THREATSPLOIT

ADVERSARY REPORT

EDITION 37

www.briskinfosec.com

INTRODUCTION

Welcome to the Threatsploit Report of September 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.

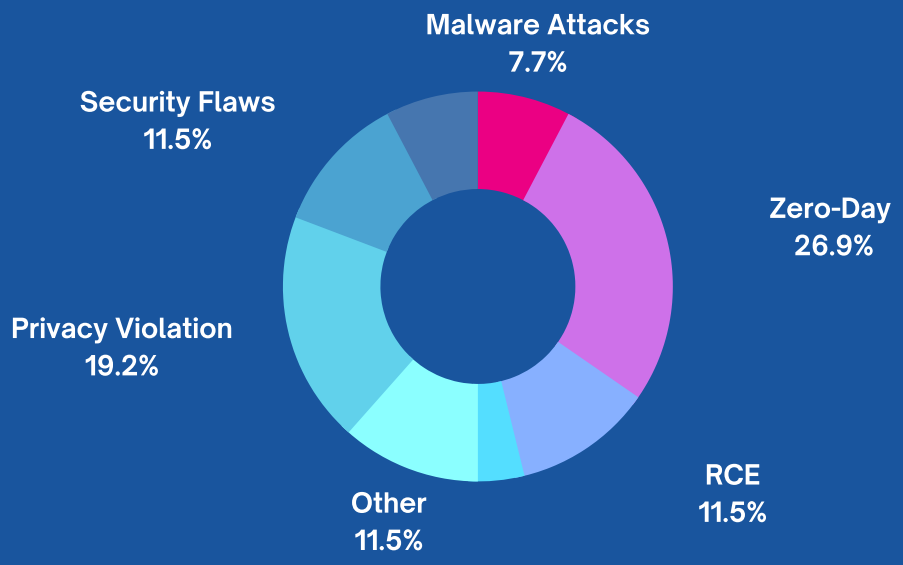
The primary reason is and has always been the same....

"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.

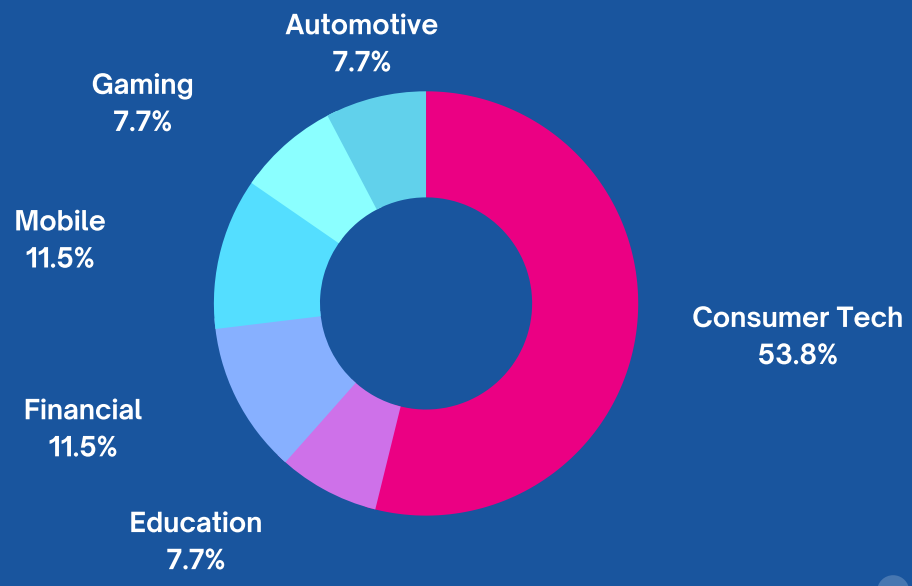
TYPES OF ATTACK VECTORS

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

AUTOMOTIVE

- Ford bug exposed customer and employee records from internal systems
- BlackBerry Security Flaw Leaves Millions of Cars, Vulnerable to Hackers

CONSUMER TECH

- Microsoft Exchange servers are getting hacked via ProxyShell exploits
- Microsoft confirms another Windows print spooler zero-day bug
- Web hosting platform cPanel & WHM is vulnerable to authenticated RCE and privilege escalation
- Nokia subsidiary discloses data breach after Conti ransomware attack
- Botnet targets hundreds of thousands of devices using Realtek SDK
- Node.js developers fix a high-risk vulnerabilities that could allow remote domain hijacking
- XSS Bug in SEOPress WordPress Plugin Allows Site Takeover
- Critical IoT security camera vulnerability allows attackers to remotely watch live video - and gain access to networks
- OpenSSL Vulnerability Can Be Exploited to Change Application Data
- Foxit - PhantomPDF, ConnectedPDF: Remote Code Execution Vulnerability
- Hackers can bypass Cisco security products in data theft attacks
- T-Mobile: More than 40 Million Customers' Data Stolen
- FireEye, CISA Warn of Critical IoT Device Vulnerability
- Fortinet delays patching zero-day allowing remote server takeover

EDUCATION

- Data breach at New York university potentially affects 47,000 citizens
- Finders, cheaters: RCE bug in Moodle e-learning platform could be abused to steal data, manipulate results

LATEST THREAT ENTRIES

FINANCIAL

- Finders, cheaters: RCE bug in Moodle e-learning platform could be abused to steal data, manipulate results
- Reindeer leaked the sensitive data of more than 300,000 people
- New Hampshire town loses $2.3 million to overseas scammers

GAMING

- Razer bug lets you become a Windows 10 admin by plugging in a mouse
- Critical Valve Bug Lets Gamers Add Unlimited Funds to Steam Wallets

MOBILE

- Malicious WhatsApp mod infects Android devices with malware
- New zero-click iPhone exploit used to deploy NSO spyware
- FlyTrap Trojan Lifts Facebook Credentials From Android Users

TOOL OF THE DAY

- FRIDALOADER
- RACOON SCANNER
- PARTH

CYBERMONDAY

- In today's Hyperconnected world, cyber security is not a luxury but an absolute necessity
- 60 Percent of Breaches involved vulnerabilities for which a patch was available but not applied
- What is Cyber Resilience?

BLOG OF THE MONTH

- END TO END EMAIL SECURITY WITH DMARC RECORDS

AUTOMOTIVE

Ford bug exposed customer and employee records from internal systems

A bug on Ford Motor Company's website allowed for accessing sensitive systems and obtaining proprietary data, such as customer databases, employee records, internal tickets, etc. The data exposure stemmed from a misconfigured instance of Pega Infinity customer engagement system running on Ford's servers. This week, researchers have disclosed a vulnerability found on Ford's website that let them peek into confidential company records, databases and perform account takeovers. The vulnerability was discovered by Robert Willis and break3r, with further validation and support provided by members of Sakura Samurai ethical hacking group—Aubrey Cottle, Jackson Henry, and John Jackson. The issue is caused by CVE-2021-27653, an information exposure vulnerability in improperly configured Pega Infinity customer management system instances.

Attack Type Data Privacy Violation | Cause of Issue Lack Of Data Protection Regulation | Type of Loss Data Loss

BlackBerry Security Flaw Leaves Millions of Cars, Vulnerable to Hackers

A security flaw in software designed by BlackBerry Limited has left almost two million cars, as well as countless devices in the medical, automotive and energy sectors, vulnerable to hackers, two federal agencies warned. On Tuesday, the US Food and Drug Administration (FDA) and Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) issued advisories regarding the vulnerability, which affects older but still widely used versions of one of BlackBerry's flagship products, an operating system called QNX. Both CISA and the FDA said they are not aware of any incidents of active exploitation of the flaw, but warned the vulnerability gives hackers a way to attack systems remotely and urged users to update their software with a newly-released security patch from BlackBerry. Once a dominant player in smartphones, BlackBerry has morphed into a software business, supplying commercial operating systems for several industries, including medtech, aerospace, defence and rail. QNX is integrated into 195 million vehicles, including those made by Ford, Volkswagen and BMW, for a range of critical functions like advanced driver assistance systems.

Attack Type Application Security Flaw | Cause of Issue Lack Of Secure Coding |
Type of Loss Reputation & Remote Takeover

CONSUMER TECH

Microsoft Exchange servers are getting hacked via ProxyShell exploits

Threat actors are actively exploiting Microsoft Exchange servers using the ProxyShell vulnerability to install backdoors for later access. The ProxyShell exploit uses three chained Microsoft Exchange vulnerabilities to perform unauthenticated, remote code execution. The three vulnerabilities were discovered by Devcore Principal Security Researcher Orange Tsai who chained them together to take over a server in April's Pwn2Own 2021 hacking contest. After watching the talk, security researchers Peter Json and Nguyen Jang published more detailed technical information about reproducing the attack.

Attack Type Zero-Day Vulnerability | Cause of Issue Lack Of Security Patches | Type of Loss Server Takeover

Microsoft confirms another Windows print spooler zero-day bug

Microsoft has issued an advisory for another zero-day Windows print spooler vulnerability tracked as CVE-2021-36958. This vulnerability is part of a class of bugs known as 'PrintNightmare' that allows local attackers to gain SYSTEM privileges on a computer. Microsoft released security updates in both July and August to fix various PrintNightmare vulnerabilities. However, a vulnerability disclosed by security researcher Benjamin Delpy still allows threat actors to quickly gain system privileges by connecting to a remote print server.

Attack Type Zero-Day Vulnerabilty | Cause of Issue Lack Of Security Patches | Type of Loss System Takeover

Web hosting platform cPanel & WHM is vulnerable to authenticated RCE and privilege escalation

Security researchers have achieved remote code execution (RCE) and privilege escalation on web hosting platform cPanel & WHM via stored cross-site scripting (XSS) vulnerability. cPanel & WHM is a suite of Linux tools that enable the automation of web hosting tasks via a graphical user interface (GUI). During a black-box pen test, RCE was also demonstrated via a “more convoluted” CSRF bypass chained with a cross-site WebSocket hijacking attack that was possible because WebSockets failed to check their requests’ Origin header, according to a technical write-up published by Adrian Tiron, the cloud AppSec consultant at UK infosec firm Fortbridge. The Websocket hijacking attack was tested in Firefox since Chrome has SameSite cookies enabled by default. The researcher suggests the issue could have been completely mitigated “by applying some filtering/encoding on that vulnerable input”.

Attack Type Remote Code Execution | Cause of Issue Lack Of Secure Coding |
Type of Loss System & Data Compromise

Nokia subsidiary discloses data breach after Conti ransomware attack

SAC Wireless, a US-based Nokia subsidiary, has disclosed a data breach following a ransomware attack. The company discovered that its network was breached by Conti ransomware operators on June 16, only after deploying their payloads and encrypting SAC Wireless systems. The Nokia subsidiary found that personal information belonging to current and former employees (and their health plans' dependents or beneficiaries) was also stolen during the ransomware attack on August 13, following a forensic investigation conducted with the help of external cyber security experts.

Attack Type Malware Attack (Data Breach) | Cause of Issue Lack Of Malware Protection Tools. |
Type of Loss Business Data Encrypted & Lost

Botnet targets hundreds of thousands of devices using Realtek SDK

A Mirai-based botnet now targets a critical vulnerability in the software SDK used by hundreds of thousands of Realtek-based devices. The bug affects 200 models from at least 65 vendors, including Asus, Belkin, D-Link, Netgear, Tenda, ZTE, and Zyxel. The security flaw that IoT Inspector security researchers found is now tracked as CVE-2021-35395 and was assigned a 9.8/10 severity rating Since the bug affects the management web interface, remote attackers can scan for and attempt to hack them to execute arbitrary code remotely on unpatched devices.

Attack Type Malware Attack software SDK (Botnet) | Cause of Issue Lack Of Malware Protection Tools. |
Type of Loss System Takeover & Data Loss

Node.js developers fix a high-risk vulnerabilities that could allow remote domain hijacking

A vulnerability in Node.js that could allow a remote actor to perform domain hijacking attacks has been fixed. The maintainers of the JavaScript runtime environment released a security advisory on August 12 warning users to update to the latest version to protect against a series of bugs. The first vulnerability CVE-2021-3672/CVE-2021-2293 is an improper handling of untypical characters in domain names, which opened the door to remote code execution (RCE), or cross-site scripting (XSS) exploits. The flaw also caused application crashes due to missing input validation of hostnames returned by DNS servers.

Attack Type Remote Code Execution | Cause of Issue Improper Patch Management And Backup |
Type of Loss System Takeover & Data Loss

XSS Bug in SEOPress WordPress Plugin Allows Site Takeover

A stored cross-site scripting (XSS) vulnerability in the SEOPress WordPress plugin could allow attackers to inject arbitrary web scripts into websites, researchers said. SEOPress is a search engine optimization (SEO) tool that lets site owners manage SEO metadata, social-media cards, Google Ad settings and more. The bug (CVE-2021-34641) allows any authenticated user to call the REST route with a valid nonce, and to update the SEO title and description for any post. Depending on what an attacker updates the name and description to, it would allow a number of malicious actions, including full site takeover.

Attack Type Stored XSS | Cause of Issue Lack Of Secure Code Implementation |
Type of Loss Data Alteration

Critical IoT security camera vulnerability allows attackers to remotely watch live video - and gain access to networks

Vulnerabilities in millions of Internet of Things (IoT) devices could allow cyber attackers to compromise devices remotely, allowing them to watch and listen to live feeds, as well as compromise credentials to prepare the ground for further attacks. Vulnerability is tracked as CVE-2021-28372 and carries a Common Vulnerability Scoring System (CVSS) score of 9.6 -- classifying it as a critical vulnerability. Upgrading to the latest version of the Kalay protocol (3.1.10) is highly recommended to protect devices and networks.

Attack Type Zero-Day Vulnerability | Cause of Issue Lack Of Security Patches | Type of Loss Remote Takeover

OpenSSL Vulnerability Can Be Exploited to Change Application Data

OpenSSL 1.1.11 patches a high-severity vulnerability that could allow an attacker to change an application's behavior or cause the app to crash. The flaw, tracked as CVE-2021-3711, has been described as a buffer overflow related to SM2 decryption.OpenSSL users have also been informed about CVE-2021-3712, a medium-severity vulnerability that can be exploited for denial-of-service (DoS) attacks, and possibly for the disclosure of private memory contents, such as private keys. Five other vulnerabilities affecting OpenSSL were disclosed this year, including two that have been rated high severity.

Attack Type Zero-Day Vulnerability | Cause of Issue Lack Of Security Awareness For Individuals | Type of Loss Disruption in Service

Foxit - PhantomPDF, ConnectedPDF: Remote Code Execution Vulnerability

The FoxitPhantomPDF - ConnectedPDF service listens for connections on TCP port 44440 on localhost and fails to sanitize input data before using it to construct queries. This allows arbitrary files to be written under the context of the user running PhantomPDF. An attacker can create a specially crafted PDF file that will abuse this vulnerability to achieve remote code execution. Each message has a Type field, denoting the message type. The vulnerability resides in the processing of message type 1004, the handler of which is characterized by string references such as “DocSearch_Locator_Table”.

Attack Type Application Security Flaw | Cause of Issue Lack Of Secure Coding | Type of Loss Remote Takeover & Data Loss

Hackers can bypass Cisco security products in data theft attacks

Cisco said that unauthenticated attackers could bypass TLS inspection filtering tech in multiple products to exfiltrate data from previously compromised servers inside customers' networks. In such attacks, the threat actors can exploit a vulnerability in the Server Name Identification (SNI) request filtering impacting 3000 Series Industrial Security Appliances (ISAs), Firepower Threat Defense (FTD), and Web Security Appliance (WSA) products. "Using SNIcat or a similar tool, a remote attacker can exfiltrate data in an SSL client hello packet because the return server hello packet from a server on the blocked list is not filtered," Cisco explained.

Attack Type SSL/TLS Vulnerabilities | Cause of Issue Lack Of Security Patches | Type of Loss Data Loss

T-Mobile: More than 40 Million Customers' Data Stolen

T-Mobile has confirmed much of what a threat actor bragged about over the weekend: Personal details for tens of millions of current, former or prospective T-Mobile customers were stolen in a huge breach of its servers. On August 16th, it disclosed further details on the data breach in a post on its website, saying that the breach affects as many as 7.8 million postpaid subscribers, 850,000 prepaid customers and "just over" 40 million past or prospective customers who've applied for credit with T-Mobile. Its investigation is ongoing, but so far, it doesn't look like financial data, credit card information, debit or other payment information was in the stolen files, T-Mobile said. The wireless carrier said that it located and "immediately" closed the access point in its servers that it believes granted access to the attacker(s). At least according to what the purported thief told cybersecurity intelligence firm Cyble, the threat actor made off with a collection of databases that total about 106GB of data, including T-Mobile's Oracle customer relationship management (CRM) database.

Attack Type Data Breach - Sensitive Data Exposure | Cause of Issue Misconfigured Access Point | Type of Loss PII Data

FireEye, CISA Warn of Critical IoT Device Vulnerability

FireEye researchers and the U.S. Cybersecurity and Infrastructure Security Agency are warning about a critical vulnerability that could allow an attacker to gain remote access to potentially millions of compromised IoT devices, such as connected security cameras. The flaw, tracked as CVE-2021-28372, is found in ThroughTek's Kalay protocol, which the FireEye researchers estimate is used in some 83 million IoT and connected devices worldwide, although it's not known how many of these devices might be affected. The bug has been assigned a CVSS score of 9.6, making the vulnerability critical. FireEye, CISA and ThroughTek are urging users and OEMs to upgrade to a newer version of the Kalay protocol to mitigate the risk.

Attack Type Zero-Day Vulnerability | Cause of Issue Lack Of Security Patches |
Type of Loss Remote Takeover & Data Loss

Fortinet delays patching zero-day allowing remote server takeover

Fortinet has delayed patching a zero-day command injection vulnerability found in the FortiWeb web application firewall (WAF) until the end of August. Successful exploitation can let authenticated attackers execute arbitrary commands as the root user on the underlying system via the SAML server configuration page. While attackers must be authenticated to the management interface of the targeted FortiWeb device to abused this bug, they can easily chain it with other vulnerabilities such as the CVE-2020-29015 authentication bypass to take full control of vulnerable servers. "An attacker can leverage this vulnerability to take complete control of the affected device, with the highest possible privilege," Rapid7 explained. "They might install a persistent shell, crypto mining software, or use the compromised platform to reach into the affected network beyond the DMZ." The zero-day discovered by Rapid7 researcher William Vu is tracked as CVE-2021-22123, and it impacts Fortinet FortiWeb versions 6.3.11 and earlier.

Attack Type Zero-Day Vulnerability | Cause of Issue Lack Of Patch Management |
Type of Loss Remote Takeover & Data Loss

EDUCATION

Data breach at New York university potentially affects 47,000 citizens

A data breach at a New York University has potentially exposed the personal information of nearly 47,000 individuals. The Research Foundation for the State University of New York (SUNY) announced it detected unauthorized access to its networks earlier this year. The incident was discovered on July 14, and reportedly involved Social Security numbers. A total of more than 46,700 individuals are said to be impacted by the data breach, although it's not stated whether these people are employees, donors, or others who might be linked to the organizations.

Attack Type Data Privacy Violation | Cause of Issue System Security Misconfiguration | Type of Loss PII Data

Finders, cheaters: RCE bug in Moodle e-learning platform could be abused to steal data, manipulate results

A critical security vulnerability in a popular e-learning platform could be abused to allow access to students' data and test papers – and possibly even manipulate exam results. Moodle is an open-source application that's said to be used by 190,000 organizations in 246 countries worldwide. The bug, a PHP object injection vulnerability in Moodle's Shibboleth authentication module, could allow unauthenticated attackers to achieve remote code execution (RCE), resulting in a complete compromise of the server. In turn, this could allow them complete access to anything on the target server, including personally identifiable information such as password hashes, exam grades, and messages. The researcher said that the vulnerability is only present in Moodle LMS server which has Shibboleth single sign-on authentication enabled. The module is disabled by default, offering some respite to the universities and institutions that make use of the platform. If enabled, however, an unauthenticated attacker can execute arbitrary system commands, the researcher explained.

Attack Type Remote Code Execution | Cause of Issue Lack Of Security Patches | Type of Loss Remote Takeover

FINANCIAL

Hacker Steals $97 Million From Crypto Exchange 'Liquid'

A hacker stole $97 million in crypto assets from the Japan-based cryptocurrency exchange Liquid, which announced the breach via Twitter late Wednesday and halted deposits and withdrawals. Liquid, one of the world's largest cryptocurrency-fiat exchange platforms, said on Twitter on 19th August that it was tracking the movement of the stolen assets and working with other exchanges to freeze and recover funds. The company says it is still assessing the technical components of the attack. "During this difficult period, we greatly appreciate the support from our customers, other exchanges, security experts, and the broader crypto community," it says. "Liquid will continue to do everything in its power to mitigate the impact from this incident and restore full service as soon as possible."

Attack Type Data Privacy Violation | Cause of Issue System Security Misconfiguration | Type of Loss Monetary Values

Reindeer leaked the sensitive data of more than 300,000 people

Security researchers found a significant breach affecting Reindeer, an American marketing company previously associated with Patrón Tequila, Tiffany & Co. and other brands. This breach exposed customers' names, date of birth, email addresses, physical addresses, phone numbers and more. The information exposed included 1,400 profile photos and the details of approximately 306,000 customers in total. Personal details include name, surname, email address, date of birth, physical address, hashed passwords, and Facebook IDs. Phone numbers and physical addresses were the rarest information compromised, but nearly 100,000 of each were exposed.

Attack Type Data Privacy Violation | Cause of Issue Security Misconfiguration| Type of Loss Data Loss

New Hampshire town loses $2.3 million to overseas scammers

Peterborough, a small New Hampshire town, has lost $2.3 million after BEC scammers redirected several bank transfers using forged documents sent to the town's Finance Department staff in multiple email exchanges. BEC scammers use various tactics (including phishing and social engineering) to compromise or impersonate their targets' business email accounts, allowing them to redirect pending or future payments to the bank accounts they control. Town officials discovered the attack on July 26 when the ConVal School District notified them that they didn't receive a $1.2 million monthly transfer. On August 18, while investigating this incident, Peterborough's Finance Department staff discovered that two other bank transfers meant for a general contractor on the town's Main Street Bridge project were diverted to attackers' bank accounts.

Attack Type Data Theft | Cause of Issue Lack Of Security Awareness | Type of Loss Monetary Values

GAMING

Razer bug lets you become a Windows 10 admin by plugging in a mouse

A Razer Synapse zero-day vulnerability has been disclosed on Twitter, allowing you to gain Windows admin privileges simply by plugging in a Razer mouse or keyboard. Razer is a very popular computer peripherals manufacturer known for its gaming mouses and keyboards. Security researcher jonhat discovered a zero-day vulnerability in the plug-and-play Razer Synapse installation that allows users to gain SYSTEM privileges on a Windows device quickly. SYSTEM privileges are the highest user rights available in Windows and allow someone to perform any command on the operating system. Essentially, if a user gains SYSTEM privileges in Windows, they attain complete control over the system and can install whatever they want, including malware. After not receiving a response from Razer, jonhat disclosed the zero-day vulnerability on Twitter yesterday and explained how the bug works with a short video.

Attack Type Zero-Day Vulnerability | Cause of Issue Lack Of Security Patches | Type of Loss System Takeover

Critical Valve Bug Lets Gamers Add Unlimited Funds to Steam Wallets

A security researcher helped Valve, the makers of the gaming platform Steam, plug an easy-to-exploit hole that allowed users to add unlimited funds to their digital wallet. Simply by changing the account's email address, the exploit allowed anyone to artificially boost their digital billfold to anything they wanted. Steam Wallet funds are exclusive to the Steam platform and are used to purchase in-game merchandise, subscriptions and Steam-related content. Valve restricts Steam credits (or money) from being transferred outside its network for purchase or trading. However, there are several unsanctioned ways to convert wallet funds into actual dollars. Working for the HackerOne bug-bounty program, security researcher DrBrix, reported the bug last Monday. By Wednesday, Valve plugged the hole and paid DrBrix $7,500 for identifying the bug.

Attack Type Workflows Instance Misconfiguration | Cause of Issue Lack Of Patch Management | Type of Loss Unknown

MOBILE

Malicious WhatsApp mod infects Android devices with malware

A malicious version of the FMWhatsappWhatsApp mod delivers a Triadatrojan payload, a nasty surprise that infects their devices with additional malware, including the very hard-to-remove xHelper trojan. FMWhatsApp promises to improve the WhatsApp user experience with added features such as better privacy, custom chat themes, access to other social networks' emoji packs, and app locking using a PIN, password, or the touch ID. However, as Kaspersky researchers found, the FMWhatsapp 16.80.0 version will also drop the Triada trojan on users' devices with the help of an advertising SDK.

Attack Type Trojan | Cause of Issue Lack Of Malware Protection Tools & Patches. | Type of Loss Data Loss

New zero-click iPhone exploit used to deploy NSO spyware

Digital threat researchers at Citizen Lab have uncovered a new zero-click iMessage exploit used to deploy NSO Group's Pegasus spyware on devices belonging to Bahraini activists. In total, nine Bahraini activists had their iPhones hacked in a campaign partially orchestrated by a Pegasus operator linked with high confidence to the government of Bahrain by Citizen Lab. The spyware was deployed on their devices after being compromised using two zero-click iMessage exploits (that do not require user interaction): the 2020 KISMET exploit and a new never-before-seen exploit dubbed FORCEDENTRY (also tracked as Megalodon).

Attack Type Zero-Day Vulnerability | Cause of Issue Lack Of Patch Management | Type of Loss Unknown

FlyTrap Trojan Lifts Facebook Credentials From Android Users

A new Android-based trojan has been discovered that can hijack the Facebook accounts of users by stealing session cookies. According to the researchers, the malware campaigns employ simple social engineering tactics. Researchers from the security firm Zimperium spotted a new Trojan called FlyTrap to extract the Facebook login credentials of users. Spread across 140 countries since March, the FlyTrap campaign involves leveraging malicious applications to spread the malware via Google Play and other third-party Android stores. Experts suspect that more than 10,000 Android users may have fallen victim to this attack campaign that uses various offers as baits. These malicious apps use a legitimate Facebook Single Sign-On (SSO) service, which prevents capturing users' credentials. To overcome this, the Trojan uses JavaScript injection to collect sensitive information. All of the information gathered was eventually uploaded to FlyTrap's C2 server. Moreover, FlyTrap's C2 server was found to have multiple security holes, which could result in the further leaks of stolen Facebook session cookies from the server.

Attack Type Trojan | Cause of Issue Lack Of Malware Protection Tools And Patches. | Type of Loss Credentials

TOOLS OF THE MONTH

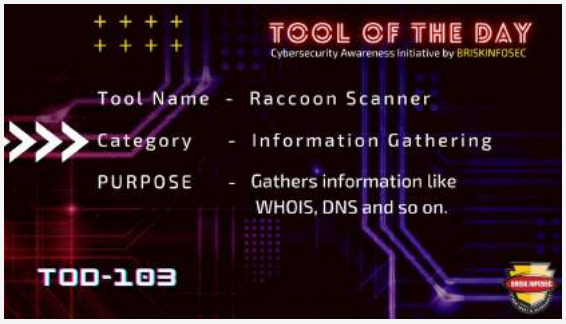
FRIDALOADER

FridaLoader is an Android app to set up Frida and launch quickly. Its a download and launch the latest version of Frida server based on the Genymotion/AVD Emulator and Rooted Android Physical Devices architecture.

Read More:
https://www.briskinfosec.com/tooloftheday/toolofthedaydetail/FridaLoader

RACOON SCANNER

Raccoon Scanner is a tool made for reconnaissance and information gathering with an emphasis on simplicity. It will do everything from fetching DNS records, retrieving WHOIS information, obtaining TLS data, detecting WAF presence and up to threaded dir busting and subdomain enumeration. Every scan output to a corresponding file. Stay Connected:



Read More:
https://www.briskinfosec.com/tooloftheday/toolofthedaydetail/Raccoon-Scanner-for-Information-Gathering-

PARTH

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

Read More:
https://www.briskinfosec.com/tooloftheday/toolofthedaydetail/Parth

CYBERMONDAY

In today's Hyper connected world, cyber security is not a luxury but an absolute necessity

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

60 Percent of Breaches involved vulnerabilities for which a patch was available but not applied

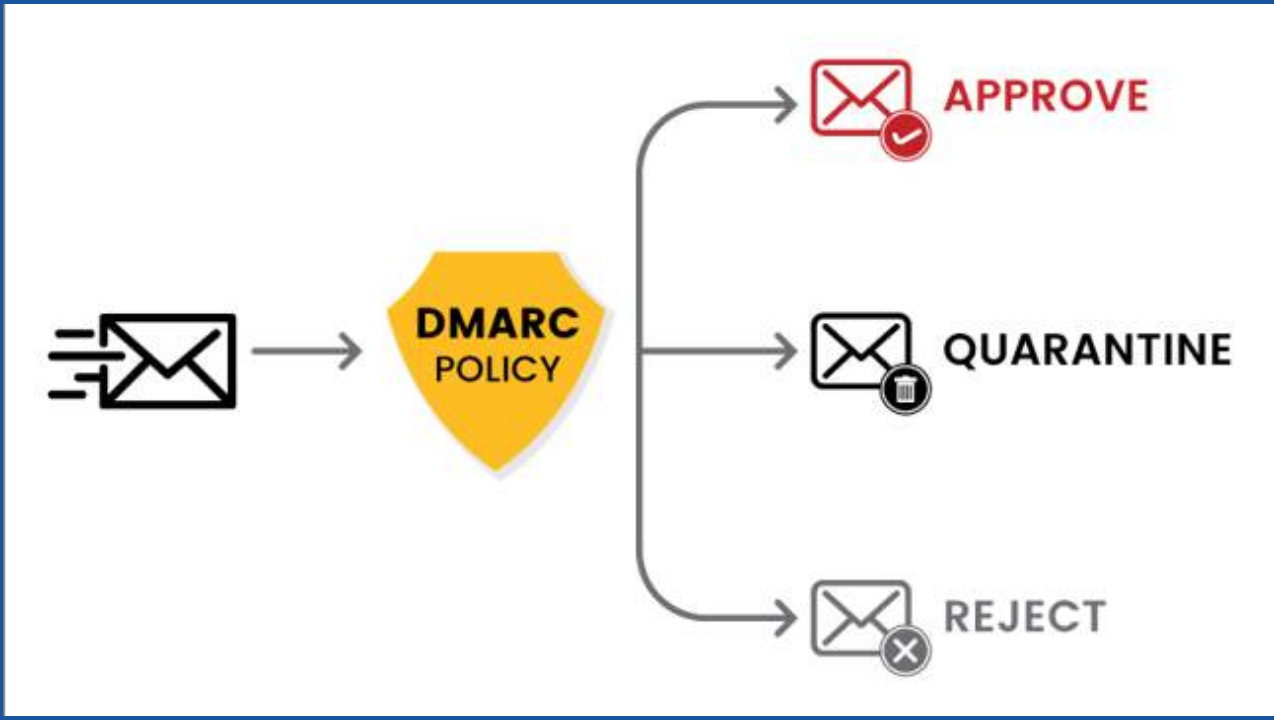
The reason why a patch is released is to completely fix the vulnerabilities and to avoid security disasters. As per the survey in 2020, it is observed that about 60% of patches weren't applied at all which caused increase in data breaches

What is Cyber Resilience?

Cyber resilience is an organization's ability to allow business acceleration (enterprise resiliency) by anticipating, reacting to, and recovering from cyber threats. A cyber-resilient organisation is capable of adapting to both known and unknown emergencies, threats, adversities, and challenge

BLOG OF THE MONTH

END TO END EMAIL SECURITY WITH DMARC RECORDS



DMARC also known as Domain Message Authentication, Reporting & Conformance is a technical standard that helps protect email senders and recipients from email related spoofing and phishing attacks which are widely used as a part of social engineering techniques to compromise user's systems. It uses SPF (Sender policy framework) and DKIM (Domain Keys Identified Mail) to validate the authenticity of a mail. DMARC record policy can be published by an organization to define their mail authentication practice and provides instructions to receiving mail servers on how to enforce them.

Read More about Dawood Ansar's Insight on Email Security: https://www.briskinfosec.com/blogs/blogsdetail/End-to-End-Email-Security-with-DMARC-Records

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

Head Office

Briskinfosec
No:21, 2nd Floor, Krishnama Road,
Nungambakkam, Chennai - 600034,
India
+91 86086 34123 | 044 4352 4537

Partners Office

Urbansoft, Manama Center, Entrance One,
Building No.58, No.316, Government Road,
Manama Area, Kingdom of Bahrain
+973 777 87226

3839 McKinney Ave, Ste 155 - 4920,
Dalls TX 75204
USA
+1 (214) 571 - 6261

Imperial House 2A,
Heigham Road, Eastham,
London E6 2JG
+44 (745) 388 4040

contact@briskinfose.com | www.briskinfosec.com