EDITION 34

THREATSPLOIT ADVERSARY REPORT

JUNE 2021

BRISK INFOSEC
CYBER TRUST & ASSURANCE

www.briskinfosec.com

Introduction

Welcome to the Threatsploit Report of June 2021 covering some of the important cybersecurity events, incidents and exploits that occurred this month. This month, the cybersecurity sector witnessed a massive rise in ransomware and data breach attacks across geographies. Besides, many other attack types were seen spiking during these recent months.

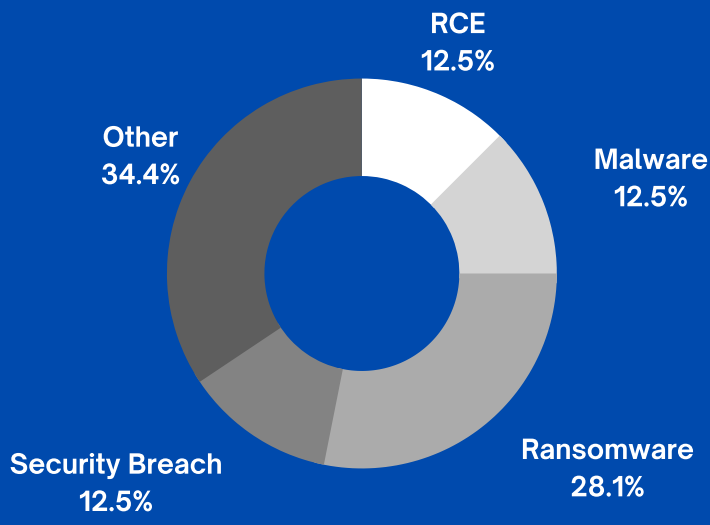
The primary reason is and has always been the same....

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

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

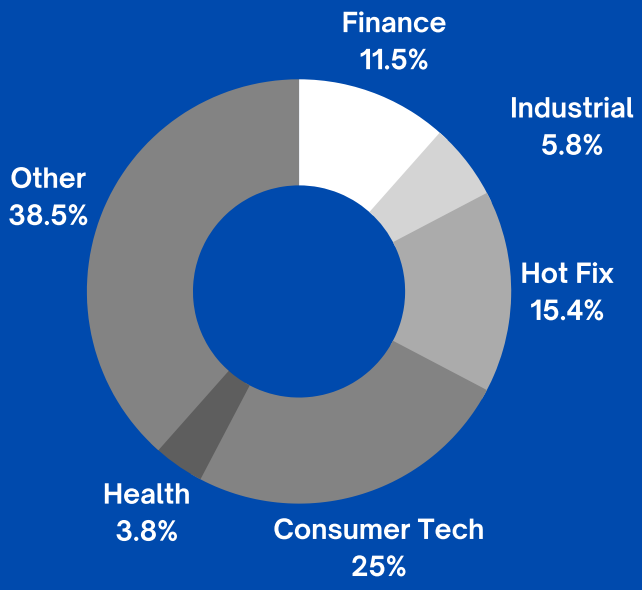
TYPES OF ATTACK VECTORS

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

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.



LATEST THREAT ENTRIES

CONSUMER TECH

1. Zero-Days in Remote Mouse App for SmartPhones
2. Moriya Rootkit attacks Windows Systems
3. PingBack Malware uses ICMP for Covert Traffic
4. Codecov hackers gained access to Monday.com source code
5. Toshiba's European Subsidiary Confirms Ransomware Attack; DarkSide's Involvement Suspected
6. Cross-browser tracking vulnerability tracks you via installed apps
7. Microsoft build tool abused to deliver password-stealing malware
8. APTs aim at Exchange servers
9. QNAP warns of eCh0raix ransomware attacks, Roon Server zero-day
10. Blind SQL Injection flaw in WP Statistics impacted 600K+ sites
11. Foxit Reader bug lets attackers run malicious code via PDFs
12. Cisco bugs allow creating admin accounts, executing commands as root
13. Qualcomm vulnerability impacts nearly 40% of all mobile phones

HEALTH

1. Ireland's Department of health hit by Conti Ransomware
2. Scripps Health Care hit by Ransomware

FINANCE

1. CNA Paid $40 Million in Ransom After March Cyber Attack
2. Insurer AXA hit by ransomware after dropping support for ransom payments
3. Trust Wallet, MetaMask crypto wallets targeted by new support scam
4. Student health insurance carrier Guard.me suffers a data breach
5. Bizarro banking malware targets 70 banks in Europe and South America
6. First Horizon bank online accounts hacked to steal customers' funds

INDUSTRIAL

1. Ransomware Attack on Colonial Pipeline
2. Researchers Find Exploitable Bugs in Mercedes-Benz Cars
3. Hack Exposes Data Of 4.5 Million Air India Passengers

HOT FIX TO LOOK FOR

1. Windows HTTP Vulnerability Exploit has been released
2. May Android security updates patch 4 zero-days exploited in the wild
3. Adobe fixes Reader zero-day vulnerability exploited in the wild
4. VMware fixes critical RCE bug in vRealize Business for Cloud
5. Pega Infinity patches authentication vulnerability
6. Apple releases fixes for three WebKit zero-days, additional patches for a fourth
7. Dell patches 12-year-old driver vulnerability impacting millions of PCs
8. SAP and Onapsis Warn of Ongoing Attacks Exploiting Vulnerabilities in Mission-Critical SAP Applications

TOOL OF THE DAY

1. WhatWeb
2. Parth
3. Webpwn3r
4. OSRFramework
5. FinalRecon
6. Massbleed

CYBER MONDAY

1. Inability to hire and retain the right cybersecurity team is one of the biggest cybersecurity problems for organisations
2. Most organisations operate with no proper cyber defenses, as they delay in deciding between internal & external security team.
3. World Policies to strengthen individual country's cyber security could lead to connected & disconnected moments.

BLOG OF THE MONTH

1. Layer Wise Analysis of Security in IoT
2. Server-Side-Request-Forgery (SSRF)
3. Command Execution Attacks on Apache Struts server CVE-2017-5638

CONSUMER TECH

Zero-Days in Remote Mouse App for SmartPhones

As many as six zero-days have been discovered in an application called Remote Mouse, allowing a remote intruder to gain complete code execution without any user interaction. The unpatched bugs, nicknamed 'Mouse Trap,' was revealed by security researcher Axel Persinger, who said, "It's obvious that this application is really vulnerable and puts users at risk due to bad authentication mechanisms, lack of encryption, and poor default configuration."

Attack Type
Remote Code Execution (CVE Finding)
Cause of Issue
Authentication Mechanisms,
Type of Loss
None
References
https://rb.gy/eey3wy

Moriya Rootkit attacks Windows Systems

Attack Type
Rootkit Backdoor
Cause of Issue
Malware
Type of Loss
Network Traffic Data
References
https://rb.gy/9frjfq

The previously unknown malware, dubbed Moriya by Kaspersky researchers who discovered it in the wild, is a passive backdoor that allows attackers to spy on their victims' network traffic and send commands to compromised hosts invisibly. The fact that the backdoor received commands in the form of custom-crafted packets concealed within the victims' network traffic, rather than reaching out to a command-and-control server, contributed to the operation's stealth, demonstrating the threat actor's emphasis on evading detection.

PingBack Malware uses ICMP for Covert Traffic

Researchers have disclosed their findings on a novel Windows malware sample that uses Internet Control Message Protocol (ICMP) for its command-and-control (C2) activities. Dubbed "Pingback," this malware targets Microsoft Windows 64-bit systems, and uses DLL Hijacking to gain persistence.

Attack Type
Malicious DLL Injection
Cause of Issue
Malware
Type of Loss
None
References
https://rb.gy/pbabxc

Codecov hackers gained access to Monday.com source code

Attack Type
Security Breach
Cause of Issue
Supply-Chain
Type of Loss
Source Code Disclosure, Customer Data Exposure
References
https://rb.gy/iadxsw

Monday.com has recently disclosed the impact of the Codecov supply-chain attack that affected multiple companies. Monday.com is an online workflow management platform used by project managers, sales and CRM professionals, marketing teams, and various other organizational departments. The platform's customers include prominent names like Uber, BBC Studios, Adobe, Universal, Hulu, L'Oreal, Coca-Cola, and Unilever.

Toshiba's European Subsidiary Confirms Ransomware Attack; DarkSide's Involvement Suspected

Toshiba's European subsidiaries have confirmed that it was targeted by a "cyberattack". As per the initial investigation, the involvement of the DarkSide ransomware gang is being suspected as the malware signatures of this attack are similar to those used in the Colonial pipeline hack.

Attack Type
Cyber Attack
Cause of Issue
Ransomware
Type of Loss
Customer Information
References
https://rb.gy/rom0v9

Cross-browser tracking vulnerability tracks you via installed apps

Attack Type
Security Research
Cause of Issue
Tracking Users
Type of Loss
None
References
https://rb.gy/cewaom

Researchers have devised a method for tracking a user through several browsers on the same computer by querying the device's installed applications. When such applications are installed, custom URL schemes are created that the browser can use to open a URL in a particular application. A researcher from one of the most common fingerprinting scripts, FingerprintJS, has disclosed a vulnerability that allows a website to monitor a device's user across browsers such as Chrome, Firefox, Microsoft Edge, Safari, and even Tor.

Microsoft build tool abused to deliver password-stealing malware

As part of an ongoing campaign, threat actors are exploiting the Microsoft Build Engine (MSBuild) to instal remote access tools (RATs) and information-stealing malware filelessly. MSBuild (msbuild.exe) is a valid and open-source Microsoft development tool for building applications, close to the Unix make utility. If an XML schema project file describing how to automate the build process is given, this development tool can build apps on any Windows system (compilation, packaging, testing, and deployment.)

Attack Type
Security Breach
Cause of Issue
Malware
Type of Loss
PII Data,
Financial Data
References
https://rb.gy/kpifex

APTs aim at Exchange servers

Attack Type
Security Research (APT Attacks)
Cause of Issue
Security Update Checking
Type of Loss
None
References
https://rb.gy/nut4xm

Research by ESET showed that the vulnerabilities CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065 were exploited by at least 10 APT groups. APTs are state-sponsored hacker groups that engage in espionage and sabotage attacks to steal sensitive data and cripple an opponent's infrastructure and defence systems. Their operations are now regarded as the biggest threat to government institutions and private organizations.

QNAP warns of eCh0raix ransomware attacks, Roon Server zero-day

Customers are being warned about an actively exploited Roon Server zero-day bug and eCh0raix ransomware attacks on their Network Attached Storage (NAS) computers, according to QNAP.
This notice comes only two weeks after QNAP users were alerted about an ongoing AgeLocker ransomware outbreak. Customers were urged by QNAP to "act immediately" to protect their data from possible eCh0raix attacks by using more secure passwords for administrator accounts, secure accounts from brute force attacks, allow IP Access Protection and avoiding the use of the default port numbers 443 and 8080.

Attack Type
Security Breach
Cause of Issue
Ransomware
Type of Loss
PII Data,
Financial Data,
Service Disruption
References
https://rb.gy/bubnzu

Foxit Reader bug lets attackers run malicious code via PDFs

Attack Type
Security Updates
Cause of Issue
Malicious
Code Execution
Type of Loss
System Compromise
References
https://rb.gy/vdx6e1

Foxit Software, the company behind the highly popular Foxit Reader, has published security updates to fix a high severity remote code execution (RCE) vulnerability affecting the PDF reader. This security flaw could allow attackers to run malicious code on users' Windows computers and, potentially, take over control.

Blind SQL Injection flaw in WP Statistics impacted 600K+ sites

Researchers from the Wordfence Threat Intelligence discovered a Time-Based Blind SQL Injection vulnerability in WP Statistics, which is a WordPress plugin with over 600,000 active installs. The vulnerability could be exploited by an unauthenticated attacker to extract sensitive information from a WordPress website using the vulnerable plugin. The flaw has been rated with a CVSS score of 7.5 (High severity), it affects plugin versions prior to 13.0.8.

Attack Type
Blind SQL Injection
Cause of Issue
Security Flaw
Type of Loss
Extracting Data from
DataBase
References
https://rb.gy/qwu2c3

Cisco bugs allow creating admin accounts, executing commands as root

Attack Type
Security Research
Cause of Issue
Security Flaw
Type of Loss
None
References
https://rb.gy/9uphot

Cisco has fixed critical SD-WAN vManage and HyperFlex HX software security flaws that could enable remote attackers to execute commands as root or create rogue admin accounts. The company also issued security updates to address high and medium severity vulnerabilities in multiple other software products that allow attackers to execute arbitrary code remotely, escalate privileges, trigger a denial of service conditions, and more on unpatched servers.

Qualcomm vulnerability impacts nearly 40% of all mobile phones

A high severity security vulnerability found in Qualcomm's Mobile Station Modem (MSM) chips (including the latest 5G-capable versions) could enable attackers to access mobile phone users' text messages, call history, and listen in on their conversations. "If exploited, the vulnerability would have allowed an attacker to use Android OS itself as an entry point to inject malicious and invisible code into phones," according to Check Point researchers who found the vulnerability tracked as CVE-2020-11292.

Attack Type
Security Research
Cause of Issue
CVE Finding
Type of Loss
None
References
https://rb.gy/hqnpqz

HEALTH

Ireland's Department of health hit by Conti Ransomware

Attack Type
Security Research
Cause of Issue
Ransomware
Type of Loss
PII Data
Service Disruption
References
https://rb.gy/myyiaw

Despite breaching the network and dropping Cobalt Strike beacons to deploy their malware across the network, the Conti ransomware gang failed to encrypt the systems of Ireland's Department of Health (DoH). On the same day, Conti operators violated Ireland's Health Service Executive (HSE), the country's publicly funded healthcare system, forcing it to shut down all IT programmes to contain the breach.

Scripps Health Care hit by Ransomware

Customers are being warned about an actively exploited Roon Server zero-day bug and eCh0raix ransomware attacks on their Network Attached Storage (NAS) computers, according to QNAP.
This notice comes only two weeks after QNAP users were alerted about an ongoing AgeLocker ransomware outbreak. Customers were urged by QNAP to "act immediately" to protect their data from possible eCh0raix attacks by using more secure passwords for administrator accounts, secure accounts from brute force attacks, allow IP Access Protection and avoiding the use of the default port numbers 443 and 8080.

Attack Type
Malware
Cause of Issue
Ransomware
Type of Loss
Financial Loss
References
https://rb.gy/vdx6e1

FINANCIAL

CNA Paid $40 Million in Ransom After March Cyber Attack

Attack Type
Security Breach
Cause of Issue
Ransomware
Type of Loss
None
References
https://rb.gy/iadxsw

The Chicago-based company paid the hackers about two weeks after a trove of company data was stolen, and CNA officials were locked out of their network. On May 12, CNA said it did “not believe that the systems of record, claims systems, or underwriting systems, where the majority of policyholder data – including policy terms and coverage limits – is stored, were impacted.”

Insurer AXA hit by ransomware after dropping support for ransom payments

Branches of insurance giant AXA based in Thailand, Malaysia, Hong Kong, and the Philippines have been struck by a ransomware cyber attack. The Avaddon ransomware group claimed on their leak site that they had stolen 3 TB of sensitive data from AXA's Asian operations. The compromised data obtained by Avaddon, according to the group, includes customer medical reports (exposing their sexual health diagnosis), copies of ID cards, bank account statements, claim forms, payment records, contracts, and more.

Attack Type
Security Breach
Cause of Issue
Ransomware
Type of Loss
PII Data,
Financial Data,
Health Records
References
https://rb.gy/oitidc

Trust Wallet, MetaMask crypto wallets targeted by new support scam

Attack Type
SpearPhishing
Cause of Issue
Malware
Type of Loss
Account Compromise via
Illegally
gaining Login Credential
References
https://rb.gy/9c4kvp

Trust Wallet and MetaMask wallet users are being targeted in ongoing and aggressive Twitter phishing attacks to steal cryptocurrency funds. The apps use this recovery phrase to create the private keys necessary to access your wallet. Anyone who has this recovery phrase can import your wallet and use the cryptocurrency funds stored in it.

Student health insurance carrier Guard.me suffers a data breach

Student health insurance carrier guard.me has taken their website offline after a vulnerability allowed a threat actor to access policyholders' personal information. guard.me is one of the world's largest insurance carriers specializing in providing health insurance to students while traveling or studying abroad in another country. On May 12th, Guard.me discovered suspicious activity on their website that led them to take down their website. Later, guard.me began emailing students a data breach notification seen by BleepingComputer that states a website vulnerability allowed unauthorized persons to access policyholders' personal information.

Attack Type
Security Breach
Cause of Issue
Lack of Security
Type of Loss
PII Data
References
https://rb.gy/fjbtqp

Bizarro banking malware targets 70 banks in Europe and South America

Attack Type
Malware
Cause of Issue
Lack of Security
Type of Loss
Financial Data
References
https://rb.gy/bmvyuj

A banking trojan named Bizarro that originates from Brazil has crossed the borders and started to target customers of 70 banks in Europe and South America. Once landed on a Windows system, the malware can force users into entering banking credentials and uses social engineering to steal two-factor authentication codes. The malware spreads through phishing emails that are typically disguised as official tax-related messages informing of outstanding obligations.

First Horizon bank online accounts hacked to steal customers' funds

Bank holding company First Horizon Corporation disclosed the some of its customers had their online banking accounts breached by unknown attackers at the beginning of the month of May. The attackers were able to gain access to customer information stored in the breached accounts and drain funds from some of them before their intrusion was discovered. The financial services firm revealed that they "fraudulently obtained an aggregate of less than $1 million from some of those accounts."

Attack Type
Security Breach
Cause of Issue
Gain access to customer information and drain funds in their account
Type of Loss
Financial Loss
References
https://rb.gy/0pnnyp

INDUSTRIAL

Ransomware Attack on Colonial Pipeline

Attack Type
Security Breach
Cause of Issue
Ransomware
Type of Loss
System Shut Down, Data Loss
References
https://rb.gy/qm1qya

Colonial Pipeline, which carries 45% of the fuel consumed on the U.S. East Coast, said it halted operations due to a ransomware attack. "On May 7, the Colonial Pipeline Company learned it was the victim of a cybersecurity attack," the company said in a statement posted on its website. "We have since determined that this incident involves ransomware. In response, we proactively took certain systems offline to contain the threat, which has temporarily halted all pipeline operations, and affected some of our IT systems."

Researchers Find Exploitable Bugs in Mercedes-Benz Cars

The vulnerabilities were found in the Mercedes-Benz User Experience (MBUX), the infotainment system initially introduced on A-class vehicles in 2018, but has since been adopted on the car maker's entire vehicle line-up. The vulnerabilities, tracked as CVE-2021-23906, CVE-2021-23907, CVE-2021-23908, CVE-2021-23909, and CVE-2021-23910, provides hackers with remote control of some of the car's functions, but not with access to physical features, such as steering or braking systems.

Attack Type
Security Research
Cause of Issue
CVE Finding
Type of Loss
Controlling CAN
References
https://rb.gy/3uplts

Hack Exposes Data Of 4.5 Million Air India Passengers

Attack Type
Security Breach
Cause of Issue
Security Mechanism
Type of Loss
Customer Data, PII Data
References
https://rb.gy/vifowf

Air India has revealed that at least 4.5 million of its passengers' personal information was compromised as a result of a third-party IT system hack. Air India revealed in a statement that in late February, SITA – the data processor of the passenger service system (which stores and processes passengers' personal data) - was the victim of a "cybersecurity attack." The breach compromised information belonging to at least 4.5 million people, including names, passport numbers, and payment information.

HOT FIX TO LOOK OUT FOR

Windows HTTP Vulnerability Exploit has been released HOT PAtches

Over the weekend, proof-of-concept exploit code for a crucial wormable vulnerability in the latest versions of Windows 10 and Windows Server was released. CVE-2021-31166, the bug, was discovered in the HTTP Protocol Stack (HTTP.sys), which is used by the Windows Internet Information Services (IIS) web server as a protocol listener for handling HTTP requests. Microsoft has patched the vulnerability during this month's Patch Tuesday, and it impacts ONLY Windows 10 versions 2004/20H2 and Windows Server versions 2004/20H2.

Attack Type
Software Vulnerability /Security Research
Cause of Issue
CVE-2021-31166
Type of Loss
None
References
https://rb.gy/6lms2p

May Android security updates patch 4 zero-days exploited in the wild

Attack Type
Security Research
Cause of Issue
Zero Day
Type of Loss
Device Compromise
References
https://rb.gy/rbou2g

Four Android security vulnerabilities were exploited in the wild as zero-day bugs before being patched earlier in May 2021. Attacks attempting to exploit these flaws were targeted and impacted a limited number of users based on information shared after this month's Android security updates were published. There are indications that CVE-2021-1905, CVE-2021-1906, CVE-2021-28663 and CVE-2021-28664 may be under limited, targeted exploitation," a recently updated version of the May 2021 Android Security Bulletin reveals.

Adobe fixes Reader zero-day vulnerability exploited in the wild

Adobe has released a massive Patch, a security update release that fixes vulnerabilities in twelve different applications, including one actively exploited vulnerability Adobe Reader. Of particular concern, Adobe warns that one of the Adobe Acrobat and Reader vulnerabilities tracked as CVE-2021-28550 has been exploited in the wild in limited attacks against Adobe Reader on Windows devices.

Attack Type
Security Update
Cause of Issue
Vulnerable Software
Type of Loss
None
References
https://rb.gy/xopxm4

VMware fixes critical RCE bug in vRealize Business for Cloud

Attack Type
RCE
Cause of Issue
Vulnerable Servers
Type of Loss
None
References
https://rb.gy/e0iorm

VMware has released security updates to address a critical severity vulnerability in vRealize Business for Cloud that enables unauthenticated attackers to remotely execute malicious code on vulnerable servers. The security vulnerability is tracked as CVE-2021-21984, and it impacts virtual appliances running VMware vRealize Business for Cloud prior to version 7.6.0. The issue was discovered and reported to VMware by Positive Technologies web security researcher Egor Dimitrenko.

Pega Infinity patches authentication vulnerability

Security researchers came across a Pega Infinity vulnerability through participation in Apple's bug bounty program. By using Burp Suite—an integrated platform for performing security testing of web applications—the security researchers discovered a password reset weakness in Pega Infinity that could allow an attacker to bypass Pega Infinity's password reset system to lead to a full compromise. Pega was quick to work with the researchers to patch the vulnerability, even though they needed time for customers running Infinity on-premises to update their installations. This process, one of the researchers said, took over three months.

Attack Type
Security Research Program
Cause of Issue
Security Flaw
Type of Loss
Account Takeover via Authentication Bypass
References
https://rb.gy/vtztan

Apple releases fixes for three WebKit zero-days, additional patches for a fourth

Attack Type
Security Research
Cause of Issue
Zero Day Finding
Type of Loss
None
References
https://rb.gy/7e8dlj

Apple has released security updates for multiple products to patch three zero-days and roll out additional patches for a fourth that the company said they might have been exploited in the wild. All four zero-days impact WebKit—the web page rendering engine at the heart of the company's Safari web browser.

Dell patches 12-year-old driver vulnerability impacting millions of PCs

The bug, tracked as CVE-2021-21551, impacts version 2.3 of DBUtil, a Dell BIOS driver that allows the OS and system apps to interact with the computer's BIOS and hardware. The security firm SentinelOne said it found a vulnerability in this driver that could be abused to allow threat actors access driver functions and execute malicious code with SYSTEM and kernel-level privileges. The threat actors who gained initial access to a computer, even to a low-level account, could abuse this bug to take full control over the compromised PC

Attack Type
Security Research
Cause of Issue
CVE Finding
Type of Loss
Malicious Code Execution, Privilege Escalation
References
https://rb.gy/uoqvyp

SAP and Onapsis Warn of Ongoing Attacks Exploiting Vulnerabilities in Mission-Critical SAP Applications

Attack Type
Security Breach
Cause of Issue
Insecure Software Update Practice
Type of Loss
Sensitive Data, Financial Fraud, Systems Disruption
References
https://rb.gy/1zkdtu

Six cybersecurity vulnerabilities in mission-critical SAP applications are being actively exploited by threat actors according to cybersecurity firm Onapsis. Exploitation of the flaws could result in the theft of sensitive data, financial fraud, and disruption of mission-critical systems, including malware and ransomware attacks. Patches were released promptly by SAP after being notified about the vulnerabilities; however, many organizations that use SAP systems have not applied the patches and are running outdated software or have misconfigured the software and are vulnerable to attack.

TOOL OF THE DAY

WhatWeb

Whatweb is a tool that tells what is the website. Whatweb can identify all sorts of information about a live website. Whatweb offers both passive scanning and aggressive testing. Passive scanning just extracts data from HTTP headers simulating a normal visit. Aggressive options get deeper with recursion & various types of queries & identify all technologies just like a vulnerability scanner.

Parth

Parth can go through your burp history, a list of URLs or it's own disocovered URLs to find such parameter names and the risks commonly associated with them. Parth is designed to aid web security testing by helping in prioritization of components for testing.

Webpwn3r

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

OSRFramework

OSRFramework is a GNU AGPLv3+ set of libraries developed by i3visio to perform Open Source Intelligence collection tasks. They include references to a bunch of different applications related to username checking, DNS lookups, information leaks research, deep web search, regular expressions extraction and many others. At the same time, using ad-hoc Maltego transforms, OSRFramework provides a way of making these queries graphically as well as several interfaces to interact with like OSRFConsole or a Web interface.

FinalRecon

FinalRecon is an automatic web reconnaissance tool written in python. The goal of FinalRecon is to provide an overview of the target in a short amount of time while maintaining the accuracy of results. Instead of executing several tools one after another, it can provide similar results keeping dependencies small and simple.

Massbleed

Massbleed is an SSL vulnerability scanner. It mainly checks vulnerability in SSL of the target sites, as per ethical hacking investigators. Massbleed is an open-source project and can be modified according to requirement. It does not contain any license.

CYBER MONDAY

Inability to hire and retain right cyber security team is one of the biggest cybersecurity problems for organisations

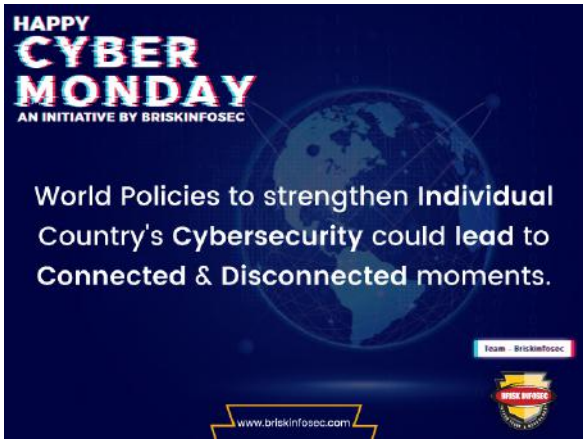
As security is one of the biggest concerns of the IT industry, so is finding the right people for the Security Team. In short, the productivity of the security team is proportional to the quality of the team members.

Most organisations operate with no proper cyber defenses, as they delay in deciding between internal & external security team.

Most firms fail to adopt security measures because they are prone to lose focus while deciding between internal and external security teams. In the end, it has an impact on the company's total security measures.

World Policies to strengthen individual country's cyber security could lead to connected & disconnected moments.

The best ideas are produced through facing and overcoming challenges. Across a world where we strive for stronger security infrastructure in all sectors. Disruptions are unavoidable as a result of an effort to establish a flawless security infrastructure.

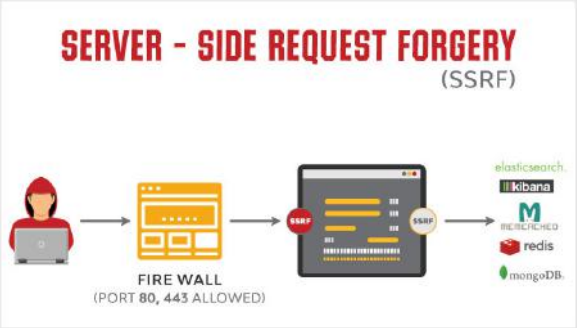


BLOG OF THE MONTH

Layer Wise Analysis of Security in IoT

We find IoT in a wide range of applications, including smart cities, control actuation and maintenance of complex systems in the industry, health, transport and much more. Needless to say, IoT touches every facet of our daily lives. Security and privacy are two of the most crucial challenges that IoT is facing. Since sensor networks are highly vulnerable to cyberattacks, it is very important to have some mechanisms that can protect the network, devices and users from all kinds of attacks.

Server-Side-Request-Forgery (SSRF)



Server-Side Request Forgery (SSRF) refers to an attack, wherein an attacker can send a maliciously crafted request from a vulnerable web application. SSRF is mainly used to target internal systems behind WAF (web application firewall), that are unreachable to an attacker from the external network. Additionally, it's also possible for an attacker to mark SSRF, for accessing services from the same server that is listening on the loopback interface.

Command Execution Attacks on Apache Struts server CVE-2017-5638

Zero-day vulnerabilities are found in various applications every day which can be exploited by intruders to exploit and compromise the security of organizations. Apache Struts RCE (CVE 2017 5638) is one of the critical remote code execution (RCE) vulnerabilities that lets unauthenticated attackers get a remote shell on the server. This blog will explain CVE 2017 5638 vulnerability in detail with exploitation and mitigation steps.

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 a drop in an ocean. There are more unreported than that meets the eye. Millions of organizations and individuals have clicked those links and have fallen victims to these baits of hackers. The most obvious reason being ‘lack of awareness. Well, as the saying goes,

"Prevention is better than Cure" - be it COVID-19 or Cyber threats.

Briskinfosec is ready to help you in your journey to protect your information infrastructure and assets. 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.

BRISK INFOSEC

CYBER TRUST & ASSURANCE

contact@briskinfose.com | www.briskinfosec.com