THREATSPLOIT

ADVERSARY REPORT

2021

BRISK INFOSEC

CYBER TRUST & ASSURANCE

EDITION 30

FEBRUARY

INTRODUCTION

Welcome to the Threatsploit report of February 2021 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....

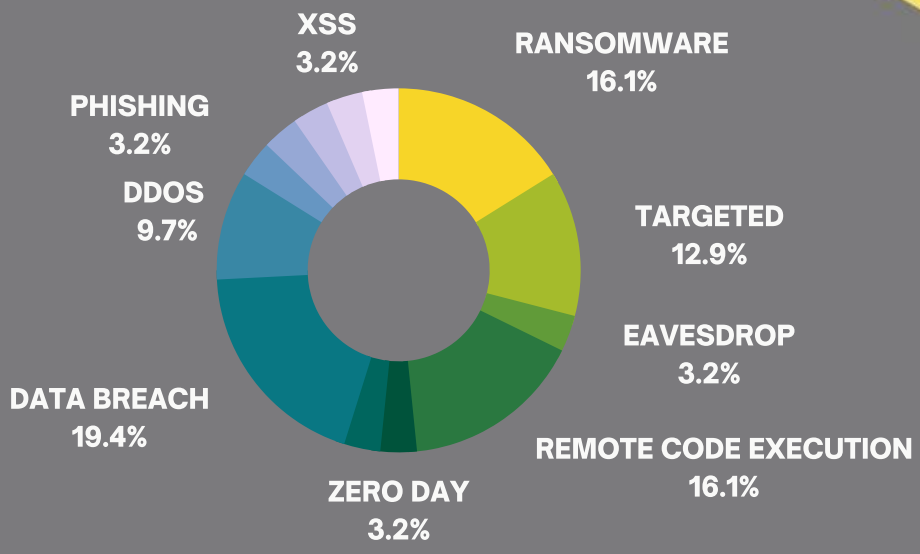
"employees and stakeholders have limited or no perception or understanding of threats and misplaced understanding of massive cyber threats or consequences".

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 this month.

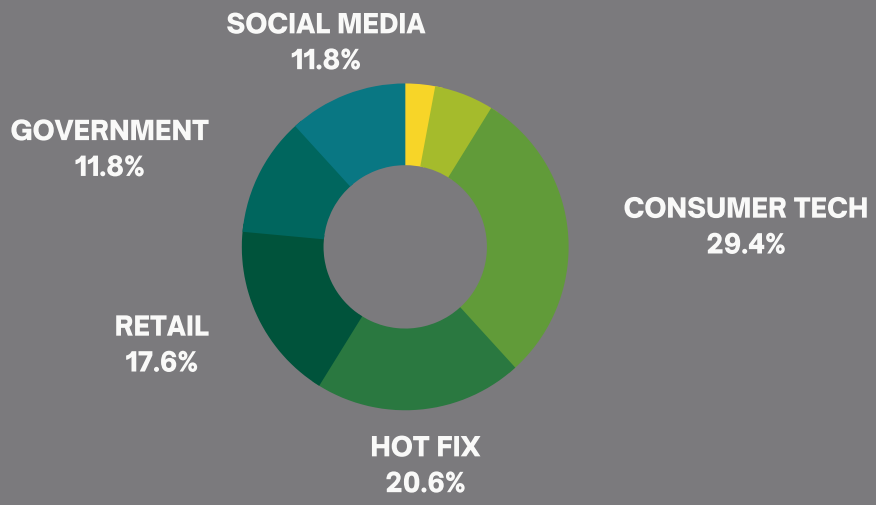
TYPES OF ATTACK VECTORS

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 consumer technology sector (29%). 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

- ADT Security Camera Flaws Open Homes to Eavesdropping
- SonicWall Hacked Using 0-Day Bugs In Its Own VPN Product
- Sharing eBook With Your Kindle Could Have Let Hackers Hijack Your Account
- Hackers Accidentally Expose Passwords Stolen From Businesses On the Internet
- Hackers Steal Mimecast Certificate Used to Securely Connect with Microsoft 365
- New Linux SUDO flaw lets local users gain root privileges
- Vulnerability Spotlight: Multiple vulnerabilities in phpGACL class
- Windows RDP servers are being abused to amplify DDoS attacks
- New 5G Network Flaws Let Attackers Track Users' Locations and Steal Data
- Valve's Steam Server Bugs Could've Let Hackers Hijack Online Games

MANUFACTURING

- Leading crane maker Palfinger hit in global cyberattack

RETAIL

- SolarWinds Hackers Also Breached Malwarebytes
- Intel Adds Hardware-Enabled Ransomware Detection to 11th Gen vPro Chips
- Pan-Asian retail giant Dairy Farm suffers REvil ransomware attack
- Bonobos clothing store suffers a data breach, hacker leaks 70GB database
- Wasabi cloud storage service knocked offline for hosting malware
- Italian mobile operator offers to replace SIM cards after massive data breach

MEDIA & ENTAINMENT

- Misconfigured Cloud Server Exposes 66,000 Gamers
- VLC Media Player 3.0.12 fixes multiple remote code execution flaws

GOVERNMENT

- Cook County Leaks 320,000 Court Records
- ASIC reports server breached via Accellion vulnerability
- Hackers publish thousands of files after government agency refuses to pay ransom
- Undisclosed Apache Velocity XSS vulnerability impacts GOV sites

LATEST THREAT ENTRIES

SOCIAL MEDIA

- TikTok Bug Could Have Exposed Users' Profile Data and Phone Numbers
- Google Details Patched Bugs in Signal, FB Messenger, JioChat Apps
- Facebook sues two Chrome extension devs for scraping user data
- Data of 533mn FB users being sold via Telegram bot

AUTOMOTIVE

- AnyVan confirms digital break-in, says customer names, emails and hashed passwords exposed

HOT FIX YOU SHOULD NOTICE..

- New Docker Container Escape Bug Affects Microsoft Azure Functions
- Apple Warns of 3 iOS Zero-Day Security Vulnerabilities Exploited in the Wild
- Experts Detail A Recent Remotely Exploitable Windows Vulnerability
- Drupal releases fix for critical vulnerability with known exploits
- Google fixes severe Golang Windows RCE vulnerability
- Critical Cisco SD-WAN Bugs Allow RCE Attacks

BRISKINFOSEC TOOL OF THE DAY

- Weevely Post-Exploitation Web Shell
- Blackwidow Tool To Perform Reconnaissance For Web Applications
- Content Discovery Script with File-Buster
- Pompem-Exploit and Vulnerability Finder
- The TIDoS Framework: The Offensive Web Application Penetration Testing Framework
- Web Scanner - Exploitation - Information Gathering

CYBER MONDAY

- Artificial Intelligence
- Cyber Security Devices & Services
- DEVOPS AND DEVSECOPS

BLOGS OF THE MONTH

- Important Vulnerabilities And Smart Ways To Be Secured From Them
- The security and privacy risks of face recognition authentication
- Why large organizations suffer frequent cyber-attacks than smaller ones

ADT Security Camera Flaws Open Homes to Eavesdropping

ATTACK TYPE
Eavesdrop
CAUSE OF ISSUE
Security flaws
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/24xCAGW

Researchers have publicly disclosed security flaws found in ADT-owned LifeShield security cameras, which, if exploited, could have allowed a local attacker to eavesdrop on victims' conversations or tap into a live video feed. Specifically affected is the LifeShield DIY HD Video Doorbell, which connects to users' Wi-Fi networks and lets them answer the door remotely using the LifeShield mobile app. However, security experts warn that ADT's glitches serve as warning and are just the latest camera maker to patch similar security issues tied to connected cameras.

SonicWall Hacked Using 0-Day Bugs In Its Own VPN Product

ATTACK TYPE
Zero Day
CAUSE OF ISSUE
Security flaw
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://zd.net/3a04UBq

Networking device maker SonicWall faced a "coordinated attack." They said that "highly sophisticated threat actors" targeted its internal systems by "exploiting probable zero-day vulnerabilities on certain SonicWall secure remote access products." Sonicwall initially listed NetExtender VPN clients and the Secure Mobile Access (SMA) gateways as impacted, but later said that only devices part of its SMA 100 series appliances are still under investigation as they contain a zero-day vulnerability. Patches for the zero-day vulnerabilities isn't available yet.

Sharing eBook With Your Kindle Could Have Let Hackers Hijack Your Account

ATTACK TYPE
RCE
CAUSE OF ISSUE
authentication
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/3ano8qB

A researcher, Yogev Bar-On, of Readlmode Labs, detailed how he chained a series of vulnerabilities to achieve remote code execution (RCE) on an Amazon Kindle e-reader. The attack – dubbed 'KindleDrip' – relied on three vulnerabilities found in the e-reader. Bar-On, however, was able to spoof a user's Kindle email address and send an e-book to their device, bypassing authentication checks. There was no indication that the e-book was received from an email message, and the e-book also appeared on the home page of the Kindle with a cover image of the attacker's choice – "which makes phishing attacks much easier.

Hackers Accidentally Expose Passwords Stolen From Businesses On the Internet

ATTACK TYPE
Phishing
CAUSE OF ISSUE
Poor security pratice
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/3mX92fz

A new large-scale phishing campaign has been found to bypass Microsoft Office 365 Advanced Threat Protection (ATP) and steal credentials belonging to over a thousand corporate employees due to operational security failure. The attack chain commenced with phishing lures that purported to be Xerox (or Xeros) scan notifications containing an HTML file attachment, that when opened, urged recipients to enter their Office 365 passwords on a fake lookalike login page, which were then extracted and sent to a remote server in a text file. With a simple Google search, anyone could have found the password to one of the compromised, stolen email addresses

Hackers Steal Mimecast Certificate Used to Securely Connect with Microsoft 365

A Mimecast-issued certificate used to authenticate some of the company's products to Microsoft 365 Exchange Web Services has been "compromised by a sophisticated threat actor," the company has announced. Mimecast provides email security services that customers can apply to their Microsoft 365 accounts by establishing a connection to Mimecast's servers. The certificate in question is used to verify and authenticate those connections made to Mimecast's Sync and Recover. A compromise means that cyberattackers could take over the connection, though which inbound and outbound mail flows.

ATTACK TYPE
Targetted
CAUSE OF ISSUE
Unauthorised access
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/3rb6ahM

New Linux SUDO flaw lets local users gain root privileges

ATTACK TYPE
Privilege escalation
CAUSE OF ISSUE
Authentication flaw
TYPE OF LOSS
Reputation
REFFERENCES
https://bit.ly/3cyKQPk

A now-fixed Sudo vulnerability allowed any local user to gain root privileges on Unix-like operating systems without requiring authentication. Sudo is a Unix program that enables system admins to provide limited root privileges to normal users listed that works on the Principle of Least Privilege. The Sudo privilege escalation vulnerability tracked as CVE-2021-3156 is an issue is a heap-based buffer overflow exploitable by any local user. The buffer overflow allowing any local user to obtain root privileges is triggered by Sudo incorrectly unescaping backslashes in the arguments.

Vulnerability Spotlight: Multiple vulnerabilities in phpGACL class

Cisco Talos recently discovered multiple vulnerabilities in the phpGACL class. One of these vulnerabilities also affects OpenEMR, a medical practice management software written in PHP. phpGACL is a PHP library that allows developers to implement permission systems via a Generic Access Control List. An adversary could exploit these vulnerabilities by sending the target machine a specially crafted, malicious HTTP request or URL. In accordance with our coordinated disclosure policy, Cisco Talos worked with phpGACL and OpenEMR to ensure that these issues are resolved and that an update is available for affected customers.

ATTACK TYPE
CSRF, Sql Injection, Open redirection
CAUSE OF ISSUE
Lack of security
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/3tc03vo

Windows RDP servers are being abused to amplify DDoS attacks

ATTACK TYPE
DDOS
CAUSE OF ISSUE
Sewcurity flaw
TYPE OF LOSS
Reputation
REFFERENCES
https://zd.net/2L91xW4

Windows RDP servers running on UDP port 3389 can be ensnared in DDoS botnets and abused to bounce and amplify junk traffic towards victim networks. Not all RDP servers can be abused, but only systems where RDP authentication is also enabled on UDP port 3389. This is called a 'DDoS amplification factor'. Netscout is now asking system administrators who run RDP servers exposed on the internet to take systems offline, switch them to the equivalent TCP port, or put the RDP servers behind VPNs in order to limit who can interact with vulnerable systems.

CONSUMER TECH

New 5G Network Flaws Let Attackers Track Users' Locations and Steal Data

New 5G Network Flaws Let Attackers Track Users' Locations and Steal Data. As 5G networks are being gradually rolled out in major cities globally, an analysis of its network architecture has revealed a number of potential weaknesses that could be exploited by hackers. But the researchers say this very stack of technologies potentially opens the door to attacks on subscribers and the operator's network that could be exploited to stage man-in-the-middle and DoS attacks

ATTACK TYPE

DDOS

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/39E1KeL

Valve's Steam Server Bugs Could've Let Hackers Hijack Online Games

ATTACK TYPE

Remote access

CAUSE OF ISSUE

Sewcurity flaw

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/36yj2qs

Critical flaws in a core networking library powering Valve's online gaming functionality could have allowed malicious actors to remotely crash games and even take control over affected third-party game servers. An attacker can remotely crash an opponent's game client to force a win or even perform a 'nuclear rage quit' and crash the Valve game server to end the game completely. Potentially even more damaging, attackers could remotely take over third-party developer game servers to execute arbitrary code.

Leading crane maker Palfinger hit in global cyberattack

Leading Austrain crane and lifting manufacturer Palfinger is targeted in an ongoing cyberattack that has disrupted IT systems and business operations. A security notice titled 'Cyber attack at PALFINGER Group' also states that their Enterprise resource planning (ERP) systems are down and that "a large proportion of the group's worldwide locations are affected." Palfinger is alerting partners of the attack and advising them to use "alternative channels (mobile phone, SMS, Whatsapp)" to communicate with Palfinger contacts.

ATTACK TYPE

Targetted

CAUSE OF ISSUE

Poor Security pratice

TYPE OF LOSS

Reputation

REFFERENCES

https://bit.ly/3jdqBrx

MANUFACTURING

SolarWinds Hackers Also Breached Malwarebytes

The security firm said the hackers breached its internal systems by exploiting a dormant email protection product within its Office 365 tenant. Microsoft was auditing its Office 365 and Azure infrastructures for signs of malicious apps created by the SolarWinds hackers, also known in cyber-security circles as UNC2452 or Dark Halo. Once it learned of the breach, it began an internal investigation to determine what hackers accessed. After an extensive investigation, we determined the attacker only gained access to a limited subset of internal company emails.

ATTACK TYPE
Data breach
CAUSE OF ISSUE
Lack of awarness
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://zd.net/3aEZwKf

RETAIL

Intel Adds Hardware-Enabled Ransomware Detection to 11th Gen vPro Chips

ATTACK TYPE
Ransomware
CAUSE OF ISSUE
Lack of awarness
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://zd.net/3thQDP8

At the 2021 Consumer Electronics Show today, Intel announced it is adding ransomware detection capabilities to its new 11th Gen Core vPro processors through improvements to its Hardware Shield and Threat Detection Technology (TDT) being a technology that locks down the UEFI/BIOS and TDT, a technology that uses CPU telemetry to detect possibly malicious code. A partnership with Boston-based Cybereason was also announced, with the security firm expected to add support for these new features to its security software in the first half of 2021.

Pan-Asian retail giant Dairy Farm suffers REvil ransomware attack

Massive pan-Asian retail chain operator Dairy Farm Group was attacked by the REvil ransomware operation. The attackers claim to have demanded a $30 million ransom. The Dairy Farm Group operates over 10,000 outlets and has 230,000 employees throughout Asia. In 2019, the Dairy Farm Group's total annual sales exceeded $27 billion. The attackers claim to still have access to the network seven days after the attack, including full control over Dairy Farm's corporate email, which they state will be used for phishing attacks.

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

Bonobos clothing store suffers a data breach, hacker leaks 70GB database

ATTACK TYPE
Data breach
CAUSE OF ISSUE
Poor security pratice
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/39E5BX1

Bonobos men's clothing store has suffered a massive data breach exposing millions of customers' personal information after a cloud backup of their database was downloaded by a threat actor. The leaked database is a monstrous 70 GB SQL file containing various internal tables used by the Bonobos website. The database also includes various data far more interesting to threat actors, such as customers' addresses, phone numbers, partial credit card numbers (last four digits), order information, password histories.

RETAIL

Wasabi cloud storage service knocked offline for hosting malware

Wasabi Cloud Storage supplier endured a blackout after an area utilized for capacity endpoints was suspended for facilitating malware. In the wake of learning of the maltreatment report, Wasabi suspended the customer facilitating the malicious content and requested that the registrar to reactivate the domain and it required thirteen hours for the registrar to reactivate the domain. It is obscure what malignant substance, or conceivably false positives, set off the domain's suspension.

ATTACK TYPE

Targetted

CAUSE OF ISSUE

Poor security pratice

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3pM4fjC

Italian mobile operator offers to replace SIM cards after massive data breach

ATTACK TYPE

Data breach

CAUSE OF ISSUE

Poor security pratice

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://zd.net/2YAm9JV

Italian mobile Operator HO owned by vodafone has suffered a massive data breach. The 2.5million customers data has been sold on dark web forum. The company immediately initially played down these initial reports, and later confirmed the incident in their official website and via SMS messages and replaced free Sim cards to avoid the threats related to telephone fraud or sim swapping attacks to all the impacted customers.

Misconfigured Cloud Server Exposes 66,000 Gamers

Tens of thousands of users have had their personal details exposed after a popular online gaming site misconfigured the Elasticsearch server they were sitting on. It was traced back to VIPGames.com, with 100,000 Google Play downloads and roughly 20,000 active daily players. It features games such as Hearts, Crazy Eights, Euchre, Rummy, Dominoes, Backgammon, Ludo and Yatzy. Over 30GB of data was leaked in the privacy snafu, including 23 million records.

ATTACK TYPE

Data exposed

CAUSE OF ISSUE

Security misconfiguration

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3aE4HRF

MEDIA & ENTERTAINMENT

VLC Media Player 3.0.12 fixes multiple remote code execution flaws

ATTACK TYPE

RCE

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/2N4ZoqT

Videolan has released a patch for VLC media player for windows, mac and linux users. It has fixed many security vulnerabilities, Some of the vulnerabilities include buffer overflow attacks in which remote user can create a specially crafted media files and tricking a user into opening them with VLC likely crash VLC Media Player, they warn that attackers could use it to leak information or remotely execute commands on the device.

GOVERNMENT

Cook County Leaks 320,000 Court Records

Over 320,000 court records containing highly sensitive data appears to have come from an internal records management system, which virtually all exposed records containing some form of personal info including: full names, home addresses, email addresses, case numbers and private case notes belonging to cook county in the US have been discovered on a misconfigured online database. “There have been several high-profile data exposures of private companies that affected Cook County residents in the past few years including a large hospital data breach.

ATTACK TYPE
Data leaks
CAUSE OF ISSUE
Security flaw
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/2NSIFN7

ASIC reports server breached via Accellion vulnerability

ATTACK TYPE
Ransomware
CAUSE OF ISSUE
Security flaw
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://zd.net/2YEOfWI

The ASIC has reported that they had hit with a security breach on the mid January.The Australian Securities and Investments Commission (ASIC) has said one of its servers was breached on January 15. It is happened on the Accellion software that is used by the ASIC to transfer files and attachment. An intrusion happened to a server that contains the documents with recent Australian credit licence applications. But ASIC confirms that only limited information has been viewed, no informations were downloaded or opened. No other ASIC infrastructure has been affected via this breach.

Hackers publish thousands of files after government agency refuses to pay ransom

Hackers attacked Scottish Environment Protection Agency (SEPA) via a Ransomware and disclosed thousands of stolen files as they refused to pay the demanded ransom. SEPA hasn't confirmed what form of ransomware it has fallen victim to, but the Conti ransomware gang claimed responsibility for the attack. Hackers steal 1.25 GB of data around 4000 files in the process. Agencies SEPA is working with in continued efforts to investigate the attack and fully restore the network

ATTACK TYPE
Ransomware
CAUSE OF ISSUE
Law of maintaince
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/24xHwvs

Undisclosed Apache Velocity XSS vulnerability impacts GOV sites

ATTACK TYPE
XSS
CAUSE OF ISSUE
Security flaw
TYPE OF LOSS
Reputation
REFFERENCES
https://bit.ly/3hDCID6

Apache has patched a XSS security flaw which can be exploited by a unauthenticated attackers to target government sites, including NASA and NOAA. Attacker can consequently trick a victim into clicking such a URL, which leads the victim to an altered phishing page, or exfiltrates their login session information. The flaw has been reported and patched before revealing it to the public .

SOCIAL MEDIA

TikTok Bug Could Have Exposed Users' Profile Data and Phone Numbers

Cybersecurity researchers on Tuesday disclosed a now-patched security flaw in TikTok that could have potentially enabled an attacker to build a database of the app's users and their associated phone numbers for future malicious activity. Although this flaw only impacts those users who have linked a phone number with their account or logged in with a phone number, a successful exploitation of the vulnerability could have resulted in data leakage and privacy violation. However, TikTok has deployed a fix to address the shortcoming following responsible disclosure.

ATTACK TYPE
DDOS
CAUSE OF ISSUE
Backdoor
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/3rCaKqx

Google Details Patched Bugs in Signal, FB Messenger, JioChat Apps

In 2019, there was a severe vulnerability in Apple's face time group chats feature that could allow attackers to eaves drop on the conversations between two persons. Similar shortcomings were also discovered in multiple video chat apps such as Signal, JioChat, Mocha, Google Duo, and Facebook Messenger by Google Project Zero researcher Natalie Silvanovich. Although the issue was fixed in this, this raises the suspicion that if other state machines had similar vulnerabilities.

ATTACK TYPE
Ransomware
CAUSE OF ISSUE
Poor security pratice
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://zd.net/2WX7acq

Data of 533mn FB users being sold via Telegram bot

Facebook user data of 533 million are being sold in telegram via a bot. User phone numbers are being sold for $20. The Facebook confirmed that data which are being sold are old and company has fixed this vulnerability in August 2019 but it still presents a cybersecurity and privacy risk to those whose phone numbers may be exposed.

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

Facebook files a case against two Portuguese for scrapping user data via browser extensions.

Facebook has filed a lawsuit against two portuguese guys namely Oink and Stuff for scraping user data on facebook sites via browser extensions. They also information from the users' browsers unrelated to Facebook. Facebook's Director of Platform Enforcement and Litigation, says that if any user visited the Facebook Website, the browser extensions were designed to scrape the consumer data like name, user ID, gender, relationship status, age group and other information from the user account.

ATTACK TYPE
Targetted
CAUSE OF ISSUE
Lack of maintaonce
TYPE OF LOSS
Reputation
REFFERENCES
https://bit.ly/3aqLpb5

HOT FIX YOU SHOULD NOTICE..

New Docker Container Escape Bug Affects Microsoft Azure Functions

Cybersecurity researcher Paul Litvak disclosed an unpatched vulnerability in Microsoft Azure Functions that could be used by an attacker to escalate privileges and escape the Docker container used for hosting them. Following disclosure to Microsoft, the Windows maker is said to have "determined that the vulnerability has no security impact on Function users, since the host itself is still protected by another defence boundary against the elevated position we reached in the container host."

ATTACK TYPE
Unauthorised access
CAUSE OF ISSUE
Security flaw
TYPE OF LOSS
Reputation
REFFERENCES
https://bit.ly/3rD8Gyk

Apple Warns of 3 iOS Zero-Day Security Vulnerabilities Exploited in the Wild

ATTACK TYPE
RCE
CAUSE OF ISSUE
Lack of maintainces
TYPE OF LOSS
Reputation
REFFERENCES
https://bit.ly/37W6S1S

Apple released updates for iOS, iPadOS, and tvOS with fixes for three security vulnerabilities that it says may have been actively exploited in the wild. Reported by an anonymous researcher, the three zero-day flaws — CVE-2021-1782, CVE-2021-1870, and CVE-2021-1871 — could have allowed an attacker to elevate privileges and achieve remote code execution while the other two issues were said to be of business logic issues. Apple said the flaws were addressed with improved locking and restrictions, respectively.

Experts Detail A Recent Remotely Exploitable Windows Vulnerability

Details have emerged about a security feature bypass vulnerability in Windows NT LAN Manager (NTLM) that was addressed by Microsoft as part of its monthly Patch updates earlier this month. The flaw, tracked as CVE-2021-1678 (CVSS score 4.3), was described as a "remotely exploitable" flaw found in a vulnerable component bound to the network stack, although exact details of the flaw remained unknown. According to researchers from Crowdstrike, the security bug if left unpatched, could allow a bad actor to achieve remote code execution via an NTLM relay.

ATTACK TYPE
RCE
CAUSE OF ISSUE
XSS flaw
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/2WS71UR

Drupal releases fix for critical vulnerability with known exploits

ATTACK TYPE
Arbitrary code execution
CAUSE OF ISSUE
Lack of security
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/39CLdpW

Drupal releases fix for critical vulnerability with known exploitsDrupal has released a security update to address a critical vulnerability in a third-party library called pear Archive_Tar library with documented or deployed exploits available in the wild. The CVE-2020-36193 . The bug causes out-of-path extraction vulnerabilities via "write operations with Directory Traversal due to inadequate checking of symbolic links." This vulnerability is related to another critical security flaw with known exploits caused by the CVE-2020-28948 bug in the PEAR Archive_Tar library that could allow for arbitrary PHP code execution on some CMS versions.

Google fixes severe Golang Windows RCE vulnerability

Japan-based security researcher has discovered a major command injection venerability in the Golang project which allows the user to execute arbitrary code while building the malicious code on windows. The user to run go get command against the malicious repository.However Google patched this vulnerability in the next update. The vulnerability, tracked as CVE-2021-3115, stems from how the compile process works when a user runs the "go get" command to fetch a repository.

ATTACK TYPE
Arbitray code
CAUSE OF ISSUE
Security flaw
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/3tk1xq8

Critical Cisco SD-WAN Bugs Allow RCE Attacks

ATTACK TYPE
Command Execution
CAUSE OF ISSUE
Lack of security
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/3rdRHIk

Critical-severity flaw was found in the Command Runner tool of Cisco DNA Center, which is Cisco's network management and command center. The flaw (CVE-2021-1264) ranks 9.6 out of 10 on the CVSS scale. This vulnerability affects Cisco DNA Center software releases earlier than 1.3.1.0; fixes are available in software releases 1.3.1.0 and later. The flaw stems from insufficient input validation by the Command Runner tool, which allows users to send diagnostic CLI commands to selected devices. An attacker could exploit this flaw by providing crafted input during command execution or via a crafted command runner API call.

AUTOMOTIVE

AnyVan confirms digital break-in, says customer names, emails and hashed passwords exposed

A European online marketplace named Anyvan that lets users buy delivery, transport, or removal services from a network of providers, has accepted that they have hit with a security incident, looting the customer's data like names, email, and a cryptographic hash of their password were accessed and 'potentially viewed' but no other personal data was unwittingly shared. The company requested all the users to change their passwords.

ATTACK TYPE
Data leak
CAUSE OF ISSUE
Law of maintaince
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/3pHPRZo

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.

BRISK INFOSEC

CYBER TRUST & ASSURANCE

TOOLS OF THE MONTH

Weevely Post-Exploitation Web Shell

Weevely is a stealth PHP web shell that simulate telnet-like connection. It is an essential tool for web application post exploitation, and can be used as stealth backdoor or as a web shell to manage legit web accounts, even free hosted ones.

Blackwidow Tool To Perform Reconnaissance For Web Applications

BlackWidow is a python based web application spider to gather subdomains, URL's, dynamic parameters, email addresses and phone numbers from a target website. This project also includes Inject-X fuzzer to scan dynamic URL's for common OWASP vulnerabilities.

Content Discovery Script with File-Buster

Filebuster is a HTTP fuzzer / content discovery script with loads of features and built to be easy to use and fast.
It uses one of the fastest HTTP classes in the world (of PERL) - Furl::HTTP. Also the thread modelling is optimized to run as fast as
possible.

Pompem-Exploit and Vulnerability Finder

Pompem is an open source tool, designed to automate the search for Exploits and Vulnerability in the most important databases. Developed in Python, has a system of advanced search, that help the work of pentesters and ethical hackers. In the current version, it performs searches in PacketStorm security, CXSecurity, ZeroDay, Vulners, National Vulnerability Database, WPScan Vulnerability Database.

The TIDoS Framework: The Offensive Web Application Penetration Testing Framework.

A complete versatile framework to cover up everything from Reconnaissance to Vulnerability Analysis.Has 5 main phases, subdivided into 14 sub-phases consisting a total of 108 modules.Reconnaissance Phase has 50 modules of its own (including active and passive recon, information disclosure modules).Scanning & Enumeration Phase has got 16 modules (including port scans, WAF analysis, etc)

Web Scanner - Exploitation - Information Gathering

Zeebsploit is a web application penetration testing tool used for information gathering, scanning, and exploiting vulnerabilities. Zeebsploit can perform the information gathering tasks about targeted web applications.

CYBER MONDAY

Artificial Intelligence

If AI based machines are not scrutinized and monitored properly, then they may go haywire and can turn to become a nightmare to the entire human race With corrupted codes and misconfigured functionality, they could represent the ultimate evilness and could cause destruction who were designed to aid humanity

Cyber Security Devices & Services

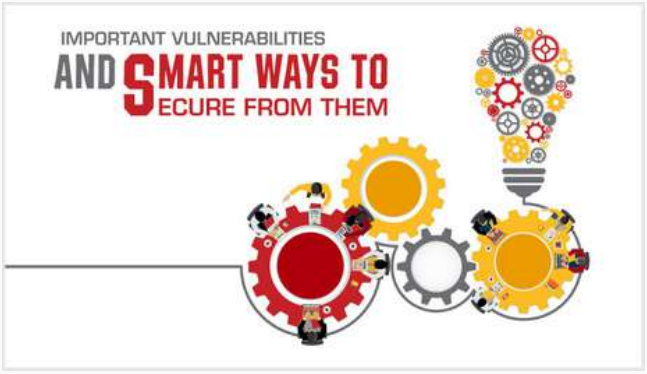
Cybersecurity is not just about spending on devices alone. Cybersecurity devices play a significant role but they alone don't amount to thr entire significance of cybersecurity. As much investment is done on these, same on services must also be done to balance it finely

DEVOPS AND DEVSECOPS

Devops stands for Development operations. These are effective but with the rampant pace of security growth, this model falls short as it is ignorant of security in it as a better alternate to it, arises DevSecOps that security in every phase of it

BLOG OF THE MONTH

Important Vulnerabilities And Smart Ways To Be Secured From Them



If AI based machines are not scrutinized and monitored properly, then they may go haywire and can turn to become a nightmare to the entire human race With corrupted codes and misconfigured functionality, they could represent the ultimate evilness and could cause destruction who were designed to aid humanity

The security and privacy risks of face recognition authentication

Biometrics has changed the way people are being identified. Since the last decade, its growth is incredible and has transformed a lot of industries from military to telecommunication. Facial recognition is one of the biometric identification types that can be easily performed without the object's knowledge unlike retinal scans, blood samples or fingerprints.

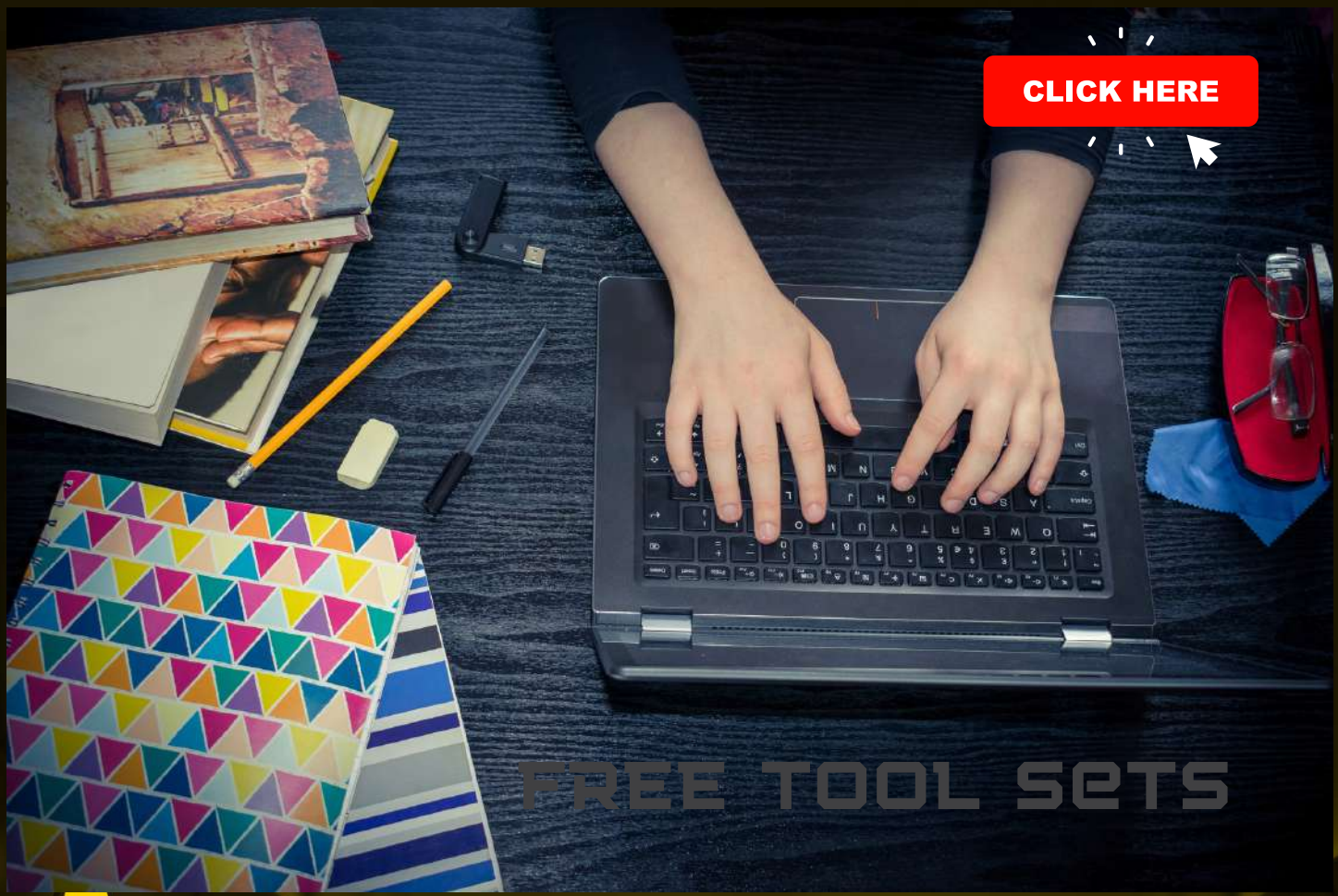
Why large organizations suffer frequent cyber-attacks than smaller ones?

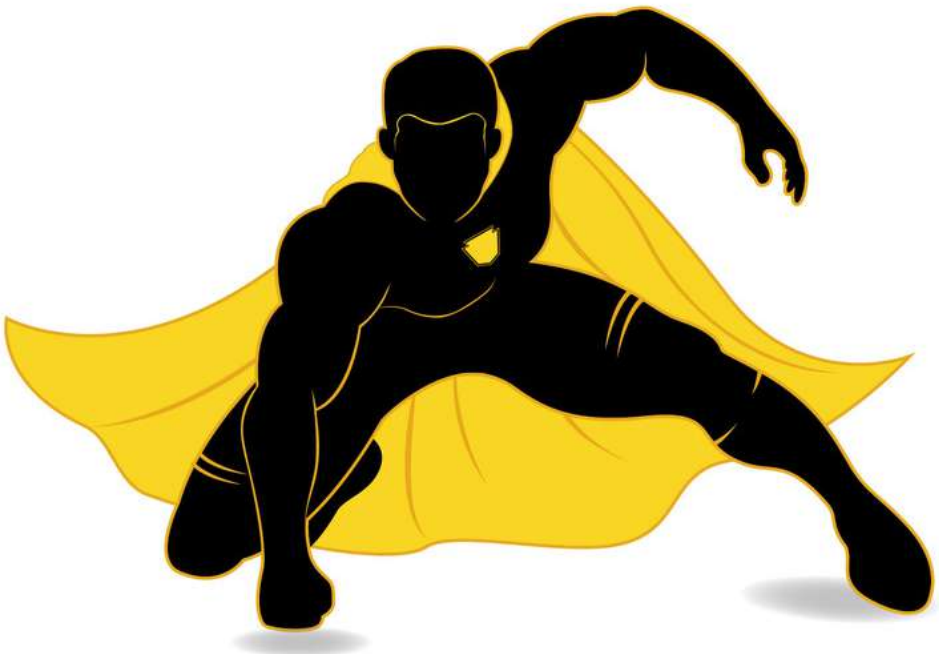
Larger organization have built lots of inefficiencies that impact their ability in managing huge amount of data created as part of their business. In most cases, the internal security team fail to identify and protect the business data. Let us explore more.

CLICK HERE

WAKE UP CXO

AN INITIATIVE BY BRISKINFOSEC





www.briskinfosec.com