



Your Security Rabbits report for February 20, 2022

Hot topics

Browser version 100

Chrome and Edge will reach version 100 by the end of March. Mozilla Firefox will reach it by May.

Experts fears that poorly written software or web sites will fail to detect the browser user agent version properly and will consider it as version 0.

Testers at Mozilla found out that Yahoo, HBO, and T-Mobile web sites for example had this problem. Have a look here <https://github.com/webcompat/web-bugs/labels/version100>

Some security solutions like proxies and web application firewalls also perform sanity checks by relying on the user agent signature. They might behave poorly. Check with your security solution providers they have anticipated this version 100 potential bug.

--
JL Dupont

Twitter



* W.
Brett
Wilson *

Could the hackers that discovered the folks donating to the Freedom Convoy now turn to figuring out who flew to the sex retreats hosted by Epstein and his lady friend? Can ya?



Watcher.Guru

JUST IN: #Coinbase has awarded \$250,000 to a white hat hacker for finding an exploit that potentially saved billions.



David
Roth

Enforcing the castle doctrine with extreme prejudice on the 15yo Estonian hacker who stole my collection of Based Shrimp NFTs.



Ran
NeuNer

GM (except to the following; @JustinTrudeau , @GaryGensler , the Opensea hacker , anyone who isnt buying this dip)



KreekCraft

That was the craziest stream ever.. We teamed up with the owner of HD Admin and caught the hackers behind all the recent game hacks like MeepCity & Find The Markers. Not only that, we talked to the entire Tubers93 hacking group on Discord. Thanks to the entire 40k who tuned in!



Lesley
Carhart

My favorite cybersecurity mentoring is honestly the random kids on Discord or middle-aged job changers at the bar who havent the foggiest who I am or that I have a Wikipedia under my gamertag, and yet want to learn how to do this work,



Hopewell
Chinono

An international watchdog that monitors cyber security and the Governance of the internet @netblocks will be monitoring Zimbabwes internet today after fears that it might be deliberately slowed down to black out #YellowSunday rally. Share you intern experiences tagging them too



True
North

Canadian hacker Aubrey Cottle has claimed responsibility for the illegal GiveSendGo data breach on Sunday that exposed the private information of thousands of people who donated to the Freedom Convoy fundraiser. Read more: #cdnpoli

Dr. @ratanlal72s @YouTube channel



Sumit
Chauhan

@Ambedkar_Nama is hacked by someone. It is sad that many of channels, who are raising questions on current regime are being attacked by hackers & @YouTubeIndia is not very helpful to recover such important voices. YouTube must restore channels.



Robert
M. Lee

Im very impressed with the professionals at the NSA, CISA, FBI, DOE, and others who have been significantly leaning in to try to be available and responsive on US infrastructure cybersecurity concerns these days. Seriously some awesome non public work taking place. Kudos yall



Ran
NeuNer

I understand why hackers would target normal (fungible) tokens, they are easy to liquidate them and can't really be traced. NFT'S are not fungible though. Anyone buying an NFT that was stolen is clearly buying stolen property. Is there really a market for marked stolen Jpegs?



Sharpp.eth

the hacker just hatched all my pixl pets and sent them back...

News



Security
Affairs

CISA compiled a list of free cybersecurity tools and services

The U.S. CISA has created a list of free cybersecurity tools and services that can help organizations increase their resilience. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) announced this week that it has compiled a list of free cybersecurity tools and services that can help organizations to reduce cybersecurity risk and increase resilience. The [...] The post CISA compiled a list of free cybersecurity tools and services appeared first on Security Affairs.



The Hacker
News

Justice Department Appoints First Director of National Cryptocurrency Enforcement Team

The U.S. Department of Justice (DoJ) earlier this week appointed Eun Young Choi to serve as the first Director of the National Cryptocurrency Enforcement Team (NCET) it established last year. The NCET was created to tackle the criminal misuse of cryptocurrencies and digital assets," with a focus on illegal activities in virtual currency exchanges, mixing and tumbling services, and money



The Hacker
News

Master Key for Hive Ransomware Retrieved Using a Flaw in its Encryption Algorithm

Researchers have detailed what they call the "first successful attempt" at decrypting data infected with Hive ransomware without relying on the private key used to lock access to the content. "We were able to recover the master key for generating the file encryption key without the attacker's private key, by using a cryptographic vulnerability identified through analysis," a group of academics



Security
Affairs

Trickbot operation is now controlled by Conti ransomware

The Conti ransomware group takes over TrickBot malware operation and plans to replace it with BazarBackdoor malware. TrickBot operation has arrived at the end of the journey, according to AdvIntel some of its top members move under the Conti ransomware gang, which is planning to replace the popular banking Trojan with the stealthier BazarBackdoor. TrickBot is [...] The post Trickbot operation is now controlled by Conti ransomware appeared first on Security Affairs.

Source: [NIST](#)

NIST CVE: Critical

Nothing today

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-2021-44731	<p>A race condition existed in the snapt 2.54.2 snap-confine binary when preparing a private mount namespace for a snap. This could allow a local attacker to gain root privileges by bind-mounting their own contents inside the snap's private mount namespace and causing snap-confine to execute arbitrary code and hence gain privilege escalation. Fixed in snapd versions 2.54.3+18.04, 2.54.3+20.04 and 2.54.3+21.10.1</p> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-02-17</div><div>Updated: 2022-02-20</div></div>	CVE-2021-44730	<p>snapt 2.54.2 did not properly validate the location of the snap-confine binary. A local attacker who can hardlink this binary to another location to cause snap-confine to execute other arbitrary binaries and hence gain privilege escalation. Fixed in snapd versions 2.54.3+18.04, 2.54.3+20.04 and 2.54.3+21.10.1</p> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-02-17</div><div>Updated: 2022-02-20</div></div>
CVE-2021-4120	<p>snapt 2.54.2 fails to perform sufficient validation of snap content interface and layout paths, resulting in the ability for snaps to inject arbitrary AppArmor policy rules via malformed content interface and layout declarations and hence escape strict snap confinement. Fixed in snapd versions 2.54.3+18.04, 2.54.3+20.04 and 2.54.3+21.10.1</p> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-02-17</div><div>Updated: 2022-02-20</div></div>		

Source: [Hybrid Analysis](#)

Top malicious files











100% Threat score	rpiboot_setup (.) exe	100% Threat score	Telegram (.) exe
100% Threat score	abobyc (.) exe	100% Threat score	tmpwvp2engj
100% Threat score	tmpdmpn6jqj	100% Threat score	eblagh (.) apk
100% Threat score	setup-multi2 (.) exe	100% Threat score	spoolsv (.) exe
100% Threat score	tmp1u1xb7p7	100% Threat score	tmpp6narih4
100%	svchost (.) com	100%	0b5aa55fa15468a285fc5c6547d3c0d9889de0af

Threat score	
100% Threat score	deemix-gui Setup (.) exe
100% Threat score	psiphon3 (.) exe
87% Threat score	sm64pcBuilder2 (.) exe
84% Threat score	macosx (.) dat
79% Threat score	ATT23968_Seadrill (.) comHYZ162HYZ38KP3KP (.) html
77% Threat score	main (.) exe
75% Threat score	setup (.) exe
75% Threat score	setup (.) exe

Threat score	(.) doc
100% Threat score	file-ake11lmwfvzcZhi64IL!J
99% Threat score	Honda CANBUS Utility (.) exe
84% Threat score	macosx (.) dat
80% Threat score	tmp6h6s7ljt
79% Threat score	4523-wav-audio-sarah (.) cotgrave-Seadrill (.) html
77% Threat score	ATT01174 (.) HTM
75% Threat score	Win_x64_814251_mini_installer (.) exe

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 Japan
	#9 Brazil		#10 Korea, Republic of

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 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.



#4 **Mint Global Marketing / Adgenics / Cabo Networks**

Florida affiliate spammers and bulletproof spam hosts



#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 **Michael Persaud**

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



#7 **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.



#8 **RR Media**

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



#9 **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.

Source: *Hybrid Analysis*

Top malicious URL

100%
Threat score

[https://tt\(.\)sigmarket\(.\)tv/\(.\)well-known/policy\(.\)php?ss=2](https://tt(.)sigmarket(.)tv/(.)well-known/policy(.)php?ss=2)

100%
Threat score

[http://61\(.\)52\(.\)35\(.\)231:56223/bin\(.\)sh](http://61(.)52(.)35(.)231:56223/bin(.)sh)

100%
Threat score

[http://cherryemoore\(.\)com/USPS/RedeliveryUSPS\(.\)jar](http://cherryemoore(.)com/USPS/RedeliveryUSPS(.)jar)

93%
Threat score

[http://5\(.\)138\(.\)236\(.\)204:53059/i](http://5(.)138(.)236(.)204:53059/i)

93%
Threat score

[http://61\(.\)54\(.\)61\(.\)37:48154/i](http://61(.)54(.)61(.)37:48154/i)

93%
Threat score

[http://115\(.\)52\(.\)173\(.\)119:48296/mozi\(.\)m](http://115(.)52(.)173(.)119:48296/mozi(.)m)

93%
Threat score

[http://115\(.\)56\(.\)165\(.\)166:35857/i](http://115(.)56(.)165(.)166:35857/i)

92%
Threat score

[http://haus-pesjak\(.\)at/Covid-19Update\(.\)jar](http://haus-pesjak(.)at/Covid-19Update(.)jar)

82%
Threat score

[https://thediscoveryrun\(.\)com/UPS/ShippingInfo\(.\)jar](https://thediscoveryrun(.)com/UPS/ShippingInfo(.)jar)

82%
Threat score

[https://www\(.\)stillval\(.\)com/USPS/RescheduleUSPS\(.\)jar](https://www(.)stillval(.)com/USPS/RescheduleUSPS(.)jar)

77%
Threat score

[http://mcusercontent\(.\)com/bab6f874a0f823a262d20bc04/files/57ba105d-a11e-97dd-d8cc-789dcc16374c/code_of_conduct\(.\)pdf](http://mcusercontent(.)com/bab6f874a0f823a262d20bc04/files/57ba105d-a11e-97dd-d8cc-789dcc16374c/code_of_conduct(.)pdf)

77%
Threat score

[http://boa\(.\)com/](http://boa(.)com/)

75% Threat score	http://www(.)0202(.)com(.)tw/~miki/9dwjrv/1mumq(.)html	74% Threat score
74% Threat score	http://msv97umqkm(.)meta-ninth(.)xyz/zhzc(.)php?anli=swar&v=ss1645346029094	https://www(.)onfeetnation(.)com/profiles/blogs/joe-biden-says-now-convinced-putin-has-decided-to-invade-ukraine

Source: *SpamHaus*

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

Source: *SpamHaus*

Top phishing countries	
	#1 United States
	#2 France
	#3 India
	#4 Germany
	#5 Russia
	#6 Hong Kong
	#7 Netherlands
	#8 Singapore
	#9 Sweden
	#10 Japan