Your Security Rabbits report for April 05, 2022

Hot topics

Nothing today

Source: Ransom Watch

Ransomware attacks

conti	panasonic	clop	ZISSERFAMILYLAW.COM
clop	THENOC.NET	clop	SSMSJUSTICE.COM
clop	SLIMSTOCK.COM	lockbit2	scoular.com
clop	SA1SOLUTIONS.COM	clop	OAKDELL.COM
clop	MTMRECOGNITION.COM	lockbit2	ferrolabella
lockbit2	noll-law.com	stormous	A message to France
clop	JDAVIDTAXLAW.COM	lockbit2	gva-atencia.es
lockbit2	sep2.com	clop	FAIR-RITE.COM
lockbit2	ascotlloyd.co.u...	lockbit2	westminster.de
conti	Woningcorporatie ZAYAZ	lockbit2	a-r-s.com

Source: NIST

NIST CVE: Critical

Nothing today

News

Cyware News - Latest Cyber News

"Free easter chocolate basket" is a social media scam after your personal details
Cadbury UK has issued a warning to its 315,000 followers on Twitter about a scam making the rounds on WhatsApp and other social media sites like Facebook. The Dorset Police Cyber Crime Unit posted an appeal about this scam on its Facebook page.

ZDNet | security RSS

Borat RAT malware: A 'unique' triple threat that is far from funny
The malware combines remote access, spyware, and ransomware into one nasty package.

Security Affairs

Brokenwire attack, how hackers can disrupt charging for electric vehicles
Boffins devised a new attack technique, dubbed Brokenwire, against the Combined Charging System (CCS) that could potentially disrupt charging for electric vehicles. A group of researchers from the University of Oxford and Armasuisse S+T has devised a new attack technique, dubbed Brokenwire, against the popular Combined Charging System (CCS) that could be exploited by remote [...] The post Brokenwire attack, how hackers can disrupt charging for electric vehicles appeared first on Security Affairs.

The Hacker News

Brokenwire Hack Could Let Remote Attackers Disrupt Charging for Electric Vehicles
A group of academics from the University of Oxford and Armasuisse S+T has disclosed details of a new attack technique against the popular Combined Charging System (CCS) that could potentially disrupt the ability to charge electric vehicles at scale. Dubbed "Brokenwire," the method interferes with the control communications that transpire between the vehicle and charger to wirelessly abort the

The Hacker News

CISA Warns of Active Exploitation of Critical Spring4Shell Vulnerability
The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Monday added the recently disclosed remote code execution (RCE) vulnerability affecting the Spring Framework, to its Known Exploited Vulnerabilities Catalog based on "evidence of active exploitation." The critical severity flaw, assigned the identifier CVE-2022-22965 (CVSS score: 9.8) and dubbed "Spring4Shell", impacts Spring

Cyware News - Latest Cyber News

Cisco software update blocks exploit chain in network management software
A security researcher was able to achieve unauthenticated remote code execution against Cisco Nexus Dashboard Fabric Controller by exploiting an obsolete Java library with known vulnerabilities.

Cyware News - Latest Cyber News

Cryptocurrency clients' mailing-list info stolen from Mailchimp
Mailchimp has confirmed a miscreant gained access to one of its internal tools and used it to steal data belonging to 100-plus high-value customers. The clients were all in cryptocurrency and finance-related industries, according to Mailchimp

Cyware News - Latest Cyber News

Cyberattack on Iberdrola Compromises Data of Millions of Customers in Spain
Spain's energy giant Iberdrola has revealed that it suffered a cyberattack on March 15 which has affected 1.3 million customers, although the company has reassured that the hackers were unable to access "sensitive" information such as bank details.

CyberScoop

Debate erupts at news the White House may scale back DOD cyber-ops authorities
Cybersecurity and homeland security experts are split on the wisdom of scaling back broad authorities that DOD has to launch cyber operations. The post Debate erupts at news the White House may scale back DOD cyber-ops authorities appeared first on CyberScoop.

Cyware News - Latest Cyber News

El Machete, Lyceum, and SideWinder Hacker Groups Capitalizing on Ukraine Conflict to Distribute Malware
The campaigns, undertaken by El Machete, Lyceum, and SideWinder, have targeted a variety of sectors, including energy, financial, and governmental sectors in Nicaragua, Venezuela, Israel, Saudi Arabia, and Pakistan.

Security Affairs

Experts spotted a new Android malware while investigating by Russia-linked Turla APT
Researchers spotted a new piece of Android malware while investigating

Cyware News - Latest Cyber News

Emma Sleep Company admits attack on online checkout

Emma Sleep Company has confirmed to The Reg that it suffered a Magecart attack which enabled the cybercriminals to skim customers' credit or debit card data from its website.

The Hacker News

Hackers Breach Mailchimp Email Marketing Firm to Launch Crypto Phishing Scams

Email marketing service Mailchimp on Monday revealed a data breach that resulted in the compromise of an internal tool to gain unauthorized access to customer accounts and stage phishing attacks. The development was first reported by Bleeping Computer. The company, which was acquired by financial software firm Intuit in September 2021, told the publication that it became aware of the incident

Naked Security

LAPSUS$ hacks continue despite two hacker suspects in court

Do you know where in your company to report security anomalies? If you receive such reports, do you have an efficient way to process them?

Cyware News - Latest Cyber News

Mars Stealer's Cryptomining Attack Campaign Targets OpenOffice

Morphisec laid bare a new Mars Stealer campaign--abusing Google Ads ranking techniques--to lure Canadian users into downloading a malicious version of OpenOffice. A bug in the configuration instructions of the cracked version of Mars Stealer, which appears to be an honest mistake by the operators, gives anyone access to the logs directory of victims. Organizations are suggested to protect sensitive data with proper access management and encryption.

IT Security Guru

New attack method could disrupt electric vehicle charging

Academics from the University of Oxford and Armasuisse S+T have identified a novel attack technique targeting the widely-used Combined Charging System (CCS). They say the method could potentially disrupt the ability to charge electric vehicles at scale. The "Brokenwire" attack method meddles with the control communications between the vehicle and charger, wirelessly aborting charging from [...] The post New attack method could disrupt electric vehicle charging appeared first on IT Security Guru.

The Hacker News

Researchers Trace Widespread Espionage Attacks Back to Chinese 'Cicada' Hackers

A Chinese state-backed advanced persistent threat (APT) group known for singling out Japanese entities has been attributed to a new long-running espionage campaign targeting new geographies, suggesting a "widening" of the threat actor's targeting. The widespread intrusions, which are believed to have commenced at the earliest in mid-2021 and continued as recently as February 2022, have been tied

The Hacker News

Researchers Uncover New Android Spyware With C2 Server Linked to Turla Hackers

An Android spyware application has been spotted masquerading as a "Process Manager" service to stealthily siphon sensitive information stored in the infected devices. Interestingly, the app -- that has the package name "com.remote.app" -- establishes contact with a remote command-and-control server, 82.146.35[.]240, which has been previously identified as infrastructure belonging to the

IT Security Guru

Spanish energy giant hit by data breach

Iberdrola, a Spanish energy provider, has suffered a data breach affecting over one million customers, local reports suggest. The company is headquartered in Bilbao and is the parent company of Scottish Power. They have reported that the attack took place on March 15 this year. The breach reportedly resulted in the theft of customer ID [...] The post Spanish energy giant hit by data breach appeared first on IT Security Guru.

IT Security Guru

The Differences in How CASB vs. SSPM Secures SaaS Apps

There is often confusion between Cloud Access Security Brokers (CASB) and SaaS Security Posture Management (SSPM) solutions, as both are designed to address security issues within SaaS applications. CASBs protect sensitive data by implementing multiple security policy enforcements to safeguard critical data. For identifying and classifying sensitive information, like Personally Identifiable Information (PII), Intellectual Property [...] The post The Differences in How CASB vs. SSPM Secures SaaS Apps appeared first on IT Security Guru.

IT Security Guru

Trezor customers phished following MailChimp breach

Trezor, who manufacture hardware devices designed to store digital currency, has warned its customers not to reply to official-looking emails after identifying a convincing phishing campaign. Several customers complained to Trezor's twitter account over the weekend to complain about a scam email claiming that a data breach had hit over 100,000 customers. The email reportedly [...] The post Trezor customers phished following MailChimp breach appeared first on IT Security Guru.

ZDNet | security RSS

US judge sentences men for $1.5 million Apple Gift Card scam

Apple is also owed over $1 million in damages.

Security Affairs

activity associated with Russia-linked APT Turla. Researchers at cybersecurity firm Lab52 discovered a new piece of Android malware while investigating into infrastructure associated with Russia-linked APT Turla. The malicious code was discovered while analyzing the Penquin-related infrastructure, the experts noticed malware was contacting IP addresses [...] The post Experts spotted a new Android malware while investigating by Russia-linked Turla APT appeared first on Security Affairs.

The Hacker News

Is API Security on Your Radar?

With the growth in digital transformation, the API management market is set to grow by more than 30% by the year 2025 as more businesses build web APIs and consumers grow to rely on them for everything from mobile apps to customized digital services. As part of strategic business planning, an API helps generate revenue by allowing customers access to the functionality of a website or computer

Security Affairs

MailChimp breached, intruders conducted phishing attacks against crypto customers

Threat actors gained access to internal tools of the email marketing giant MailChimp to conduct phishing attacks against crypto customers. During the weekend, multiple owners of Trezor hardware cryptocurrency wallets reported having received fake data breach notifications from Trezor, BleepingComputer first reported. The fake data breach notification emails urged Trezort customers to reset the PIN of [...] The post MailChimp breached, intruders conducted phishing attacks against crypto customers appeared first on Security Affairs.

The Hacker News

Multiple Hacker Groups Capitalizing on Ukraine Conflict for Distributing Malware

At least three different advanced persistent threat (APT) groups from across the world have launched spear-phishing campaigns in mid-March 2022 using the ongoing Russo-Ukrainian war as a lure to distribute malware and steal sensitive information. The campaigns, undertaken by El Machete, Lyceum, and SideWinder, have targeted a variety of sectors, including energy, financial, and governmental

CyberScoop

Notorious hacking group FIN7 adds ransomware to its repertoire

Ransomware strains such as Maze, Ryuk and BlackCat have increasingly been part of FIN7's playbook in recent years, Mandiant says. The post Notorious hacking group FIN7 adds ransomware to its repertoire appeared first on CyberScoop.

Cyware News - Latest Cyber News

Researchers Uncover New Android Spyware With C2 Server Linked to Turla Hacker Group

An Android spyware application made by the Turla APT has been spotted masquerading as a "Process Manager" service to stealthily siphon sensitive information stored in the infected devices.

Cyware News - Latest Cyber News

Serious RCE Bug Found in Spring Cloud

A serious vulnerability has been discovered in the Spring Cloud Java Framework that may lead to RCE or result in the compromise of an entire host. Tracked as Spring4 Shell, it was found circulating on a Chinese cybersecurity site and QQ chat service. Currently, a way to partially stop Spring4Shell attacks is to disallow certain patterns to be passed to the Spring Core DataBinder functionality.

CyberScoop

State Department's cyber bureau begins operations

The announcement comes after years of back-and-forth between Congress and multiple presidential administrations about consolidating how the department handles cyber diplomacy. The post State Department's cyber bureau begins operations appeared first on CyberScoop.

Blog â€“ Flashpoint

Top 10 Ransomware Trends: Board Responsibilities, Tracking Ransomware, and Mitigating Risk in 2022

From summer 2021 to early 2022, the ransomware ecosystem changed from high-profile, high-impact, big-game hunting activity to a period of relative quiet characterized by mid-level targets, higher ransom demands, and the first hacktivist ransomware attack on critical infrastructure. The ecosystem shift is primarily the result of three factors: the international notoriety of certain 2021 attacks [...] The post Top 10 Ransomware Trends: Board Responsibilities, Tracking Ransomware, and Mitigating Risk in 2022 appeared first on Flashpoint.

ZDNet | security RSS

Turkey seeks 40,000-year sentences for alleged cryptocurrency exit scammers

21 suspects are wanted in connection to a defunct Turkish crypto exchange.

Cyware News - Latest Cyber News

Utilizing biological algorithms to detect cyber attacks

A standard approach to addressing spoofed domains is to compare them to a database of known domains and to look for differences. Since the traditional method is sometimes insufficient, researchers have turned to a method called biomimicry.

VMware released updates to fix the Spring4Shell vulnerability in multiple products

Cyware News - Latest Cyber News

VMware patches Spring4Shell RCE flaw in multiple products
VMware has published security updates for the critical remote code execution vulnerability known as Spring4Shell, which impacts several of its cloud computing and virtualization products.

Security Affairs

VMware released security updates to address the critical remote code execution vulnerability known as Spring4Shell. VMware has published security updates to address the critical remote code execution vulnerability known as Spring4Shell (CVE-2022-22965). According to the virtualization giant, the flaw impacts many of its cloud computing and virtualization products. The Spring4Shell issue was disclosed last week, [...] The post VMware released updates to fix the Spring4Shell vulnerability in multiple products appeared first on Security Affairs.

Cyware News - Latest Cyber News

WordPress Overtakes Magento in Credit Card Skimmers
Three main malware signatures account for roughly 40% of all detected credit card skimmers since January 2021. All three of them are most commonly found on WordPress websites.

Twitter

Sanjay Pandey

On a different note i m happy to train on cybrsecurity. Hope this does carry the message home. #cybersecurity

FBI

Join #FBI Cyber Section Chief Bryan Smith in this weeks panel discussion on emerging #cyber trends and shake-ups of 2021, including the landscape precipitating these trends and what cybersecurity leaders learned in response. Register at .

Spiros Margaris

15 Tech Leaders On The #NextBigThing In #Cybersecurity #fintech #blockchain #SaaS #privacy @Shirastweet @m49D4ch3lly @mclynd @missdkingsbury @ChuckDBrooks @digitalcloudgal @Forbes

Source: Have I been pwned?

Have I been pwnd

Nothing today

Source: Imperva DDOS Map

Top DDOS attackers

Source: Imperva DDOS Map

Top DDOS country targets

Source: Imperva DDOS Map

Top DDOS techniques

Source: Imperva DDOS Map

Top DDOS industry targets

Source: Hybrid Analysis

Top malicious URL

100% Threat score	https://hostrola.com/nhr/LW/B2/OlPLO72V.zip	100% Threat score	http://wallpaper.skin/office/updates/Gtkj
95% Threat score	http://182.117.48.237:34529/Mozi.m	91% Threat score	http://115.58.137.125:41971/i
91% Threat score	http://115.53.23.206:42862/bin.sh	91% Threat score	http://42.224.25.76:45434/Mozi.m
84% Threat score	https://bit.ly/3j8NOfg	82% Threat score	https://tiny-files.com/5f97de253f2435329c56e546/445686002),%202nd%20Edition%20by%20Kelly%20S
80% Threat score	https://placourier.com.pk/git/Fha/YTr/HRp/Uuba4AW.zip	78% Threat score	https://dlfreight.com/
77% Threat score	http://filecloudonline.com/	77% Threat score	http://hyla.org/
77% Threat score	http://clt954132.bmetrack.com/c/l?u=DAB8741&e=14261C3&c=E8F14&t=0&l=79C0788B&email=M%2Fex3Hy7rZ%2Fl6Q8FYFXtzrsUGZcpa2n9&seq=3	77% Threat score	http://carlosclassicmusclecars.com.au/
74% Threat score	http://119su.bg/	74% Threat score	http://gacogroupbd.com/
74% Threat score	http://gtjl7sc523.pdcdn1.top/		

Source: NIST

NIST CVE: High

Nothing today

Source: NIST

NIST CVE: Medium

Nothing today

Source: NIST

NIST CVE: Low

Nothing today

Source: NIST

NIST CVE: Unrated

CVE-2021-44109
A buffer overflow in lib/sbi/message.c in **Open5GS** 2.3.6 and earlier allows remote attackers to Denial of Service via a crafted sbi request.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-25154
A DLL hijacking vulnerability in **Samsung** portable SSD T5 PC software before 1.6.9 could allow a local attacker to escalate privileges. (An attacker must already have user privileges on **Windows** 7, 10, or 11 to exploit this vulnerability.)
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-23732
A path traversal vulnerability was identified in **GitHub Enterprise Server management console** that allowed the bypass of CSRF protections. This could potentially lead to privilege escalation. To exploit this vulnerability, an attacker would need to target a user that was actively logged into the management console. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.5 and was fixed in versions 3.1.19, 3.2.11, 3.3.6, 3.4.1. This vulnerability was reported via the GitHub Bug Bounty program.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-25356
ALIN **MDaemon Security Gateway** through 8.5.0 allows XML Injection.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2021-45893
An issue was discovered in Softwarebuero Zauner ARC 4.2.0.4. There is Improper Handling of Case Sensitivity, which makes password guessing easier.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2021-45891
An issue was discovered in Softwarebuero Zauner ARC 4.2.0.4., that allows attackers to escalate privileges within the application, since all permission checks are done client-side, not server-side.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-26281
BigAnt Server v5.6.06 was discovered to contain an incorrect access control issue.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-26619
Halo Blog CMS v1.4.17 was discovered to allow attackers to upload arbitrary files via the Attachment Upload function.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0789
Heap buffer overflow in ANGLE in **Google Chrome** prior to 99.0.4844.51 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0604
Heap buffer overflow in Tab Groups in **Google Chrome** prior to 98.0.4758.102 allowed an attacker who convinced a user to install a malicious extension and **engage** in specific user interaction to potentially exploit heap corruption via a crafted HTML page.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0807
Inappropriate implementation in Autofill in **Google Chrome** prior to 99.0.4844.51 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-26615
A cross-site scripting (XSS) vulnerability in College Website Content Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the User Profile Name text fields.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2021-44108
A null pointer dereference in src/amf/namf-handler.c in **Open5GS** 2.3.6 and earlier allows remote attackers to Denial of Service via a crafted sbi request to amf.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2021-39114
Affected versions of **Atlassian Confluence** Server and **Data Center** allow users with a valid account on a Confluence Data Center instance to execute arbitrary **Java** code or run arbitrary system commands by injecting an **OGNL** payload. The affected versions are before version 6.13.23, from version 6.14.0 before 7.4.11, from version 7.5.0 before 7.11.6, and from version 7.12.0 before 7.12.5.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2021-45894
An issue was discovered in Softwarebuero Zauner ARC 4.2.0.4. There is Cleartext **Transmission** of Sensitive Information.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2021-45892
An issue was discovered in Softwarebuero Zauner ARC 4.2.0.4. There is storage of Passwords in a Recoverable Format.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2021-42324
An issue was discovered on DCN (Digital China Networks) S4600-10P-SI devices before R0241.0470. Due to improper parameter validation in the console interface, it is possible for a low-privileged authenticated attacker to escape the sandbox environment and execute system commands as root via shell metacharacters in the capture command parameters. Command output will be shown on the Serial interface of the device. Exploitation requires both credentials and physical access.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0806
Data leak in **Canvas** in **Google Chrome** prior to 99.0.4844.51 allowed a remote attacker who convinced a user to **engage** in **screen** sharing to potentially leak cross-origin data via a crafted HTML page.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0454
Heap buffer overflow in ANGLE in **Google Chrome** prior to 98.0.4758.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0800
Heap buffer overflow in Cast UI in **Google Chrome** prior to 99.0.4844.51 allowed a remote attacker who convinced a user to **engage** in specific user interaction to potentially exploit heap corruption via a crafted HTML page.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2021-43008
Improper Access Control in Adminer versions 1.12.0 to 4.6.2 (fixed in version 4.6.3) allows an attacker to achieve Arbitrary File Read on the remote server by requesting the Adminer to **connect** to a remote **MySQL** database.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0466
Inappropriate implementation in Extensions Platform in **Google Chrome** prior to 98.0.4758.80 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted HTML page.

UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0455 Inappropriate implementation in Full **Screen** Mode in **Google Chrome** on **Android** prior to 98.0.4758.80 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0802 Inappropriate implementation in Full **screen** mode in **Google Chrome** on **Android** prior to 99.0.4844.51 allowed a remote attacker to **hide** the contents of the Omnibox (URL bar) via a crafted HTML page.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0804 Inappropriate implementation in Full **screen** mode in **Google Chrome** on **Android** prior to 99.0.4844.51 allowed a remote attacker to **hide** the contents of the Omnibox (URL bar) via a crafted HTML page.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0610 Inappropriate implementation in Gamepad API in **Google Chrome** prior to 98.0.4758.102 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0803 Inappropriate implementation in Permissions in **Google Chrome** prior to 99.0.4844.51 allowed a remote attacker to tamper with the contents of the Omnibox (URL bar) via a crafted HTML page.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0467 Inappropriate implementation in Pointer **Lock** in **Google Chrome** on **Windows** prior to 98.0.4758.80 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0462 Inappropriate implementation in Scroll in **Google Chrome** prior to 98.0.4758.80 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0799 Insufficient policy enforcement in Installer in **Google Chrome** on **Windows** prior to 99.0.4844.51 allowed a remote attacker to perform local privilege escalation via a crafted offline installer file.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0608 Integer overflow in Mojo in **Google Chrome** prior to 98.0.4758.102 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-26585 **Mingsoft MCMS** v5.2.7 was discovered to contain a SQL injection vulnerability via /cms/content/list.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0797 Out of bounds memory access in Mojo in **Google Chrome** prior to 99.0.4844.51 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0470 Out of bounds memory access in V8 in **Google Chrome** prior to 98.0.4758.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0809 Out of bounds memory access in WebXR in **Google Chrome** prior to 99.0.4844.51 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0792 Out of bounds read in ANGLE in **Google Chrome** prior to 99.0.4844.51 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0461 Policy bypass in COOP in **Google Chrome** prior to 98.0.4758.80 allowed a remote attacker to bypass **iframe** sandbox via a crafted HTML page.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-28355 randomUUID in **Scala**.js before 1.10.0 generates predictable values.
UNRATED Vector: unkown Created: 2022-04-02 Updated: 2022-04-05

CVE-2021-33616 RSA **Archer** 6.x through 6.9 SP1 P4 (6.9.1.4) allows stored XSS.
UNRATED Vector: unkown Created: 2022-04-04 Updated: 2022-04-05

CVE-2022-25584 Seyeon Tech Co., Ltd FlexWATCH FW3170-PS-E Network Video System 4.23-3000_GY allows attackers to access sensitive information.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-24231 Simple **Student Information System** v1.0 was discovered to contain a SQL injection vulnerability via add/Student.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-1213 SSRF filter bypass port 80, 433 in **GitHub** repository livehelperchat/livehelperchat prior to 3.67v. An attacker could make the application perform arbitrary requests, bypass CVE-2022-1191
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2021-33207 The HTTP client in MashZone NextGen through 10.7 GA deserializes untrusted data when it gets an HTTP response with a 570 **status** code.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-28380 The rc-httpd component through 2022-03-31 for 9front (Plan 9 fork) allows ..%2f directory traversal if **serve-static** is used.
UNRATED Vector: unkown Created: 2022-04-03 Updated: 2022-04-05

CVE-2022-23909 There is an unquoted service path in Sherpa **Connector** Service (SherpaConnectorService.exe) 2020.2.20328.2050. This might allow a local user to escalate privileges by creating a "C:\Program Files\Sherpa Software\Sherpa.exe" file.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0795 Type confusion in **Blink** Layout in **Google Chrome** prior to 99.0.4844.51 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0457 Type confusion in V8 in **Google Chrome** prior to 98.0.4758.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0463 Use after free in Accessibility in **Google Chrome** prior to 98.0.4758.80 allowed a remote attacker who convinced a user to **engage** in specific user interaction to potentially exploit heap corruption via user interaction.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0464 Use after free in Accessibility in **Google Chrome** prior to 98.0.4758.80 allowed a remote attacker who convinced a user to **engage** in specific user interaction to potentially exploit heap corruption via user interaction.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0606 Use after free in ANGLE in **Google Chrome** prior to 98.0.4758.102 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0609 Use after free in Animation in **Google Chrome** prior to 98.0.4758.102 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0805 Use after free in Browser Switcher in **Google Chrome** prior to 99.0.4844.51 allowed a remote attacker who convinced a user to **engage** in specific user interaction to potentially exploit heap corruption via user interaction.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0469 Use after free in Cast in **Google Chrome** prior to 98.0.4758.80 allowed a remote attacker who convinced a user to **engage** in specific interactions to potentially exploit heap corruption via a crafted HTML page.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0793 Use after free in Cast in **Google Chrome** prior to 99.0.4844.51 allowed an attacker who convinced a user to install a malicious extension and **engage** in specific user interaction to potentially exploit heap corruption via a crafted Chrome Extension.
UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0790
Use after free in Cast UI in **Google Chrome** prior to 99.0.4844.51 allowed a remote attacker who convinced a user to **engage** in specific user interaction to potentially perform a sandbox escape via a crafted HTML page.

UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0808
Use after free in **Chrome** OS Shell in **Google** Chrome on **Chrome OS** prior to 99.0.4844.51 allowed a remote attacker who convinced a user to **engage** in a series of user interaction to potentially exploit heap corruption via user interactions.

UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0465
Use after free in Extensions in **Google Chrome** prior to 98.0.4758.80 allowed a remote attacker to potentially exploit heap corruption via user interaction.

UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0603
Use after free in **File Manager** in **Google Chrome** on **Chrome OS** prior to 98.0.4758.102 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0607
Use after free in GPU in **Google Chrome** prior to 98.0.4758.102 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0796
Use after free in Media in **Google Chrome** prior to 99.0.4844.51 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0798
Use after free in MediaStream in **Google Chrome** prior to 99.0.4844.51 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension.

UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0791
Use after free in Omnibox in **Google Chrome** prior to 99.0.4844.51 allowed a remote attacker who convinced a user to **engage** in specific user interactions to potentially exploit heap corruption via user interactions.

UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0468
Use after free in **Payments** in **Google Chrome** prior to 98.0.4758.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0453
Use after free in **Reader** Mode in **Google Chrome** prior to 98.0.4758.80 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.

UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0452
Use after free in **Safe** Browsing in **Google Chrome** prior to 98.0.4758.80 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.

UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0459
Use after free in **Screen** Capture in **Google Chrome** prior to 98.0.4758.80 allowed a remote attacker who had compromised the renderer process and convinced a user to **engage** in specific user interaction to potentially exploit heap corruption via a crafted HTML page.

UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0458
Use after free in Thumbnail Tab Strip in **Google Chrome** prior to 98.0.4758.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0456
Use after free in **Web Search** in **Google Chrome** prior to 98.0.4758.80 allowed a remote attacker to potentially exploit heap corruption via profile destruction.

UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0794
Use after free in WebShare in **Google Chrome** prior to 99.0.4844.51 allowed a remote attacker who convinced a user to **engage** in specific user interaction to potentially exploit heap corruption via a crafted HTML page.

UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0605
Use after free in Webstore API in **Google Chrome** prior to 98.0.4758.102 allowed an attacker who convinced a user to install a malicious extension and convinced a user to enage in specific user interaction to potentially exploit heap corruption via a crafted HTML page.

UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-0460
Use after free in Window Dialogue in **Google Chrome** prior to 98.0.4758.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-1212
Use-After-Free in str_escape in mruby/mruby in **GitHub** repository mruby/mruby prior to 3.2. Possible arbitrary code execution if being exploited.

UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-1236
Weak Password Requirements in **GitHub** repository weseek/growi prior to v5.0.0.

UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

CVE-2022-1235
Weak secrethash can be brute-forced in **GitHub** repository livehelperchat/livehelperchat prior to 3.96.

UNRATED Vector: unkown Created: 2022-04-05 Updated: 2022-04-05

Source: SpamHaus

Top spamming countries


#1 United States of America


#2 China


#3 Russian Federation


#4 Mexico


#5 Dominican Republic


#6 Saudi Arabia


#7 India


#8 Uruguay


#9 Brazil


#10 Japan

Source: SpamHaus

Top spammers

#1 **Canadian Pharmacy**
A long time running pharmacy spam operation. They send tens of millions of spams per day using botnet techniques. Probably based in Eastern Europe, Ukraine/Russia. Host spammed web sites on botnets and on bulletproof Chinese & Russian web hosting.


#2 **PredictLabs / Sphere Digital**
This operation uses dozens of "hosting" companies as fronts to lease IP addresses which are then used to send spam. Based in Chicago, Illinois and Tangier, Morocco.


#3 **Hosting Response / Michael Boehm**
Snowshoe spam organization that uses large numbers of inexpensive, automated VPS hosting IP addresses and domains in whatever TLD is currently cheapest to


#4 **Michael Persaud**

send high volumes of spam to extremely dirty, scraped lists. Operates under many business and individual names. Owner or manager of these companies seems to be Michael Boehm and Associates.

Long time snowshoe type spammer, raided by FBI then indicted in 2017 on federal wire fraud charges tied to his spamming operations.

#5 **RetroCubes**
Web development, application development, and business training company that spams email appended lists, usually through ESPs that offer automated provisioning and services directed at small businesses.

#6 **Cyber World Internet Services/ e-Insites**
Bulletproof spam host operating Cyber World Internet Services / e-Insites, and currently spamming using a variety of aliases such as Brand 4 Marketing, Ad Media Plus, Site Traffic Network, RCM Delivery, and eBox. The company is owned or managed by Alvin Slocombe.

#7 **RR Media**
A high volume spam operation based in or run from Huntington Beach, CA, USA. The operation uses a variety of different names.

#8 **Kobeni Solutions**
High volume snowshoe spam operation based in Florida. The manager or owner of the company seems to be a Yair Shalev / . (Former?) partner-in-spam of ROKSO spammer Darrin Wohl. Son-in-law of ROKSO-listed spammer Dan Abramovich. Sued for fraud by the US FTC in 2014.

#9 **Richpro Trade Inc. / Richvestor GmbH**
Uses botnets or hires botnet spammers to send spam linking back to suspect investment, "quack-health-cures" and other sites that he owns or is an affiliate of. Botnet spamming and hosting sites on hacked servers is fully criminal in much of the world. Managed or owned by a Timo Richert.

Source: SpamHaus

Top countries with botnet

#1 China	#2 India
#3 United States of America	#4 Indonesia
#5 Thailand	#6 Algeria
#7 Viet Nam	#8 Brazil
#9 Pakistan	#10 Venezuela (Bolivarian Republic of)

Source: SpamHaus

Top phishing countries

#1 United States	#2 Russia
#3 Japan	#4 Germany
#5 Singapore	#6 United Kingdom
#7 Netherlands	#8 Ukraine
#9 Hong Kong	#10 Iran

Source: Hybrid Analysis

Top malicious files

100% Threat score	c59afba3f20006c146145d129ff5327255b25451ca7c39af68af749356061050	100% Threat score	%5cprogram files%5ccommon files%5cmicrosoft shared%5coffice12%5cmssoap30.dll
100% Threat score	ZoomInstaller.exe	100% Threat score	DentalCADApp.exe
100% Threat score	winrar.exe	100% Threat score	api-ms-win-base-util-l1-1-1.dll
100% Threat score	refresh	100% Threat score	signoPAD-API_Web_3.2.1.exe
100% Threat score	tmp_kp5u5c_	83% Threat score	Invoice INV-0152.html
76% Threat score	WYSIWYG Web Builder 17.exe		