THREATSPLOIT ADVERSARY REPORT

APRIL 2021

BRISK INFOSEC

CYBER TRUST & ASSURANCE

EDITION 32

www.briskinfosec.com

INTRODUCTION

Welcome to latest edition Threatsploit by Briskinfosec Technology. This edition of the Threatsploit accounts for significant cyber-security incidents across the globe that occurred in the previous month. The most significant attacks of the month were Ransomware, RCE, Data Breaches and DDOS. And the industries which were most affected by the mentioned attacks included the education sector, retail industry, government sectors and banking sector,

Besides these major attacks, many attacks have caught the attention of the cyber crowd. These attacks have been mentioned in the report.

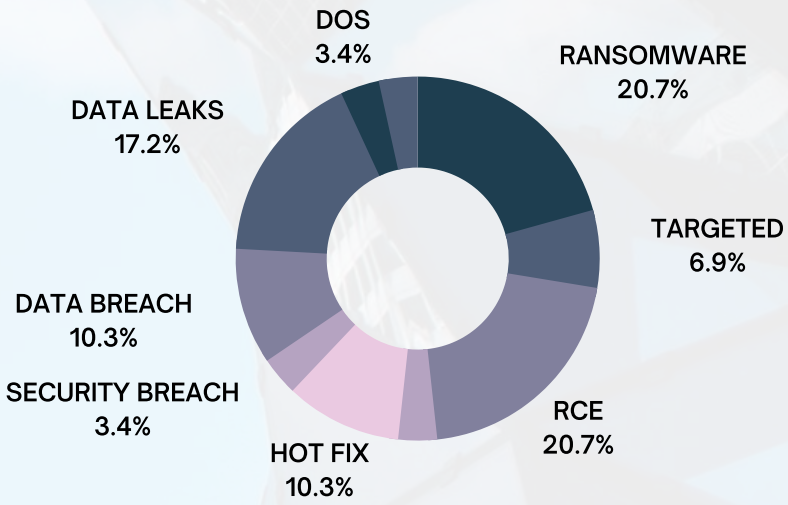
"Majority number of employees/stakeholders have failed to equip themselves or the organization about the concept of cyber-security and its relevance and impact on the modern industry"

Ever since the pandemic, the probability of being exposed to a cyber-threat is way higher than any time. Briskinfosec Technology takes an initiative to address the audience to create awareness about cyber-security with this report. The report's main objective is to educate people about the different types of attacks that occur across the globe.

The following sections of the report contrast various security incidents that have occurred in the previous month.

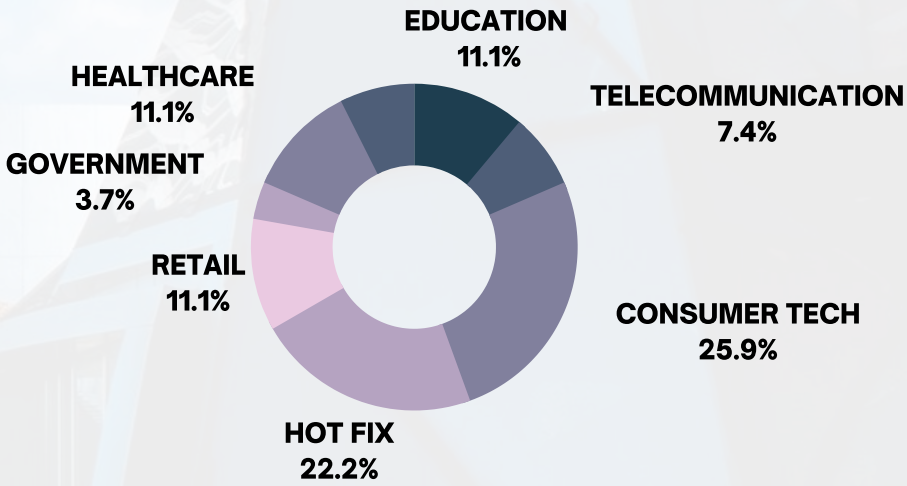
TYPES OF ATTACK VECTORS

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 (26%). To prevent any attack, organizations need the best of cybersecurity partners. Needless to say, Cybersecurity as a function is assuming very high importance like the Operations, Sales, Finance or Human Resources.

LATEST THREAT ENTRIES

CONSUMER TECH

- PHP's Git Server Hacked to Insert Secret Backdoor to Its Source code
- Another Critical RCE Flaw Discovered in SolarWinds Orion Platform
- Popular Netop Remote Learning Software Found Vulnerable to Hacking
- Critical RCE Vulnerability Found in Apache OFBiz ERP Software
- New Zoom Screen-Sharing Bug Lets Other Users Access Restricted Apps
- Flaws in Two Popular WordPress Plugins Affect Over 7 Million Websites
- Microsoft Account Hijack Vulnerability

RETAIL

- ‘Largest KYC leak ever’: Data of 10 crore Indians exposed at MobiKwik
- Extortion Gang Breaches Cybersecurity Firm Qualys Using Accellion Exploit
- Forex Broker Leaks Billions of Customer Records Online

BANKING AND FINANCE

- Insurance Giant CNA hit by new Phoenix CryptoLocker Ransomware
- Payroll Giant PrismHR outage likely caused by Ransomware Attack

EDUCATION

- The University of Northampton Hit By Cyber Attack
- London’s Biggest School Trust Hit By Ransomware
- Cyberattack Shuts Down Online Learning At 15 UK Schools

GOVERNMENT

- Ransomware Gang Leaks Data from US Military Contractor the PDI Group

TELECOMMUNICATION

- New 5G Flaw Exposes Priority Networks to Location Tracking and Other Attacks
- Call Center Provider Experiences Major Data Leak

LATEST THREAT ENTRIES

TRANSPORTATION

- Air Charter Firm Solairus Aviation Suffers Data Breach
- Data of 580,000 SIA Customers Leaked In Security Breach

HEALTHCARE

- Ransomware Attack on Oloron-Sainte-Marie hospital
- Home Health Firm Affects By Ransomware Attack
- New York Charity Leaves Sensitive Patients' Data Unsecured

HOT FIX

- Apple Issues Urgent Patch Update for Another Zero-Day Under Attack
- OpenSSL Releases Patches for 2 High-Severity Security Vulnerabilities
- Critical RCE Flaw Reported in MyBB Forum Software
- Google Chrome 0-Day Bug Found Actively Exploited In-the-Wild
- Microsoft's March Patch Tuesday: Critical Remote Code Execution Flaws, IE Zero-Day Fixed
- Critical Cisco Jabber Bug Could Let Attackers Hack Remote Systems

BRISKINFOSEC TOOL OF THE DAY

- Perform risk analysis with RiskInDroid
- Tulpar Web Application Vulnerability Scanner
- SKIPFISH Web application recon tool
- Clickjacking Tester
- SQLiv – Massive SQL Injection Scanner
- Inspect your application with ClassShark

CYBER MONDAY

- Browser Security
- Docker Platform
- Host Level Security

BLOGS OF THE MONTH

- Secure your github repository
- Important things to secure your healthcare application
- Chat-Bot Security

PHP's Git Server Hacked to Insert Secret Backdoor to Its Source code

Unknown actors hacked the official Git server of the PHP programming language and pushed unauthorized updates to insert a secret backdoor into its source code. In an attempt to compromise the PHP codebase, two malicious commits were pushed to the official PHP Git repository yesterday. The incident is alarming considering PHP remains the server-side programming language to power over 79% of the websites on the Internet. As a precaution following this incident, PHP maintainers have decided to migrate the official PHP source code repository to GitHub. "While the investigation is still underway, we have decided that maintaining our own git infrastructure is an unnecessary security risk and that we will discontinue the git.php.net server." said the company.

ATTACK TYPE
Unauthorized access

CAUSE OF ISSUE
Security flaws

TYPE OF LOSS
Reputation/Data

REFFERENCES
https://zd.net/3dxMijV

Another Critical RCE Flaw Discovered in SolarWinds Orion Platform

ATTACK TYPE
RCE

CAUSE OF ISSUE
Security flaw

TYPE OF LOSS
Reputation

REFFERENCES
https://bit.ly/3sDJCap

SolarWinds has released critical security updates to address four vulnerabilities impacting the company's Orion IT monitoring platform, two of them allowing attackers to execute arbitrary code remotely. The Orion Platform is an IT administration solution that enables enterprise organizations to manage, optimize, and monitor their on-premises, hybrid, or software as a service (SaaS) IT infrastructures. Chief among them is a JSON deserialization flaw that allows an authenticated user to execute arbitrary code. It has been rated critical in severity. Orion users are recommended to update to the latest release, "Orion Platform 2020.2.5," to mitigate the risk associated with the security issues.

Popular Netop Remote Learning Software Found Vulnerable to Hacking

Cybersecurity researchers disclosed multiple critical vulnerabilities in remote student monitoring software Netop Vision Pro that a malicious attacker could abuse to execute arbitrary code and take over Windows computers. These findings allow for elevation of privileges and ultimately remote code execution which could be used by a malicious attacker within the same network to gain full control over students computers said in an analysis. The vulnerabilities, tracked as CVE-2021-27192, CVE-2021-27193, CVE-2021-27194, and CVE-2021-27195, were reported to Netop and company fixed the issues in an update (version 9.7.2).

ATTACK TYPE
RCE

CAUSE OF ISSUE
Security flaw

TYPE OF LOSS
Reputation/Data

REFFERENCES
https://bit.ly/3fsNNSQ

Critical RCE Vulnerability Found in Apache OFBiz ERP Software

ATTACK TYPE
RCE

CAUSE OF ISSUE
Security flaw

TYPE OF LOSS
Reputation/Data

REFFERENCES
https://bit.ly/3cCw179

The Apache Software Foundation addressed a high severity vulnerability in Apache OFBiz that could have allowed an unauthenticated adversary to remotely seize control of the open-source enterprise resource planning (ERP) system. OFBiz is a Java-based web framework for automating enterprise processes and offers a wide range of functionality, including accounting, customer relationship management, manufacturing operations management, order management, supply chain fulfillment, and warehouse management system, among others. Tracked as CVE-2021-26295, the flaw affects all versions of the software prior to 17.12.06.

CONSUMER TECH

New Zoom Screen-Sharing Bug Lets Other Users Access Restricted Apps

A newly discovered glitch in Zoom's screen sharing feature can accidentally leak sensitive information to other attendees in a call, according to the latest findings. Tracked as CVE-2021-28133, the unpatched security vulnerability makes it possible to reveal contents of applications that are not shared, but only briefly, thereby making it harder to exploit it in the wild. When Zoom users share a particular application window through the screen Sharing'feature, other meeting participants can easily see the content of other application windows that are not explicitly shared said by researchers.

ATTACK TYPE
Information disclosure
CAUSE OF ISSUE
Unpatched vulnerability
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/39uoaNO

Flaws in Two Popular WordPress Plugins Affect Over 7 Million Websites

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

Researchers have disclosed vulnerabilities in multiple WordPress plugins that, if successfully exploited, could allow an attacker to run arbitrary code and take over a website in certain scenarios. The flaws were uncovered in Elementor, a website builder plugin used on more than seven million sites, and WP Super Cache, a tool used to serve cached pages of a WordPress site. According to Wordfence, which discovered the security weaknesses in Elementor, the bug concerns a set of stored cross-site scripting (XSS) vulnerabilities (CVSS score: 6.4), which occurs when a malicious script is injected directly into a vulnerable web application.

Microsoft account hijack vulnerability

The researcher found a security flaw that could "have allowed anyone to take over any Microsoft account without consent [or] permission."In order to reset a password for a Microsoft account, the company requires an email address or phone number to be submitted through a "Forgotten Password" page. A seven-digit security code is then sent as a method of verification and needs to be provided in order to create a new password. Utilizing a brute-force attack to obtain the seven-digit code would lead to password resets without the account owner's permission. However, to stop these attacks in their tracks, rate limits, encryption, and checks are imposed.

ATTACK TYPE
Account takeover
CAUSE OF ISSUE
Authentication flaw
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/3uncMLN

'Largest KYC leak ever': Data of 10 crore Indians exposed at MobiKwik

ATTACK TYPE
Data leak
CAUSE OF ISSUE
Lack of security
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/3cF4WHI

Independent cybersecurity researchers have claimed that a database containing KYC details of nearly 3.5 million users of Indian payment app MobiKwik, in addition to personal and payments data of about 99,224,559 users, is up for sale on the Dark Web. The Gurugram-based fintech company has continued to deny its role in the leak, calling the researchers that made the breach public "media-crazed" and accusing them of presenting "concocted files" as evidence. "We thoroughly investigated and did not find any security lapses. Our user and company data is completely safe and secure," said by Mobikwik.

RETAIL

RETAIL

Extortion Gang Breaches Cybersecurity Firm Qualys Using Accellion Exploit

Enterprise cloud security firm Qualys has become the latest victim to join a long list of entities to have suffered a data breach after zero-day vulnerabilities in its Accellion File Transfer Appliance (FTA) server were exploited to steal sensitive business documents. As proof of access to the data, the cybercriminals behind the recent hacks targeting Accellion FTA servers have shared screenshots of files belonging to the company's customers on a publicly accessible data leak website operated by the CLOP ransomware gang. The investigation confirmed that the unauthorized access was limited to the FTA server and did not impact any services provided or access to customer data hosted by the Qualys Cloud Platform.

ATTACK TYPE
Data breach
CAUSE OF ISSUE
Zero-day
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/3wajqXr

Forex Broker Leaks Billions of Customer Records Online

ATTACK TYPE
Data leak
CAUSE OF ISSUE
Lack of security
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/38eyqt1

Over 20TB of sensitive customer data has been accidentally leaked online by a popular online trading broker after it misconfigured a cloud database.
According to the report, the database contained over 16 billion records, exposing millions of customers' personally identifiable information (PII).
These included: full names, email and billing addresses, phone numbers, IP addresses, passport numbers, social media IDs, and ID verification scans including national ID cards, driver's licenses, bank account statements, utility bills and credit cards.

BANKING AND FINANCE

Insurance giant CNA hit by new Phoenix CryptoLocker ransomware

Insurance giant CNA has suffered a ransomware attack using a new variant called Phoenix CryptoLocker that is possibly linked to the Evil Corp hacking group. On March 2021, CNA determined that it sustained a sophisticated cybersecurity attack. The attack caused a network disruption and impacted certain CNA systems, including corporate email, CNA disclosed in a statement. The attack on CNA could have tremendous impact on other companies, especially those that have cyber insurance policies through the company. Conducting attacks on companies with cyber insurance policies are often lucrative for ransomware gangs as the insurance companies may be more likely to pay the ransom.

ATTACK TYPE
Ransomware
CAUSE OF ISSUE
Poor security pratice
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/2Pe1URt

Payroll giant PrismHR outage likely caused by ransomware attack

ATTACK TYPE
Ransomware
CAUSE OF ISSUE
Unauthorised access
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/31BQ8CJ

Leading payroll company PrismHR is suffering a massive outage after suffering a cyberattack this weekend that looks like a ransomware attack from conversations with customers. PrismHR is an online payroll, benefits, and human resources platform used by Professional employer organizations (PEO). PEOs use this platform to provide payroll, HR, and benefits services to their clients, commonly small and medium-sized businesses. PrismHR is a massive business services company servicing over 80,000 organizations with 2 million employees and total annual payrolls of over $80 billion.

University of Northampton hit by cyber attack

The University of Northampton has been hit by a cyberattack that resulted in the disruption of its IT and telephone systems and servers. The university said that the attack was detected on March 17, that it has notified the ICO and, as a precaution, is liaising with the police to investigate the attack further. It has rolled out a number of "temporary solutions" to support students and staff. University working to resolve this issue as quickly as possible, including legal counsel and IT forensics investigators. The University of Northampton stated that we take the safety and security of our information as well as the continuity of our systems and services extremely seriously - and will continue to take every action to protect the organization against cyber attacks.

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

EDUCATION

London's biggest school trust hit by ransomware

ATTACK TYPE
Ransomware
CAUSE OF ISSUE
Poor security pratice
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/3wh1pl2

London's biggest multi-academy school trust, the Harris Federation, was hit by ransomware, bringing down IT systems, email servers, and phone lines at primary and secondary academies across London. The attack performed when school staff returned to work and couldn't access internal applications and documents. The school trust's IT staff responded by taking down IT systems, including disabling devices it provided to pupils, in order to prevent the ransomware from spreading and encrypting their data as well.The incident, which took place on March 2021, represents the largest ransomware attack against a UK educational organization known to date.

Cyberattack shuts down online learning at 15 UK schools

15 schools in the United Kingdom have been unable to provide online learning due to a cyberattack. According to Nova Education Trust, a threat actor was able to access the trust's central network infrastructure and while an investigation took place, all existing phone, email, and website communication had to be pulled. The incident has been reported to the Department for Education and the Information Commissioner's Office (ICO), and the trust is currently working with the National Cyber Security Centre (NCSC) and additional security professionals to resolve the matter," Nova Education Trust said. All trust employees have been advised to take the necessary precautions.

ATTACK TYPE
Data exposed
CAUSE OF ISSUE
Security misconfiguration
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/39t14Hc

Ransomware gang leaks data from US military contractor the PDI Group

ATTACK TYPE
Data leak
CAUSE OF ISSUE
Ransomware
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://zd.net/3kuF96U

A major supplier of military equipment to the US Air Force and militaries across the globe appears to have fallen victim to a ransomware attack. The victim is the PDI Group, an Ohio-based company that manufactures a wide range of ground support equipment for military needs, such as dollies, trollies, and platforms for transporting weapons, engines, and airplane parts during servicing operations. The criminal group behind the Babuk Locker ransomware created a page on their "leak site" under the company's name threatening to leak more than 700 GB of data they claim to have stolen from PDI's internal network unless the company gave in to its ransom demands.

GOVERNMENT

TELECOMMUNICATION

New 5G Flaw Exposes Priority Networks to Location Tracking and Other Attacks

ATTACK TYPE
DOS
CAUSE OF ISSUE
Lack of security
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/3ftH3Eh

New research into 5G architecture has uncovered a security flaw in its network slicing and virtualized network functions that could be exploited to allow data access and denial of service attacks between different network slices on a mobile operator's 5G network. This weakness tracked as CVD-2021-0047. The study suggests enhancing the Service Communication Proxy (SCP) to validate the correctness of message formats, match the information between layers and protocols, and provide load-related functionality to prevent DoS attacks

Call Center Provider Experiences Major Data Leak

ATTACK TYPE
Data leak
CAUSE OF ISSUE
Poor security pratice
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/3ftQ4NN

IT security researcher discovered an insecure database that had no password protection and contained a large number of phone call records as well as VOIP (Voice Over Internet Protocol) related data. The dataset was exposed for almost 24 hours and the database kept growing in real-time with thousands of calls per hour being added to the records. From the time when it was exposed till when it was secured again, the database logged 1.48 million robocalls altogether and the majority of the calls were outgoing but some call-backs were also logged.In total, according to researchers, 1,481,280 records were accessible and they continued to increase until the access was restricted. Exposed records contained internal information, SIP, Caller ID, call pathways IPs, and Ports.

TRANSPORTATION

Air Charter Firm Solairus Aviation Suffers Data Breach

ATTACK TYPE
Data breach
CAUSE OF ISSUE
Poor security pratice
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/31AtU4k

Private aviation services provider Solairus Aviation announced that some employee and customer data was compromised in a security incident at third-party vendor Avianis. Solairus data stored in that environment possibly includes employee and client names, along with information such as dates of birth, Social Security numbers, driver's license numbers, passport numbers, and financial account numbers, the company says. An investigation into the incident has revealed that some of Solairus' data that was hosted on that environment were indeed accessed by an unknown party.

Data of 580,000 SIA customers leaked in security breach

ATTACK TYPE
Security breach
CAUSE OF ISSUE
Poor security pratice
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://zd.net/3sGCv0B

Singapore Airlines (SIA) customers have been affected by a data leak at an external firm. SIA said in a statement that the breach did not involve the members' passwords or credit card information. There was also no leak of itineraries, reservations, ticketing information, passport numbers, and e-mail addresses. But, it is not possible for someone to access any confidential customer data or their miles with only the leaked information. The airline said it will also review current procedures and take all necessary steps to improve data security.

Ransomware Attack on Oloron-Sainte-Marie hospital

A ransomware attack paralyzed the systems at the Oloron-Sainte-Marie hospital in southwest France. The incident took place on Monday, the ransomware gang is demanding the payment of a ransom of $50,000 worth of Bitcoin. The infection was first discovered by an engineer in charge of all the installations. In response to the attack, the IT staff took offline part of the hospital network to prevent the spread of the malware. Attacks against hospitals and health care organizations are very dangerous, especially during the ongoing pandemic, At the time of the attack, the French hospital was taking part in vaccination efforts against Covid-19.

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

Home Health Firm affects by ransomware attack

ATTACK TYPE
Ransomware
CAUSE OF ISSUE
Lack of security
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/2Pf2MFu

A "Home Healthcare Company" says a data breach affecting more than 753,000 patients, employees, and former workers stems from a ransomware attack on its private cloud hosted by managed service providers. The company reported a similar incident 15 months ago. Patient information exposed includes health plan benefit numbers, medical record numbers, names, addresses, telephone numbers, dates of birth, Social Security numbers, and financial information, including check copies, credit card numbers, and bank account information, and employ details too.

New York charity leaves sensitive patients' data unsecured

An unsecured database that appears to belong to one of the largest charities in New York. The unsecured database contained more than 2,000 CSV and TXT files, each with hundreds or thousands of entries related to patients' medical records, children's legal guardians, caseworkers, doctors, and other child welfare specialists. Some documents even contained social security numbers. The files were stored on an unsecured Microsoft Azure Blob that was publicly accessible, meaning that anyone with the URL was able to download the data. Many of the email and physical addresses within the database point to the New York Foundling organization, which provides many services related to child protection, foster care and adoption, disabilities services, and more.

ATTACK TYPE
Ransomware
CAUSE OF ISSUE
Poor security pratice
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/39x7jJ4

HOT FIX YOU SHOULD NOTICE..

Apple Issues Urgent Patch Update for Another Zero-Day Under Attack

Apple has issued yet another security update for iPhone, iPad, and Apple Watch to fix a critical zero-day weakness that it says is being actively exploited in the wild. Tracked as CVE-2021-1879, the vulnerability relates to a WebKit flaw that could enable adversaries to process maliciously crafted web content that may result in universal cross-site scripting attacks. Update are available for ios 12.5.2, iOS 14.4.2, iPadOS 14.4.2, watchOS 7.3.3. In the meanwhile, users of Apple devices are advised to install the updates as soon as possible to mitigate the risk associated with the flaw.

ATTACK TYPE
Hot fix
CAUSE OF ISSUE
Security flaw
TYPE OF LOSS
Reputation
REFFERENCES
https://bit.ly/2Pq1Kci

OpenSSL Releases Patches for 2 High-Severity Security Vulnerabilities

ATTACK TYPE
Hot fix
CAUSE OF ISSUE
Security flaw
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://bit.ly/3m7sojm

OpenSSL is a software library consisting of cryptographic functions that implement the Transport Layer Security protocol with the goal of securing communications sent over a computer network. The maintainers of OpenSSL have released a fix for two high-severity security flaws in its software that could be exploited to carry out denial-of-service (DoS) attacks and bypass certificate verification. Tracked as CVE-2021-3449 and CVE-2021-3450, both the vulnerabilities have been resolved in an update (version OpenSSL 1.1.1k) released on Thursday. While CVE-2021-3449 affects all OpenSSL 1.1.1 versions, CVE-2021-3450 impacts OpenSSL versions 1.1.1h and newer.

Critical Cisco Jabber Bug Could Let Attackers Hack Remote Systems

Cisco released software updates to address multiple vulnerabilities affecting its Jabber messaging clients across Windows, macOS, Android, and iOS. Successful exploitation of the flaws could permit an "attacker to execute arbitrary programs on the underlying operating system with elevated privileges, access sensitive information, intercept protected network traffic, or cause a denial of service (DoS) condition," the networking major said in an advisory. The issues concern a total of five security vulnerabilities, three of which (CVE-2021-1411, CVE-2021-1417, and CVE-2021-1418) were reported to the company and with two others (CVE-2021-1469 and CVE-2021-1471).

ATTACK TYPE
Hot Fix
CAUSE OF ISSUE
Security flaw
TYPE OF LOSS
Reputation
REFFERENCES
https://bit.ly/3m60dBo

HOT FIX YOU SHOULD NOTICE..

Critical RCE Flaw Reported in MyBB Forum Software

A pair of critical vulnerabilities in a popular bulletin board software called MyBB could have been chained together to achieve remote code execution (RCE) without the need for prior access to a privileged account. According to the researchers, the first issue — a nested auto URL persistent XSS vulnerability (CVE-2021-27889) — stems from how MyBB parses messages containing URLs during the rendering process, thus enabling any unprivileged forum user to embed stored XSS payloads into threads, posts, and even private messages. The second vulnerability concerns an SQL injection (CVE-2021-27890) in a forum's theme manager that could result in an authenticated RCE. MyBB users are advised to upgrade to the latest version to mitigate the risk associated with the flaws.

ATTACK TYPE
RCE
CAUSE OF ISSUE
Security flaw
TYPE OF LOSS
Reputation
REFFERENCES
https://bit.ly/3wc5vjs

Google Chrome 0-Day Bug Found Actively Exploited In-the-Wild

ATTACK TYPE
Zero day
CAUSE OF ISSUE
Security flaw
TYPE OF LOSS
Reputation
REFFERENCES
https://zd.net/2NRvDPI

Google has addressed yet another actively exploited zero-day in Chrome browser, marking the second such fix released by the company within a month. The browser maker released 89.0.4389.90 for Windows, Mac, and Linux, which is expected to be rolling out over the coming days/weeks to all users. While the update contains a total of five security fixes, the most important flaw rectified by Google concerns a use after free vulnerability in its Blink rendering engine. The bug is tracked as CVE-2021-21193. According to IBM, the vulnerability is rated 8.8 out of 10 on the CVSS scale, and could allow a remote attacker to execute arbitrary code on the target system. "By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service condition on the system," the report stated.

Microsoft's March Patch Tuesday: Critical remote code execution flaws, IE zero-day fixed

Microsoft plugged as many as 89 security flaws as part of its monthly Patch updates released, including fixes for an actively exploited zero-day in Internet Explorer that could permit an attacker to run arbitrary code on target machines. Of these flaws, 14 are listed as Critical, and 75 are listed as Important in severity, out of which two of the bugs are described as publicly known, while five others have been reported as under active attack at the time of release. Among those five security issues are a clutch of vulnerabilities known as ProxyLogon (CVE-2021-26855, 2021-26857, CVE-2021-26858, and CVE-2021-27065) that allows adversaries to break into Microsoft Exchange Servers in target environments and subsequently allow the installation of unauthorized web-based backdoors to facilitate long-term access. users are advised to upgrade to the latest version to mitigate the risk associated with the flaws.

ATTACK TYPE
RCE
CAUSE OF ISSUE
Security flaw
TYPE OF LOSS
Reputation/Data
REFFERENCES
https://zd.net/3bMRDTw

TOOLS OF THE MONTH

Perform risk analysis with RiskInDroid

RiskInDroid (Risk Index for Android) is a tool for quantitative risk analysis of Android applications written in Java (used to check the permissions of the apps) and Python (used to compute a risk value based on apps' permissions). The tool uses classification techniques through scikit-learn, a machine learning library for Python, in order to generate a numeric risk value between 0 and 100 for a given app.

Tulpar Web Application Vulnerability Scanner

Tulpar is an open-source penetration testing tool that can find web application vulnerabilities such as SQL injection, Cross-site Scripting (XSS), Command injection, Directory traversal, E-mail disclosure, Credit card disclosure, and File inclusion attacks.

SKIPFISH Web application recon tool

Skipfish is an active web application security reconnaissance tool. It prepares an interactive sitemap for the targeted site by carrying out a recursive crawl and dictionary-based probes. The resulting map is then annotated with the output from a number of active (but hopefully non-disruptive) security checks. The final report generated by the tool is meant to serve as a foundation for professional web application security assessments.

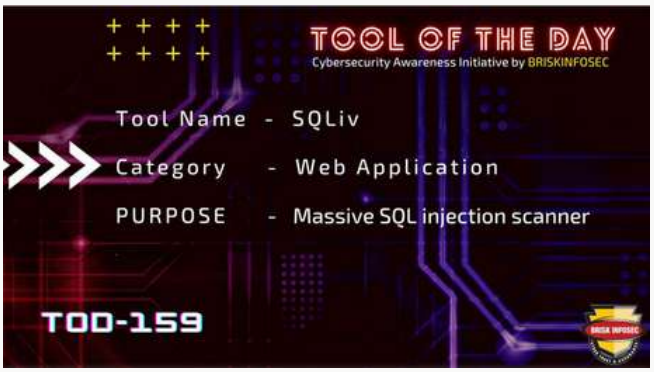
TOOLS OF THE MONTH

Clickjacking Tester

A python script designed to check if the website is vulnerable to clickjacking and creates a POC. Clickjacking is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element.

SQLiv – Massive SQL Injection Scanner

SQL injection is one of the most prominent vulnerabilities for web-based applications. In last article, we've used viSQL through which we scanned the whole server for SQL Injection vulnerabilities with the help of Crawling and Reverse IP domain check feature.



Inspect your application with ClassShark

ClassyShark is a standalone binary Inspection tool for Android developers/testers. It can reliably browse any Android executable and show important Info such as class interfaces and members, dex counts and dependencies. ClassyShark supports multiple formats including libraries (.dex, .aar, .so), executables (.apk, Jar, .class) and all Android binary XMLs: AndroidManlfest, resources, layouts etc.

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.

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

Secure your github repository

GitHub is a hosting platform that helps developers to collaborate In building software. It helps the developers to manage source code management. GitHub lets the project owner and others work on your project. As we all know, GitHub is open source and provides unlimited free private repositories. In this article, we are going to see how to avoid security loopholes and utilize GitHub In a secure way.

Important things to secure your healthcare application

The health care or medical trade is extraordinarily necessary that has totally different parts together with hospitals, doctors, nursing diagnostic laboratories, pharmacies, medical device makers, and other components of the health care system. Health care is very important to individuals round the world and as-well on the worldwide economies

Chat-Bot Security

Before the Chat-bots became ubiquitous, Consumers had to contact the customer care office for any enquiry regarding their product. This demands human presence all the time to address their needs anytime, unlike Chat-bot which is automated. This blog will cover the security of Chat-bot, in detail.

CONCLUSION

It is clear from the above attacks that any infrastructure/individual can be exploited with the simplest means. As mentioned, cyber-attacks have risen in magnitude in terms of the attack vector and data compromised. The report has been successful to provide an insight into the latest attacks that occurred across the globe. Due to certain limitations, the reports have not been able to cover all the attacks but have covered the significant attacks.

We would like to believe that these attacks occurred due to a lack of awareness. As for the objective, Briskinfosec Technology believes to complete the objective, which is to educate the audience about common cyber-attacks.

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

"Keep ourselves safe in both Physical and Virtual Realms.

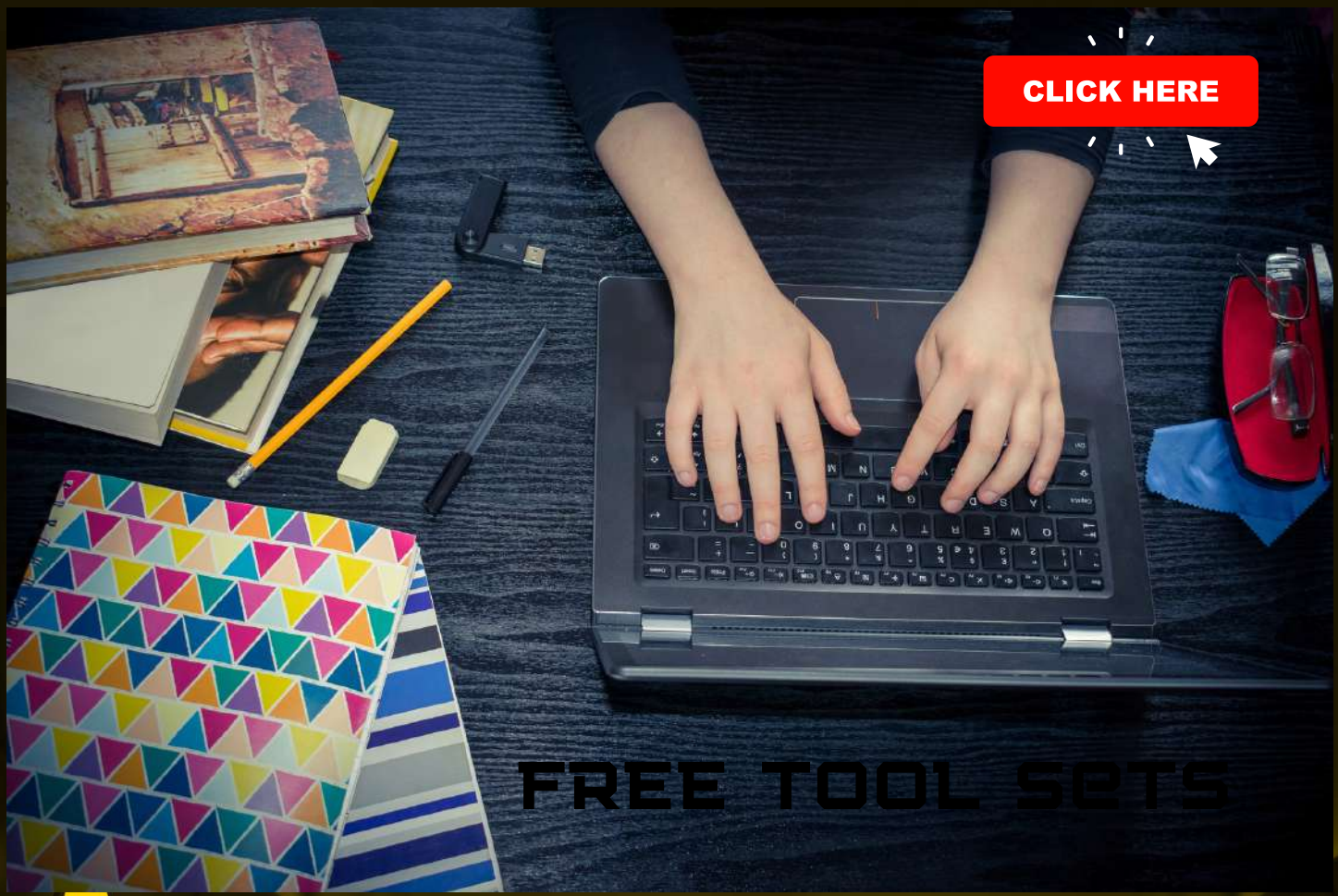
BRISK INFOSEC

CYBER TRUST & ASSURANCE

CLICK HERE

WAKE UP CXO

AN INITIATIVE BY BRISKINFOSEC



contact@briskinfosec.com
www.briskinfosec.com