Threatsploit _Adversary Report

Edition 43

BRISK INFOSEC

CYBER TRUST & ASSURANCE

www.briskinfosec.com

Introduction

This month's report proves it to be even more accurate. We have released Threatsploit Adversary Report for March 2022. Half a million "extremely susceptible" people are still at risk because of an unpatched vulnerability in the Red Cross Society. Umbraco, a widely used open-source CMS, has been found to have security flaws that could allow unauthorised access to a user's account. Misconfigured security is to blame for this type of problem. The most traded and sought-after data on the internet is healthcare data, according to statistics. The Covid-19 healthcare data leak has been acknowledged by the California Public Health agency.

The primary cause is a third-party security misconfiguration that resulted in the public disclosure of patient information. Eyemeds was forced to pay $600,000 in damages as a result of a breach of patient data. Hackers used a phishing scam to get access to the patient's account. Fantasy leagues have been spawned by the introduction of league games in either cricket or football. Credential Stuffing compromise occurred in one of the English Premier League's applications. Hackers were able to access a video feed thanks to a flaw in an app. Here's the one about which we're all well-aware, yet nevertheless oblivious. Ukraine is under attack not only from the ground but also from the air and, increasingly, from the internet.

Data-erasing malware has surfaced at the same time that the country has been physically invaded. Another shocking development: the data of 80,000 members of the Internet Society has been leaked. More than a million JSON files containing personal information such as complete names, e-mail addresses, and passwords were available on an unsecured Microsoft Azure cloud repository. In this case, a security configuration error is to blame. Misconfigured security is at blame for the majority of problems. Please be cautious, and we thank you in advance for your cooperation. We take your safety very seriously.

"Two categories of businesses exist : those that have been hacked and those that are expected to be hacked."

Director of the FBI since 2012,
Robert Mueller.

_Contents

Security vulnerabilities in Umbraco CMS could lead to account takeover_

Umbraco is a free and popular open source content management system (CMS) provider with more than 730,000 active installations.Vulnerabilities in CMS platform Umbraco could allow an attacker to takeover a user's account, Umbraco has two seperatevulnerabilities, an application URL overwrite (CVE-2022-22690) and a persistent password reset bug (CVE-2022-22691).Umbraco CMS uses a configuration named 'ApplicationUrl', which is used whenever application code needs to build a URL pointing back to the site. For example, when a user resets their password, the application provides a password reset URL.In Umbraco versions less than 9.2.0, if the application URL is not specifically configured, an attacker can manipulate this value and point users to a URL of their choosing.After being alerted to the security vulnerabilities, Umbraco released fixes to help protect users from exploitation.The password reset and user invites no longer use the cached ApplicationUrl. If no UmbracoApplicationUrl is configured, the value is enumerated again to use the hostname of the request invoking the password reset.

"The URL to reset the password is poisoned as before, however the user receives the email unexpectedly which would lower the likelihood of a successful attack (CVE-2022-22691)."Users should update to version 9.2.0 or higher. The Daily Swig has reached out to Umbraco to determine whether a complete fix will be released.

Attack Type	Cause of Issue	Domain
Security Misconfiguration	Account Takeover	CMS Platform Provider

_Java Script Injection F5 fixes high-risk NGINX Controller vulnerability in January patch rollout

Networking and application delivery technology vendor F5 has fixed a pair of high impact, web security-related vulnerabilities."An authenticated attacker with access to the 'user' or 'admin' role can use undisclosed API endpoints on NGINX Controller API Management to inject JavaScript code that is executed on managed NGINX data plane instances."The vulnerability – tracked as CVE-2022-23008 – earns a CVSS score of 8.7, marking it out as the highest severity flaw in F5's latest patch batch.Successful exploitation of the flaw would allow an attacker to read and/or write files on the NGINX data plane instance. Users are advised to upgrade to version3.19.1. BIG-IP load balancer

Also of note is a DOM-based cross-site scripting (XSS) vulnerability involving F5's BIG-IP load balancer. The CVE-2022-23013 vulnerability in BIG-IP configuration utility could allow an attacker to execute JavaScript in the context of the current logged-in user.The flaw earns a CVSS score of 7.5, marking it out as another high severity threat. Many of the flaws involve memory handling or system crashing (denial of service) risks.

Attack Type	Cause of Issue	Domain
Java Script Injection	DOS	Network Provider

California public office admits Covid-19 healthcare data breach _

A misconfigured databased managed by a California public office has potentially exposed the sensitive medical information of citizens.County of Kings, in mid-California, announced that the security flaw in its public web server made limited information on Covid-19 cases available on the internet.The incident was discovered on November 24, 2021, and involved records obtained by the County's Public Health Department from the California Department of Public Health and County healthcare providers.An investigation determined that the misconfiguration resulted from an error made by a third-party contractor and existed on the county's public web server from February 15, 2021, until it was fully corrected on December 6, 2021.In a notice (PDF) posted online, County of Kings said that names, dates of birth, addresses, and Covid-19-related health information was among the datasets available to view.The government department said it has "no reason to believe that individuals' information has been or will be misused", but has informed all potential victims by post.It added that no further action needs to be taken by the individuals, but has set up a dedicated call center, details of which can be found in the notice.

Attack Type	Cause of Issue	Domain
Security Misconfiguration	Data Breech	Healthcare

Android security tool APKLeaks patches critical vulnerability

The maintainers of APKLeaks have patched a critical vulnerability that could be exploited for the remote execution of arbitrary code. APKLeaks is open source software for scanning Android application package (APK) files for URLs, endpoints, and secrets. This security flaw "allows remote authenticated attackers to execute arbitrary OS commands via [the] package name inside application manifest".The vulnerability, described as an improper neutralization of argument delimiters, is tracked as CVE-2021-21386 and has been issued a CVSS severity score of 9.3, an escalation from an original CVSS score of 7.3.The critical security issue surrounds a failure to protect against attackers issuing arguments that can trigger "unintended" commands, executing code remotely, or reading or tampering with sensitive information.No authentication was required to exploit the vulnerability.A patch to resolve the flaw released with APKLeaks version 2.0.3 failed to fully remedy the issue.

Attack Type	Cause of Issue	Domain
Improper Neutralization	Data Breech	Software Provider

US healthcare company EyeMed reaches settlement following 2020 data breach _

US healthcare company EyeMed has reached a $600,000 settlement following a data breach that compromised the records of 1.2 million people.EyeMed has agreed to pay New York State $600,000 in settlement fees, as well as to adhere to a list of security practices including encrypting sensitive data and conducting penetration testing.During a week-long intrusion, the attacker had access to, and was able to view, emails and attachments dating back six years prior, an investigation found (PDF).The emails contained one or more of the following consumer data elements: names; contact information including addresses; dates of birth; account information including identification numbers for health insurance accounts and vision insurance accounts; full or partial Social Security Numbers; Medicaid, drivers' license or other government ID numbers; birth or marriage certificates; and medical diagnoses and treatment information.the attacker sent approximately 2,000 phishing emails from the compromised email account to EyeMed clients, seeking login credentials for their accounts.

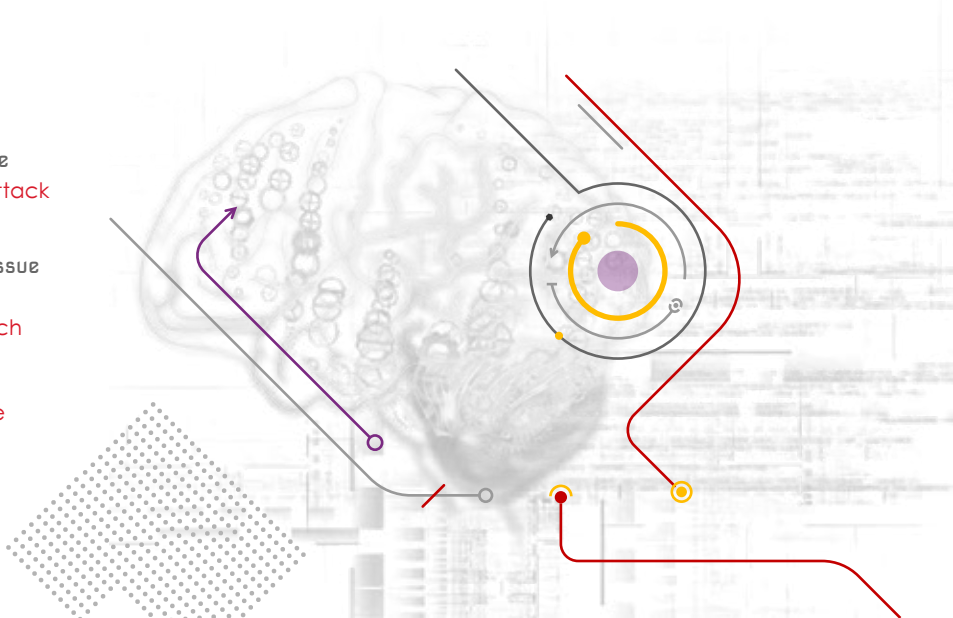
EyeMed blocked the attacker's access after noticing the phishing emails and receiving enquiries from clients about these emails.In September 2020, the company began notifying affected consumers whose personal information was compromised.A report from the New York attorney general reads: "EyeMed failed to implement multi-factor authentication (MFA) for the affected email account, despite the fact that the account was accessible via a web browser and contained a large volume of consumers' sensitive personal information.

The company also failed to employ "sufficient password management" protocols."EyeMed betrayed that trust by failing to keep an eye on its own security system, which in turn compromised the personal information of millions of individuals.

Attack Type
Phishing Attack

Cause of Issue
$600,000
Data Breech

Domain
Healthcare



_Fantasy Premier League account hack surge prompts plans to introduce extra login checks for football fans

A spate of account takeover hacks has prompted the English Premier League to promise to introduce two-factor authentication (2FA) controls to its official Fantasy Premier League game (FPL) from next season.FPL has more than eight million players, who sign up with a standard email address and password, although 2FA is not offered as an optionA wave of hacks this season has seen attackers seemingly targeting successful teams ranked in the top 100,000. The FPL game is free to enter and the chances of winning a prize, such as a trip to see a football game or Premier League merchandise, is slim to none.The game has also spawned a vibrant community of YouTube channels, discussion, and (several subscription-based) team aid selection websites.-The Premier League has reacted to the escalating prevalence of hacks over recent weeks on its official Twitter account, advising users to frequently change or update their password on a regular basis."Updating passwords on a regular basis is old and bad advice… you [should] use long and unique passwords for each service… coupled with 2FA," Per Thorsheim, security expert and founder of the PasswordsCon conference.

"There is no indication or evidence of a security breach on the accounts of these individuals via fantasy.premierleague.com or the Premier League mobile app," it said at the time.FPL players often use third-party websites or applications to aid team management. Many are assumed to be using the same login credentials across multiple sites, leaving them wide open to credential stuffing attacks if any site they have visited suffers a breach.

Attack Type
Credential Stuffing

Domain
Sports

Cause of Issue
Account Compromise

Email platform Zimbra issues hotfix for XSS vulnerability under active exploitation _

Business email platform Zimbra has released a hotfix for a cross-site scripting (XSS) vulnerability whose abuse has underpinned a series of spear-phishing campaigns.A suspected, previously unknown Chinese APT group has been attempting to leverage the flaw in order to load malicious JavaScript that exfiltrates mail data and attachments, according to an analysis by incident response outfit Volexity.he attackers could potentially also exfiltrate cookies and gain persistent access to mailboxes, send further phishing messages to victims' contacts, and dupe targets into inadvertently downloading malware.researchers detected around 33,000 mail servers running on Zimbra, but noted that the company says its open source software is used by 200,000 businesses and more than 1,000 government and financial institutions.

The attack hinged on the victim visiting a malicious link while logged into the Zimbra webmail client from a web browser. "The link itself, however, could be launched from an application to include a thick client, such as Thunderbird or Outlook," Zimbra announced on Friday (February 4) that the hotfix would "be available to Zimbra customers through Zimbra Support".Volexity has provided a list of infrastructure that Zimbra customers should block and advised them to "analyze historical referrer data for suspicious access and referrers".Volexity said the exploit was less damaging than the then zero-day Microsoft Exchange vulnerabilities it disclosed in March 2021, but that it

> "can still have catastrophic consequences for organizations"

Attack Type
Java Script Injection

Cause of Issue
Account Takeover

Domain
Business

_ Zero-day vulnerabilities in Nooie baby monitors could allow video feed hijack

Updated Security vulnerabilities in baby monitors from Nooie could allow attackers to either access the camera feed or execute malicious code on vulnerable devices.The Nooie Cam software has 50,000–100,000 installs on the Google Play Store – an indication that the technology is fairly widely used.First up was a stack-based buffer overflow or memory corruption vulnerability that could lead to remote code execution. The vulnerability – tracked as CVE-2020-15744 – is categorised as critical and relates to flaws in IoT software from Victure, the focus of previous research by Bitdefender.Another flaw enables attackers to access the RTSPS (audio-video) feed of an arbitrary cameras.Nooie's baby cameras rely on the MQTT protocol to announce the status of IoT devices and receive a URL location linked to RTSPS audio/video streams for each individual IoT device.Nooie's baby cameras use Amazon Web Services (AWS) to store recordings on the cloud."An attacker can easily spoof the camera and forge a request on its behalf and gain illicit access to the credentials," according to Bitdefender.

"The only prerequisites are the IDs leaked on the MQTT server (uuid and uid). After gaining access to the credentials, they can access the camera's stored recordings.Bitdefender privately disclosed these various vulnerabilities in November 2020 before following up with proof of concept code and requests for an update on progress in developing patches.

Attack Type	Cause of Issue	Domain
Zero-day Vulnerability	Malicious Code Execution	Security Cam

Cyber-attack at Vodafone Portugal knocks mobile network services offline _

A "deliberate and malicious" cyber-attack targeting Vodafone Portugal knocked mobile networks offline across the country this week.The incident, which started on Monday evening (February 7), suspended 4G and 5G networks for customers, as well as digital TV and SMS services.Vodafone said it has seen "no evidence" that customer data has been accessed or compromised due to the attack.In a statement, Vodafone Portugal blamed the outage on a "deliberate and malicious" cyber-attack.It added: "Vodafone was the target of a network disruption that began on the night of February 7, 2022, due to a deliberate and malicious cyber-attack intended to cause damage and disruption."As soon as the first sign of a problem on the network was detected, Vodafone acted immediately to identify and contain the [impact] and restore services."We have already recovered mobile voice services and mobile data services are available exclusively on the 3G network in almost the entire country but, unfortunately, the scale and seriousness of the criminal act to which we were subjected implies careful and prolonged work for all other services.

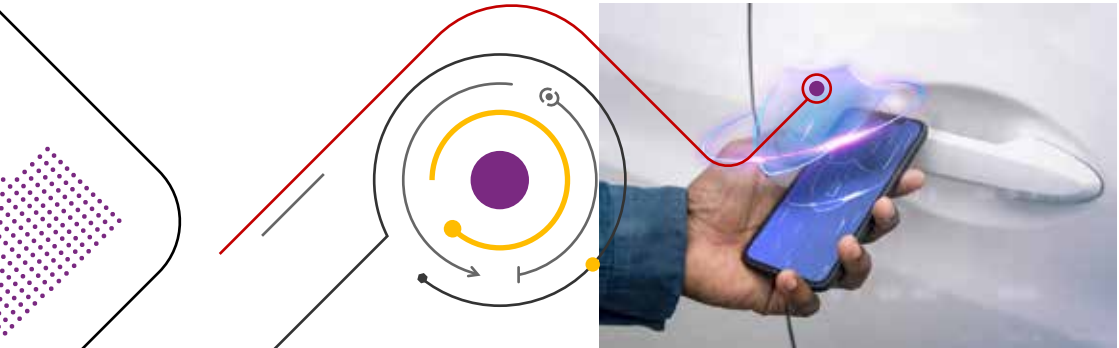
"At the time of writing, Vodafone said it had restored voice messaging and has started to restore 4G services across certain parts of the country.The company added that the remediation is "gradually being expanded to the greatest possible number of customers".Vodafone said its cybersecurity team is working with authorities as it investigates the incident.

Attack Type	Cause of Issue	Domain
Security Misconfiguration	Malicious Attack	Mobile Network

_ Ransomware surge prompts joint NCSC, CISA warning to safeguard systems

The UK's National Cyber Security Centre (NCSC), the US Cybersecurity and Infrastructure Security Agency (CISA), and the Australian Cyber Security Centre published a joint advisory (PDF) on Wednesday that highlighted the evolution of techniques deployed by cybercriminals and the growing maturity of the ransomware-as-a-service business model.Attackers have long used a combination of phishing, stolen Remote Desktop Protocol (RDP) credentials, and vulnerabilities to plant file-encrypting ransomware and demanding payment in exchange for decryption keys.Ransomware groups have increased their impact by targeting managed service and cloud infrastructure providers, according to the NCSC and other members of the Five Eyes intel sharing alliance."Ransomware developers targeted cloud infrastructures to exploit known vulnerabilities in cloud applications, virtual machine software, and virtual machine orchestration software," according to the joint advisory."Ransomware threat actors also targeted cloud accounts, cloud application programming interfaces (APIs), and data backup and storage systems to deny access to cloud resources and encrypt data."US authorities logged attempts by ransomware authors to target large organizations in high profile attacks. Victims included the Colonial Pipeline, JBS Foods, and Kaseya.Ransomware groups suffered disruptions from US authorities in mid-2021. As a result, miscreants redirecting ransomware efforts away from "big-game" and toward mid-sized victims, particularly in the US.

Attack Type	Cause of Issue	Domain
Ransomware	Malicious Attack	Security Agency



Internet Society data leak exposed 80,000 members' login details _

The Internet Society (ISOC), a non-profit dedicated to keeping the internet open and secure, has blamed the inadvertent exposure of its 80,000-plus members' personal data on a third-party vendor.The data, which was publicly accessible on an unprotected Microsoft Azure cloud repository, comprised millions of JSON files including, among other things, full names, email and mailing addresses, and login details."Based on the size and nature of the exposed repository, we can assume that all of the members' login and adjacent information was open to the public internet for an undefined period of time,"Clario said that if cybercriminals had accessed the data, it could have left victims more vulnerable to phishing attacks, identity theft, and fraud."The breach suggests ISOC needs to do more to enhance their security infrastructure and adhere to the best practices they champion around making the internet stronger and more secure," Clario advised potentially impacted members to change their online ISOC passwords, be on guard for suspicious-looking emails or links.

This is the second incident Clario has disclosed this month in which a third-party vendor has been blamed for sensitive personal data being exposed within an unprotected Microsoft Azure blob repository.

Attack Type	Cause of Issue	Domain
Sensitive Data Exposure	Data Breech	Internet Society

_New tool can uncover redacted, pixelated text to reveal sensitive data

The tool, called Unredacter, was released by Bishop Fox to demonstrate that pixilation is "a no-good, bad, insecure, surefire way to get your sensitive data leaked", it was designed to take redacted pixelized text and reverse it back into its reveal the supposedly hidden "clear text".Bishop Fox has a "long-standing policy" to only redact information using black bars, which the company says is the only secure way technique."Sometimes, people like to be clever and try some other redaction techniques like blurring, swirling, or pixilation," "But this is a mistake."because "It's just not a secure way to redact information," he explained. "But you see it all the time out there on the internet, often by journalists."Clearly the community needed to be convinced that pixilation is bad, and a tool to un-redact is the best way to do it."the tool is aimed at being used by "possibly Red Teams", but added that it "is mostly a proof-of-concept to drive home a point – never redact text with anything other than black bars fully covering the text".The researcher added: "Redacted data can be almost anything from passwords in a pen test report to victim names in a criminal report."The consequences to insecurely redacting information is highly context-dependent, but generally, someone redacts information because they don't want it to be read."

Attack Type
Security Misconfiguration

Cause of Issue
Sensitive Data Breech

Domain
Security Agency

MFA fatigue attacks: Users tricked into allowing device access due to overload of push notifications

Malicious hackers are targeting Office 365 users with a spare of 'MFA fatigue attacks', bombarding victims with 2FA push notifications to trick them into authenticating their login attempts.-Multi-factor authentication (MFA) fatigue is the name given to a technique used by adversaries to flood a user's authentication app with push notifications in the hope they will accept and therefore enable an attacker to gain entry to an account or device.GoSecure noted that the attack is particularly effective – not because of the technology involved, but because it targets the human factor via social engineering."Many MFA users are not familiar with this type of attack and would not understand they are approving a fraudulent notification,"Research from Mandiant detailed how threat actors were observed executing multiple authentication attempts in short succession against accounts secured with MFA."Many MFA providers allow for users to accept a phone app push notification or to receive a phone call and press a key as a second factor."The threat actor took advantage of this and issued multiple MFA requests to the end user's legitimate device until the user accepted the authentication, allowing the threat actor to eventually gain access to the account."

GoSecure warned: "As app-based authentication mechanisms are being adopted increasingly as a safer way to authenticate a user (versus SMS or phone call) it is expected that this tendency will grow in the future, even be encouraged by Microsoft itself."

Attack Type
MFA Fatigue Attack

Cause of Issue
Account Takeover

Domain
Business

Red Cross servers 'were hacked via unpatched ManageEngine flaw'

The Red Cross has revealed that personal data belonging to more than half a million "highly vulnerable" people was compromised via the abuse of an unpatched vulnerability.The International Committee of the Red Cross (ICRC) had encountered a "highly sophisticated and targeted" attack.Attackers had optimized malicious code for ICRC servers and anti-malware defenses, deployed sophisticated obfuscation techniques, and used hacking tools "primarily used by advanced persistent threat groups" in order to "disguise themselves as legitimate users or administrators", said the humanitarian organization.

The attack vector was apparently a critical REST API authentication bypass in Zoho ManageEngine ADSelfService Plus, a password management and single sign-on (SSO) platform.The failure to apply the fix for this remote code execution (RCE) threat has prompted "immediate changes" to vulnerability management processes and tools, said the ICRC, as well as the acceleration of security improvements already in place.Data breach victims include "missing people and their families, detainees, and other people receiving services from the Red Cross and Red Crescent Movement as a result of armed conflict, natural disasters, or migration".The data relates to the activities of Restoring Family Links, a Red Cross program dedicated to reuniting families caught up in conflicts or natural disasters.The program was initially paused in the wake of the attack, but ICRC director-general Robert Mardini said in an open letter: "We have managed to ensure that the vital work of locating missing family members has continued, albeit at minimal service levels, through low-tech solutions (using simple spreadsheets, for example), while we work toward resuming full service with enhanced security features."

Attack Type	Cause of Issue	Domain
Remote Code Execution	Server Compromise	API Management

Introducing Ghostbuster – AWS security tool protects against dangling elastic IP takeovers _

An open source security tool has been launched with the promise of a "fool-proof way" to detect dangling elastic IP takeovers.Organizations leave themselves vulnerable to these subdomain takeover attacks when they delete Amazon Web Services (AWS) EC2 instances or assign them new IPs but forget to remove DNS records that point to IPs associated with the instances.Attackers can identify these vulnerable subdomains by continually claiming elastic IPs until they find an IP associated with the subdomain of a targeted organization. the 'Ghostbuster' tool, developed by Australian cybersecurity firm Assetnote, offers a different approach: It enumerates all public IPs associated with an organization's AWS accounts and checks for DNS records pointing to elastic IPs that its AWS accounts don't own.Shubham Shah, co-founder and CTO at Assetnote, said the firm's own hit-and-miss experiments with the lottery approach had prompted AWS to tell its researchers to stop using the technique.Because the lottery approach is the only approach attackers can use, with Ghostbuster, you can eliminate dangling elastic IP takeovers entirely.Dangling elastic IP subdomain takeovers are one of many frequently occurring misconfiguration vulnerabilities to arise from the "shared responsibility" security model used by major cloud providers.

As well as hosting malicious content or leveraging a 'trusted' domain for phishing attacks, attackers can also potentially claim the subdomain's SSL certificates via ACME TLS challenges; intercept sensitive information being sent to the subdomain; and run server-side scripts that steal HTTPOnly cookies, thus enabling one-click account takeover attacks.

Attack Type	Cause of Issue	Domain
Sensitive Data Exposure	Subdomain Takeover	Cloud Provider

Jaw-dropping Coinbase security bug allowed users to steal unlimited cryptocurrency

A security researcher has netted a $250,000 bug bounty for disclosing a vulnerability in Coinbase that could have allowed a user to 'sell' currency they did not own.The bug was spotted by security engineer 'Tree of Alpha', whose disclosure led to them receiving the cryptocurrency exchange's biggest ever bounty payout this month.This could have potentially allowed an attacker to steal unlimited cryptocurrency from the platform.A blog post from Coinbase describes the attack: "A user has an account with 100 SHIB, and a second account with 0 BTC."The user submits a market order to the BTC-USD order book to sell 100 BTC, but manually edits their API request to specify their SHIB account as the source of funds."Here, the validation service would check to determine whether the source account had a sufficient balance to complete the trade, but not whether the source account matched the proposed asset for submitting the trade.A market order to sell 100 BTC on the BTC-USD order book would be entered on the Coinbase Exchange.Alpha described on Twitter how they used 0.0243 ETH to sell 0.0243 BTC on the BTC-USD pair, "a pair I do not have access to, without holding any BTC".

On discovering the issue, Alpha reported the bug to the Coinbase bug bounty program, managed by HackerOne.They also took to Twitter to find a contact at Coinbase, to warn them of the "potentially market-nuking" discovery.Coinbase responded and the bug was fixed in less than six hours, with the exchange "conclusively determining" that it had never been maliciously exploited."There were mitigating factors that would have limited the impact of this flaw had it been exploited at scale.Alpha was awarded $250,000, the highest payout from Coinbase to date, though the potential amount of funds lost if the vulnerability was exploited pales in comparison.

Attack Type	Cause of Issue	Domain
Security Misconfiguration	BTC Hijacking	Bug Bounty

Zero-day RCE flaw among multiple bugs found in Extensis Portfolio - research

Researchers have disclosed critical vulnerabilities in Extensis Portfolio, including a zero-day flaw that's yet to be patched.On February 17, White Oak Security researchers Michael Rand and Talis Ozols publicly disclosed vulnerabilities in digital asset management software Extensis Portfolio.Extensis Portfolio comprises a user-facing main content management application, an administrator portal, and a content hosting application.The pen testers then examined the source code of Extensis Portfolio version 3.6.3 and found a total of five vulnerabilities that required immediate attention :

CVE-2022-24251 – RCE via unrestricted file upload

CVE-2022-24255 – Hardcoded credentials in the main and administrator portals (authentication bypass)

CVE-2022-24252 – Unrestricted file upload and path traversal error leading to RCE in the main portal

CVE-2022-24254 – Authenticated archive 'zip-slip', a directory traversal bug, exploitable for RCE

CVE-2022-24253 – Authenticated, but unrestricted file upload flaw in admin portal leading to RCE

CVE numbers have been assigned and are on a 'reserved' status at the time of writing. It is not known if any of these vulnerabilities are being exploited in the wild.The researchers spent the month of August 2021 trying to contact the vendor through online forms, sales channels, and social media, only to be promised a security contact that never materialized.White Oak Security confirmed that the original RCE vulnerability was unpatched in v4.0.0, and after requesting further information from the vendors on the fixes, there was radio silence.A total of 164 days passed since disclosure before the researchers decided to take their findings public. According to White Oak Security, Extensis said "these security issues had not been prioritized and Extensis did not have an expected date for remediation".

Attack Type	Cause of Issue	Domain
Zero-Day	Remote Code Execution	Software Management

_EU countries offer cyber-defense assistance to Ukraine

European Union countries have reportedly agreed to offer Ukraine help in fighting against potential Russian cyber-attacks.The support is apparently being provided via the EU's Cyber Rapid Response Teams (CRRTs) – a recently announced project supported by the governments of Croatia, Estonia, Lithuania, the Netherlands, Poland, and Romania.The six participating member states "made a decision to activate the team" in support of Ukraine, according to Lithuanian defence minister Margiris Abukevičius, Politico reports.Amid escalating tensions with Russia, Ukraine has asked for help from Western governments to bolster its cybersecurity, and Australia and several EU countries have heeded the call.Earlier this month, Ukraine's defense ministry and two banks suffered denial-of-service attacks.In a further escalation this week, Russia recognized the self-declared Donetsk and Luhansk republics in eastern Ukraine, announcing it planned to deploy "peacekeeping troops" in the region.

Cyber conflict experts predict that any advances by Russian tanks into Ukrainian territory are likely to be accompanied by cyber-attacks against telecommunications and other infrastructure as well as disinformation campaigns.These attacks have the potential not only to have a debilitating effect on Ukraine but to also affect Western countries, as explained in some depth in a thread on Twitter by former UK National Cyber Security Centre chief executive Ciaran Marti.

Attack Type	Cause of Issue	Domain
DOS Attack	Cyber-Attacks	Government

_Apple fixes actively exploited iOS, macOS zero-day (CVE-2022-22620)

Another month, another zero-day (CVE-2022-22620) exploited in the wild that has been fixed by Apple.CVE-2022-22620 is a use after free issue in WebKit, the browser engine used in Safari and all iOS web browsers.Apple fixed it in iOS 15.3.1 and iPadOS 15.3.1, macOS Monterey 12.2.1, and Safari 15.3."Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited," the company noted in the security update release notes, and credited an anonymous researcher with reporting it."WebKit vulnerabilities are typically exploited by exposing the device to a malicious webpage, but anything rendered using the WebKit engine could potentially be used to expose the vulnerability,"

Attack Type	Cause of Issue	Domain
Zero-Day	Arbitrary Code Execution	Apple Technologies

Russian nation-state hackers targeting US contractors for sensitive defense information, FBI warns_

Russian state-sponsored operatives are targeting US contractor networks to obtain sensitive defense information, the FBI has warned, with some gaining persistent access for at least six months.The joint release from CISA, the FBI, and NSA states that both large and small CDCs and subcontractors with varying levels of cybersecurity protocols and resources have been targeted.These CDCs support contracts for the US Department of Defense (DoD) and wider intelligence community in various areas, including software development, data analytics, logistics, surveillance, reconnaissance, and targeting.Russian actors maintained persistent access to multiple CDC networks, in some cases for at least six months, said CISA.The FBI, NSA, and CISA noted regular and recurring exfiltration of emails and data.

According to the agency, the threat actors used tactics including spear-phishing, credential harvesting, and brute-force attacks against accounts and networks with weak security. "These actors take advantage of simple passwords, unpatched systems, and unsuspecting employees to gain initial access before moving laterally through the network to establish persistence and exfiltrate data," "The actors often maintain persistence by using legitimate credentials and a variety of malware when exfiltrating emails and data."This has enabled them to access "sensitive, unclassified information", as well as CDC-proprietary and export-controlled technology.Mitigations include employing multi-factor authentication (MFA), using strong, unique passwords, and implementing a software patch management program to reduce the number of known vulnerabilities in a CDC's network.

Attack Type	Cause of Issue	Domain
DOS Attack	Data Breech	Government

_ AirTag clone bypassed Apple's tracking-protection features, claims researcher

A security researcher claims he bypassed the tracking protection features built into Apple's Find My app and AirTag tracking devices with a custom-made AirTag clone.Launched in April 2021, AirTags communicate with Apple's Find My service to help users keep track of personal items such as keys, wallets, and luggage.However, several reports of malicious misuse have surfaced, from devices planted to facilitate grand theft auto to those surreptitiously slipped into victims' coat pockets.Apple moved to address fears around unwanted tracking earlier this month by unveiling a raft of safety warning enhancements.The most common method for detecting unwanted AirTags – iPhone notifications that are triggered when AirTags are separated from their owner's device but observed moving with another device – was readily bypassed by programming the clone "to continuously broadcast new, never-seen-before public keys".The clone, which had no speaker, was also undetectable by beeping alerts.While the clone went undetected by Apple's asset-tracking apps for the iOS and Android ecosystems – Find My and Tracker Detect, respectively – it was spotted by a third-party alternative.AirGuard, which was developed by the Secure Mobile Networking Lab (SEEMOO) at the Technical University of Darmstadt's computer science department, discovered the clone in 'manual scan' mode.

"iOS and Tracker Detect ignore those devices since they mimic a lost iPhone," Despite its success against Bräunlein's AirTag imitator, AirGuard was actually designed to detect off-the-shelf devices, such as the Chipolo One Spot and modified, speaker-free AirTags, which Heinrich said are fuelling stalking.

Attack Type	Cause of Issue	Domain
Malicious Attack	Data Leakage	Apple Technologies

Zero-day XSS vulnerability in Horde webmail client can be triggered by file preview function

A zero-day cross-site scripting (XSS) vulnerability in Horde webmail client could allow an attacker to steal a victim's emails and infiltrate their network, researchers warn.The stored XSS is triggered by the process of rendering an OpenOffice file into a viewable format.An OpenOffice document is a ZIP file containing XML documents and other files.When Horde is asked to convert an OpenOffice document to HTML to be previewed, it uses XSLT (eXtensible Stylesheet Language Transformations).The security flaw can give an attacker access to all information a victim has stored in their email account and could allow them to gain further access to the internal services of an organization.The company went public with its findings this week despite no patch being available and advised users to apply alternative mitigations."This can be done easily by disabling the affected feature, which does not have a big impact on the usability of the software," Scannell said.Users will still be able to download the OpenOffice documents and view them locally, but Horde won't attempt to render it in the browser."By releasing the vulnerability and patch details, we hope to raise visibility and to enable administrators to secure their servers," added Scannell.

Attack Type	Cause of Issue	Domain
Zero-day XSS Vulnerability	Phishing Attack	Email Providers

Data wiper deployed in cyber-attacks targeting Ukrainian systems

A newly discovered strain of data-wiping malware has surfaced in Ukraine, coinciding with the physical invasion of the country by Russian forces.The Windows-specific data wiper has appeared on "hundreds of machines", according to telemetry from information security firm ESET."The wiper abuses legitimate drivers from the EaseUS Partition Master software in order to corrupt data," according to a series of posts on ESET Research's official Twitter account over the past 24 hours."In one of the targeted organizations, the wiper was dropped via the default (domain policy) GPO meaning that attackers had likely taken control of the Active Directory server."

Date stamps on the malware indicate that it was compiled two months ago – evidence that the attack was possibly premeditated.The discovery of the HermeticWiper malware followed a run of distributed denial-of-service (DDoS) attacks on Ukrainian websites.The websites of the Ukrainian parliament, council of ministers, and foreign affairs ministry all became unreachable in the face of an apparent onslaught.Elsewhere, security researchers discovered a "GRU-linked [Russian military intelligence] malware server that contained a trojan-rigged clone of the site of the Ukrainian president", Volodymyr Zelenskyy.Russia's invasion of Ukraine, a looming threat over recent weeks, is arguably the biggest news story of 2022 so far.

Attack Type
DDOS Attack

Cause of Issue
Cyber Attack

Domain
Government Sector

Equifax finalizes data breach settlement with US regulators _

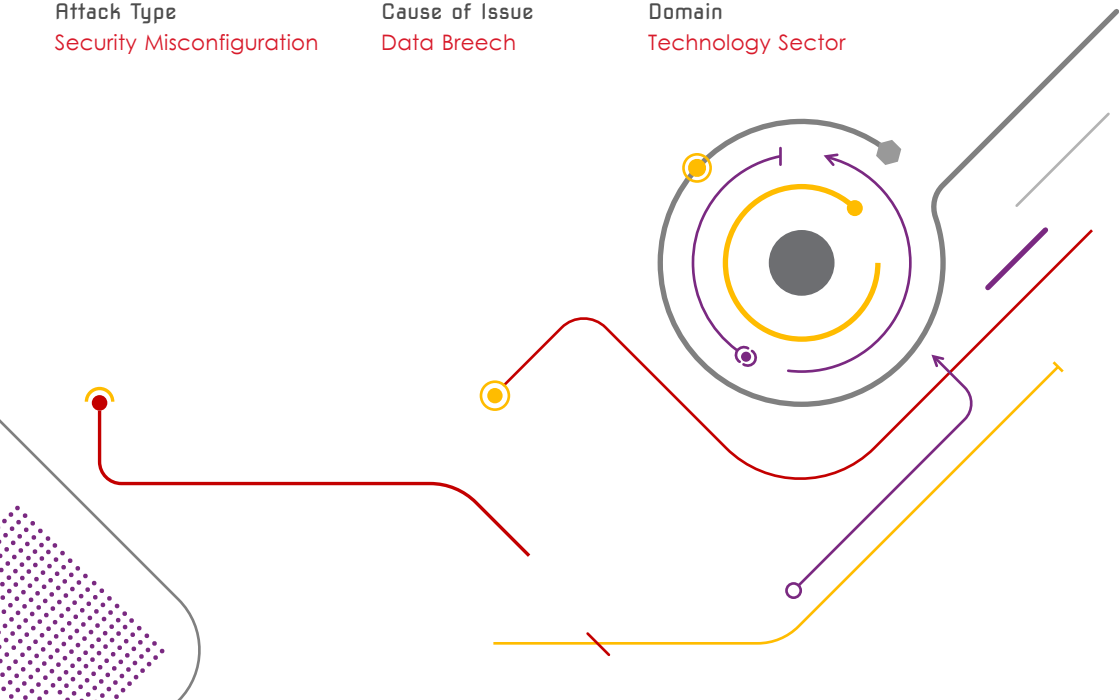
Credit reference agency Equifax has finalized a settlement for a 2017 data breach that affected more than 147 million US citizens and 15 million Brits.The breach exposed the credit card data of a smaller subset of around 209,000 victims.

An estimated 15 million British citizens were affected by the incident, of which 694,000 had sensitive data exposed. A smaller number of Canadians were also affected.The root cause of the attack was a critical Apache Struts vulnerability, discovered and resolved in March 2017, that was left unresolved on at least one web-facing Equifax server.Attackers took advantage of an unpatched Apache Struts installation to hack into Equifax's dispute resolution portal.This compromised server acted as a springboard that allowed hackers to access Equifax's internal systems before stealing credentials that allowed them to query its databases.Database queries were stored in compressed files that were slowly and systematically siphoned off.Equifax has agreed to a global settlement with the Federal Trade Commission (FTC), the Consumer Financial Protection Bureau, and 50 US states and territories.The settlement includes up to $425 million to help people affected by the data breach, as explained in an update from the FTC.

Attack Type
Security Misconfiguration

Cause of Issue
Data Breech

Domain
Technology 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