed to be impacting consumer technology sector (25%). To prevent any attack, organisations need the best of cyber security partners. Needless to say, Cyber security as a function is assuming very high importance like the Operations, Sales, Finance or Human Resources.

LATEST THREAT ENTRIES

RETAIL

- Eatigo reports data breach, personal data from customer accounts listed for sale online
- Prestige Software data breach exposes millions of user records
- Ransomware hits e-commerce platform X-Cart
- South Korea’s largest retailers E-Land hit by ransomware attack

MEDIA AND ENTERTAINMENT

- Gaming Partners International (GPI) has become the latest victim of Russian hacker group REvil
- Data breach at Mashable leaks users information
- Capcom discloses cyberattack impacting email, file servers
- France Banijay Group hit by Ransomware

HEALTHCARE

- Chesapeake Regional Healthcare data breach exposes 23,000 individuals sensitive information
- Lupin, has reported a cybersecurity attack on its IT systems
- Louisiana Hospitals Report Data Breach
- Personal data of 16 million Brazilian COVID-19 patients exposed online

CONSUMER TECH

- Cobalt Strike source code reportedly leaked on GitHub
- Baidu's Android apps caught collecting sensitive user details
- Hacker leaks the user data of event management app Peatix
- GitHub has finally fixed a high severity security flaw
- Unpatched Bug in GO SMS Pro App Exposes Millions of Media Messages
- SAD DNS — New Flaws Re-Enable DNS Cache Poisoning Attacks
- Apple Lets Some of its Big Sur macOS Apps Bypass Firewall and VPNs
- Robotic vacuum cleaners can be remotely hacked to be able to pick up audio

LATEST THREAT ENTRIES

SOCIAL MEDIA

- Facebook Messenger Bug Lets Hackers Listen to You Before You Pick Up the Call
- TikTok patches reflected XSS bug, one-click account takeover exploit

AUTOMATION

- Critical Flaw Affecting Industrial Automation Systems
- New Bluetooth Attack Can Steal a Tesla Model X in Minutes

HOT FIX YOU SHOULD NOTICE..

- Microsoft Releases Windows Security Updates For Critical Flaws
- 3 Actively Exploited 0-Days Discovered on IOS
- Researcher Discloses Critical RCE Flaws In Cisco Security Manager
- VMware fixed SD-WAN flaws that could allow hackers to target enterprise networks
- Drupal-based sites open to attack via double extension files
- 2-Factor Authentication Bypass Flaw Reported in cPanel and WHM Software

Briskinfosec Tool of the day

- Corsy web application vulnerability scanner
- SNIPPER vulnerability scanner
- RACCON scanner
- MobSF Mobile security scanner
- APKTool for reverse engineeringtool
- Arachini vulnerability scanner

Cyber Monday

- Cloud Threats
- Cybersecurity Problem
- Cyber security Strategy

Blogs of the month

- Controller area network
- Web services and api
- Cyber security products Vs Cyber security services

Eatigo reports data breach, personal data from customer accounts listed for sale online

Personal data from potentially 2.8 million Eatigo accounts were illegally assessed in a data breach. The Singapore based restaurant reservation platform said that along with other e-commerce sites, it was the subject of "a data security incident involving unauthorised access to our customer database and the information has been illegally accessed over 18 months ago that included customer names, email addresses and phone numbers". But, they confirmed that passwords are encrypted and safe.

ATTACK TYPE
Data breach
CAUSE OF ISSUE
Unauthorised access
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/2VeTqRR

Prestige Software data breach exposes millions of user records

ATTACK TYPE
Data breach
CAUSE OF ISSUE
Security misconfiguration
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/33tF4FD

Prestige Software, the company behind hotel reservation software used by Expedia, booking.com, Hotels.com and other travel companies, has exposed millions of hotel guest records in a data breach. The company's Cloud Hospitality software had been storing guest data on an unsecured Amazon Web Services cloud database for seven years. The exposed information included full names, email addresses, national ID numbers, phone numbers, card numbers, cardholder's name, CVV, and expiration date, as well as the details of the hotel reservation.

Ransomware hits e-commerce platform X-Cart

E-commerce software vendor X-Cart suffered a ransomware attack that brought down customer stores hosted on the company's hosting platform. The incident is believed to have taken place after attackers exploited a vulnerability in a third-party software to gain access to X-Cart's store hosting systems. Cohen said the attackers gained access to a small number of servers which they encrypted but our core systems were not impacted.

ATTACK TYPE
Ransomware
CAUSE OF ISSUE
Poor security pratice
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://zd.net/3Ij8obD

South Korea's largest retailers E-Land hit by ransomware attack

ATTACK TYPE
Ransomware
CAUSE OF ISSUE
Lack of security
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/361pod7

E-Land said its corporate network system was attacked early in the morning, forcing it to close 23 of its 50 NC department stores and NewCore outlets. McAfee advises all e-commerce businesses to have a page on their site dedicated to educating customers on what to look out for to avoid scams, and to communicate any scams that have been reported. Additionally, employees should be trained in what to look for in order to better identify potential scams that may be occurring.

Gaming Partners International (GPI) has become the latest victim of Russian hacker group REvil

ATTACK TYPE
Data Leak
CAUSE OF ISSUE
Ransomware attack
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/2VdLmrQ

Land-based casino equipment supplier Gaming Partners International (GPI) has become the latest victim of Russian hacker group REvil. Revil revealed that the group has stolen 540 gigabytes of sensitive data from GPI, including financial documents, contracts and technical documentation for all of the company's gaming machines and hacked the GPI servers as well. They've threatened to leak all sensitive information publicly if ransom through crypto currency isn't paid inside 72 hours.

Data breach at Mashable leaks users information

ATTACK TYPE
Data breach
CAUSE OF ISSUE
Lack of security
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/2JnqZW0

Data belonging to users of American culture and technology news website Mashable has been leaked on the internet. The exposed data is linked to a sign-in feature that is no longer in use on the Mashable website. Information leaked included first and last names, location data, email addresses, gender, date of registration, IP addresses. Mashable has temporarily disabled access to all accounts impacted by the security breach as a cautionary measure.

Capcom discloses cyberattack impacting email, file servers

ATTACK TYPE
Unauthorized access
CAUSE OF ISSUE
Lack of maintenance
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/3ojFMRB

Capcom has disclosed a cyberattack that impacted the company's operations over the weekend. The Osaka, Japan-based video game developer said in a notice "some of the Capcom Group networks experienced issues that affected access to certain systems" due to a cyberattack impacting email and file servers. Unauthorized access conducted by a third-party is the reason for this disaster confirmed Capcom and as a mitigation, some operations on its internal networks were halted.

France Banijay Group hit by Ransomware

ATTACK TYPE
Ransomware
CAUSE OF ISSUE
Lack of security
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/3mk3P2b

France-based Entertainment Company Banijay Group is reported to have become a victim of a ransomware attack where hackers accessed and stole sensitive details of employee, including bank details and home addresses. High placed sources say that the cyber attack where hackers are seen demanding millions to decrypt or unlock the data disrupted the servers. It was discovered that the attack was carried out on Endemol Shine Group, and the hackers infiltrated other networks through this database.

Chesapeake Regional Healthcare data breach exposes 23,000 individuals sensitive information

A data breach at Chesapeake Regional Healthcare in Virginia revealed that the personal data of 23,058 patients, donors, and employees have been accessed as a result of a third-party breach. The compromised information like names, mail addresses, email addresses, and demographics, such as donation dates and amounts, were included in the leak. Those affected by the incident have been notified by first class mail and email.

ATTACK TYPE
Data breach
CAUSE OF ISSUE
Lack of security
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/3ojFMRB

Lupin, has reported a cybersecurity attack on its IT systems

ATTACK TYPE
Ransomware
CAUSE OF ISSUE
Poor security pratice
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/21qH6CZ

Another leading Indian pharmaceutical, Lupin, has reported a cybersecurity attack on its IT systems within two weeks of a ransomware attack on Dr Reddy's Laboratories. The incident affected multiple internal systems. The attack also reportedly forced the company to shut down its manufacturing facilities across the world to minimise the attack's impact. Amongst all, the healthcare industry also takes the longest amount of time to detect a breach and then contain the attack.

Louisiana Hospitals Report Data Breach

The data of thousands of patients has been exposed following a cyber-attack on Louisiana State University medical centers. LSU Health New Orleans issued a HIPAA breach notification on November 20 after detecting a cyber-intrusion into an employee's electronic mailbox. Data exposed in the attack may have included patients' names, medical record numbers, account numbers, dates of birth, Social Security numbers, dates of service, types of services received, phone numbers and/or addresses, and insurance identification numbers.

ATTACK TYPE
Data breach
CAUSE OF ISSUE
Poor security pratice
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/3fLpGwV

Personal data of 16 million Brazilian COVID-19 patients exposed online

ATTACK TYPE
Data Leak
CAUSE OF ISSUE
Human error
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://zd.net/33rGwMi

The personal and health information of more than 16 million Brazilian COVID-19 patients has been leaked online after a hospital employee uploaded a spreadsheet with usernames, passwords, and access keys to sensitive government systems on GitHub this month. The leak came to light after a GitHub user spotted the spreadsheet containing the passwords on the personal GitHub account of an employee of the Albert Einstein Hospital in the city of Sao Paolo. Later, spreadsheet was removed and officials changed passwords and revoked access keys to resecure their systems.

CONSUMER TECH

Cobalt Strike source code reportedly leaked on GitHub

ATTACK TYPE
Data Leak
CAUSE OF ISSUE
Security misconfiguration
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/36hVc2d

The source code for the well-known penetration testing tool Cobalt Strike appears to have been leaked on GitHub and immediately forked to at least 20 other accounts. The software is used for adversary simulations and so-called red team operations. The source code was made available on GitHub and decompiled before it was posted on the source code repository and the licence check code has been edited out.

Baidu's Android apps caught collecting sensitive user details

ATTACK TYPE
Targetted
CAUSE OF ISSUE
Poor security pratice
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://zd.net/3qbbEcx

Data collection issue identified in Baidu Maps and Baidu Search Box apps. Both apps were removed from the Play Store in October 2020 after a Google investigation revealing that they contained codes regarding users information. The code collected details such as phone model, MAC address, carrier information, and IMSI (International Mobile Subscriber Identity) number. While some of the collected information was "rather harmless," some data like the IMSI code "can be used to uniquely identify and track a user, even if that user switches to a different phone."

Hacker leaks the user data of event management app Peatix

ATTACK TYPE
Data Leak
CAUSE OF ISSUE
Lack of security
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://zd.net/2Inkj1f

A hacker has leaked this month the data of more than 4.2 million users registered on Peatix, an event organizing platform, currently ranked among the Alexa Top 3,500 most popular sites on the internet. The leaked information included full names, usernames, emails, and salted and hashed passwords. Peatix reassured users that no financial data was involved as all payments were handled through third-party platforms, and nothing was stored inside its database.

GitHub has finally fixed a high severity security flaw

ATTACK TYPE
Injection attacks
CAUSE OF ISSUE
Lack of maintenance
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://zd.net/3lo4NsK

GitHub has finally fixed a high severity security flaw reported to it by Google Project Zero more than three months ago. The bug affected GitHub's Actions feature – a developer workflow automation tool – that Google Project Zero researcher Felix Wilhelm said was "highly vulnerable to injection attacks". GitHub's Actions support a feature called workflow commands as a communication channel between the Action runner and the executed action. While Google described it as a 'high severity' bug, GitHub argued it was a 'moderate security vulnerability.'

CONSUMER TECH

Unpatched Bug in GO SMS Pro App Exposes Millions of Media Messages

GO SMS Pro, a popular messaging app for Android with over 100 million installs, has been found to have an unpatched security flaw that publicly exposes media transferred between users, including private voice messages, photos, and videos. The sensitive media shared between users of this messenger app is at risk of being compromised by an unauthenticated attacker or curious user due to this security flaw. According to investigation, the shortcoming was spotted in version 7.91 of the app, which was released on the Google Play Store.

ATTACK TYPE
Data Leak
CAUSE OF ISSUE
Security flaw
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/3qbLzdt

SAD DNS — New Flaws Re-Enable DNS Cache Poisoning Attacks

ATTACK TYPE
SAD DNS attack
CAUSE OF ISSUE
Security flaw
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/2VdcdEr

Dubbed "SAD DNS attack" (short for Side-channel Attack D DNS), the technique makes it possible for a malicious actor to carry out an off-path attack, rerouting any traffic originally destined to a specific domain to a server under their control, thereby allowing them to eavesdrop and tamper with the communications. "The attack allows an off-path attacker to inject a malicious DNS record into a DNS cache." Tracked as CVE-2020-25705, the findings were presented at the ACM Conference on Computer, and Communications Security (CCS '20) held this week.

Apple Lets Some of its Big Sur macOS Apps Bypass Firewall and VPNs

Apple is facing the heat for a new feature in macOS Big Sur that allows many of its own apps to bypass firewalls and VPNs, thereby potentially allowing malware to exploit the same shortcoming to access sensitive data stored on users' systems and transmit them to remote servers. Of particular note is the possibility that the bypass can leave macOS systems open to attack, not to mention the inability to limit or block network traffic at users' discretion. 50 Apple-specific apps and processes have been exempted from firewalls like Little Snitch and Lulu.

ATTACK TYPE
Authentication
CAUSE OF ISSUE
Security misconfiguration
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/3o6BnkB

Robotic vacuum cleaners can be remotely hacked to be able to pick up audio

ATTACK TYPE
Eavesdropping
CAUSE OF ISSUE
Security flaw
TYPE OF LOSS
Reputation/Data
REFFERENCES
http://dailym.ai/3110Icm

Scientists have found that robotic vacuum cleaners could allow snoopers to remotely listen to household conversations, despite not being fitted with microphones. They found they can perform a remote eavesdropping attack on a Roborock robot cleaner by remotely accessing its Lidar readings – which helps these cleaners to avoid bumping into furniture. This flaw could reveal the confidential business information from a teleconferencing meeting or credit card information recited during a phone call.

SOCIAL MEDIA

Facebook Messenger Bug Lets Hackers Listen to You Before You Pick Up the Call

Facebook has patched a bug in its widely installed Messenger app for Android that could have allowed a remote attacker to call unsuspecting targets and listen to them before even they picked up the audio call. The flaw resides in WebRTC's Session Description Protocol (SDP) — which defines a standardized format for the exchange of streaming media between two endpoints. Silvanovich was awarded a $60,000 bug bounty for reporting the issue, one among Facebook's three highest bug bounties to date.

ATTACK TYPE

Eavesdropping

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/37mnGqS

TikTok patches reflected XSS bug, one-click account takeover exploit

ATTACK TYPE

XSS

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://zd.net/3mfqPz8

TikTok has patched a reflected XSS security flaw and a bug leading to account takeover impacting the firm's web domain. Reported via the bug bounty platform HackerOne by researcher Muhammed Taskiran, the first vulnerability relates to a URL parameter on the tiktok.com domain which was not properly sanitized. In addition, Taskiran found an endpoint vulnerable to Cross-Site Request Forgery (CSRF), an attack in which threat actors can dupe users into submitting actions on their behalf to a web application as a trusted user.

Critical Flaw Affecting Industrial Automation Systems

A critical vulnerability uncovered in Real-Time Automation's (RTA) 499ES EtherNet/IP (ENIP) stack could open up the industrial control systems to remote attacks by adversaries. RTA's ENIP stack is one of the widely used industrial automation devices and is billed as the "standard for factory floor I/O applications in North America." "Successful exploitation of this vulnerability could cause a denial-of-service condition, and a buffer overflow may allow remote code execution," the US cybersecurity and infrastructure agency (CISA) said in an advisory.

ATTACK TYPE

RCE

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3mlBPev

AUTOMATION

New Bluetooth Attack Can Steal a Tesla Model X in Minutes

ATTACK TYPE

Targetted

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/36jsMoD

A security researcher, Lennert Wouter, has shown how vulnerabilities in the Tesla Model X's keyless entry system allow a different sort of update: A hacker could rewrite the firmware of a key fob via Bluetooth connection, lift an unlock code from the fob, and use it to steal a Model X in just a matter of minutes. In just 90 seconds, the hardware can extract a radio code that unlocks the owner's Model X. Once the car thief is inside, a second, distinct vulnerability Wouters found would allow the thief to pair their own key fob with the victim's vehicle after a minute's work and drive the car away.

HOT FIX YOU SHOULD NOTICE..

Microsoft Releases Windows Security Updates For Critical Flaws

Microsoft formally released fixes for 112 newly discovered security vulnerabilities as part of its November 2020 Patch Tuesday, including an actively exploited zero-day flaw disclosed by Google's security team last week. The rollout addresses flaws, 17 of which are rated as Critical, 93 are rated as Important. It's highly recommended that Windows users and system administrators apply the latest security patches to resolve the threats associated with these issues.

ATTACK TYPE

Hot fix

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/39pCesA

3 Actively Exploited 0-Days Discovered on IOS

ATTACK TYPE

Hot fix

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3mkQwym

Apple on Thursday released multiple security updates to patch three zero-day vulnerabilities that were revealed as being actively exploited in the wild. Rolled out as part of its iOS, iPadOS, macOS, and watchOS updates, the flaws reside in the FontParser component and the kernel, allowing adversaries to remotely execute arbitrary code and run malicious programs with kernel-level privileges. The zero-days were discovered and reported to Apple by Google's Project Zero security team. They are working on fixing this ASAP.

Researcher Discloses Critical RCE Flaws In Cisco Security Manager

Cisco has published multiple security advisories concerning critical flaws in Cisco Security Manager (CSM) a week after the networking equipment maker quietly released patches with version 4.22 of the platform. The development comes after Code White researcher Florian Hauser (frycos) yesterday publicly disclosed proof-of-concept (PoC) code for as many as 12 security vulnerabilities affecting the web interface of CSM that makes it possible for an unauthenticated attacker to achieve remote code execution (RCE) attacks.

ATTACK TYPE

RCE

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/2Vjq8j2

HOT FIX YOU SHOULD NOTICE..

Drupal-based sites open to attack via double extension files

Drupal content management system (CMS) has released this week security updates to patch a critical vulnerability that is easy to exploit and can grant attackers full control over vulnerable sites. Tracked as CVE-2020-13671, the vulnerability is ridiculously simple to exploit and relies on the good ol' "double extension" trick. Attackers can add a second extension to a malicious file, upload it on a Drupal site through open upload fields, and have the malicious executed. For example, a malicious file like malware.php could be renamed to malware.php.txt.

ATTACK TYPE

Double extension

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://zd.net/3mjqiwh

2-Factor Authentication Bypass Flaw Reported in cPanel and WHM Software

cPanel, a provider of popular administrative tools to manage web hosting, has patched a security vulnerability that could have allowed remote attackers with access to valid credentials to bypass two-factor authentication (2FA) protection on an account. The issue, tracked as "SEC-575" and discovered by researchers from Digital Defense, has been remedied by the company in versions 11.92.0.2, 11.90.0.17, and 11.86.0.32 of the software. To date, over 70 million domains have been launched on servers using cPanel's software suite.

ATTACK TYPE

Authentication bypass

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3o6CFvX

VMware fixed SD-WAN flaws that could allow hackers to target enterprise networks

VMware last week addressed six vulnerabilities (CVE-2020-3984, CVE-2020-3985, CVE-2020-4000, CVE-2020-4001, CVE-2020-4002, CVE-2020-4003) in its SD-WAN Orchestrator product, including some issues that can be chained by an attacker to hijack traffic or shut down an enterprise network. Various vulnerabilities include SQL injection, RCE, directory traversal, MITM, privilege escalation and other such.

ATTACK TYPE

Hot fix

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation/Data

REFFERENCES

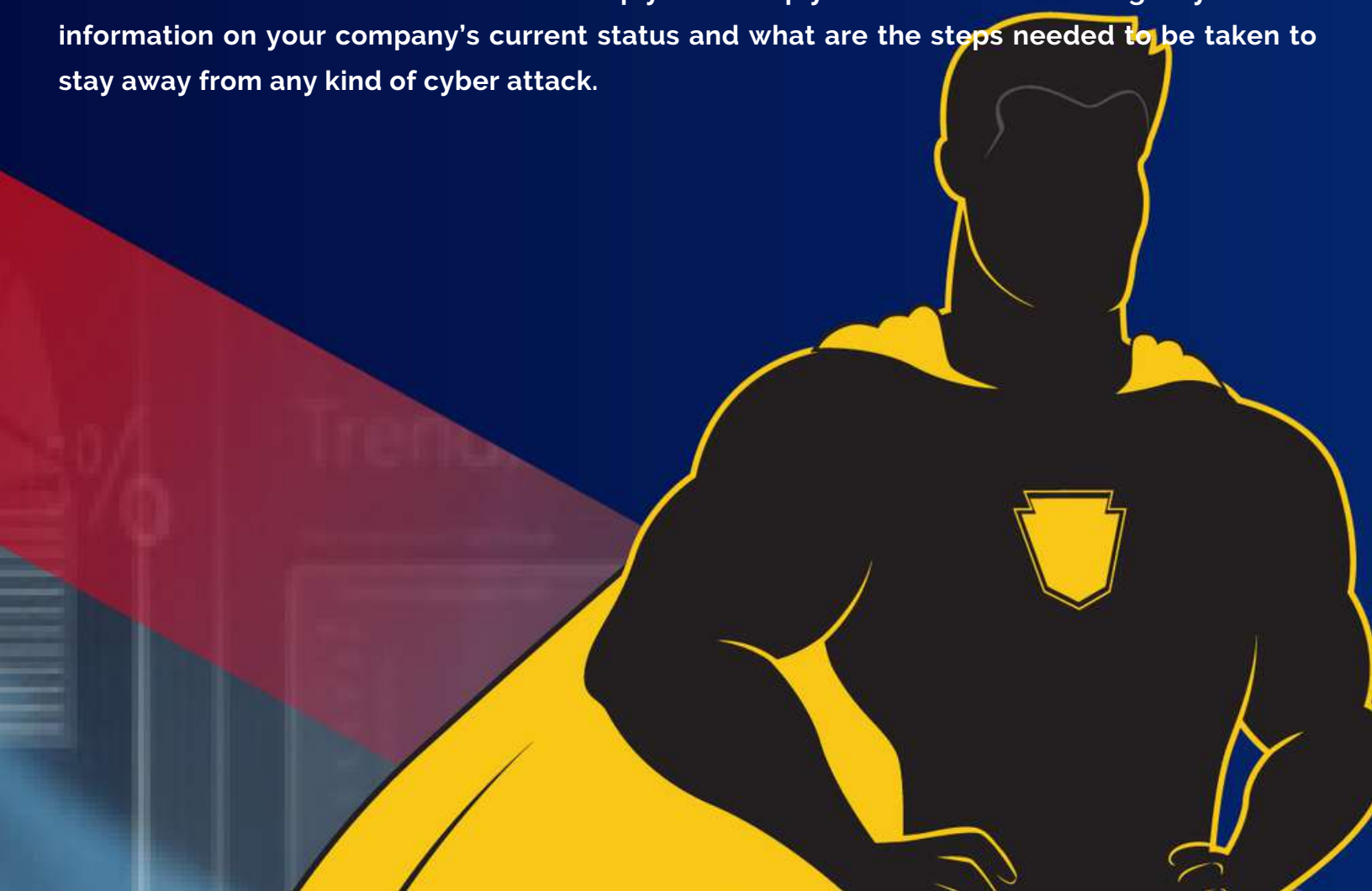
https://zd.net/3mjqiwh

CONCLUSION

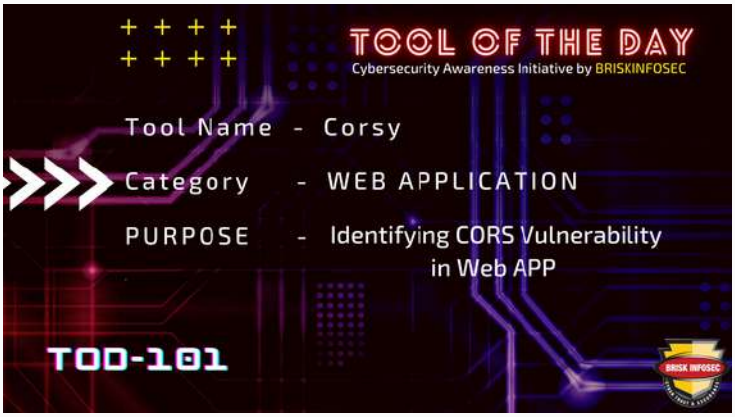
According to an article, online threats has risen by as much as six-times their usual levels recently as the Covid 19 pandemic provided greater scope for cyber attacks. All the attacks mentioned above - their types, the financial and reputation impacts they have caused to organizations, the loopholes that paved way for such attacks invariably causing disaster to organizations - are just like 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 the assets. We assure 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.



CORSY Web Application Vulnerability scanner

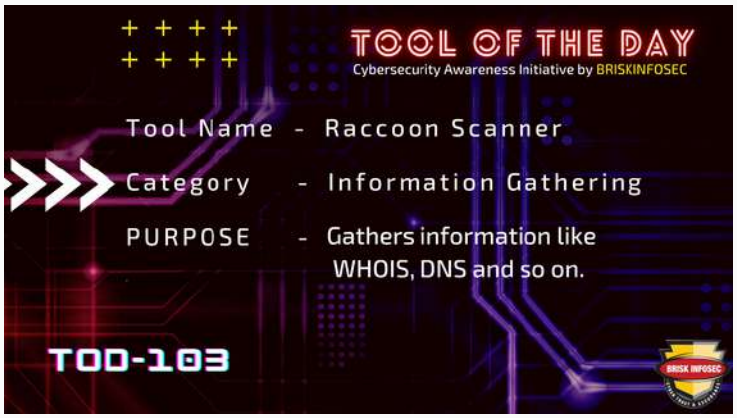


Corsy is a lightweight program that scans for all known misconfigurations in CORS implementations. Cross-Origin Resource Sharing (CORS) is a technology used by websites to make web browsers relax the Same Origin Policy, enabling cross-domain communication between different websites.

SNIPPER vulnerability scanner

Sn1per is an automated scanner that can be used during a penetration test to enumerate and scan for vulnerabilities. Sn1per Professional is Xero Security's premium reporting addon for Professional Penetration Testers, Bug Bounty Researchers and Corporate Security teams to manage large environments and pentest scopes.

Raccoon Scanner for Information Gathering



Offensive Security Tool for Reconnaissance and Information Gathering. Raccoon is a tool made for reconnaissance and information gathering with an emphasis on simplicity. It will do everything from fetching DNS records, retrieving WHOIS information, obtaining TLS data, detecting WAF presence and up to threaded dir busting and subdomain enumeration. Every scan output to a corresponding file.

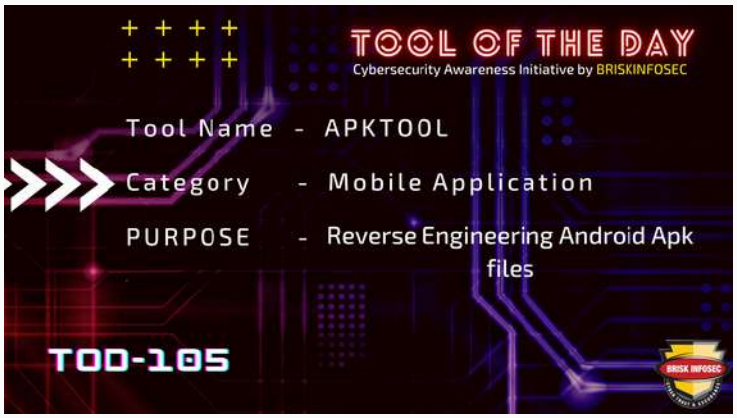
TOOLS OF THE MONTH

MobSF-Mobile Security Framework

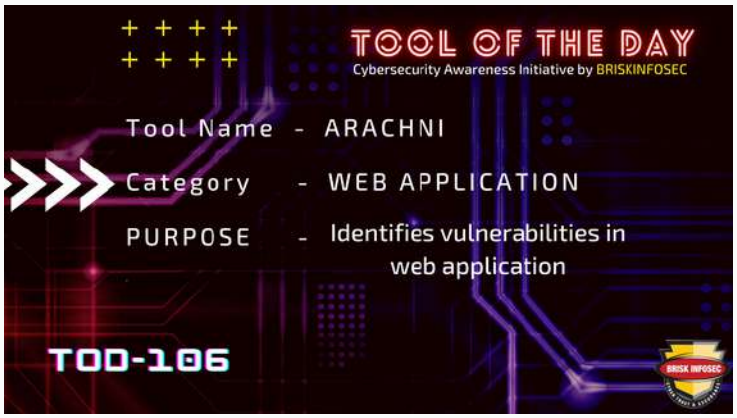
Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) Static and Dynamic analysis, malware analysis and security assessment framework capable of performing static and dynamic analysis. MobSF support mobile app binaries (APK, IPA & APPX) along with zipped source code and provides REST APIs for seamless integration.

APKTOOL for Reverse Engineering Android Apk File

Apktool is a tool for reverse engineering 3rd party, closed, binary Android apps. It can decode resources to nearly original form and rebuild them after making some modifications; it makes possible to debug smali code step by step. Also it makes working with app easier because of project-like files structure and automation of some repetitive tasks like building apk, etc.



Arachni Web Application Vulnerabilities Identifier



Arachni is a Free/Public-Source Web Application Security Scanner aimed ... Arachni provides first-class coverage, vulnerability detection and accuracy for modern ... enabling the identification of custom-404 handlers, server health, etc.

CYBER MONDAY

Cloud Threats

Since many people are predominately migrating towards the usage of cloud based services, securing them is of utmost priority. As a dedicated security organisation, it is our responsibility to address the two most widespread issues notably security misconfiguration and account takeover.

Cybersecurity Problems

Skillset gap is one of the pathetic factors in cybersecurity and finding skilled and dedicated security folks is a challenging one. Even if found and hired, care must be taken by the organization to retain all effectively working staffs by helping them work with job satisfaction.

Cyber Security Strategy

Security is a constantly evolving sector and so must the organizations and employees working in it in order to be coherent and equipped with the requirements of cyber security. Regular discussions between brass and techies would also aid greatly.

BLOG OF THE MONTH

Controller Area Network CAN

Controller Area Network (CAN) is the widely used In-vehicle networking when seen from a normal point of view, CAN is really powerful in transmitting all the critical and non-critical systems data to all the ECU's (Electronic Controller Unit) and other units. So, when it comes down to the understanding of CAN systems, it becomes a bit tedious.

WEB SERVICES AND API

Web Service is a software service used to create a communication between 2 devices connected over a network through internet. In terms of applications, web services help a technology like PHP to communicate with another technology like JAVA or .NET in order to accomplish some user action like retrieving data from the server.

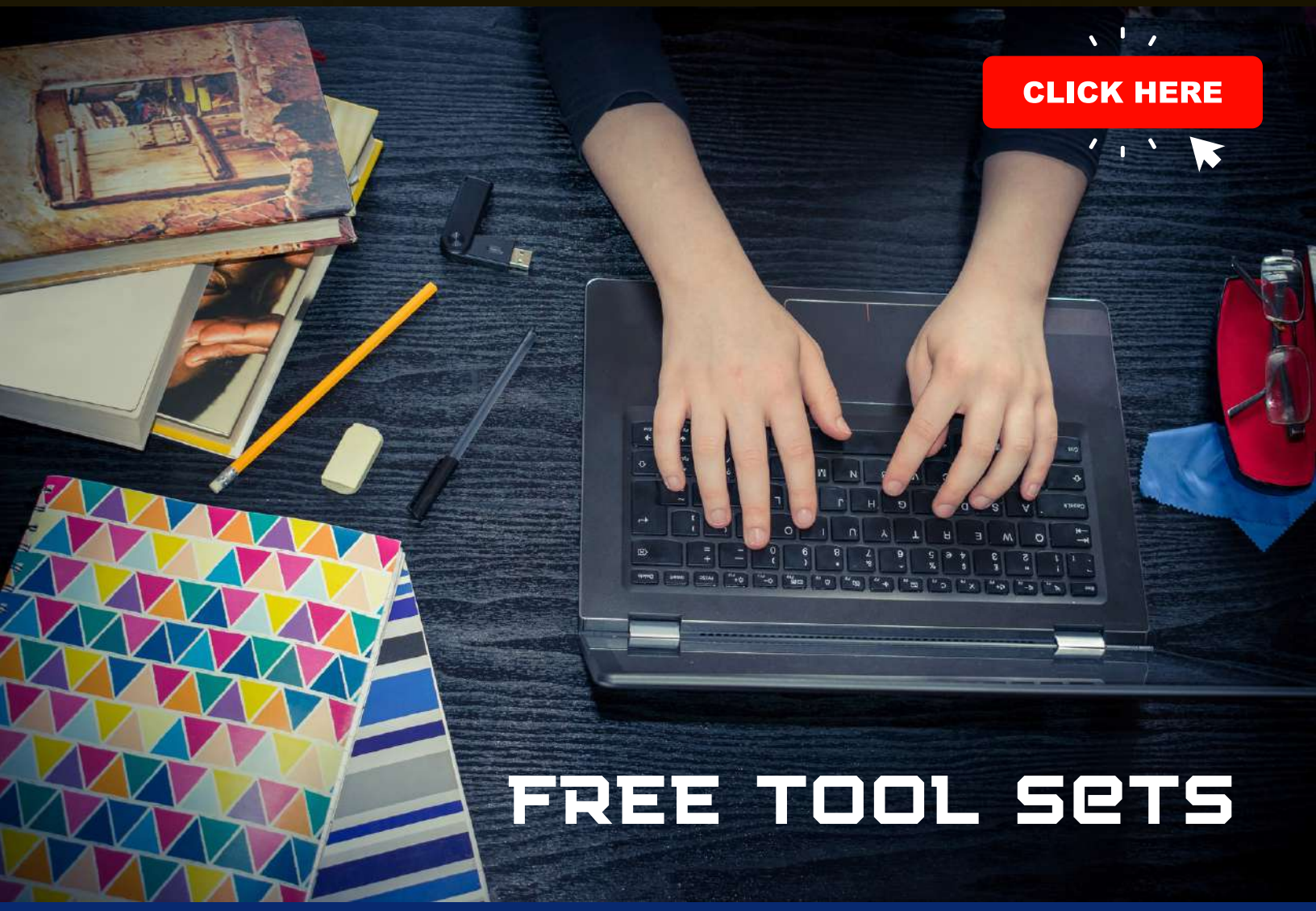
Cyber Security Products Vs Cyber Security Services

Cyberattacks have become more frequent in today's generation. The critical environment is the highly targeted area for attackers. Organisations must consider their protection in order to avoid critical breaches. There are certain attack categories.

CLICK HERE

WAKE UP CXO

AN INITIATIVE BY BRISKINFOSEC



CLICK HERE

FREE TOOL SETS

FEEL FREE TO REACH US FOR ALL YOUR CYBERSECURITY NEEDS

contact@briskinfosec.com | www.briskinfosec.com