Threatsploit

Adversary Report

Edition 44

APRIL -2022

"A breach alone is not a disaster, but mishandling it is"

www.briskinfosec.com

Introduction

No technology that is connected to the internet is unhacakable- Cyber Sophia

It's true, as Cyber Sophia points out. On the internet, there is no such thing as a 100% safety. There is no such thing as total security, and no one can claim to have it. It's all about making the life of the hacker more difficult by increasing the number of levels of security. For this month, we'll be highlighting newsworthy events that affect both you and us.

For those who want to construct websites, Wordpress has proven an excellent platform. But,vulnerabilities have been reported that are 150 times greater than those predicted for 2020 over the last several years, however. Please read this if you use Wordpress. This month's headlines feature a "browser on browser" attack. Last month our colleague was directed to a fake SBI site after clicking on a phishing link. On our LinkedIn page, we've released a video of the same. For GPU enthusiasts, Nvidia is a household name. However, we just learned of their ransomware-enabled incarceration and subsequent demand that the GPUs be made open source earlier last month.

The FBI claimed that RagnarLocker, which first appeared on the cyber world two years ago, is still a problem for many. The continuous conflict between Russia and Ukraine made the news. The Ukrainian Internet Service Provider (ISP) was taken down by Russian hackers. It had a profound effect on everyone, military personnel included. Another attack that surprised the world was a deep fake of Ukraine's president that was extremely detailed . His speech to the parliament is shown in this fake video, in which he makes critical decisions, including surrender. It was taken down once it was discovered to be a hoax. Fake footage is causing a lot of confusion.

We've got everything together for your understanding. "Why third-party maturity audit is a necessary for firms purchasing cybersecurity products?" was a topic we discussed on LinkedIn live last week. We are posting the hyperlink here.

We've done everything we possibly can to ensure that you get the most out of your time spent here. Please feel free to distribute this issue to any of your coworkers, friends, or partners who could benefit from it. We hope you have a safe and enjoyable month of surfing the web.

There are only 2 types of companies in the world
Those that have been breached and know it
and
Those that have been breached and don't know it

Ted Schlein

Contents

Government agencies in Ukraine targeted in cyber-attacks deploying MicroBackdoor malware

A cyber-attack campaign targeting Ukrainian government agencies with MicroBackdoor malware has been confirmed by the country's Computer Emergency Response Team (CERT-UA).According to intelligence gathered by the agency, phishing emails containing a file named 'dovidka.zip', which contains a contextual help file (Microsoft Compiled HTML Help) 'dovidka.chm'.The file contained the bait image 'image.jpg', which CERT-UA said was information on the procedure for frequent artillery shelling, and HTA-file 'file.htm' which contained malicious code in VBScript.Execution of the malicious code would result in the running of the dropper 'ignit.vbs', which will decode the .NET loader 'core.dll', later executing the MicroBackdoor malware.According to CERT-UA, the backdoor and loader were created in January 2022, before Russia's invasion of the country.The agency claims that malware campaign bares similarities to the activities of the UAC-0051 threat group, also known as 'unc1151', which according to Mandiant has links to the Belarussian government.

The statement from CERT-UA contains further information on the attack.Although primarily directed towards Ukraine, the newly named 'HermeticWiper' malware strain has also been detected in the Baltic states of Latvia and Lithuania.Date stamps on the malware indicate that it was compiled two months ago – evidence that the attack was possibly premeditated.At least 30 Ukrainian university websites were also hacked in a targeted attack allegedly conducted by threat actors identified as the 'Monday Group', which has reportedly publicly supported Russia's recent actions.The group, whose members refer to themselves as 'the Mx0nday', have targeted the WordPress-hosted sites more than 100,000 times since the invasion.

Attack Type	Cause of Issue	Domain
Cyber Attack	**Remote Command Execution**	**Government Sector**

Stats widget hacked in attempt to breach Russian government agency websites

"Russian authorities claim they quickly thwarted a cyber-attack that sought to compromise government websites via a hacked statistics widget.The software, developed by the Russian Ministry of Economic Development and built into the websites of several state-run agencies, Tthis allowed unidentified hackers to ''publish incorrect content on the pages of the websites'', a representative of Russia's communications agency told official news agency Interfax.Interfax reports that the compromised websites included those maintained by the ''Russian Federal Penitentiary Service, the Federal Bailiff Service, the Federal Antimonopoly Service, the Culture Ministry, the Energy Ministry, the Federal State Statistics Service, and a number of other agencies''.Days after Russia invaded Ukraine, a destructive wiper malware strain – dubbed 'HermeticWiper' – was unleashed.The malware – first spotted by independent security researchers MalwareHunterTeam at the start of March, is written in the .NET programming language and spreads as a worm by copying itself under the file name 'Россия-Украина_Война-Обновление.doc[dot]exe' ('Russia-Ukraine_War-Update.doc[dot]exe').The note was originally written in Bengalese. These and other factors have allowed Trend Micro to speculate that the author is a native of western India who has developed other strains of malware previously linked to cryptocurrency mining''.

Attack Type	Cause of Issue	Domain
Cyber Attack	**Websites Breach**	**Government Sector**

Israeli government websites temporarily knocked offline by ‘massive’ cyber-attack

A “massive” cyber-attack knocked several Israeli government websites offline.The incident was confirmed online by the Israel National Cyber Directorate, which said that a DDoS attack denied access to services “for a short time”.Unconfirmed reports allege that Iran’s Islamic Revolutionary Guard Corps has claimed responsibility for what’s being labeled as a “massive” cyber-attack.Local media also quoted Communications Minister Yoaz Hendel as stating that sites with gov.il extensions were unable to be reached for at least an hour. All sites are now reported to be back online.

Attack Type	Cause of Issue	Domain
DDOS Attack	**Data Breach**	**Government Sector**

Published Zelenskyy Deepfake Video Demonstrates the Modern War is Online

The video uploaded to a hacked Ukrainian news website shows how far the technology has come, how it can be used in social engineering, as well as how the tech still needs to improve.While much of the headlines today around the Russian invasion of Ukraine focus on the war on the ground and in the air, behind the scenes, a cyberwar is being waged. It began with wiper ransomware attacks on Ukrainian businesses and government agencies, and has culminated so far with a newly released deepfake video of Ukrainian president Zelenskyy asking his troops to lay down their weapons and surrender.At face value, the deepfake looks pretty good, but if one is paying attention, it becomes obvious this isn’t the real president and the video can be seen for what it truly is. The use of cyberattacks – whether based on malware, social engineering, or both – is the new front lines of modern warfare. Yesterday, the White House even put out a statement about how both government and private sector businesses should harden their cyberdefenses immediately in light of possible cyberattacks from Russia.And because the modern war is online, no business within a targeted country is safe – that’s not FUD; that’s fact. We’ve historically seen cyberattacks executed in both a random spray using millions of email addresses, as well as precision-targeted attacks on specific people within one organization – and everything in between.The deepfake video also shows how cyberattackers will use the most credible and effective means to get targeted victims of an attack to take the desired action – whether it’s laying down a weapon, clicking a link, or opening at attachment; each one can have devastating results in their own right.

Attack Type	Cause of Issue	Domain
Social Engineering Attack	**Loss of Reputation**	**Government Sector**

"Prison service for England and Wales recorded more than 2,000 data breaches over 12 months"

The UK Ministry of Justice (MoJ) has defended its data protection practices following allegations it failed to support an employee affected by a data breach of an MoJ service.The employee's sensitive personal data was apparently exposed because of unauthorized access gained to the Justice Academy, an online learning and careers platform used by MoJ and other public sector staff.These claims were documented in a blog post published by CEL Solicitors, a UK law firm representing the employee.CEL Solicitors also revealed that Her Majesty's Prison and Probation Service (HMPPS), part of the MoJ, recorded 2,152 data breaches in the 12 months up to September 2021.One of the breaches was sufficiently serious to be reported to the Information Commissioner's Office (ICO), according to a response from the MoJ, issued in October 2021, to a Freedom of Information Act (FOIA) request.HMPPS runs prisons in England and Wales and has more than 58,000 full-time staff.The MoJ's latest Annual Report and Accounts (PDF) revealed that 16 data security incidents were identified across the government department during 2020 and 2021 were reported to the ICO.

These improvements include notifying anyone potentially affected by breaches via the MoJ's "intranet and other internal communication channels", an enhanced process for processing data breach compensation claims, and the involvement of unions to ensure affected staff are supported.CEL Solicitors said having a robust data protection regime was particularly vital in the context of environments like HMPPS, where "employees are working with and around dangerous individuals" and are already "at increased risk of being blackmailed and personally targeted by criminal groups".

Attack Type	Cause of Issue	Domain
Cyber Attack	**2,000Data Breach**	**Government Sector**

Unpatched plugins threaten millions of WordPress websites

A year-on-year surge has been observed in the number of security vulnerabilities found in the WordPress ecosystem.The number of flaws reported in plugins and themes for WordPress was 150% higher in 2021 than in 2020, according to researchers at WordPress security firm Patchstack. As many as 29% of critical vulnerabilities were never patched.WordPress powers just over 40% of all websites, but bugs in plugins and themes can render those sites vulnerable to SQL injection, arbitrary file upload, remote code execution (RCE) or privilege escalation attacks, among others.Patchstack's State of WordPress Security report found that relatively few vulnerabilities affected WordPress core, which accounted for just 0.58% of WordPress security bugs in 2021. The problem instead lies in the profusion of third-party add-ons that broaden the platform's functionality and appeal.Patchstack gathered data from some 50,000 websites that use its own WordPress security tool.Researchers found more than 50 critical vulnerabilities in themes and 35 in plugins. Alarmingly, two of the vulnerabilities were in plugins found in more than one million websites.The researchers found that 12.4% of WordPress theme vulnerabilities had a CVSS score of between 9 and 10, the maximum severity. The most serious flaw was an arbitrary file upload bug threatening full site compromise. This affected 10 themes.

Attack Type	Cause of Issue	Domain
SQL Injection	**Wordpress Websites**	**Content Management System**

Google WAF bypassed via oversized POST requests

Security limitations in the default protection offered by Google's web application firewall (WAF) make it possible to bypass the company's cloud-based defenses.Researchers at security consultancy Kloudle found they were able to bypass both Google Cloud Platform (GCP) and Amazon Web Services (AWS) web app firewalls just by making a POST request more than 8KB in size.WAFs are supposed to protect against web-based attacks including SQL Injection and cross-site scripting – even in cases where an underlying application is still vulnerable.Bypassing this protection would take a potential attacker one step closer to attacking a web-hosted application, provided a targeted endpoint accepts HTTP POST requests "in a manner which could trigger an underlying vulnerability".“This issue can be exploited by crafting an HTTP POST request with a body size exceeding the 8KB size limitation of Cloud Armor, where the payload appears after the 8192th byte/character in the request body," The Cloud Armor WAF from Google comes with a set of preconfigured firewall rules that draw from the open source OWASP ModSecurity Core Rule Set.Users can block the potential attack vector by configuring a custom Cloud Armor rule to block HTTP requests where the request body is larger than 8192 bytes – a general rule that can be further tweaked to accept defined exceptions.

Attack Type	Cause of Issue	Domain
WAF Attack	**Data Compromise**	**Cloud Platform**

"Exploit chain allows security researchers to compromise Pascom phone systems"

Security researchers have been able to chain together three separate vulnerabilities to achieve the complete compromise of Pascom's Cloud Phone System.Full pre-authenticated remote code execution (RCE) on the business-focused Voice over IP (VoIP) and more general communication platform was achieved by Daniel Eshetu of Ethiopian infosec firm Kerbit by combining a trio of less serious security flaws.The three components of the successful exploit were made up from a path traversal vulnerability, a server side request forgery (SSRF) flaw in an external piece of software, and a post-authentication RCE issue.All three bugs have been patched in 7.20.x versions of Passcom's Cloud Phone System, released in January, long before Kerbit published its findingsBusinesses using cloud-based versions of the technology were automatically updatedThe SSRF problem stemmed from an outdated Openfire (XMPP server) jar that was vulnerable to a flaw tracked as CVE-2021-45967. This tracks back to a vulnerability discovered around three years ago, CVE-2019-18394, involving Openfire's technology.

Attack Type	Cause of Issue	Domain
Server Side Request Forgery	**VOIP Device Compromised**	**Digital Communication**

Data breach at US heart disease treatment center impacts 287,000 individuals

A data breach at US health clinic South Denver Cardiology Associates (SDCA) has exposed the medical information of more than 287,000 people.In a data breach notice (PDF), SDCA admitted that an unnamed attacker broke into its systems and had access to confidential databases for three days between January 2, 2022, and January 5, 2022, before the breach was detected and thwarted.This investigation revealed that attackers accessed files containing a variety of sensitive information.The exposed data included “patients’ names, dates of birth, Social Security numbers and/or drivers’ license numbers, patient account numbers, health insurance information, and clinical information, such as physician names, dates and types of service, and diagnoses”. a bid to reassure potential concerned patients, SDCA said there has been “no impact to the contents of patient medical records and no unauthorized access to the patient portal”.Despite these assurances, the exposed healthcare and other personal data leaves affected parties more exposed to phishing attacks and the like, leveraging the compromised information to run more convincing scams.As a precaution, SDCA has begun a mailout to patients that includes guidance on how to protect their information alongside an offer of complimentary credit monitoring and identity protection services. SDCA has also set up a dedicated, toll-free call center to answer patients’ questions.

Attack Type
Cross Site Request Forgery

Cause of Issue
Data Breach

Domain
Healthcare

Apple Safari empowers developers to mitigate web flaws with WebKit CSP enhancements

"Apple has added a raft of new features to WebKit, including improved support for Content Security Policy (CSP) Level 3, with the latest release of Safari version 15.4.This, say the developers, gives enhanced security control over the loading of content, and helps web developers to mitigate the risks of cross-site scripting (XSS) and other vulnerabilities.Blocked resource violation reporting for inline script, inline style, and eval execution has been updated to match web standards too.“This is critical for developers who want to mitigate XSS, one of the most prominent web vulnerabilities, using a CSP based on nonces or hashes instead of an allowlist-based CSP, which our research has shown can be trivially bypassed in more than 90% of cases when it comes to XSS mitigation,” “Google is protecting over 80% of its sensitive web traffic with a strict nonce-based CSP, and has mitigated a large number of XSS vulnerabilities this way. Now we can also protect our users on Safari and iOS where all browsers are using WebKit as a rendering engine.”Meanwhile, there’s also support for ‘unsafe-hashes’, allowing inline event handlers to be hashed in the same way as CSP hashes allow hashing of inline scripts.With the new release, developers can also safely include external JavaScript in their pages using new support for hash source expressions.And finally, support has been removed for the XSS Auditor, which, say the developers, has been superseded by modern cross-origin defenses like CSP and COEP."

Attack Type
Cross Site Scripting

Domain
Apple Technologies

NPM maintainer targets Russian users with data-wiping ‘protestware’

A maintainer who sabotaged a popular NPM package in protest at Russia’s invasion of Ukraine has been criticised for undermining trust in the open source ecosystem.If developers download the poisoned package and are geo-located in either Russia or Belarus, the malware wipes file contents and replaces them with a heart emoji. It also adds a WITH-LOVE-FROM-AMERICA.txt file containing a peace message onto the user’s desktop directory.The malware and NPM package, called ‘peacenotwar’, affected users of popular frontend JavaScript framework Vue.js, since node-ipc is a nested dependency for Vue.js’s command line tool, Vue.js CLI.Several developers also criticised the package sabotage on a related GitHub thread, in which RIAEvangelist responded that “you are free to lock your dependency to a version that does not include this”. They added that it “should serve as a safe example of why we teams should use explicit dependency versions. So it is always our choice to upgrade or not”. RIAEvangelist maintains more than 40 NPM packages in total, together accounting for several million weekly downloads. RIAEvangelist published peacenotwar on March 8 with the source-code description : “This code serves as a non-destructive example of why controlling your node modules is important. It also serves as a non-violent protest against Russia's aggression that threatens the world right now. This module will add a message of peace on your users’ desktops, and it will only do it if it does not already exist just to be polite.”Peacenotwar began accruing downloads when the module became a dependency to node-ipc, an inter-process communication module that is downloaded more than one million times a week.

Attack Type	Cause of Issue	Domain
Malware Attack	**File Contents**	**Government Sector**

Nvidia hackers allegedly attempting to blackmail company into open-sourcing GPU drivers

" Attackers responsible for the recent hack of chipmaker Nvidia have apparently attempted to blackmail the company into open-sourcing its graphics processing unit (GPU) drivers.According to screenshots circulating on social media, the Lapsus$ ransomware gang that claimed responsibility for the attack is now threatening to leak files related to Nvidia’s GPUs if the company fails to comply with its request.“On February 23, 2022, NVIDIA became aware of a cybersecurity incident which impacted IT resources. Shortly after discovering the incident, we further hardened our network, engaged cybersecurity incident response experts, and notified law enforcement. “We have no evidence of ransomware being deployed on the NVIDIA environment or that this is related to the Russia-Ukraine conflict. However, we are aware that the threat actor took employee credentials and some NVIDIA proprietary information from our systems and has begun leaking it online. Our team is working to analyze that information. We do not anticipate any disruption to our business or our ability to serve our customers as a result of the incident. While generally condemning the hackers’ actions, numerous messages on Reddit suggested that if Nvidia acceded to its demands it would at least result in enhanced Linux support for its drivers."

Attack Type	Cause of Issue	Domain
Ransomeware Attack	**Files Leakage**	**Nvidia Company**

RagnarLocker ransomware struck 52 critical infrastructure entities within two years – FBI

The FBI says it has identified at least 52 critical infrastructure entities infected by RagnarLocker ransomware since it arrived on the cybercrime scene nearly two years ago.RagnarLocker threat actors and variants have impacted organizations operating in 10 sectors classified as critical infrastructure, including energy, financial services, government, information technology, and vital manufacturing operations, said the US law enforcement agency.The law enforcement agency noted how RagnarLocker uses the Windows API GetLocaleInfoW to identify the location of an infected machine, in order to halt potential attacks against organizations operating in Russia, Ukraine, Azerbaijan, Armenia, Belarus, Kazakhstan, Kyrgyzstan, Kyrgyz, Moldova, Tajikstan, Turkmenistan, Uzbekistan, and Georgia.While the malware itself curtails attacks in countries within Russia's sphere of influence, Tim Erlin, vice president of strategy at cybersecurity software company Tripwire, said "it's a mistake to conflate the tool used with the actor executing that tool.RagnarLocker favors the in-vogue 'double extortion' tactic, where in addition to the inducement of decrypting compromised data, attackers also threaten to leak sensitive information if ransom demands are not met.The FBI noted that "instead of choosing which files to encrypt, RagnarLocker chooses which folders it will not encrypt. Taking this approach allows the computer to continue to operate 'normally' while the malware encrypts files with known and unknown extensions containing data of value to the victim".

The FBI issued its usual advice that victim organizations should not pay ransoms to cybercriminals, as it funds and incentivize further attacks and does not guarantee data recovery.The agency also urged organizations to report ransomware incidents to their local FBI field office, and bolster their defenses with the help of the Cybersecurity and Infrastructure Security Agency's (CISA's) Stop Ransomware resource, MS-ISAC Joint Ransomware Guide (PDF), and Ransomware Readiness Assessment (RRA), a module within its Cyber Security Evaluation Tool (CSET).

Attack Type	Cause of Issue	Domain
Ransomeware Attack	**Organization Operations Compromise**	**Cybercrime**

Rust patches sneaky ReDoS bug

"The Rust security team has fixed a bug in the regex crate that allowed Denial of Service (DoS) attacks to be launched against applications.When a regular expression string is too long to parse, it consumes resources and causes application servers to slow down.Attackers use this feature to launch Regex Denial of Service (ReDoS) attacks against application features like search pages and APIs.Most programming languages, including Rust, have built-in defences to keep regex strings simple and prevent ReDoS attacks.However, a newly discovered bug in Rust's regex library depleted server resources in ways not anticipated by the default defence methods.""The most common type of ReDoS occurs when an attacker gains control of a regex input and is able to load regexes that [will] either fill or empty the input.the bug's discoverer, a security researcher""Empty regex subexpressions with large repetitions avoided triggering any of the existing mitigations, which were aimed at memory usage rather than compilation time,"" according to the patch commit.

As a result, carefully crafted regexes may cause the regex compiler to generate an exponentially growing number of empty subexpressions.According to Crump, the bug has been present in the affected library's Git history since 2018, when the regex-syntax was rewritten.""When the'regex' crate is used to parse untrusted regexes, the severity of this vulnerability is 'high,'"" according to a Rust Security Response Workgroup advisory. "

Attack Type
ReDOS Attack

Domain
System Programming Language

Flash loan attack on One Ring protocol nets Crypto-thief $1.4 million

One Ring Finance, a blockchain platform, has revealed that hackers stole $1.4 million from the One Ring protocol through a flash loan attack.According to One Ring, a'multi-chain cross-stable yield optimizer platform,' the attack cost the company $2 million in swap and flash loan fees.According to a One Ring post-mortem, the hacker used Solidly flash loans to borrow $80 million in USDC to boost the price of the underlying LP tokens during the block span.OneRing (RING) tokens, liquidity pools, or "farming opportunities in the Fantom space" were not affected by the attack, according to the company.The hacker, who made off with more than $1.4 million in USDC stablecoin, set the contract used in the attack to "self-destruct at a specific block, making it almost impossible to track what happened." "We're already in contact with node providers to obtain information about the block where the contract was deployed," One Ring added."We think we'll be able to locate the bytecode, decompile it, and get a rough idea of how this contract was put together."The hacker's Ethereum wallet was funded by Tornado Cash and the stolen funds were turned into the same tumbling protocol, which obfuscates transaction history. This made "it almost impossible to track" the source of the attacker's funding or warn other platforms of the attacker's activities".

Attack Type
Flash Loan Attack

Cause of Issue
$1.4 million Cryptothief

Domain
Blockchain Platform

Washington residents' medical data exposed by phishing attack on Spokane Regional Health District

After a successful phishing attack against a local public health agency, the sensitive medical data of over 1,200 Washington residents was exposed.During the incident on Feb 24, 2022, an attacker may have "previewed" "files containing client protected health information" associated with 1,260 individuals and two departments, according to Spokane Regional Health District (SRHD).According to SRHD, 1,060 people's first and last names, initials, dates of birth, and medical information may have been compromised. Test results, medications and prescription reasons, medical referrals, client notes, and pregnancies delivery dates were among the health-related data exposed.The other 200 victims potentially had their first and last names, initials, dates of birth, phone numbers, "shelter locations", test dates, and notes exposed. The first and last names, initials, dates of birth, phone numbers, "shelter locations," test dates, and notes of the other 200 victims may have been exposed. SRHD said it had "implemented appropriate corrective actions" to prevent further breaches, related to cybersecurity training, use of multi-factor authentication (MFA), and testing related systems. One of 34 local public health agencies in Washington state, Spokane Regional Health District serves a population of more than 400,000 in Spokane County.

Attack Type
Phishing Attack

Cause of Issue
Data Breach

Domain
Healthcare

"HTTP request smuggling bug patched in mitmproxy"

Mitmproxy, an open source interactive HTTPS proxy service, has fixed a potentially dangerous bug that allowed attackers to stage HTTP request smuggling attacks against backend servers.HTTP request smuggling attacks take advantage of inconsistencies in how intermediary and backend servers handle requests to get around security controls, gain unauthorised access to sensitive data, or compromise other app users.Zhang Zeyu, the security researcher who reported the bug, discovered that an attacker could smuggle a request/response through mitmproxy as part of another request/response's HTTP message body. An issue with the parsing of whitespace in header names caused mitmproxy and a downstream server to possibly have different interpretations of HTTP headers in the case of mitmproxy.A problem with the parsing of whitespace in header names caused mitmproxy and a downstream server to possibly have different interpretations of HTTP headers in the case of mitmproxy."Removing this type of vulnerability is difficult because it requires different HTTP implementations (proxy and target server) to agree on a common interpretation of HTTP messages," says the researcher.HTTP/1 services that follow the RFC7230 specification and reject headers with whitespace would also be immune against the request smuggling bug found in mitmproxy. The security bug would also be useless to attackers if the target web application is not vulnerable in some other way.“From a practical point of view, I'd argue that the impact is non-existent for the vast majority of users,” Hils said. “There are a lot of not-so-common preconditions that need to be met. I'd say quite a few stars need to align for this to have an actual impact in the wild.”

Attack Type
Http Request Smuggling

Cause of Issue
Sensitive Data Exposure

Domain
Technology Sector

Microweber developers resolve XSS vulnerability in CMS software

Microweber, an open source website builder and content management system, has been found to have a stored cross-site scripting (XSS) vulnerability by security researchers (CMS).Researchers James Yeung and Bozhidar Slaveykov discovered the security flaw, which was tracked as CVE-2022-0930 in Microweber version 1.2.12.The issue arose as a result of flaws in previous versions of Microweber's content filtering protections.Because of these flaws, attackers were able to upload an XSS payload as long as it contained a file ending in 'html' – a category that encompasses far more than just plain.html file. Once this payload has been uploaded, a URL containing malicious HTML can be accessed and malicious JavaScript can be run.These shortcomings meant it was possible for attackers to upload an XSS payload, providing it contained a file whose name ended with ‘html’ – a category that includes far more than just simple .html files.Once this payload is uploaded, a URL with malicious HTML can be accessed and malicious JavaScript executed. By controlling a script that is executed in the victim’s browser, it would be possible for an attacker to steal cookies before impersonating a victim, potentially the administrator of a compromised system.

Attack Type
Cross Site Scripting

Cause of Issue
Security Misconfigration

Domain
Content Management System

Sophos fixes SQL injection vulnerability in UTM appliance

Sophos has resolved a severe vulnerability in the software running on its all-in-one Universal Threat Management (UTM) appliances.A post-authentication SQL injection vulnerability in the Mail Manager component of the appliance created a means for attackers to run hostile code on a Sophos UTM appliance.The vulnerability (CVE-2022-0386), discovered by Sophos during internal security testing, can be resolved by updating to version 9.710 of the softwareThe same update also removes an obsolete SSL VPN client, as well as addressing a lesser and unrelated security vulnerability – tracked as CVE-2022-0652 – that resulted in password hashes being written into system log files.Although not directly exploitable, these password hashes were left in locations where they might potentially be harvested and abused in offline brute-force attacks.UTM devices bundle a variety of security functions into a single appliance that typically includes a network firewall, intrusion prevention, gateway antivirus, web proxy technology, and other security functions.Such devices are touted for ease of management, but they do bring with them the disadvantage of creating a single point of failure.

Attack Type
SQL Injection

Domain
Universal Threat Management (UTM)

‘Browser in a browser’: Phishing technique simulates pop-ups to exploit users

"A security researcher has demonstrated the potential dangers from a phishing technique that involves simulating a pop-up window in order to spoof a legitimate domain.The technique highlighted by the researcher, who goes by the online name of mr.d0x, illustrates a known issue that is somewhat underpublicized rather than wholly new hacking trick.The approach of spoofing a pop-up page login window is nonetheless dangerous because it undermines the standard advice that surfers should “check the URL” of sites.The major limitation of the so-called ‘browser in a browser’ attack is that a potential target would first need to be tricked into visiting an attacker-controlled website before the pop-up window is displayed.“But once landed on the attacker-owned website, the user will be at ease as they type their credentials away on what appears to be the legitimate website The spoofed pop-up window will not autofill passwords, a potential limitation to the technique which is nonetheless tricksy.“This type of attack is a difficult to detect visually speaking because the fake window looks exactly the same as a real window with a few minor differences that are quite difficult to notice."

Attack Type
Phishing Attack

Cause of Issue
Domain Spoofing

ENISA urges data-handling innovation amid growing tide of healthcare breaches

The EU's cybersecurity agency has called for further research into the use of pseudonymization to help bolster data protection measures in the healthcare sector.Pseudonymization de-associates a data subject's identity from their personal data by replacing personal identifiers with pseudonyms, or fictitious names.The European Union Agency for Cybersecurity (ENISA) has urged researchers, regulators, and application developers to play their part in improving pseudonymization techniques and best practices amid evolving medical technologies, a ballooning attack surface, and soaring numbers of cyber-attacks."This is not only relevant to the choice of the technique itself but also to the overall design of the pseudonymization process including, especially, the protection of the additional information," says ENISA in a new report that considers healthcare use cases of pseudonymization techniques.If attackers separately obtain this "additional information" they could potentially correlate breached, pseudonymized data with specific individuals, meaning pseudonymized data still falls under the ambit of the General Data Protection Regulation (GDPR).The most common methods for generating pseudonyms include counter, random number, encryption, hash function, and hash-based message authentication code (HMAC) techniques.

"Different solutions might provide equally good results in specific scenarios, depending on the requirements in terms of protection, utility, scalability, etc," said ENISA.ENISA recommends that clinical trials, which typically gather sensitive information such as age, gender, and home address, pseudonymize participants' main identifying data and use multiple pseudonyms for each identifying data for various clinical parameters."Such an approach could limit the personal data related to each pseudonym that, paired with a robustness that can be enforced using a solid hashing function like SHA-2 with a random seed value […] would make re-identification even more difficult."

Attack Type	Cause of Issue	Domain
Cryptography	**Data Breach**	**Healthcare**

Attackers getting faster at latching onto unpatched vulnerabilities for stealth hacking campaigns – report

Attackers are exploiting security vulnerabilities more quickly, often within a week of their public disclosure, according to a study by Rapid7.The latest edition of Rapid7's annual Vulnerability Intelligence Report, published today (March 28), finds that the average time to known exploitation of vulnerabilities is down to 12 days – markedly down from the 42 days recorded in last year's edition of the same study.Rapid7 said that the trend meant that enterprises needed to be ready with "battle-tested emergency patching and incident response procedures" to have any hope of staying on top of the increasingly challenging security threat environment.State-sponsored cyber-espionage groups (APTs) and opportunistic scammers attempting to enrich themselves through cryptojacking scams were also a problem.Rapid7, the firm behind the Metasploit penetration testing tool, logged 20 CVEs that were exploited as zero-days during 2021 – more than double the number of exploits that figured in the previous edition of its study."While a few of the zero-day vulnerabilities in the report were leveraged by ransomware groups from the start, most weren't used in ransomware operations until after an initial wave of exploitation."

Attack Type	Cause of Issue
Zero Day Vulnerability	**Device Compromise**

Ukrainian ISP used by military disrupted by ‘powerful’ cyber-attack

"A Ukrainian internet service provider (ISP) that supplies the country’s military was hit by a cyber-attack yesterday (March 28), knocking networks offline.The State Service of Special Communications and Information Protection (SSSCIP) of Ukraine confirmed that the “powerful” assault against Ukrtelecom was repelled, however there was disruption to networks.Some customers were restricted access in order to preserve communications networks for military and other high priority users.Russia has so far conducted fewer acts of cyberwar than expected in the eyes of the world’s media.

The SSSCIP has, however, been collating evidence of attacks against Ukraine infrastructure which show no signs of slowing down."

Attack Type
Cyber Attack

Cause of Issue
Disruption of Networks

Domain
Government Sector

Corporate Offices

INDIA

Briskinfosec

No:21, 2nd Floor, Krishnama Road,

Nungambakkam, Chennai - 600034.

+91 86086 34123 | 044 4352 4537

USA

3839 McKinney Ave,

Ste 155 - 4920,

Dalls TX 75204.

+1 (214) 571 - 6261

UK

Imperial House 2A,

Heigham Road, Eastham,

London E6 2JG.

+44 (745) 388 4040

BAHRAIN

Urbansoft, Manama Center, Entrance One,

Building No.58, No.316, Government Road,

Manama Area, Kingdom of Bahrain.

+973 777 87226

contact@briskinfose.com | www.briskinfosec.com