BRISK INFOSEC
CYBER TRUST & ASSURANCE

Edition 29
January

THREATSPLOIT
ADVERSARY REPORT

2021

INTRODUCTION

Welcome to the Threatsploit report of January 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....

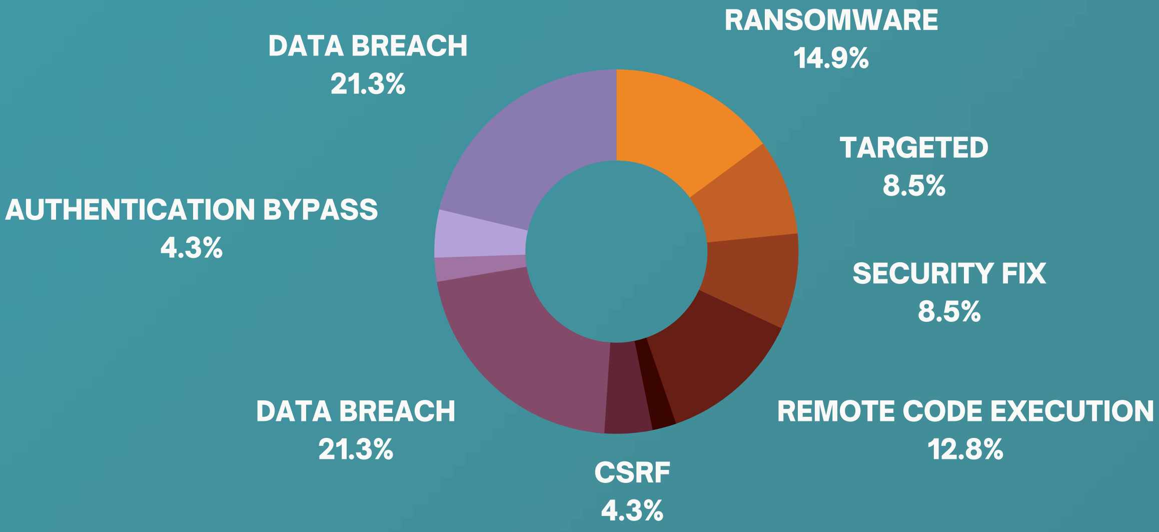
"employees and stakeholders have limited or no perception or understanding of threats and misplaced understanding of massive cyber threats or consequences".

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.

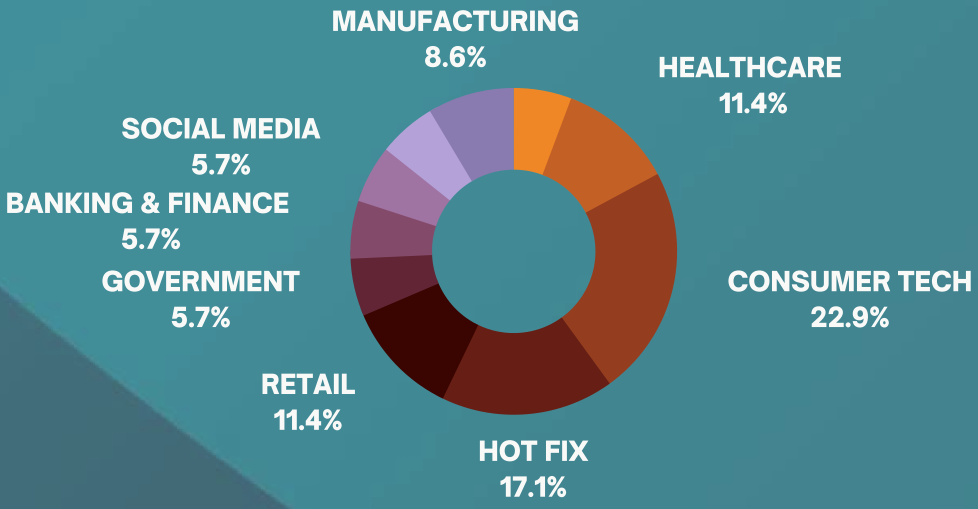
TYPES OF ATTACK VECTORS

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 (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

HEALTHCARE

- Hackers breach Pfizer/BioNTech COVID-19 vaccine data in cyberattack
- More than 45 million medical images openly accessible online
- US mental health provider admits email breach exposed patient data
- Ransomware Attack on Maryland’s GBMC Healthcare

CONSUMER TECH

- Microsoft confirms it was also breached in recent SolarWinds
- A Google Docs Bug Could Have Allowed Hackers See Your Private Documents
- Critical CSRF vulnerability found on Glassdoor
- Remote code execution vulnerability uncovered in Starbucks mobile platform
- Air-Gap Attack Turns Memory Modules into Wi-Fi Radios
- HR Giant Randstad Hit by Egregor Ransomware
- New 5G Network Flaws Let Attackers Track Users' Locations and Steal Data
- Valve's Steam Server Bugs Could've Let Hackers Hijack Online Games

GOVERNMENT

- Software Supply-Chain Attack Hits Vietnam Government Certification Authority
- Four U.S. cities attacked by ransomware

BANKING AND FINANCE

- Credential Stealer Targets US, Canadian Bank Customers
- Payment Processing Giant TSYS: Ransomware Incident “Immaterial” to Company

SOCIAL MEDIA

- Anna Kendrick's Twitter Briefly Hacked, Series of Offensive Tweets Posted
- Farah Khan, Vikrant Massey's social media accounts hacked

LATEST THREAT ENTRIES

EDUCATION

- Rajasthan Technical University website hacked
- Kent State University systems potentially hacked

MANUFACTURING

- Kawasaki Heavy Industries reports data breach
- Hackers demand $34.7 million in Bitcoin after ransomware attack on Foxconn
- Intel's Habana Labs hacked by Pay2Key ransomware, data stolen

ENERGY

- Cyberattack on US Nuclear agency, Microsoft Prez says it’s a moment of reckoning

RETAIL

- High-security registration plate: Bookmyhsrp hacked
- Ransomware attack cripples Vancouver public transportation agency
- Spotify security vulnerability exposed personal data to business partners
- Cloudflare WAF Bypass Via New Padding Technique

TELECOMMUNICATION

- ‘Amnesia:33’ TCP/IP Flaws Affect Millions of IoT Devices

HOT FIX YOU SHOULD NOTICE..

- 5M WordPress Sites Running ‘Contact Form 7’ Plugin Open to Attack
- Zero-Click Wormable RCE Vulnerability in Cisco Jabber
- QNAP High-Severity Flaws Plague NAS Systems
- Firefox Patches Critical Mystery Bug, Also Impacting Google Chrome
- Google Discloses Poorly-Patched, Now Unpatched, Windows 0-Day Bug
- Trend Micro inter scan web security appliance security patch

BRISKINFOSEC TOOL OF THE DAY

- Subbrute Tool to Identifies sub domains by bruteforcing
- WafW00f Tool to Fingerprint and identify Web Application FirewalL
- Wapiti Tool for web application security auditor
- Turbolist3r Tool Web Application Subdomain Discover
- FinalRecon is a fast and simple python script for web reconnaissance
- Fuzz Faster U Fool Tool to Fuzzing Get and Post data

CYBER MONDAY

- Browser Security
- Docker Platform
- Host Level Security

BLOGS OF THE MONTH

- Detection and Exploitation of XML External Entity Attack XXE
- Layer Wise Analysis of Security in IOT
- Host Header Inection Vulnerability

Hackers breach Pfizer/BioNTech COVID-19 vaccine data in cyberattack

The German based healthcare firm released a statement given by European medical agency on 9 December 2020 that some documents relating to the regulatory submission for Pfizer and BioNTech's COVID-19 vaccine candidate, BNT162b2, which has been stored on an EMA server, had been unlawfully accessed. However the health care firm has confirmed the cyber attack will have no effect or delay in the review of the vaccine.

ATTACK TYPE

Data breach

CAUSE OF ISSUE

Unauthorised access

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3n2ynEW

More than 45 million medical images openly accessible online

Millions of medical images such as X-rays, MRIs, and CT scans are available unsecured on the open web, an investigation by threat intelligence has revealed. The research team says it found unprotected connected storage devices with ties to hospitals and medical centers worldwide that were leaking more than 45 million unique imaging files. Millions of images were unencrypted and could be accessed without password protection.

ATTACK TYPE

Insecure storage

CAUSE OF ISSUE

Poor security pratice

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3hwH5Kp

US mental health provider admits email breach exposed patient data

People Incorporated Mental Health Services, a Minnesota-based US healthcare provider, has admitted that an email security data breach has exposed sensitive patient records, along with an unspecified volume of financial data. A notice on the US government Health and Human Services website states that 27,500 people were affected by the breach. After discovering the problem, People Incorporated shut off access to the compromised email accounts before applying a mandatory, company-wide password reset.

ATTACK TYPE

Data breach

CAUSE OF ISSUE

Unauthorised access

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/34XBPdV

Ransomware Attack on Maryland's GBMC Healthcare

GBMC HealthCare in Maryland is currently operating under planned EHR downtime procedures, after falling victim to a ransomware attack on December 6. The malware infected its IT systems, forcing many GBMC systems offline. Screenshots of the ransom note shows the attack was likely launched by Egregor, which is reportedly the follow-up hacking group to Maze. The investigation into the incident is ongoing, while GBMC is working with outside experts and law enforcement in response to the event.

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3mX92fz

Microsoft confirms it was also breached in recent SolarWinds

Microsoft on 17 December 2020 released a statement that they found SolarWinds Orion apps in its environment after CISA alerted about the SolarWinds supply chain attack and its impact on government agencies, critical infrastructure entities, and private sector organizations. In a statement, Microsoft admitted to finding trojanized SolarWinds Orion apps in its environment, but not to hackers pivoting to production systems and then using those systems against its customers

ATTACK TYPE

Data breach

CAUSE OF ISSUE

Unauthorised access

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://zd.net/3r0zxaW

A Google Docs Bug Could Have Allowed Hackers See Your Private Documents

Google has patched a bug in its feedback tool incorporated across its services that could be exploited by an attacker to potentially steal screenshots of sensitive Google Docs documents simply by embedding them in a malicious website. Many of Google's products, including Google Docs, come with a "Send feedback" option that allows users to send feedback along with an option to include a screenshot something that's automatically loaded to highlight specific issues.

ATTACK TYPE

Google Docs

CAUSE OF ISSUE

Sewcurity misconfiguration

TYPE OF LOSS

Reputation

REFFERENCES

https://bit.ly/3prGsVs

Critical CSRF vulnerability found on Glassdoor

Security Researcher found vulnerability of severity 9-10 in galssdoor company which was described as cross-site request forgery (CSRF). This vulnerability allow attackers to obtain a CSRF token from the firm's server to hijack accounts from logged-in victims. This could include establishing new administrators on employer accounts, deleting information on job seekers and employers, adding fake reviews, deleting CVs, as well as posting, applying for, and deleting job listings.

ATTACK TYPE

CSRF

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://zd.net/3rEap6B

Remote code execution vulnerability uncovered in Starbucks mobile platform

A potential remote code execution (RCE) bug has been patched in one of Starbucks' mobile domains. Bug bounty hunter discovered an .ashx endpoint on mobile.starbucks.com.sg that was intended for handling image files. However, the endpoint did not restrict file type uploads, which means that attackers abusing the issue could potentially upload malicious files and remotely execute arbitrary code.

ATTACK TYPE

RCE

CAUSE OF ISSUE

Sewcurity flaw

TYPE OF LOSS

Reputation

REFFERENCES

https://zd.net/2MdH8iJ

CONSUMER TECH

Air-Gap Attack Turns Memory Modules into Wi-Fi Radios

Secure air gapped computers are found a vulnerable to a new malware at the start of month that can turn pc memory module into modified radio poc was submitted by Mordechai guri. He said since the clock speed of memory modules is typically around the frequency of 2.4ghz or its harmonics the memory operation generate electromagnetic emissions around the IEEE 802.11 wifi frequency bands. The hack requires perfectly timed read-write operations, which would be driven by malware installed on the targeted computer.

ATTACK TYPE

Malware

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation

REFFERENCES

https://bit.ly/3rH9sdy

HR Giant Randstad Hit by Egregor Ransomware

ATTACK TYPE

Data breach

CAUSE OF ISSUE

Ransomware

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3aWEmZA

Human resources giant Randstad revealed that its IT systems were targeted in a recent cyberattack involving a relatively new piece of ransomware named Egregor.Randstad said the incident impacted a limited number of servers and its operations have not been disrupted. However, it has confirmed that the attackers have accessed some data. Hackers have so far released roughly 60Mb of information stolen from Randstad systems. The leaked files are mainly financial documents, mostly PDFs and Excel spreadsheets.

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

As 5G networks are being gradually rolled out in major cities across the world, an analysis of its network architecture has revealed a number of potential weaknesses that could be exploited to carry out a slew of cyber assaults, including denial-of-service (DoS) attacks to deprive subscribers of Internet access and intercept data traffic. The network becomes vulnerable to denial of service due to exploitation of vulnerabilities in the PFCP protocol,"

ATTACK TYPE

Data leak

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3rHQdR9

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/381KKkE

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. The four flaws (CVE-2020-6016 through CVE-2020-6019) were uncovered in Valve's Game Networking Sockets (GNS) or Steam Sockets library, an open-sourced networking library that provides a "basic transport layer for games," enabling a mix of UDP and TCP features with support for encryption, greater reliability, and (P2P) communications.

GOVERNMENT

Software Supply-Chain Attack Hits Vietnam Government Certification Authority

Cybersecurity researchers today disclosed a new supply-chain attack targeting the Vietnam Government Certification Authority (VGCA) that compromised the agency's digital signature toolkit to install a backdoor on victim systems. According to ESET's telemetry, the breach happened from at least July 23 to August 16, 2020, with the two installers in question — "gca01-client-v2-x32-8.3.msi" and "gca01-client-v2-x64-8.3.msi" for 32-bit and 64-bit Windows systems — tampered to include the backdoor.

ATTACK TYPE

Data breach

CAUSE OF ISSUE

Backdoor

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3rCaKqx

Four U.S. cities attacked by ransomware

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Poor security pratice

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3mYEfzb

Pensacola government telephone and email systems, internet servers, and the online payment system at the sanitation department and Pensacola Energy were rendered inoperable during a cyberattack on December 7. A state of emergency was declared in New Orleans after ransomware infected city servers and computers on December 13. In Galt, a suburb of Sacramento, city email and telephone systems were knocked offline on December 16. And on December 17, the St. Lucie County Sheriff's office was knocked offline, including the sheriff's office email server.

BANKING & FINANCE

Credential Stealer Targets US, Canadian Bank Customers

In mid-December, we discovered a campaign that distributed a credential stealer. We also learned that the main code components of this campaign is written in AHK. By tracking the campaign components, we found out that its activity has been occurring since early 2020. The malware infection consists of multiple stages that start with a malicious Excel file. In turn, this file contains an AHK script compiler executable, a malicious AHK script file, and a Visual Basic for Applications (VBA) AutoOpen macro.

ATTACK TYPE

Malware

CAUSE OF ISSUE

Law of maintaince

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3n0bzpp

Payment Processing Giant TSYS: Ransomware Incident "Immaterial" to Company

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Poor security pratice

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3mYEfzb

Payment card processing giant TSYS suffered a ransomware attack. TSYS said the attack did not affect systems that handle payment card processing. We experienced a ransomware attack involving systems that support certain corporate back office functions of a legacy TSYS merchant business," TSYS said. We immediately contained the suspicious activity and the business is operating normally.But, TSYS declined to say whether it paid any ransom to the hackers group.

SOCIAL MEDIA

Anna Kendrick's Twitter Briefly Hacked, Series of Offensive Tweets Posted

Hollywood actress Anna Kendrick became the latest victim of social media hacking as her official Twitter account was hacked for a brief period, and posted a series of offensive tweets. A series of tweets were sent out to Kendrick's 7.2 million followers that used offensive language. The posts caught the attention of social media users, who started commenting that Kendrick's account was compromised. The "Pitch Perfect" actor's Instagram account was unaffected. After a period of time , the tweets were deleted and the website on Kendrick's account reverted back.

ATTACK TYPE

Targetted

CAUSE OF ISSUE

Lack of awarness

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3o3NU90

Farah Khan, Vikrant Massey's social media accounts hacked

ATTACK TYPE

Targetted

CAUSE OF ISSUE

Lack of awarness

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/34Y4M9L

Farah Khan and actor Vikrant Massey became the victim of social media hacking. Choreographer-director Farah Khan and actor Vikrant Massey said the security of their social media accounts has been compromised and efforts are going on to restore their hacked profiles. Khan said while both her social media accounts such as Twitter and Instagram page were hacked.

EDUCATION

Rajasthan Technical University website hacked

Rajasthan Technical University's official website was hacked to support the students demanding an online examination. The official website was hacked by white hat hackers as they wanted to help the students who raised their voices against offline exams decided in the varsity amid this pandemic.The Technical University is one of the biggest varsity that controls all engineering colleges in the state.

ATTACK TYPE

Targetted

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3hwNqWl

Kent State University systems potentially hacked

ATTACK TYPE

Targetted

CAUSE OF ISSUE

Poor security pratice

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3b9gRwL

Kent State University is among at least 24 other organizations that are potentially affected by a widespread software hack. At this time, there is no evidence that indicates the hackers used this back door to access the Kent State network," the university said, in a statement sent out to students, faculty and staff Dec. 23. "Working in conjunction with industry experts, Kent State has taken necessary industry reasonable steps to address further attempts at compromise.

Kawasaki Heavy Industries reports data breach

A security incident at Kawasaki Heavy Industries has potentially exposed sensitive data to external parties, the company has confirmed.The hack may have targeted defense-related information held by Kawasaki Heavy, which produces aircraft and submarines for the Defense Ministry. Kawasaki Heavy said it has already strengthened its information security measures. No unauthorized access has been confirmed since August this year, according to the company.

ATTACK TYPE

Data breach

CAUSE OF ISSUE

Poor security pratice

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3puna1u

MANUFACTURING

Hackers demand $34.7 million in Bitcoin after ransomware attack on Foxconn

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Poor security pratice

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3mYEfzb

A ransomware attack on Taiwanese electronics giant Foxconn has resulted in hackers demanding $34.7 million in Bitcoin. Cybercriminals infiltrated Foxconn’s networks on November 29, stealing and encrypting files and deleting data from servers at the company’s Mexican facility, The attack was reportedly carried out by ransomware gang DoppelPaymer, which is demanding $34.7 million in cryptocurrency for the return of files.

Intel's Habana Labs hacked by Pay2Key ransomware, data stolen

Intel-owned AI chipmaker Habana Labs was hacked by Pay2key ransomware operators who claim to have stolen from the company.
The group announced the hack on Twitter, they claim to have stolen sensitive data, The hacked shared a link to a leak directory and images of the source code and internal processes belonging to the hacked company. The Pay2Key leak directory includes Windows domain controller data and a file listing from the Gerrit development code review system.

ATTACK TYPE

Data leak

CAUSE OF ISSUE

Ransomware

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/2JvvpLF

Cyberattack on US Nuclear agency, Microsoft Prez says it’s a moment of reckoning

ATTACK TYPE

Data breach

CAUSE OF ISSUE

Backdoor

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3rCaKqx

Microsoft earlier this month has declared that it found an malicious version of the software from solar winds in their environment which they found it and removed it. They same happened with the us nuclear agency and other goverment organization in the US but it did not affect any national security.This major breach has been told by microsoft CEO as recklessness which the whole US has to take care from now.

ENERGY

High-security registration plate: Bookmyhsrp hacked

The website bookmyhsrp.com was hacked, causing inconvenience of hundreds of vehicle owners as they were unable to book a slot for affixing high-security registration plate. A spokesperson of HSRP manufacturer said, A DDOS (Distributed Denial-of-Service) attempt was observed on www.bookmyhsrp.com and our domain name IP was mapped for compromise by unauthorised attempt through international traffic with virtual multiple counts hitting the domain creating a false overloading of high volume traffic. No data breach has happened in this event.

ATTACK TYPE

DDOS

CAUSE OF ISSUE

Backdoor

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3rCaKqx

Ransomware attack cripples Vancouver public transportation agency

ATTACK TYPE

Ransomware

CAUSE OF ISSUE

Poor security pratice

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://zd.net/2WX7acq

A ransomware attack has crippled the operations of TransLink, the public transportation agency for the city of Vancouver, Canada. Vancouver residents unable to use their Compass metro cards or pay for new tickets via the agency's Compass ticketing kiosks. Based on the ransom's note, TransLink had its systems infected with a version of the Egregor ransomware. TransLink says it has restored access to its Compass kiosks so customers can resume using its Tap to Pay feature to pass through fare gates .

Spotify security vulnerability exposed personal data to business partners

An unspecified number of Spotify users have had their passwords reset after their personal data was inadvertently exposed to business partners of the music streaming service. Spotify said it had “contained and remediated” the data breach after discovering a security vulnerability in its system that revealed users’ account registration information to the third parties. Exposed data may have included email addresses, display names, passwords, gender, and date of birth, said the music streaming giant.

ATTACK TYPE

Data exposed

CAUSE OF ISSUE

Law of maintaince

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3ht4BrY

Cloudflare WAF Bypass Via New Padding Technique

ATTACK TYPE

WAF bypass

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation

REFFERENCES

https://bit.ly/3hDClD6

Researchers have discovered vulnerability leading to Cloudflare WAF bypass via padding. Exploiting this vulnerability could threaten the security of web applications using Cloudflare WAF. This eventually allowed an adversary to malicious payloads to bypass WAF and exploit other app vulnerabilities. Under the default configuration, Cloudflare WAF allowed HTTP malicious requests and file uploads with padding. Cloudflare Product Manager, Michael Tremante, advised applying rule 100048 that prevents padding attacks.

TELECOMMUNICATION

ATTACK TYPE

RCE

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation

REFFERENCES

https://bit.ly/3hvG1zM

‘Amnesia:33’ TCP/IP Flaws Affect Millions of IoT Devices

Earlier this month the CISA had warned a set of serious vulnerabilities affecting TCP/IP stacks.33 vulnerabilities were found in which 4 were critical. Most of the flaws stem from memory corruption and information leaks to remote code execution.The flaws are found in four TCP/IP stacks (including uIP, picoTCP, FNET and Nut/Net), which are a set of communication protocols used by internet-connected devices.Still now no official patch is given but researchers have given solutions which could block this attack.

HOT FIX YOU SHOULD NOTICE..

5M WordPress Sites Running ‘Contact Form 7’ Plugin Open to Attack

A patch for the common WordPress plugin named Make contact with Kind 7 was introduced and fixes a critical bug that permits an unauthenticated adversary to takeover a internet site managing the plugin or maybe hijack the total server hosting the web site. The patch arrives in the sort of a 5.3.2 variation update to the Make contact with Variety 7 plugin. The critical vulnerability (CVE-2020-35489) is classified as an unrestricted file upload bug in Contact Form 7 will allow an unauthenticated visitor to gain unauthorized access.

ATTACK TYPE

Unauthorised access

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation

REFFERENCES

https://bit.ly/3rD8Gyk

Zero-Click Wormable RCE Vulnerability in Cisco Jabber

Researchers have found that the previous patched version for cross site scripting is still open. Using this an attacker could exploit this vulnerability by sending specially crafted XMPP messages to the affected software. A successful exploit could allow the attacker to cause the application to execute arbitrary programs on the targeted system with the privileges of the user account that is running the Cisco Jabber client software, possibly resulting in arbitrary code execution

ATTACK TYPE

RCE

CAUSE OF ISSUE

Lack of maintainces

TYPE OF LOSS

Reputation

REFFERENCES

https://bit.ly/37W6S1S

QNAP High-Severity Flaws Plague NAS Systems

NAS devices are systems that consist of one or more hard drives that are constantly connected to the internet – acting as a backup “hub” or storage unit that stores all important files and media such as photos, videos and music. Overall, QNAP on Monday issued patches for cross-site scripting (XSS) flaws tied to six CVEs. Two of these XSS flaws (CVE-2020-2495 and CVE-2020-2496) could allow remote attackers to inject malicious code into File Station.

ATTACK TYPE

RCE

CAUSE OF ISSUE

XSS flaw

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/2WS7JUR

Firefox Patches Critical Mystery Bug, Also Impacting Google Chrome

A Mozilla Foundation update to the Firefox web browser, critical vulnerability and a handful of high-severity bugs. The update, released as Firefox version 84, is also billed by Mozilla as boosting the browser's performance and adding native support for macOS hardware running on its own Apple processors. In total, six high-severity flaws were fixed, in addition to the critical bug, tracked as CVE-2020-16042. The specific critical bug in Firefox was also highlighted earlier this month in Google's Chrome browser security update, where it was rated as a high-severity flaw.

ATTACK TYPE

Hot fix

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation

REFFERENCES

https://bit.ly/3mWTdWk

Google Discloses Poorly-Patched, Now Unpatched, Windows 0-Day Bug

ATTACK TYPE

Zero day

CAUSE OF ISSUE

Lack of security

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/3rGduCX

Google's Project Zero team has made public details of an improperly patched zero-day security vulnerability in Windows print spooler API that could be leveraged by a bad actor to execute arbitrary code. Details of the unpatched flaw were revealed publicly after Microsoft failed to rectify it within 90 days of responsible disclosure on September 24. Originally tracked as CVE-2020-0986, the flaw concerns an elevation of privilege exploit in the GDI Print / Print Spooler API ("splwow64.exe") that was reported to Microsoft by an anonymous user working with Trend Micro's Zero Day Initiative (ZDI) back in late December 2019.

Trend Micro inter scan web security appliance security patch

Trend micro is a web gateway that helps to protect their system against online which found major vulnerabilities on 17 December 2020 and released a major patch update of their product which could have caused major cyber attacks.The vulnerabilities was found by Wolfgang Ettlinger, a researcher at Austria-based cybersecurity consultancy SEC Consult he found six major vulnerabilities in the product which lists CSRF protection bypass, XSS, authorization and authentication bypass, command execution, and command injection issues.

ATTACK TYPE

Hot fix

CAUSE OF ISSUE

Security flaw

TYPE OF LOSS

Reputation/Data

REFFERENCES

https://bit.ly/2XbA34N

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.

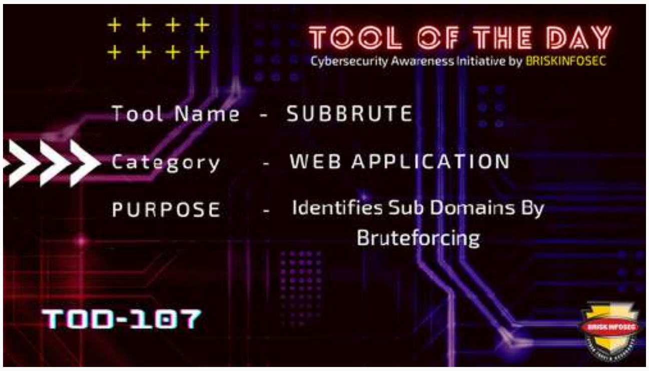
We assure that we will help you to keep your data safe and also give you clear information on your company's current status and what are the steps needed to be taken to stay away from any kind of cyber attack.

BRISK INFOSEC

CYBER TRUST & ASSURANCE

TOOLS OF THE MONTH

Subbrute Tool to Identifies sub domains by bruteforcing



TOOL OF THE DAY
Cybersecurity Awareness Initiative by BRISKINFOSEC

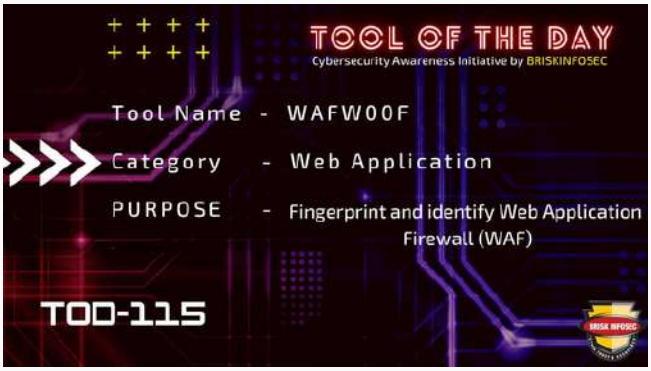
Tool Name - SUBBRUTE
Category - WEB APPLICATION
PURPOSE - Identifies Sub Domains By Bruteforcing

TOD-107

SubBrute is an open source subdomain enumeration tool. It is community maintained and aims to be the fastest and most accurate domain finding tool. It makes use of open DNS resolvers to bypass rate-limiting restrictions.

WafW00f Tool to Fingerprint and identify Web Application Firewall

WAFW00F is a Python tool to help you fingerprint and identify Web Application Firewall (WAF) products. It is an active reconnaissance tool as it actually connects to the web server, but it starts out with a normal HTTP response and escalates as necessary



TOOL OF THE DAY
Cybersecurity Awareness Initiative by BRISKINFOSEC

Tool Name - WAFW00F
Category - Web Application
PURPOSE - Fingerprint and identify Web Application Firewall (WAF)

TOD-115

Wapiti Tool for web application security auditor

TOOL OF THE DAY
Cybersecurity Awareness Initiative by BRISKINFOSEC

Tool Name - WAPITI
Category - Web Application
PURPOSE - Web Application Security Auditor.

TOD-122

Wapiti is an open source tool that scans web applications for multiple vulnerabilities including data base injections, file disclosures, cross site scripting, command execution attacks, XXE injection, and CRLF injection.

Turbolist3r Tool Web Application Subdomain Discover

TOOL OF THE DAY

Cybersecurity Awareness Initiative by BRISKINFOSEC

Tool Name - Turbolist3r

Category - Web Application

PURPOSE - Discover Subdomain.

TOD-123

Turbolist3r is a fork of the sublist3r subdomain discovery tool. In addition to the original OSINT capabilties of sublist3r, turbolist3r automates some analysis of the results, with a focus on subdomain takeover. Turbolist3r queries public DNS servers for each discovered subdomain.

FinalRecon is a fast and simple python script for web reconnaissance

Final Recon is a fast and simple python script for web reconnaissance. It follows a modular structure so in future new modules can be added with ease. The tool is available in Black Arch Linux and SecBSD.

TOOL OF THE DAY

Cybersecurity Awareness Initiative by BRISKINFOSEC

Tool Name - Final Recon

Category - Web Application

PURPOSE - Reconnaissance for Web Application

TOD-125

Fuzz Faster U Fool Tool to Fuzzing Get and Post data

TOOL OF THE DAY

Cybersecurity Awareness Initiative by BRISKINFOSEC

Tool Name - Fuzz Faster U Fool

Category - Web Application

PURPOSE - Fuzzing Get and Post data.

TOD-117

Fuzz Faster U Fool is a great tool used for fuzzing. It has become really popular lately with bug bounty hunters. Ffuf is used for fuzzing Get and Post data but can also be used for finding hidden files, directories or subdomains.

CYBER MONDAY

HAPPY
CYBER
MONDAY
"NEVER STILL BELIEVE THAT YOUR BROWSER
HAS THE BEST SECURITY QUALITY
EVEN THE EARTH'S BEST BROWSER IS LATELY
AFFECTED WITH CVE 2019-5786"
Arulselvar Thomas
Founder-Briskinfosec
BRISK INFOSEC
www.briskinfosec.com

Browser Security

Chrome may be the widely used browser but that doesn't mean it's the most secured one. It's good to know that an object lifetime issue in Google Chrome's Blink prior to 72.0.3626.121 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.

Docker Platform

There are many obsolete techniques to hack your server and attention to mitigate them are given. But, using docker to compromise the server is the becoming the new trend and awareness to be resilient against that needs significant attention.

HAPPY
CYBER
MONDAY
"NEVER THINK YOU'RE SECURED WITH YOUR
INFRA-DEVICES OBTAINED FROM OEM'S,
YOU STILL DEMAND HOST-LEVEL SECURITY
ASSESSMENTS, FOR AVERTING MAYHEM'S."
Host-Level Assessment :
Device/Server Hardening, Secure Config Review and Firewall Gap Analysis
Arulselvar Thomas
Founder-Briskinfosec
BRISK INFOSEC
www.briskinfosec.com

Host Level Security

Never ever get complacent with the fact that just because your digital asset is purchased from an elite manufacturer, it is absolutely secured. The truth is, from whichever OEM it may be, that asset needs to be assessed and hence, host level assessment is mandatory!

BLOG OF THE MONTH

Detection and Exploitation of XML External Entity Attack XXE

XML External Entity Attack happens when an application allows an input parameter to be XML or incorporated into XML, which is passed to an XML parser running with sufficient privileges to include external or system files, which results in vulnerabilities like file inclusion, Server side request forgery and Remote Code Execution.

Layer Wise Analysis of Security in IOT

We come across the word “smart” in our daily life which directly relates to many aspects in technology. In this context, we would be covering IoT devices and its vulnerabilities. IoTs are more vulnerable as it deals more with the sensor and wireless connectivity mediums.

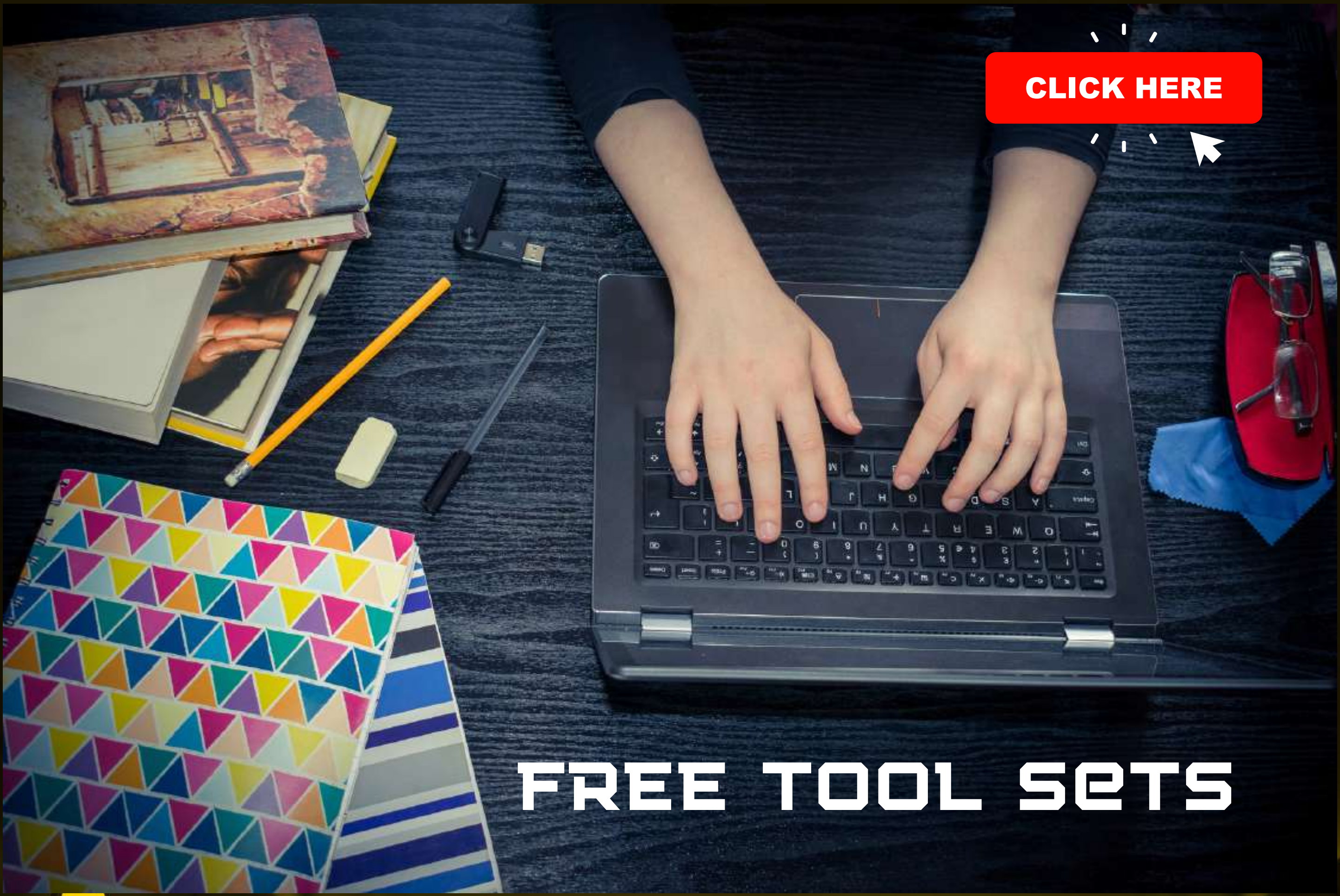
Host Header Inection Vulnerability

A Web server handles the Host header value to dispatch the request to the destination domain. An attacker can manipulate this Host header with some fake Domains to steal sensitive information. Here we are going to deal with Host Header Injection, its risk, forms, and impacts and how to mitigate it.

CLICK HERE

WAKE UP CXO

AN INITIATIVE BY BRISKINFOSEC



www.briskinfosec.com