THREATSPLOIT
ADVERSARY REPORT

EDITION 38

www.briskinfosec.com

INTRODUCTION

Welcome to the Threatsploit Report of October 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.

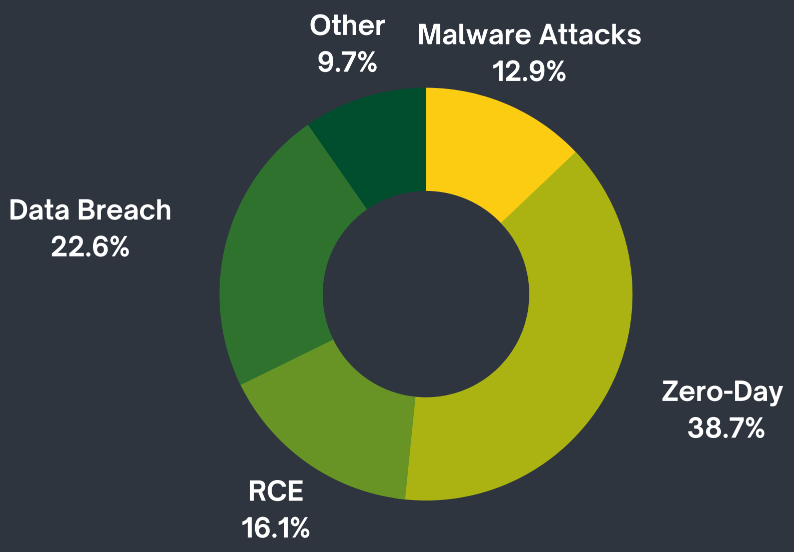
The primary reason is and has always been the same....

"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.

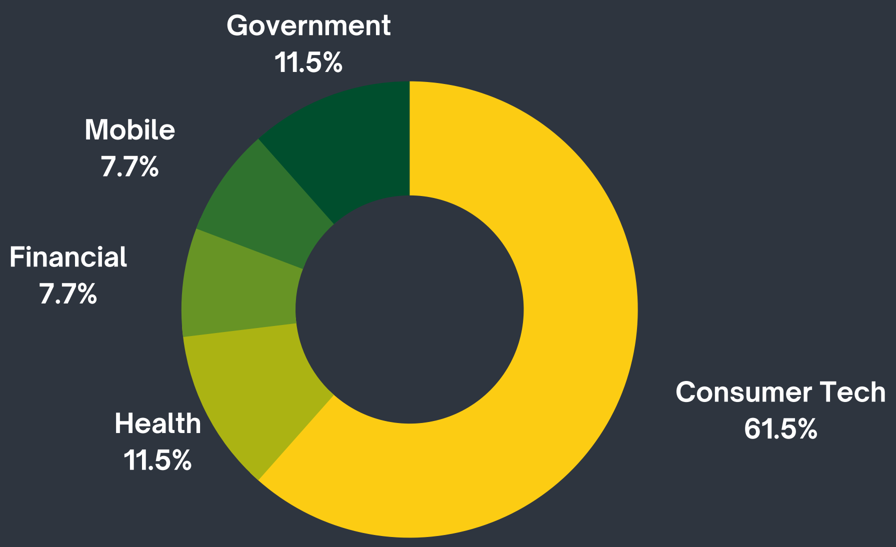
TYPES OF ATTACK VECTORS

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

- Travis CI Flaw Exposed Secrets From Public Repositories
- Microsoft asks Azure Linux admins to manually patch OMIGOD bugs
- Malicious Actor Discloses FortiGate SSL-VPN Credentials
- GitHub finds 7 code execution vulnerabilities in 'tar' and npm CLI
- Hacker-made Linux Cobalt Strike beacon used in ongoing attacks
- Google patches 10th Chrome zero-day exploited in the wild this year
- New Zloader attacks disable Windows Defender to evade detection
- Microsoft: Windows MSHTML bug now exploited by ransomware gangs
- New Windows security updates break network printing
- FBI and CISA warn of state hackers exploiting critical Zoho bug
- VMware security warning: Multiple vulnerabilities in vCenter Server could allow remote network access
- Epik hack exposes lax security practices at controversial web host
- Millions of HP OMEN gaming PCs impacted by driver vulnerability
- New macOS zero-day bug lets attackers run commands remotely
- Netgear fixes dangerous code execution bug in multiple routers
- Microsoft Exchange Autodiscover bugs leak 100K Windows credentials

FINANCIAL

- New "Elon Musk Club" crypto giveaway scam promoted via email
- Cryptocurrency miner is exploiting the new Confluence remote code execution bug

LATEST THREAT ENTRIES

GOVERNMENT

- MyRepublic discloses data breach exposing government ID cards
- Personal Details of 8,700 French Visa Applicants Exposed by Cyber-Attack
- United Nations Says Attackers Breached Its Systems

HEALTH

- BlackMatter ransomware hits medical technology giant Olympus
- Hacker steals 40,000 patients' data from kidney hospital
- Arizona Medical Practice Permanently Loses EHR Data

MOBILE

- Apple fixes iOS zero-day used to deploy NSO iPhone spyware
- New iCloud Private Relay service leaks users' true IP addresses, researcher claims

TOOL OF THE DAY

- LYNIS
- VULSCAN
- GRAPEFRUIT

CYBERMONDAY

- World Policies to strengthen individual country's cyber security could lead to connected & disconnected moments.
- What is the purpose of a Cybersecurity Audit?
- If you think technology can solve your security problems; then you don't understand the problems and the technology.

BLOG OF THE MONTH

- HOW CAN THE OWASP DEPENDENCY TRACKER BE USED TO IMPROVE THE APPLICATION?

CONSUMER TECH

Travis CI Flaw Exposed Secrets From Public Repositories

Travis CI, a Berlin-based continuous integration vendor, has patched a serious flaw that exposed signing keys, API keys and access credentials, potentially putting thousands of organizations at risk. The vulnerability, which was discovered by Felix Lange, was reported to Travis CI on September 7th, Szilágyi tweeted. Travis CI says it began patching the issue on September 3rd, which would indicate it had picked up on the problem before it was notified, but the timeline isn't clear. The effects of the vulnerability meant that if a public repository was forked, someone could file a pull request and then get access to the secrets attached to the original public repository, according to Travis CI's explanation.

🔗 Attack Type Data Breach | Cause of Issue Lack Of Data Protection Policies & Methodologies | Type of Loss Sensitive API Keys

Microsoft asks Azure Linux admins to manually patch OMIGOD bugs

Microsoft has issued additional guidance on securing Azure Linux machines impacted by recently addressed critical OMIGOD vulnerabilities. The four security flaws (allowing remote code execution and privilege escalation) were found in the Open Management Infrastructure (OMI) software agent silently installed on more than half of Azure instances. According to Wiz researchers Nir Ohfeld and Shir Tamari, these bugs impact thousands of Azure customers and millions of endpoints. OMIGOD affects Azure VMs who use Linux management solutions with services such as Azure Automation, Azure Automatic Update, Azure Operations Management Suite (OMS), Azure Log Analytics, Azure Configuration Management, or Azure Diagnostics. Successful exploitation enables attackers to escalate privileges and execute code remotely on compromised Linux VMs.

🔗 Attack Type Zero-Day Vulnerability (RCE) | Cause of Issue Improper Patch Management & Backup | Type of Loss PII Data

Malicious Actor Discloses FortiGate SSL-VPN Credentials

Fortinet has become aware that a malicious actor has recently disclosed SSL-VPN access information to 87,000 FortiGate SSL-VPN devices. These credentials were obtained from systems that remained unpatched against FG-IR-18-384 / CVE-2018-13379 at the time of the actor's scan. While they may have since been patched, if the passwords were not reset, they remain vulnerable. This incident is related to an old vulnerability resolved in May 2019. At that time, Fortinet issued a PSIRT advisory and communicated directly with customers. Later, Fortinet subsequently issued multiple corporate blog posts detailing this issue, strongly encouraging customers to upgrade affected devices. In addition to advisories, bulletins, and direct communications, these blogs were published in August 2019, July 2020, April 2021, and again in June 2021.

🔗 Attack Type Zero-Day Vulnerability | Cause of Issue Lack of Security Patch Management | Type of Loss Data Loss

GitHub finds 7 code execution vulnerabilities in 'tar' and npm CLI

MyRepublic Singapore has disclosed a data breach exposing the personal information of approximately 80,000 mobile subscribers. On September 9th, MyRepublic Singapore began emailing data breach notifications disclosing that customers' personal information was exposed after an unauthorized person gained access to a third-party data storage platform. MyRepublic states that the data storage has since been secured, but not before an unauthorized person had accessed the data of 79,388 mobile subscribers based in Singapore. The exposed data include identity verification documents for applications for mobile services, including For affected Singapore citizens, permanent residents, and employment and dependent pass holders – scanned copies of both sides of NRICs; For affected foreigners – proof of residential address documents e.g., scanned copies of a utility bill; and For affected customers porting an existing mobile service – name and mobile number. There is no indication that account or payment information was accessed as part of this incident.

🔗 Attack Type Zero-Day Vulnerability | Cause of Issue Lack of Secure Coding & Patch Management |
Type of Loss System Compromise

Hacker-made Linux Cobalt Strike beacon used in ongoing attacks

An unofficial Cobalt Strike Beacon Linux version made by unknown threat actors from scratch has been spotted by security researchers while actively used in attacks targeting organizations worldwide. Cobalt Strike is also used by threat actors (commonly dropped in ransomware attacks) for post-exploitation tasks after deploying so-called beacons, which provide persistent remote access to compromised devices. Over time, cracked copies of Cobalt Strike have been obtained and shared by threat actors, becoming one of the most common tools used in cyberattacks leading to data theft and ransomware. However, Cobalt Strike has always had a weakness – it only supports Windows devices and does not include Linux beacons.

🔗 Attack Type Malware Attack | Cause of Issue Lack of Malware Protection tools |
Type of Loss System compromise & Data Loss

Google patches 10th Chrome zero-day exploited in the wild this year

Google has released Chrome 93.0.4577.82 for Windows, Mac, and Linux to fix eleven security vulnerabilities, two of them being zero-days exploited in the wild. "Google is aware that exploits for CVE-2021-30632 and CVE-2021-30633 exist in the wild," the company revealed in the release notes for the new Chrome version. The two zero-day vulnerabilities fixed today were disclosed to Google on September 8th, 2021, and are both memory bugs. The CVE-2021-30632 is an out-of-bounds write in the V8 JavaScript engine, and the CVE-2021-30633 bug is a use-after-free bug in the Indexed DB API. While these bugs often lead to browser crashes, threat actors can sometimes exploit them to perform remote code execution, sandbox escapes, and other malicious behavior. While Google has disclosed that both bugs have been exploited in the wild, they have not shared further information regarding the attacks.

🔗 Attack Type Zero-Day Vulnerability | Cause of Issue Lack of Security Patch Management |
Type of Loss Browser Data Loss

New Zloader attacks disable Windows Defender to evade detection

An ongoing Zloader campaign uses a new infection chain to disable Microsoft Defender Antivirus (formerly Windows Defender) on victims' computers to evade detection. The attackers have also changed the malware delivery vector from spam or phishing emails to TeamViewer Google ads published through Google Adwords, redirecting the targets to fake download sites. From there, they are tricked into downloading signed and malicious MSI installers designed to install Zloader malware payloads on their computers. "The attack chain analyzed in this research shows how the complexity of the attack has grown in order to reach a higher level of stealthiness," said SentinelLabs security researchers Antonio Pirozzi and Antonio Cocomazzi in a report published today. "The first stage dropper has been changed from the classic malicious document to a stealthy, signed MSI payload. It uses backdoored binaries and a series of LOLBAS to impair defences and proxy the execution of their payloads.

🔗 Attack Type Malware Attack | Cause of Issue Lack of Secure Malware Protection & Patches | Type of Loss PII Data

Microsoft: Windows MSHTML bug now exploited by ransomware gangs

Microsoft says multiple threat actors, including ransomware affiliates, are targeting the recently patched Windows MSHTML remote code execution security flaw. In the wild exploitation of this vulnerability (tracked as CVE-2021-40444) began on August 18 according to the company, more than two weeks before Microsoft published a security advisory with a partial workaround. According to telemetry data analyzed by security analysts at the Microsoft 365 Defender Threat Intelligence Team and the Microsoft Threat Intelligence Center (MSTIC), the small number of initial attacks (less than 10) used maliciously crafted Office documents. These attacks targeted the CVE-2021-40444 bug as part of an initial access campaign that distributed custom Cobalt Strike Beacon loaders. Microsoft also observed a massive increase in exploitation attempts within 24 hours after the CVE-2021-40444 advisory was published.

🔗 Attack Type Zero-Day Vulnerability (RCE) | Cause of Issue Lack of Security Patch Management | Type of Loss PII Data

New Windows security updates break network printing

Windows administrators report wide-scale network printing problems after installing this week's September 2021 Patch Tuesday security updates. On September 14th, Microsoft released sixty security updates and fixes for numerous bugs as part of their monthly Patch Tuesday updates, including a fix for the last remaining PrintNightmare vulnerability tracked as CVE-2021-36958. This vulnerability is critical to fix as it is used by numerous ransomware gangs and threat actors to immediately gain SYSTEM privileges on vulnerable devices. However, many Windows system administrators are now reporting that their computers can no longer print to network printers after installing the PrintNightmare fixes on their print servers. In conversations with multiple Windows admins dealing with these issues, they all told BleepingComputer that the updates are breaking their network printing, and they can only fix them by removing the updates.

🔗 Attack Type Improper Security Update | Cause of Issue Improper Patch Management | Type of Loss Business & Reputation Loss

FBI and CISA warn of state hackers exploiting critical Zoho bug

The FBI, CISA, and the Coast Guard Cyber Command (CGCYBER) today warned that state-backed advanced persistent threat (APT) groups are actively exploiting a critical flaw in a Zoho single sign-on and password management solution since early August 2021. The vulnerability tracked as CVE-2021-40539 was found in the Zoho ManageEngine ADSelfService Plus software, and it allows attackers to take over vulnerable systems following successful exploitation. This joint security advisory follows a previous warning issued by CISA last week, also alerting CVE-2021-40539 in the wild attacks that could allow threat actors to execute malicious code remotely on compromised systems. The exploitation of ManageEngine ADSelfService Plus poses a serious risk to critical infrastructure companies, In incidents where CVE-2021-40539 exploits have been used, attackers have been observed deploying a JavaServer Pages (JSP) web shell camouflaged as an x509 certificate.

🔗 Attack Type Zero-Day Vulnerability | Cause of Issue Lack of Patch Management | Type of Loss PII Data

VMware security warning: Multiple vulnerabilities in vCenter Server could allow remote network access

Multiple critical security vulnerabilities in two VMware network administration tools that could allow an attacker to have full access to an organization's network have been patched. Users of the vCenter Server and Cloud Foundation products are urged to update immediately to protect against the issues, which are being tracked collectively as VMSA-2021-0020. The most critical issue (CVE-2021-22005) is a file upload vulnerability that can be used to execute commands and software on the vCenter Server Appliance. A security advisory issued on September 21st warns that the vulnerability can be used by anyone who can reach vCenter Server over the network to gain access, regardless of the configuration settings of vCenter Server.

🔗 Attack Type Zero-Day Vulnerability | Cause of Issue Lack of Security Patch Management | Type of Loss System Compromise & Data Loss

Epik hack exposes lax security practices at controversial web host

Hacktivists affiliated with Anonymous are pouring over the entrails of a cyber-attack against controversial web host Epik that led onto the leak of customer data. Anonymous hacked and defaced the Epik-hosted Republican Party of Texas on September 11th, following this up with an assault on Epik's infrastructure days later. Masses of stolen data from Epik were subsequentially released through the DDoSecrets organization. Hacktivists boasted of releasing a "decade's worth of data" in databases containing domain ownership records, transaction details, emails, and unsorted or at least unindexed, encryption keys among the 32GB trove of leaked data.

🔗 Attack Type Data Breach | Cause of Issue Lack Of Data Protection Policies & Methodologies | Type of Loss Data Loss

Millions of HP OMEN gaming PCs impacted by driver vulnerability

Millions of HP OMEN laptop and desktop gaming computers are exposed to attacks by a high severity vulnerability that can let threat actors trigger denial of service states or escalate privileges and disable security solutions. The security flaw (tracked as CVE-2021-3437) was found in a driver used by the OMEN Gaming Hub software that comes pre-installed on all HP OMEN desktops and laptops. CVE-2021-3437 is caused by HP's choice to use vulnerable code partially copied from WinRing0.sys, an open source driver, to build the HpPortIox64.sys driver the OMEN Gaming Hub software uses to read/write kernel memory, PCI configurations, IO ports, and Model-Specific Registers (MSRs).

🔗 Attack Type Zero-Day Vulnerability | Cause of Issue Lack of Security Patch Management |
Type of Loss PII Data & Reputation Loss

New macOS zero-day bug lets attackers run commands remotely

Security researchers disclosed today a new vulnerability in Apple's macOS Finder, which makes it possible for attackers to run commands on Macs running any macOS version up to the latest release, Big Sur. The bug, found by independent security researcher Park Minchan, is due to how macOS processes inetloc files, which inadvertently causes it to run any commands embedded by an attacker without any warnings or prompts.

🔗 Attack Type Zero-Day Vulnerability (RCE) | Cause of Issue Lack of Security Patch Management |
Type of Loss System Compromise

Netgear fixes dangerous code execution bug in multiple routers

Netgear has fixed a high severity remote code execution (RCE) vulnerability found in the Circle parental control service, which runs with root permissions on almost a dozen modern Small Offices/Home Offices (SOHO) Netgear routers. While one would expect the attack vector exposed by Circle security flaw (tracked as CVE-2021-40847) would be removed after the service is stopped, the Circle update daemon containing the bug is enabled by default and it can be exploited even if the service is disabled.

🔗 Attack Type Zero-Day Vulnerability (RCE) | Cause of Issue Lack of Security Patch Management |
Type of Loss Network Device Compromise

Microsoft Exchange Autodiscover bugs leak 100K Windows credentials

Bugs in the implementation of Microsoft Exchange's Autodiscover feature have leaked approximately 100,000 login names and passwords for Windows domains worldwide. In a new report by Amit Serper, Guardicore's AVP of Security Research, the researcher reveals how the incorrect implementation of the Autodiscover protocol, rather than a bug in Microsoft Exchange, is causing Windows credentials to be sent to third-party untrusted websites.

🔗 Attack Type Data Breach | Cause of Issue Lack Of Data Protection Policies & Methodologies |
Type of Loss PII Data

FINANCIAL

New "Elon Musk Club" crypto giveaway scam promoted via email

A new Elon Musk-themed cryptocurrency giveaway scam called the "Elon Musk Mutual Aid Fund" or "Elon Musk Club" is being promoted through spam email campaigns that started over the past few weeks. While most cryptocurrency scams target social media users, scammers now use email spam to promote a new "Elon Musk Club" or "Elon Musk Mutual Aid Fund" giveaway. The https://msto.me/elonmusk/ site will pretend to be an "Elon Musk - Mutual aid fund" that promises to send 0.001 to 0.055 bitcoins to all users who participate. However, the bitcoin addresses are owned by the scammers who take your donation but do not send anything in return. While the scammers have only earned ~$3,661 from the two addresses, many other bitcoin addresses are likely used in this scam.

🔗 Attack Type Social Engineering | Cause of Issue Lack Of Security Awareness | Type of Loss Financial Loss

Cryptocurrency miner is exploiting the new Confluence remote code execution bug

The z0Miner cryptojacker is now weaponizing a new Confluence vulnerability to mine for cryptocurrency on vulnerable machines. Trend Micro researchers said on September 21st that the cryptocurrency mining malware is now exploiting a recently-disclosed Atlassian Confluence remote code execution (RCE) vulnerability, which was only made public in August this year. Tracked as CVE-2021-26084, the vulnerability impacts Confluence server versions 6.6.0, 6.13.0, 7.4.0, and 7.12.0. Issued a CVSS severity score of 9.8, the critical security flaw is an Object-Graph Navigation Language (ONGL) injection vulnerability that can be exploited to trigger RCE -- and is known to be actively exploited in the wild.

🔗 Attack Type Malware Attack | Cause of Issue Lack of Malware Protection Tools | Type of Loss System Compromise

GOVERNMENT

MyRepublic discloses data breach exposing government ID cards

MyRepublic Singapore has disclosed a data breach exposing the personal information of approximately 80,000 mobile subscribers. On September 9th, MyRepublic Singapore began emailing data breach notifications disclosing that customers' personal information was exposed after an unauthorized person gained access to a third-party data storage platform. MyRepublic states that the data storage has since been secured, but not before an unauthorized person had accessed the data of 79,388 mobile subscribers based in Singapore. The exposed data include identity verification documents for applications for mobile services, including: For affected Singapore citizens, permanent residents, and employment and dependent pass holders — scanned copies of both sides of NRICs; For affected foreigners — proof of residential address documents e.g., scanned copies of a utility bill; and For affected customers porting an existing mobile service — name and mobile number. There is no indication that account or payment information was accessed as part of this incident.

🔗 Attack Type Data Breach | Cause of Issue Lack Of Data Protection Policies & Methodologies | Type of Loss User Data Loss & Reputation Loss

Personal Details of 8,700 French Visa Applicants Exposed by Cyber-Attack

A cyber-attack has compromised the data of around 8700 people applying for French visas via the France-Visas website. The French Ministry of Foreign Affairs and the Ministry of the Interior announced on Friday (August 3) that the cyber-attack targeted a section of the site, which receives around 1.5 million applications per month. In a statement, the ministries claimed that the attack had "been quickly neutralized," but personal details — including names, passport and identity card numbers, nationalities and dates of birth — had been leaked.

🔗 Attack Type Data Breach | Cause of Issue Lack Of Data Protection Policies & Methodologies | Type of Loss PII Data

United Nations Says Attackers Breached Its Systems

The United Nations says that its networks were accessed by intruders earlier this year, leading to follow-on intrusions. One cybercrime analyst reports that he'd alerted NATO after seeing access credentials for one of its enterprise resource planning software systems being offered for sale via the cybercrime underground. "Unknown attackers were able to breach parts of the United Nations infrastructure in April," the U.N. says. Although the U.N. says the intrusion occurred in April, the initial access appears to date back to at least February, Holden says, based on when a threat actor privately offered for sale access credentials to Umoja, which is the U.N.'s enterprise resource planning software.

🔗 Attack Type Data Theft | Cause of Issue Lack Of Data Protection Policies & Methodologies | Type of Loss System Compromise

HEALTH

BlackMatter ransomware hits medical technology giant Olympus

Olympus, a leading medical technology company, is investigating a "potential cybersecurity incident" that impacted some of its EMEA (Europe, Middle East, Africa) IT systems. While Olympus did not share any details on the attackers' identity, ransom notes left on systems impacted during the breach point to a BlackMatter ransomware attack were reported. The same ransom notes also point to a Tor website the BlackMatter gang has used in the past to communicate with victims. BlackMatter is a relatively new ransomware operation that surfaced at the end of July 2021 and was initially believed to be a rebrand of DarkSide ransomware. From samples collected by researchers after some of their subsequent attacks, it was later confirmed that BlackMatter ransomware's encryption routines were the same custom and unique ones that DarkSide used.

🔗 Attack Type Malware Attack (Ransomware) | Cause of Issue Lack of Malware Protection Tools |
Type of Loss System compromise & PII data loss

Hacker steals 40,000 patients' data from kidney hospital

The personal details of more than 40,000 patients at Bhumirajanagarindra Kidney Institute Hospital have been stolen by a hacker. The stolen data included patients' personal information and treatment history. Dr Thirachai, Director of the Hospital said a man speaking in English called the hospital later on Monday claiming he had hacked the system. He said he would call again on Tuesday to arrange payment in exchange for returning the information.

🔗 Attack Type Data Breach | Cause of Issue Lack Of Data Protection Policies & Methodologies |
Type of Loss Loss of Health Records

Arizona Medical Practice Permanently Loses EHR Data

A medical practice in Arizona has lost nearly all the data entered into its electronic health record (EHR) system due to a cyber-attack. Desert Wells Family Medicine, which has been serving patients in Queens Creek for 20 years, was attacked by cyber-criminals on May 21. The practice had backed up all its EHR data before the attack took place, but the attackers managed to encrypt both the original files and the backup files using ransomware. The practice has begun notifying 35,000 patients that their protected health information has been compromised. Information that attackers may have accessed during the security incident included patient names, dates of birth, addresses and billing account numbers. Personal information also included medical record numbers, treatment information and Social Security numbers. All EHR information added into Desert Wells' system prior to the attack has been lost forever, and the practice is currently constructing an entirely new EHR system.

🔗 Attack Type Data Breach | Cause of Issue Lack Of Data Protection Policies & Methodologies |
Type of Loss Loss of Health Records

MOBILE

Apple fixes iOS zero-day used to deploy NSO iPhone spyware

Apple has released security updates to fix two zero-day vulnerabilities that have been seen exploited in the wild to attack iPhones and Macs. One is known to be used to install the Pegasus spyware on iPhones. The vulnerabilities are tracked as CVE-2021-30860 and CVE-2021-30858, and both allow maliciously crafted documents to execute commands when opened on vulnerable devices. The CVE-2021-30860 CoreGraphics vulnerability is an integer overflow bug discovered by Citizen Lab that allows threat actors to create malicious PDF documents that execute commands when opened in iOS and macOS. CVE-2021-30858 is a WebKit use after free vulnerability allowing hackers to create maliciously crafted web page that execute commands when visiting them on iPhones and macOS. Apple states that this vulnerability was disclosed anonymously.

🔗 Attack Type Zero-Day Vulnerability (RCE) | Cause of Issue Lack of Security Patch Management | Type of Loss PII Data

New iCloud Private Relay service leaks users' true IP addresses, researcher claims

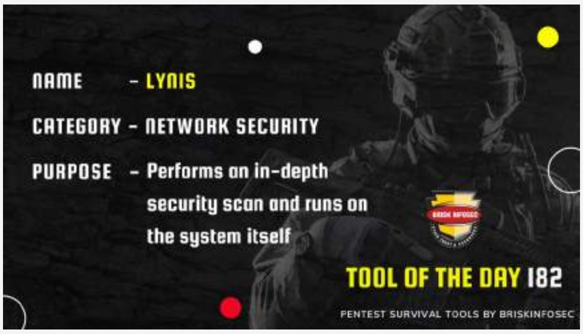
An as-yet-unpatched vulnerability in Apple's new iCloud Private Relay service for iOS 15 means it can leak users' true IP addresses, a security researcher has claimed. a security researcher has discovered that it can leak IP addresses through WebRTC, a browser API that allows websites to establish direct communication between website visitors – and which has been associated with similar weaknesses in other browsers in the past. WebRTC sets up communications by using the ICE (interactive connectivity establishment) framework. This involves collecting 'ICE candidates' that include the IP address or domain name, port, protocol, and other information. The browser will then return the ICE candidates to the browser application. However, writes Sergey Mostsevenko, a researcher and developer at browser fingerprinting library FingerprintJS, Safari is passing ICE candidates containing real IP addresses to the JavaScript environment.

🔗 Attack Type Zero-Day Vulnerability | Cause of Issue Lack of Security Patch Management | Type of Loss PII Data

TOOLS OF THE MONTH

LYNIS

Lynis is a security auditing tool for systems based on UNIX like Linux, macOS, BSD, and others. It performs an in-depth security scan and runs on the system itself. The primary goal is to test security defences and provide tips for further system hardening. It will also scan for general system information, vulnerable software packages, and possible configuration issues. Lynis was commonly used by system administrators and auditors to assess the security defences of their systems.



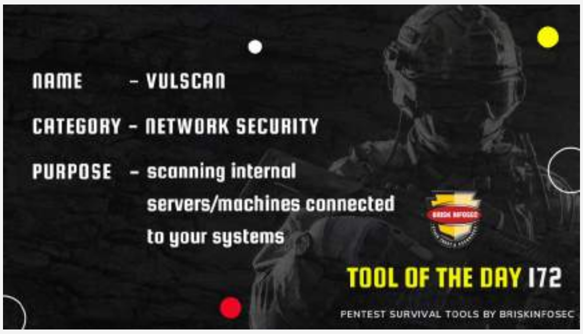
NAME - LYNIS
CATEGORY - NETWORK SECURITY
PURPOSE - Performs an in-depth security scan and runs on the system itself

TOOL OF THE DAY 182

PENTEST SURVIVAL TOOLS BY BRISKINFOSEC

VULSCAN

Vulscan is a module that enhances nmap to a vulnerability scanner. The nmap option -sV enables version detection per service which is used to determine potential flaws according to the identified product. The data is looked up in an offline version of VulDB



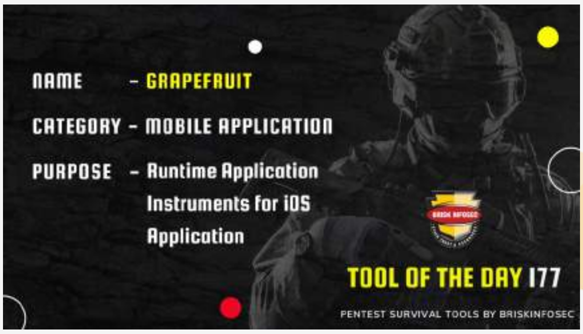
NAME - VULSCAN
CATEGORY - NETWORK SECURITY
PURPOSE - scanning internal servers/machines connected to your systems

TOOL OF THE DAY 172

PENTEST SURVIVAL TOOLS BY BRISKINFOSEC

GRAPEFRUIT

Grapefruit is a runtime Application Instruments for iOS applications and previously it was known by passionfruit. It is used in runtime analysis, which can able to get iOS app details like binary information, listing classes, methods, browsing application's files in real-time, etc..



NAME - GRAPEFRUIT
CATEGORY - MOBILE APPLICATION
PURPOSE - Runtime Application Instruments for iOS Application

TOOL OF THE DAY 177

PENTEST SURVIVAL TOOLS BY BRISKINFOSEC

CYBERMONDAY

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.

HAPPY
CYBER
MONDAY
AN INITIATIVE BY BRISKINFOSEC
World Policies to strengthen Individual Country's Cybersecurity could lead to Connected & Disconnected moments.
Team - Briskinfosec
www.briskinfosec.com

What is the purpose of a Cybersecurity Audit?

A cybersecurity audit serves as a 'checklist' to ensure that the policies stated by a cybersecurity team are currently in effect and that there are control structures in place to implement them.

HAPPY
CYBER
MONDAY
AN INITIATIVE BY BRISKINFOSEC
WHAT IS THE PURPOSE OF CYBERSECURITY AUDIT?
ENSURE THAT THE SECURITY REQUIREMENTS CONTROLS ARE DERIVED, TESTED AND OPERATING EFFECTIVELY.
Team - Briskinfosec
www.briskinfosec.com

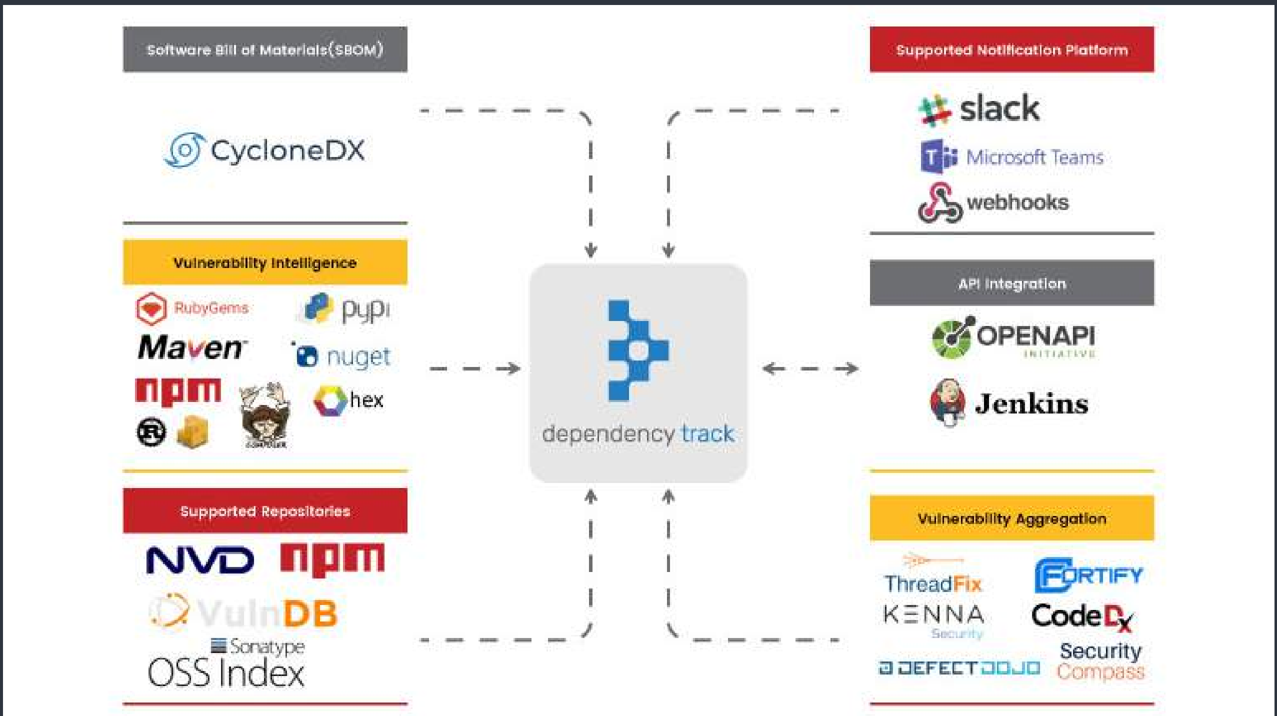
If you think technology can solve your security problems; then you don't understand the problems and the technology.

Simply put, not all security problems are caused by technology. As a result, technology cannot solve the problems. There are several factors that contribute to the nature of a security issue. Some examples include human errors, negligence, complex coding, insider misuse, and so on. For all of these reasons, technology may be a band-aid rather than a panacea.

HAPPY
CYBER
MONDAY
“ IF YOU THINK TECHNOLOGY CAN SOLVE YOUR SECURITY PROBLEMS, THEN YOU DON'T UNDERSTAND THE PROBLEMS AND THE TECHNOLOGY ”
Bruce Schneier
www.briskinfosec.com

BLOG OF THE MONTH

HOW CAN THE OWASP DEPENDENCY TRACKER BE USED TO IMPROVE THE APPLICATION?



Dependency Track is a free, open-source continuous component analysis platform that helps businesses discover and mitigate supply chain risk. In addition, the software keeps track of the vulnerabilities associated with the libraries in the portfolio, as well as their versions, to decide whether the library is outdated, deprecated, or current. Currently, the OWASP Dependency-Check supports five programming languages. Java and.NET are fully supported, with Ruby, Node.js, and Python receiving experimental support

Read More about Sanju Thomas's Insight on OWASP Dependency Tracker: https://www.briskinfosec.com/blogs/blogsdetail/HOW-CAN-THE-OWASP-DEPENDENCY-TRACKER-BE-USED-TO-IMPROVE-THE-APPLICATION-SECURITY-LIFECYCLE-

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

Partner Offices

Urbansoft,
Manama Center, Entrance One,
Building No.58, No.316,
Government Road, Manama
Area, 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