EDITION 31

MARCH

THREATSPLOIT

ADVERSARY REPORT

BRISK INFOSEC

CYBER TRUST & ASSURANCE

2021

INTRODUCTION

Welcome to the Threatsploit report of March 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....

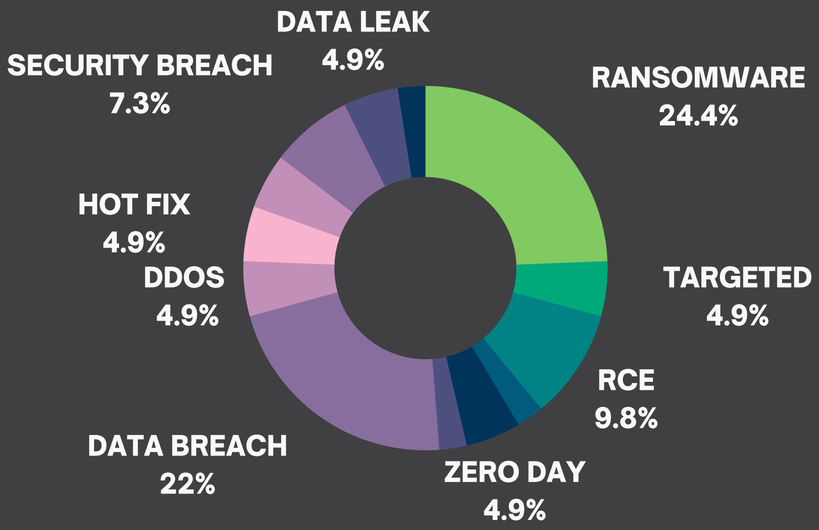
"employees and stakeholders have limited or no perception or understanding of threats and misplaced understanding of massive cyber threats or consequences".

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 in this month.

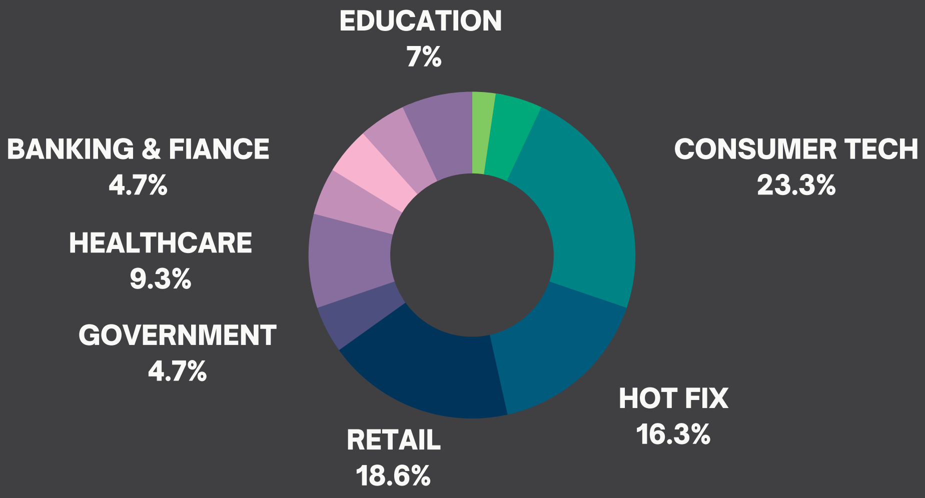
TYPES OF ATTACK VECTORS

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

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 the consumer technology sector (23%). 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

CONSUMER TECH

- A zero-day vulnerability in SonicWall products actively exploited in the wild
- Three More Vulnerabilities Found in SolarWinds Products
- WordPress security flaws: 800,000 sites running NextGen Gallery plugin potentially vulnerable to pwnage
- Critical RCE flaws affect VMware ESXi and vSphere clients
- Privacy Bug in Brave Browser Exposes Dark-Web Browsing History of Its Users
- Malicious Amazon Alexa Skills Can Easily Bypass Vetting Process
- Cisco Releases Security Patches for Critical Flaws Affecting its Products
- Unpatched ShareIT Android App Flaw Could Let Hackers Inject Malware
- Underwriters Laboratories (UL) certification giant hit by ransomware
- Singtel breach compromises data of customers, former employees

ENTERTAIMENT

- Video game Cyberpunk 2077 hit by a cyberattack; hackers demand a ransom
- Justpay Data Breach: Information of Over 10 Crore Debit, Credit Cardholders Leaked on Dark Web

HEALTHCARE

- Dax-Côte d’Argent hospital in France hit by a ransomware attack
- French hospitals crippled by cyberattacks
- Over 8 million COVID-19 test results leaked online
- California Medical Imaging Group Describes Data Exposure

RETAIL

- Filipino credit app Cashalo suffers data breach
- Experian Breach in South Africa Affects 24 Million Consumers
- Misconfigured Cloud Server Exposes 66,000 Gamers
- Web hosting provider shuts down after cyberattack
- Researchers discover an exposed Comcast database containing 1.5 billion records
- Singtel breach compromises data of customers, former employees
- Finnish IT services giant TietoEVRY discloses ransomware attack
- 360 Security Center hit by ransomware attack.

LATEST THREAT ENTRIES

BANKING & FINANCE

- DDoS attack takes down EXMO cryptocurrency exchange servers
- Ransomware hack on Ecuador's largest private bank, Ministry of Finance

GOVERNMENT

- Jamaica’s immigration website exposed thousands of travelers’ data
- US cities disclose data breaches after vendor's ransomware attack

TELECOMMUNICATION

- T-Mobile discloses data breach after SIM swapping attacks
- Yandex Data Breach Exposes 4K+ Email Accounts

OIL & ENERGY

- Npower app attack exposed customers' bank details
- Eletrobras, Copel energy companies hit by ransomware attacks

EDUCATION

- SFU warns cyberattack exposed the personal information of about 200,000 students, staff, and alumni
- Lakehead University shuts down campus network after a cyberattack
- Syracuse University data breach exposes nearly 10,000 names, Social Security numbers

AUTOMOTIVE

- Kia Motors America suffers ransomware attack, $20 million ransom

LATEST THREAT ENTRIES

HOT FIX YOU SHOULD NOTICE..

- Microsoft February 2021 Patch Tuesday fixes 56 bugs, including Windows zero-day
- Apple Patches 10-Year-Old macOS SUDO Root Privilege Escalation Bug
- Google patches an actively exploited Chrome zero-day
- Cisco Releases Security Patches for Critical Flaws Affecting its Products
- SQLite patches use-after-free bug that left apps open to code execution, denial-of-service exploits
- Python programming language hurries out update to tackle remote code vulnerability

BRISKINFOSEC TOOL OF THE DAY

- Convert .dex file into jar.
- Web Application Vulnerability Scanner
- Fuzzing Web application
- A Multi-threaded vulnerability scanner
- Scan your web application using spaghetti scanner
- Secure code reviewer for mobile application

CYBER MONDAY

- Cyber Security
- Patch Management
- Cyber Security Attack

BLOGS OF THE MONTH

- Will your backups protect you against ransomware?
- Cloud Security And The Best Ways To Secure It From Breaches
- This Awesome Stuff Will Make You Understand What Red Team And Blue Team Is

Zero-day vulnerability in SonicWall products actively exploited in the wild

A zero-day vulnerability in SonicWall enterprise security products is being actively exploited in the wild. Network security provider SonicWall confirmed there had been a “highly sophisticated, coordinated” attack on its systems.The company, which develops networking tools, cybersecurity products, and cloud platform solutions, said that an unknown assailant leveraged zero-day vulnerabilities in its products to gain access to its infrastructure. Investigation revealed there is a zero-day vulnerability in the company’s SMA 100 series of secure remote access devices, which is actively being exploited.

ATTACK TYPE

Zeroday

CAUSE OF ISSUE

Security flaws

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/2NGwtyt

Three More Vulnerabilities Found in SolarWinds Products

Security researchers have discovered three more vulnerabilities in SolarWinds products, including a critical remote code execution bug. The IT Management sofwares are targeted by the hackers to steal the governmental data. flaws are found in the SolarWinds Orion User Device Tracker and one is in the firm’s Serv-U FTP product. This leads to take the control of whole System RCE. SolarWinds credentials are stored in an insecure manner which could allow local users to take complete control over the SOLARWINDS_ORION database.

ATTACK TYPE

RCE

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation

REFFERENCES

https://bit.ly/3uH1T8p

WordPress security flaws: 800,000 sites running NextGen Gallery plugin potentially vulnerable to pwnage

Users of NextGEN Gallery, the image management plugin for WordPress, have been urged to update their websites after the discovery of serious cross-site request forgery (CSRF) vulnerabilities. The most serious of two flaws found by security researchers – each residing in separate functions – could lead to remote code execution (RCE) and stored cross-site scripting (XSS). As a result, attackers could take control of a website, inject it with spam links, or redirect visitors to phishing domains.

ATTACK TYPE

RCE, CSRF, XSS

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/2OeiejW

Critical RCE flaws affect VMware ESXi and vSphere clients

VMware has addressed multiple critical remote code execution (RCE) vulnerabilities in VMware ESXi and vSphere Client virtual infrastructure management platform that may allow attackers to execute arbitrary commands and take control of affected systems. The vulnerability, tracked as CVE-2021-21972, has a CVSS score of 9.8 out of a maximum of 10, making it critical in severity. Separately, a second vulnerability (CVE-2021-21973, CVSS score 5.3) allows unauthorized users to send POST requests, permitting an adversary to mount further attacks, including the ability to scan the company's internal network and retrieve specifics about the open ports of various services.

ATTACK TYPE

RCE

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3b88h0R

Privacy Bug in Brave Browser Exposes Dark-Web Browsing History of Its Users

Brave has fixed a privacy issue in its browser that sent queries for .onion domains to public internet DNS resolvers rather than routing them through Tor nodes, thus exposing users' visits to dark web websites. Brave ships with a built-in feature called "Private Window with Tor" that integrates the Tor anonymity network into the browser, allowing users to access .onion websites, which are hosted on the darknet, without revealing the IP address information to internet service providers (ISPs), Wi-Fi network providers, and the websites themselves. DNS requests, by design, are unencrypted, meaning that any request to access .onion sites in Brave can be tracked.

ATTACK TYPE

Privacy issue

CAUSE OF ISSUE

Unauthorised access

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3kz1LUZ

Malicious Amazon Alexa Skills Can Easily Bypass Vetting Process

Researchers have uncovered gaps in Amazon's skill vetting process for the Alexa voice assistant ecosystem that could allow a malicious actor to publish a deceptive skill under any arbitrary developer name and even make backend code changes after approval to trick users into giving up sensitive information. Researchers built a trip planner skill that allows a user to create a trip itinerary that was subsequently tweaked after initial vetting to "inquire the user for his/her phone number so that the skill could directly text (SMS) the trip itinerary," thus deceiving the individual into revealing his personal information.

ATTACK TYPE

Sensitive information leakage

CAUSE OF ISSUE

Broken access control

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3bQIj1U

Cisco Releases Security Patches for Critical Flaws Affecting its Products

Cisco has addressed a maximum severity vulnerability in its Application Centric Infrastructure (ACI) Multi-Site Orchestrator (MSO) that could allow an unauthenticated, remote attacker to bypass authentication on vulnerable devices." An attacker could exploit this vulnerability by sending a crafted request to the affected API," the company said in an advisory published yesterday. "A successful exploit could allow the attacker to receive a token with administrator-level privileges that could be used to authenticate to the API on affected MSO and managed Cisco Application Policy Infrastructure Controller (APIC) devices."

ATTACK TYPE

Privilege escalation

CAUSE OF ISSUE

Authentication flaw

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/374X14H

Unpatched ShareIT Android App Flaw Could Let Hackers Inject Malware

Multiple unpatched vulnerabilities have been discovered in SHAREit, a popular app with over one billion downloads, that could be abused to leak a user's sensitive data, execute arbitrary code, and possibly lead to remote code execution. One of the flaws arises from the manner the app facilitates sharing of files (via Android's FileProvider), potentially allowing any third-party to gain temporary read/write access permissions and exploit them to overwrite existing files in the app's data folder. The company said that “we released a patch to address the alleged vulnerabilities."

ATTACK TYPE

Malware

CAUSE OF ISSUE

Poor security pratice

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/374X2FN

CONSUMER TECH

Underwriters Laboratories (UL) certification giant hit by ransomware

UL LLC, better known as Underwriters Laboratories, has suffered a ransomware attack that encrypted its servers and caused them to shut down systems while they recover. UL suffered a ransomware attack last weekend that encrypted devices in their data center. To prevent further spread of the attack, the company shut down its systems, making it impossible for some employees to perform their jobs. UL told employees not to contact the threat actors or visit any sites related to the ransomware operation. According to a source familiar with the attack, UL has decided not to pay the ransom and is restoring from backups instead.

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Lack of maintaince

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3wJVWaD

Singtel breach compromises data of customers, former employees

ATTACK TYPE

Security breach

CAUSE OF ISSUE

Poor security pratice

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3uDW81y

Personal data of 129,000 customers, including birth dates and mobile numbers, as well as financial details of the Singapore telco's former staff and employees of a corporate customer have been leaked in a security breach involving a third-party file-sharing system. Singtel has confirmed that personal details of 129,000 customers, as well as financial information of its former employees, have been compromised in a security breach that involved a third-party file-sharing system. Credit card details belonging to the staff of a corporate client and information tied to 23 enterprises, including suppliers and partners, also have been leaked in the incident.

ENTERTAINMENT

Video game Cyberpunk 2077 hit by a cyber attack; hackers demand a ransom

CD Projekt Red said hackers had accessed its internal network, digitally scrambled some of its data servers and tried to blackmail it. The perpetrators claim to have stolen source code for several of the firm's games which they said they would leak unless a payment was made. But the Polish games company said it would not negotiate. In a statement on Twitter, CD Projekt Red posted a copy of the ransom note which said the hackers had copied code from Cyberpunk 2077, Gwent, and Witcher 3, including an unreleased version of the latter.

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/38eyqt1

Juspay Data Breach: Information of Over 10 Crore Debit, Credit Cardholders Leaked on Dark Web

ATTACK TYPE

Data breach

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3sB1x2K

Private data of over 10 Crore credit and debit cardholders have been leaked on the dark web, as per a security researcher. According to reports, the sensitive information has been leaked from a faulty serve of Juspay, a mobile payments company. This included the names, phone numbers, and email addresses of the cardholders as well as the first and last digits of cards. Private data of over 10 Crore credit and debit cardholders have been leaked on the dark web, as per a security researcher.

Dax-Côte d'Argent hospital in France hit by ransomware attack

A hospital in southwest France is scrambling to recover from a ransomware attack that has caused significant operational disruption. The Center Hospitalier de Dax-Côte d'Argent revealed that it had fallen prey to a cyber-attack and was trying to restore systems that included the telephone switchboard. Phone lines at the healthcare facility had been partially restored, it added, but encrypted data remained inaccessible.In a press conference held on February 11, the publication continued, senior hospital officials said staff were resorting to pen and paper, and that radiotherapy care was among the most severely disrupted departments.

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Poor security pratice

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3bOCqRN

French hospitals crippled by cyberattacks

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3sBOo81

Three hospital buildings near the city of Lyon have fallen prey this week to hackers using ransomware. This type of attack blocks computer systems and demands a payment in exchange for their release. The hospital group in Villefranche-sur-Saône has backup procedures to continue to treat most patients, but planned surgical operations have been suspended, and emergencies are being redirected elsewhere near Lyon.

Over 8 million COVID-19 test results leaked online

Millions of COVID-19 test reports were found to be publicly accessible due to flawed online system implementation. The leak, comprising over 8 million COVID-19 test results, has been attributed to the Health and Welfare Department of West Bengal, India. These reports have sensitive information about the citizens in them like name, age, date and time of sample testing, residence address. At the time of his original discovery, the researcher suspected the number of publicly accessible reports was crossing the 8 million mark.

ATTACK TYPE

Data leak

CAUSE OF ISSUE

Authentication flaw

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3sBOo81

California Medical Imaging Group Describes Data Exposure

ATTACK TYPE

Data breach

CAUSE OF ISSUE

Unauthorised access

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3r66199

A California medical imaging group practice says vulnerabilities in its picture archiving and communications system left patient data at risk of unauthorized access for more than a year. PACS system had been vulnerable to hacking. "After thorough investigation, SBI determined that, due to these IT vulnerabilities, certain SBI patient information may have been accessed by unauthorized parties," the imaging group says in a statement. The practice's administrator tells Information Security Media Group that the vulnerabilities left accessible "names of about 100,000 patients on a worklist."

Filipino credit app Cashalo suffers data breach

A data breach at a Filipino credit company has exposed customers' sensitive personal details. Cashalo, a fintech company offering cash loans and other financial services to customers in the Philippines, confirmed that "illegal access" of a database has resulted in the leak of some personally identifiable information. Exposed details include the names, email addresses, phone numbers, device IDs, and passwords of customers. Cashalo stressed that passwords were encrypted and said that no accounts were compromised as a result of the data breach.

ATTACK TYPE

Data breach

CAUSE OF ISSUE

Poor security pratice

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/2MAhtS7

Experian Breach in South Africa Affects 24 Million Consumers

ATTACK TYPE

Data breach

CAUSE OF ISSUE

Poor security pratice

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3kxAC3o

A data breach affecting the South African branch of credit reporting company Experian exposed information on an estimated 24 million consumers and almost 800,000 businesses, according to the South African Banking Risk Information Center, a nonprofit financial crime risk information center. But Experian says no consumer credit or financial information was exposed and also claims there is no evidence indicating whether the stolen data includes consumers' credit or financial information.

Adorcam App Leaks Millions of User Records via ElasticSearch Database

An unsecured ElasticSearch database belonging to the Adorcam app exposed credentials, hostname, and port for the MQTT server, allowing threat actors to download, delete, or modify data. The database contained over 124 million rows of data (around 51 GB in size) that belonged to several thousands of Adorcam app users. The exposed data included user email addresses, hashed passwords, Wi-Fi network name, client IP, user Id, web camera serial number, web camera settings including microphone state, country geolocation, SSID / wireless network, name, and images captured by the web cameras.

ATTACK TYPE

Data exposed

CAUSE OF ISSUE

Security misconfiguration

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/2My27xi

Web hosting provider shuts down after cyberattack

ATTACK TYPE

Security breach

CAUSE OF ISSUE

Unknown

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://zd.net/3kuF96U

Two other UK web hosting providers also suffered similar hacks over the weekend, although it's unconfirmed if the attacks are related. A web hosting company named No Support Linux Hosting announced today it was shutting down after a hacker breached its internal systems and compromised its entire operation. According to a message posted on its official site [archived], the company said it was breached on February 8. The hacker appears to have "compromised" the company's entire operation, including its official website, admin section, and customer database.

RETAIL

Researchers discover exposed Comcast database containing 1.5 billion records

Researchers discovered a non-password-protected database that contained more than 1.5 billion records. The database belonged to American cable and internet giant Comcast, and the publicly visible records included dashboard permissions, logging, client IPs, @comcast email addresses, and hashed passwords. There were a large number of remote and internal IP addresses, node names, and other details that could provide a blueprint for internal functionality, logging, and overall structure of the network.

ATTACK TYPE

Unprotected Database

CAUSE OF ISSUE

Poor security pratice

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3r5Azyt

Singtel breach compromises data of customers, former employees

ATTACK TYPE

Data breach

CAUSE OF ISSUE

Poor security pratice

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3uDW8Iy

Singtel has confirmed that personal details of 129,000 customers, as well as financial information of its former employees, have been compromised in a security breach that involved a third-party file-sharing system. Credit card details belonging to the staff of a corporate client and information tied to 23 enterprises, including suppliers and partners, also have been leaked in the incident. Singapore telco revealed "files were taken" in an attack that affected a file-sharing system, called FTA, which was developed two decades ago by Accellion. Singtel said it had used the software internally and with external stakeholders.

Finnish IT services giant TietoEVRY discloses ransomware attack

TietoEVRY is a Finnish software development and IT services company that employs 24,000 people throughout 80 countries. The technical issues for 25 customers in the retail, manufacturing, and service-related industries, which was later learned to be caused by a ransomware attack. After learning of the attack, TietoEVRY disconnected the affected infrastructure and services to prevent the ransomware's further spread. "Due to the ransomware, the affected infrastructure and services were disconnected. Together with the affected customers and our partners, we are working to enable recovery of the operations soonest. "All affected customers have been informed and regular updates are being shared with them on the progress," TietoEVRY disclose.

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Poor Security pratice

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3dTw7Pp

360 Security Center hit by ransomware attack.

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/2ZXInaN

360 Security Center detected a ransomware that disguised commonly used software and appeared on the network. The virus called itself DarkWorld in the ransom letter. After the virus encrypts the victim's files, it will ask for a Bitcoin ransom equivalent to $300. However, users do not need to worry, the 360 Total Security can intercept and kill the ransomware before problems occur. After the DarkWorld ransomware runs, it will encrypt the file using the Rijndael encryption algorithm, and then add the suffix of the encrypted file ".dark", and create "Important.txt" as a ransom letter.

BANKING & FINANCE

DDoS attack takes down EXMO cryptocurrency exchange servers

The servers of British cryptocurrency exchange EXMO were taken offline temporarily after being targeted in a distributed denial-of-service (DDoS) attack. "We are currently experiencing a DDoS attack on our platform," the exchange said. "Please note that the EXMO exchange website is now under the DDoS attack. The servers are temporarily unavailable." In a separate alert issued through the company's official Twitter account, EXMO said that it's working on addressing the issue. While no update was published since the DDoS attack was announced, the platform's servers and website are now back online.

ATTACK TYPE

DDOS

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/2ZZCpF9

Ransomware hack on Ecuador's largest private bank, Ministry of Finance

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Poor security pratice

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/2NFQJ3d

A hacking group called 'Hotarus Corp' has hacked Ecuador's Ministry of Finance and the country's largest bank, Banco Pichincha, where they claim to have stolen internal data. The ransomware gang first targeted Ecuador's Ministry of Finance, the Ministerio de Economía y Finanzas de Ecuador, where they deployed a PHP-based ransomware strain to encrypt a site hosting an online course. Soon after the attack, the threat actors released a text file containing 6,632 login names and hashed password combinations on a hacker forum.

GOVERNMENT

Jamaica’s immigration website exposed thousands of travelers’ data

Security lapse by a Jamaican government contractor has exposed immigration records and COVID-19 test results for hundreds of thousands of travelers who visited the island over the past year. The Jamaican government-contracted Amber Group to build the JamCOVID19 website and app, which the government uses to publish daily coronavirus figures and allows residents to self-report their symptoms. But a cloud storage server storing those uploaded documents was left unprotected and without a password, and was publicly spilling out files onto the open web.

ATTACK TYPE

Data leak

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3q3GBhQ

US cities disclose data breaches after vendor's ransomware attack

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Lack of awarness

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3bSXpDb

A ransomware attack against the widely used payment processor ATFS has sparked data breach notifications from numerous cities and agencies within California and Washington. As the data is used for billing and verifying customers and residents is wide and varied, this attack could have a massive and widespread impact.The cyberattack has since caused significant disruption to AFTS' business operations, making their website unavailable and impacting payment processing. When visiting their site, people are greeted with a message, stating, "The website for AFTS and all related payment processing website are unavailable due to technical issues.

TELECOMMUNICATION

T-Mobile discloses data breach after SIM swapping attacks

American telecommunications provider T-Mobile has disclosed a data breach after an unknown number of customers were apparently affected by SIM swap attacks. SIM swap fraud (or SIM hijacking) allows scammers to take control of targets' phone numbers after porting them using social engineering or after bribing mobile operator employees to a SIM controlled by the fraudsters. Subsequently, they receive the victims' messages and calls which allows for easily bypassing SMS-based multi-factor authentication (MFA), stealing user credentials, as well taking over the victims' online service accounts.

ATTACK TYPE

Data breach

CAUSE OF ISSUE

Sim swapping

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3pM4fjC

Yandex Data Breach Exposes 4K+ Email Accounts

ATTACK TYPE

Data breach

CAUSE OF ISSUE

Poor security pratice

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3b3Eeaj

Yandex – one of Europe's largest internet companies – is warning of a data breach that compromised 4,887 email accounts. The breach stems from an insider threat. The most-used search engine in Russia. Beyond its search engine, Yandex's internet product lineup includes email services, online advertising, app analytics and more.The company found that a Yandex employee had been providing unauthorized access to users' mailboxes "for personal gain." This employee was one of three system administrators, who had the access privileges to provide technical support for mailboxes, said Yandex.

Npower app attack exposed customers' bank details

Energy firm Npower has closed down its app following an attack that exposed some customers' financial and personal information. Contact details, birth dates, addresses and partial bank account numbers are among details believed stolen.The firm did not say how many accounts were affected by the breach. But, the affected accounts had been locked, Npower told the BBC. "We identified suspicious cyber-activity affecting the Npower mobile app, where someone has accessed customer accounts using login data stolen from another website. This is known as 'credential stuffing'," the firm said in a statement.

ATTACK TYPE

Targetted

CAUSE OF ISSUE

Poor security pratice

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bbc.in/2NP9IxB

OIL & ENERGY

Eletrobras, Copel energy companies hit by ransomware attacks

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Poor security pratice

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/2OajEvY

Centrais Eletricas Brasileiras (Eletrobras) and Companhia Paranaense de Energia (Copel), two major electric utilities companies in Brazil have announced that they suffered ransomware attacks over the past week. State-controlled, both are key players in the country. Copel being the largest in the state of Paraná while Eletrobras is the largest power utility company in Latin America and also owns Eletronuclear, a subsidiary involved in the construction and operations of nuclear power plants. Both ransomware attacks disrupted operations and forced the companies to suspend some of their systems, at least temporarily.

EDUCATION

SFU warns cyberattack exposed personal information of about 200,000 students, staff and alumni

Simon Fraser University is warning its school community about a cyberattack that breached a server that stored information on student and employee ID numbers and other data, including admissions or academic standing. The school says about 200,000 people were affected by the breach. The university said its Information Technology Services staff discovered the attack on one of the school's servers on Feb. 5 and isolated the server. The server contained personal information for some current and former students, faculty, staff and student applicants.

ATTACK TYPE

Security breach

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/37Zcq51

Lakehead University shuts down campus network after cyberattack

ATTACK TYPE

Targetted

CAUSE OF ISSUE

Poor security pratice

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3sGDjCT

Canadian undergraduate research university Lakehead has been dealing with a cyberattack that forced the institution earlier this week to cut off access to its servers. Lakehead University provided some details about the attack saying that it was aimed at its file share servers. The school did not disclose the nature of the incident, though. “As soon as Lakehead’s Technology Services Centre (TSC) became aware of the potential threat to our servers, TSC removed all access to them,” the University said. An investigation is underway, trying to determine what servers and information have been impacted by the security incident.

Syracuse University data breach exposes nearly 10,000 names, Social Security numbers

The names and Social Security numbers of about 9,800 Syracuse University students, alumni, and applicants have been exposed after someone gained unauthorized access to an employee’s email account. Upon learning of the breach, SU secured the account and launched an investigation that determined in early January that emails or attachments in the account contained names and Social Security numbers, a letter sent to affected students reads. The investigation was unable to determine whether the unauthorized party ever viewed the personal information in the account.

ATTACK TYPE

Data breach

CAUSE OF ISSUE

Unauthorized access

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3r5ELhH

AUTOMOTIVE

Kia Motors America suffers ransomware attack, $20 million ransom

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/2NYZogT

Kia Motors America has suffered a ransomware attack by the DoppelPaymer gang, demanding $20 million for a decryptor and not to leak stolen data. KMA has nearly 800 dealers in the USA with cars and SUVs manufactured out of West Point, Georgia. The outage has affected their mobile UVO Link apps, phone services, payment systems, owner's portal, and internal sites used by dealerships. When visiting their sites, users are met with a message stating that Kia is "experiencing an IT service outage that has impacted some internal networks

Microsoft February 2021 Patch Tuesday fixes 56 bugs, including Windows zero-day

Microsoft has released its monthly batch of security-update that addresses 56 security vulnerabilities, including a Windows bug that was out in the wild, without any detection. The zero-day exploit tracked as CVE-2021-1732 is said to be a 'Windows Win32k Elevation of Privilege Vulnerability,' meaning it allows an attacker or malicious program to elevate their privileges to administrative privileges. These include CVE-2021-1721 (.NET Core and Visual Studio Denial of Service Vulnerability), CVE-2021-1733 (Sysinternals PsExec Elevation of Privilege Vulnerability), CVE-2021-26701 (.NET Core Remote Code Execution Vulnerability), CVE-2021-1727 (Windows Installer Elevation of Privilege Vulnerability), CVE-2021-24098 (Windows Console Driver Denial of Service Vulnerability), and CVE-2021-24106 (Windows DirectX Information Disclosure Vulnerability).

ATTACK TYPE

Hot fix

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation

REFFERENCES

https://zd.net/3kCdFMz

Apple Patches 10-Year-Old macOS SUDO Root Privilege Escalation Bug

ATTACK TYPE

Root Privilege Escalation

CAUSE OF ISSUE

Lack of maintainces

TYPE OF LOSS

Reputation

REFFERENCES

https://bit.ly/3sCEjb3

Apple has rolled out a fix for a critical sudo vulnerability in macOS Big Sur, Catalina, and Mojave that could allow unauthenticated local users to gain root-level privileges on the system."A local attacker may be able to elevate their privileges," Apple said in a security advisory. "This issue was addressed by updating to sudo version 1.9.5p2." Sudo is a common utility built into most Unix and Linux operating systems that lets a user without security privileges access and run a program with the credentials of another user. Tracked as CVE-2021-3156 (also called "Baron Samedit"), the vulnerability existence of a heap-based buffer overflow, which it said had been "hiding in plain sight" for almost 10 years.

Google patches an actively exploited Chrome zero-day

Google has patched a zero-day vulnerability in Chrome web browser for desktop that it says is being actively exploited in the wild. The company released 88.0.4324.150 for Windows, Mac, and Linux, with a fix for a heap buffer overflow flaw (CVE-2021-21148) in its V8 JavaScript rendering engine. "Google is aware of reports that an exploit for CVE-2021-21148 exists in the wild," the company said in a statement.But despite how this zero-day was exploited, regular users are advised to use Chrome's built-in update feature to upgrade their browser to the latest version as soon as possible. This can be found via the Chrome menu, Help option, and About Google Chrome section.

ATTACK TYPE

Zero day

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation

REFFERENCES

https://zd.net/2NRvDPI

Cisco Releases Security Patches for Critical Flaws Affecting its Products

Cisco has addressed a maximum severity vulnerability in its Application Centric Infrastructure (ACI) Multi-Site Orchestrator (MSO) that could allow an unauthenticated, remote attacker to bypass authentication on vulnerable devices."An attacker could exploit this vulnerability by sending a crafted request to the affected API," the company said in an advisory published yesterday. "A successful exploit could allow the attacker to receive a token with administrator-level privileges that could be used to authenticate to the API on affected MSO and managed Cisco Application Policy Infrastructure Controller (APIC) devices."

ATTACK TYPE

Unauthorised access

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation

REFFERENCES

https://bit.ly/3rD8Gyk

SQLite patches use-after-free bug that left apps open to code execution, denial-of-service exploits

ATTACK TYPE

Dos, Code execution

CAUSE OF ISSUE

Lack of maintainces

TYPE OF LOSS

Reputation

REFFERENCES

https://bit.ly/37Sl5Gv

SQLite has issued a security patch after the discovery of a use-after-free bug that, if triggered, could lead to arbitrary code execution or denial of service (DoS). The highest threat to systems running affected versions of SQLite, a C-language library that implements an SQL database engine, is to system availability. If an SQL injection bug exists on a target system then it might be possible – dependent on other protections in place – to cause SQLite to read a previously freed data structure and potentially cause a crash and it will just cause SQLite to return a goofy answer.” This problem allows an attacker to escalate an SQL injection vulnerability in the application into a denial of service.”

Python programming language hurries out update to tackle remote code vulnerability

The Python Software Foundation (PSF) has rushed out Python 3.9.2 and 3.8.8 to address two notable security flaws, including one that is remotely exploitable but in practical terms can only be used to knock a machine offline. PSF is urging its legion of Python users to upgrade systems to Python 3.8.8 or 3.9.2, in particular to address the remote code execution (RCE) vulnerability that's tracked as CVE-2021-3177. The project expedited the release after receiving unexpected pressure from some users who were concerned over the security flaw. Since the announcement of the release candidates for 3.9.2 on 3.8.8, we received a number of inquiries from end users urging us to expedite the final releases due to the security content, especially CVE-2021-3177," said the Python release team.

ATTACK TYPE

RCE

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://zd.net/3bMRDTw

CONCLUSION

According to an article, online threats have 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 the assets.

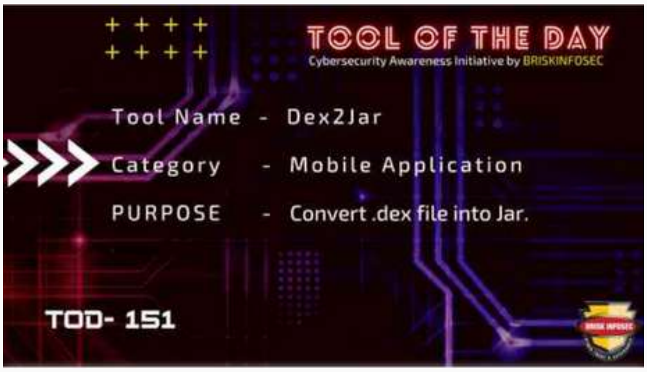
We assure that we will help you to keep your data safe and also give you clear information on your company's current status and what are the steps needed to be taken to stay away from any kind of cyber attack.

BRISK INFOSEC

CYBER TRUST & ASSURANCE

TOOLS OF THE MONTH

Convert .dex file into jar.



TOOL OF THE DAY
Cybersecurity Awareness Initiative by BRISKINFOSEC

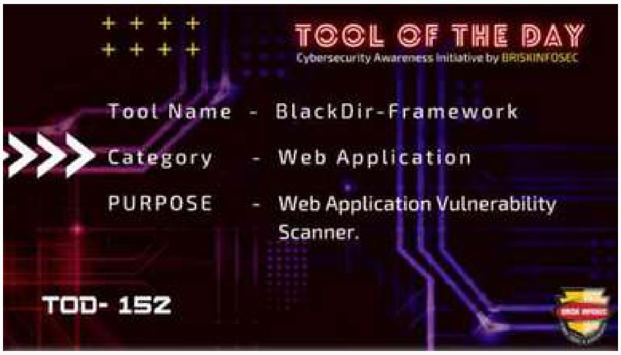
Tool Name - Dex2Jar
Category - Mobile Application
PURPOSE - Convert .dex file into Jar.

TOD- 151

Dex-reader is designed to read the Dalvik Executable (.dex/.odex) format. It has a lightweight API similar to ASM.dex-translator is designed to do the convert job. It reads the dex instruction to dex-or format, after some optimize, convert to ASM format. dex-tools tools to work with .class files. here are examples: Modify a apk, DeObfuscate a jar.

Web Application Vulnerability Scanner

Web Application Vulnerability Scanners are automated tools that scan web applications, normally from the outside, to look for security vulnerabilities such as Cross-site scripting, SQL Injection, Command Injection, Path Traversal and insecure server configuration

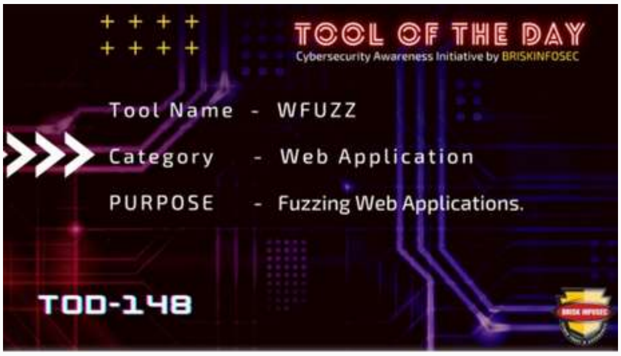


TOOL OF THE DAY
Cybersecurity Awareness Initiative by BRISKINFOSEC

Tool Name - BlackDir-Framework
Category - Web Application
PURPOSE - Web Application Vulnerability Scanner.

TOD- 152

Fuzzing Web application



TOOL OF THE DAY
Cybersecurity Awareness Initiative by BRISKINFOSEC

Tool Name - WFUZZ
Category - Web Application
PURPOSE - Fuzzing Web Applications.

TOD-148

Wfuzz is a tool designed for bruteforcing Web Applications, it can be used for finding resources not linked (directories, servlets, scripts, etc), bruteforce GET and POST parameters for checking different kind of injections (SQL, XSS, LDAP,etc), bruteforce Forms parameters(User/Password), Fuzzing,etc.

TOOLS OF THE MONTH

A Multi-threaded vulnerability scanner

TOOL OF THE DAY
Cybersecurity Awareness Initiative by BRISKINFOSEC
Tool Name - RVuln
Category - Web Application
PURPOSE - A multi-threaded Vulnerability Scanner.
TOD- 153

A multi-threaded Vulnerability Scanners are automated tools that scan the web applications, normally from the outside, to look for security vulnerabilities such as Cross-site scripting, SQL Injection, Command Injection, Path Traversal, and insecure server configuration

Scan your web application using spaghetti scanner

Spaghetti is an Open Source web application scanner, it is designed to find various default and insecure files, configurations, and misconfiguration. Spaghetti is built on python2.7 and can run on any platform which has a Python environment.

TOOL OF THE DAY
Cybersecurity Awareness Initiative by BRISKINFOSEC
Tool Name - Spaghetti
Category - Web Application
PURPOSE - Open Source Web Application Scanner.
TOD- 150

Secure code reviewer for mobile application

TOOL OF THE DAY
Cybersecurity Awareness Initiative by BRISKINFOSEC
Tool Name - Insider
Category - Mobile Application
PURPOSE - Secure Code Reviewer.
TOD-149

Insider is focused on covering the OWASP Top 10, to make source code analysis to find vulnerabilities right in the source code, focused on a agile and easy to implement software inside your DevOps pipeline.

CYBER MONDAY

HAPPY
CYBER
MONDAY
AN INITIATIVE BY BRISKINFOSEC
" IN TODAY'S HYPER CONNECTED WORLD,
CYBER SECURITY IS NOT A LUXURY
BUT AN ABSOLUTE NECESSITY "
Team - Briskinfosec
BRISK INFOSEC
www.briskinfosec.com

Cyber Security

In a world where digital advancements are rampant and security-related concerns are at peak for every digital organization and for digital assets using individuals, security is not just an option but an unavoidable compulsion

Patch Management

The reason why a patch is released is to completely fix the vulnerabilities and to avoid security disasters. As per the survey in 2020, it is observed that about 60% of patches weren't applied at all which caused increase in data breaches

Cyber Security Attack

For people who still believe the misconception that a firewall or an anti-virus deployed in their organization is more than sufficient to prevent cyberattacks, here's a startling truth that for every half a minute, a new and constantly evolving cyber attack is emerging as per Google's survey.

BLOG OF THE MONTH

Will your backups protect you against ransomware?

In this Digital world, everything is information, so-called data. If you don't protect these data in the backup then the business would fail. Those backups will help in case of disaster and cyber attack to overcome the losses and helps the organization rebuild the business as soon as possible without losing the business data. In several ransomware attacks, backup plays a huge role in protecting the data of organizations.

Cloud Security And The Best Ways To Secure It From Breaches

For business needs, the cloud environment is more useful for users due to the friendliness and the easiness to access data securely from anywhere. The working environment is ideal and during the disaster phase, recovery for organizations in order to back up all their hosted information is easier. One major benefit of the cloud environment is it's very flexible and people can scale up or scale down their storage capacity depending on their needs.

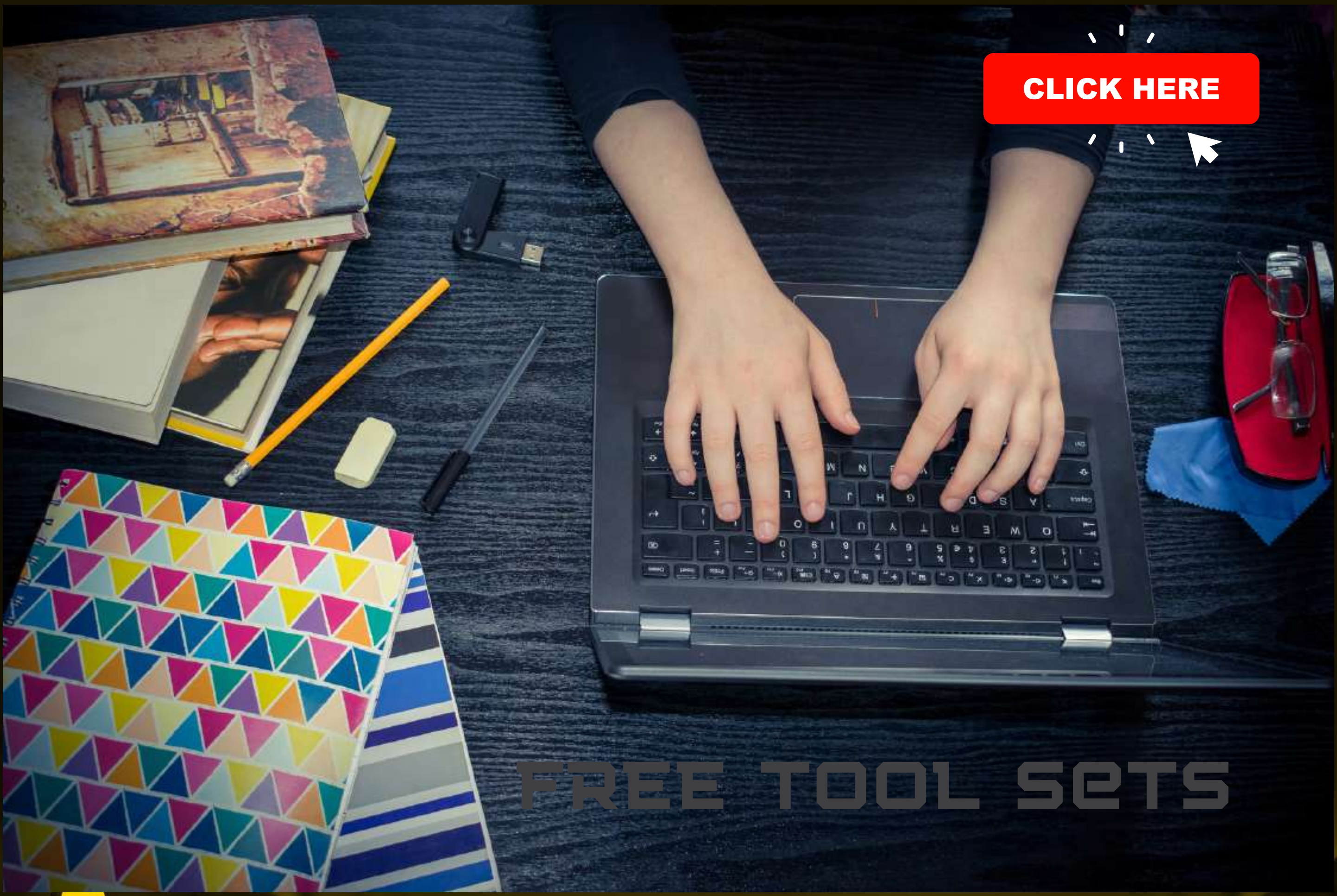
This Awesome Stuff Will Make You Understand What Red Team And Blue Team Is

Most people think that Red Teaming and Blue Teaming are different approaches for testing and identifying security flaws. But, if you examine closely, you'll find that they aren't different but complementary approaches to each other. The red team refers to the team who use their skills to mimic the mindset of an attacker, whereas Blue team use their skills to defend.

CLICK HERE

WAKE UP CXO

AN INITIATIVE BY BRISKINFOSEC



contact@briskinfosec.com
www.briskinfosec.com