Your Security Rabbits report for February 02, 2023

Hot topics

Nothing today

Source: CISA

CISA exploits

Nothing today

Source: Ransom Watch

Ransomware attacks

royal	wwwcasaleycommx/	lockbit3	pharmagestaocombr
alphv	SOTO Consulting Engineers	bianlian	N** ******

Source: NIST

NIST CVE: Critical

Nothing today

News

The Hacker News

Auditing Kubernetes with Open Source SIEM and XDR

Container technology has gained traction among businesses due to the increased efficiency it provides. In this regard, organizations widely use Kubernetes for deploying, scaling, and managing containerized applications. Organizations should audit Kubernetes to ensure compliance with regulations, find anomalies, and identify security risks. The Wazuh open source platform plays a critical role in

Cyware News - Latest Cyber News

BlackCat Ransomware Hits Defence Contractor, Steals Weapons Data

The BlackCat ransomware group claimed to have breached Solar Industries India and stolen 2 TB worth of data, containing military data related to weapons production. The stolen data includes details about the company's employees and customers, armament supply chains, and information about the other partners and contractors of the firm.

Cyware News - Latest Cyber News

BOXX Insurance raises $14.4 million to help customers stay ahead of cyber threats

The latest investment was led by Zurich Insurance Company (Zurich). BOXX also unveiled that its business met its combined goal to grow 10x in the last 24 months whilst continuing to outperform its underwriting targets.

The Hacker News

Experts Warn of 'Ice Breaker' Cyberattacks Targeting Gaming and Gambling Industry

A new attack campaign has been targeting the gaming and gambling sectors since at least September 2022, just as the ICE London 2023 gaming industry trade fair event is scheduled to kick off next week. Israeli cybersecurity company Security Joes is tracking the activity cluster under the name Ice Breaker, stating the intrusions employ clever social engineering tactics to deploy a JavaScript

CyberScoop

GoodRx will settle claim it shared sensitive health data with advertisers

The telehealth and discount drug provider promised health data would remain confidential and then allowed it to be used for targeted ads. The post GoodRx will settle claim it shared sensitive health data with advertisers appeared first on CyberScoop.

Cyware News - Latest Cyber News

IT Army of Ukraine Gained Access to a 1.5GB Archive From Russia's Gazprom

The group of Ukrainian hacktivists announced the hack on their Telegram channel claiming that the archive contains more than 6,000 files of the companies of the Gazprom group.

WeLiveSecurity

Less is more: Conquer your digital clutter before it conquers you

Lose what you don't use and other easy ways to limit your digital footprint and strengthen your online privacy and security The post Less is more: Conquer your digital clutter before it conquers you appeared first on WeLiveSecurity

Cyware News - Latest Cyber News

Microsoft's Verified Publisher Status Abused in Email Theft Campaign

The campaign mainly targeted Microsoft customers in Ireland and the UK. The tech giant has taken steps to disrupt the operation and it has published an article on how users can protect against these threats, which the company calls consent phishing.

Cyware News - Latest Cyber News

Mix of legacy OT and connected technologies creates security gaps

Rising threats to vehicles and industrial operational technology (OT) have led a growing number of enterprises worldwide to invest in advanced technologies and services to better secure their assets, according to an ISG research report.

Security Affairs

Nevada Ransomware Has Released Upgraded Locker

Researchers from Resecurity have identified a new version of Nevada Ransomware which recently emerged on the Dark Web right before the start of 2023. Resecurity, California-based cybersecurity company protecting Fortune 500 globally, has identified a new version of Nevada Ransomware which recently emerged on the Dark Web right before the start of 2023. The actors [...] The post Nevada Ransomware Has Released Upgraded Locker appeared first on Security Affairs.

Security Affairs

New LockBit Green ransomware variant borrows code from Conti ransomware

Lockbit ransomware operators have released a new version of their malware, LockBit Green, that also targets cloud-based services. Lockbit ransomware operators have implemented a new version of their malware, dubbed LockBit Green, which was designed to include cloud-based services among its targets. This is the third version of the ransomware developed by the notorious gang, [...] The post New LockBit Green ransomware variant borrows code from Conti ransomware appeared first on Security Affairs.

Security Affairs

New Prilex PoS Malware evolves to target NFC-enabled credit cards

Authors of the Prolex PoS malware improved their malicious code to target contactless credit card transactions. The threat actors behind the sophisticated point-of-sale (PoS) malware Prilex have have improved its capabilities to block contactless payment transactions. Researchers from Kaspersky Lab discovered three new versions of the PoS malware designed to target credit cards using NFC technology. [...] The post New Prilex PoS Malware evolves to target NFC-enabled credit cards appeared first on Security Affairs.

Cyware News - Latest Cyber News

New Sh1mmer ChromeBook exploit unenrolls managed devices

Security researchers from the Mercury Workshop Team have developed a new exploit called 'Shady Hacking 1nstrument Makes Machine Enrollment Retreat', or 'Sh1mmer,' that lets users unenroll their Chromebooks from enterprise management.

The Hacker News

New SH1MMER Exploit for Chromebook Unenrolls Managed ChromeOS Devices

A new exploit has been devised to "unenroll" enterprise- or school-managed Chromebooks from administrative control. Enrolling ChromeOS devices makes it possible to enforce device policies as set by the organization via the Google Admin console, including the features that are available to users. "Each enrolled device complies with the policies you set until you wipe or deprovision it," Google

The Hacker News

New Threat: Stealthy HeadCrab Malware Compromised Over 1,200 Redis Servers
At least 1,200 Redis database servers worldwide have been corralled into a botnet using an "elusive and severe threat" dubbed HeadCrab since early September 2021. "This advanced threat actor utilizes a state-of-the-art, custom-made malware that is undetectable by agentless and traditional anti-virus solutions to compromise a large number of Redis servers," Aqua security researcher Asaf Eitani

Security Affairs

Over 30k Internet-Exposed QNAP NAS hosts impacted by CVE-2022-27596 flaw
Censys found 30,000 internet-facing QNAP appliances potentially impacted by a recently disclosed critical code injection flaw. On January 30, Taiwanese vendor QNAP released QTS and QuTS firmware updates to address a critical vulnerability, tracked as CVE-2022-27596 (CVSS v3 score: 9.8), that affects QNAP NAS devices. A remote attacker can exploit the vulnerability to inject malicious code [...] The post Over 30k Internet-Exposed QNAP NAS hosts impacted by CVE-2022-27596 flaw appeared first on Security Affairs.

Naked Security

Password-stealing "vulnerability" reported in KeePass - bug or feature?
Is it a vulnerability if someone with control over your account can mess with files that your account is allowed to access anyway?

Cyware News - Latest Cyber News

Planet Ice Suffers Hack Resulting in Theft of 240,000 Customers' Accounts Details
The data from 240,488 customer accounts is now in the hands of hackers, including dates of birth, names, and genders of children having parties, email addresses, IP addresses, passwords, phone numbers, physical addresses, and purchases.

Cyware News - Latest Cyber News

Porsche halts NFT launch, phishing sites fill the void
Porsche cut its minting of a new NFT collection short after a dismal turnout and backlash from the crypto community, allowing threat actors to fill the void by creating phishing sites that steal digital assets from cryptocurrency wallets.

The Hacker News

Prilex PoS Malware Evolves to Block Contactless Payments to Steal from NFC Cards
The Brazilian threat actors behind an advanced and modular point-of-sale (PoS) malware known as Prilex have reared their head once again with new updates that allow it to block contactless payment transactions. Russian cybersecurity firm Kaspersky said it detected three versions of Prilex (06.03.8080, 06.03.8072, and 06.03.8070) that are capable of targeting NFC-enabled credit cards, taking its

Security Affairs

Pro-Russia Killnet group hit Dutch and European hospitals
The Dutch National Cyber Security Centre (NCSC) confirmed that Pro-Russia group Killnet hit websites of national and European hospitals. The Dutch National Cyber Security Centre (NCSC) reported that the websites of several hospital in the Netherlands and Europe were hit by DDoS attacks carried out by pro-Russia hacking group Killnet. The group of hackers launched [...] The post Pro-Russia Killnet group hit Dutch and European hospitals appeared first on Security Affairs.

Cyware News - Latest Cyber News

Pro-Russian DDoS attacks raise alarm in Denmark, U.S.
Since Russia began its invasion of Ukraine 11 months ago, hacking groups like Killnet and NoName057 have targeted an array of government institutions, businesses, and organizations across Europe and the United States.

Cyware News - Latest Cyber News

Ransomware Attack Forces the Closure of Four Public Schools in Nantucket
A ransomware attack forced the closure Tuesday of four public schools serving 1,700 students on the island of Nantucket, Massachusetts, the school district's superintendent said in an email to parents.

The Hacker News

Researchers Uncover New Bugs in Popular ImageMagick Image Processing Utility
Cybersecurity researchers have disclosed details of two security flaws in the open source ImageMagick software that could potentially lead to a denial-of-service (DoS) and information disclosure. The two issues, which were identified by Latin American cybersecurity firm Metabase Q in version 7.1.0-49, were addressed in ImageMagick version 7.1.0-52, released in November 2022. A

Cyware News - Latest Cyber News

Update: LockBit takes credit for November ransomware attack on Sacramento PBS station
The PBS station KVIE announced the attack on November 23, noting that some of its internal systems were affected on October 31. It immediately took systems offline, notified law enforcement, and hired experts to investigate the incident.

Cyware News - Latest Cyber News

Update: POC exploit released for VMware vRealize Log Insight vulnerabilities
Updates for the vulnerabilities are available for VMware vRealize Log Insight in the form of version 8.10.2. VMware also published workarounds as an alternative for affected customers.

CyberScoop

Vulnerabilities could let hackers remotely shut down EV chargers, steal electricity
The emerging market's uneven response to fix the flaws suggests cybersecurity could be a growing concern in electric car charging networks. The post Vulnerabilities could let hackers remotely shut down EV chargers, steal electricity appeared first on CyberScoop.

CyberScoop

Watchdog warns FDIC fails to test banks' cyberdefenses effectively
The agency's Office of Inspector General says staff at the prudential regulator are not being kept abreast of the latest cyberthreats. The post Watchdog warns FDIC fails to test banks' cyberdefenses effectively appeared first on CyberScoop.

Twitter

Binance

#Binance hosted a two-day cybersecurity training workshop in Colombia as part of our efforts to: Promote best practices Protect consumers Combat local crypto crime with law enforcement. We look forward to hosting tomorrow's forum as we close this series of workshops.

Linus Tech Tips

The best protection starts with common sense, but its not foolproof. Thats where @Bitdefender can help. Find the perfect #cybersecurity solution for you and your loved ones: #ad

Governor Tate Reeves

China is not our friend. Its time we realize that and recognize that TikTok is a major cybersecurity threat thats being used against Americans. Enjoyed discussing this and more with Neil Cavuto!

Gate.io

Get the latest scoop from the Fed FOMC meeting and how it affects #crypto Also, Uniswap governance voting will decide an important cybersecurity issue! Watch Now #Gateio #DailyNews #cryptomarket

Gautam S. Mengle

Not sure what the focus group for this research was but the women I know can talk very insightfully about politics, cybersecurity, international affairs, gender issues, inclusivity, psychology and art, to name a few subjects off the top of my head.

Source: Have I been pwned?

Have I been pwnd

School District 42 (sd42.ca)
In January 2023, Pitt Meadows School District 42 in British Columbia suffered a data breach. The incident exposed the names and email addresses of approximately 19k students and staff which were consequently redistributed on a popular hacking forum.

Count: 18850 Created: 2023-01-15 Updated: 2023-02-02

Source: Imperva DDOS Map

Top DDOS country targets

United States (44%)

Australia (11%)

Brazil (7%)

Source: Imperva DDOS Map

Top DDOS attackers

United States (38%)

Germany (15%)

Australia (9%)

Source: Imperva DDOS Map

Top DDOS techniques

50%	OWASP
41%	Automated Threat
9%	DDoS

Source: Imperva DDOS Map

Top DDOS industry targets

23%	Business
15%	Computing & IT
13%	Financial Services

Source: Hybrid Analysis

Top malicious URL

100% Threat score	http://c-agricolefrinfofr/
73% Threat score	https://bdd9a897-e3ab-4751-820e-8d9e152b9721idreplco/
72% Threat score	https://palatableutterdirectoriesicohsaversi0n1replco/
72% Threat score	https://ficoggs6788--enmanuelcorderoreplco/

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-2023-25014
UNRATED
Vector: unkown
Created: 2023-02-02
Updated: 2023-02-02

An issue was discovered in the **femanager** extension before 5.5.3, 6.x before 6.3.4, and 7.x before 7.1.0 for **TYPO3**. Missing access checks in the InvitationController allow an unauthenticated user to delete all frontend users.

CVE-2023-25013
UNRATED
Vector: unkown
Created: 2023-02-02
Updated: 2023-02-02

An issue was discovered in the **femanager** extension before 5.5.3, 6.x before 6.3.4, and 7.x before 7.1.0 for **TYPO3**. Missing access checks in the InvitationController allow an unauthenticated user to set the password of all frontend users.

CVE-2023-25015
UNRATED
Vector: unkown
Created: 2023-02-02
Updated: 2023-02-02

Clockwork Web before 0.1.2, when **Rails** before 5.2 is used, allows CSRF.

CVE-2023-23969
UNRATED
Vector: unkown
Created: 2023-02-01
Updated: 2023-02-02

In **Django** 3.2 before 3.2.17, 4.0 before 4.0.9, and 4.1 before 4.1.6, the parsed values of Accept-Language headers are **cached** in order to avoid repetitive parsing. This leads to a potential denial-of-service vector via excessive memory usage if the raw value of Accept-Language headers is very large.

CVE-2023-25012
UNRATED
Vector: unkown
Created: 2023-02-02
Updated: 2023-02-02

The **Linux** kernel through 6.1.9 has a Use-After-Free in bigben_remove in drivers/hid/hid-bigbenff.c via a crafted USB device because the LED controllers remain registered for too long.

Source: SpamHaus

Top spamming countries

#1 China	#2 United States of America
#3 Germany	#4 Saudi Arabia
#5 Mexico	#6 India

#7 Turkey

#8 Japan

#9 Dominican Republic

#10 France

Source: Hybrid Analysis

Top malicious files

100% Threat score	FreemakeVideoConverterSetup_3be2f2d1-ceb3-1cff-7d2d-89702e4ded84exe	100% Threat score	å¤©é©¬G å¯åŠ¨å™¨(ç¨³å®šç‰ˆ)exe
100% Threat score	Bonjour64msi	100% Threat score	bb2018dll
100% Threat score	4virus	100% Threat score	movieexe
100% Threat score	kswapd0_	100% Threat score	ADMGH_Installerexe
100% Threat score	avg_antivirus_free_setupexe	100% Threat score	winrar-x64-620exe
100% Threat score	vlc-setup-win64exe	100% Threat score	monkey-windows-64exe
100% Threat score	d835e918736fdcbe6a4b952f59059d9d1df2956f5c63758ed626cb2571a3e7eajs	100% Threat score	592217d2590ae9ca688346688b2d7d13a78190f9562889597ebb79060136034cexe
100% Threat score	3a7eef995236c7e9b182cb440127021ea5b5e105f54a900c11b7c1bb47512f41exe	100% Threat score	8ecc4898d03bf034a6586ff886d9883b2ac27d08bdfe70dbd9878a4d77d5dce8exe
100% Threat score	Assassins Creed Valhalla v102-v162 Plus 20 Trainerexe	100% Threat score	[1080p] - Copyscr
94% Threat score	Link_to_Windows_Service_LinkToWindowsServiceapk	85% Threat score	InstallVoodooShieldexe
75% Threat score	ScBr_x86_64	75% Threat score	gWEYuyexe
75% Threat score	nnhuWEYuyexe	75% Threat score	IPAssign_v113exe
73% Threat score	microexe		

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 **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 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.

#3 **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.

#4 **Michael Persaud**
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 **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.

#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 **Maili.ee**
Estonian B2B spammer for hire that spams mostly people in the Baltics and surrounding countries. The main company domain is "maili.ee". This spam entity is currently doing business as "Alfa Company Services OU", but the company name changes every few months. This operation is owned or managed by an individual who has in the past used the alias "Mihail Fortis" in domain registration records. Obtains service on VPS and cloud hosting providers using a large number of borrowed or forged identities.

#9 **SyedsMarketing**
Pakistan-based bulk email marketing company that spams opt-out lists of email addresses through purpose-created Google Groups. Businesses that use SyedsMarketing services are generally based in Pakistan, although some have been based in Middle Eastern countries as well.

Source: SpamHaus

Top countries with botnet

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

Source: SpamHaus

Top phishing countries

 #1 United States	 #2 France
 #3 Germany	 #4 Russia
#5 Singapore	 #6 Netherlands
 #7 Hong Kong	 #8 Italy
 #9 Australia	 #10 United Kingdom