



Your Security Rabbits report for March 13, 2022

Source: [Ransom Watch](#)

Ransomware attacks

lockbit2	Target: ambujaneotia . co . . . (2022-03-13)	vicesociety	Target: SENADO Argentina(2022-03-13)
lockbit2	Target: scanvogn . com(2022-03-13)	lockbit2	Target: danubiushotels (2022-03-13)
lockbit2	Target: etrps . de(2022-03-13)	lockbit2	Target: ikk-group . com(2022-03-13)
lockbit2	Target: ymcad(2022-03-12)	everest	Target: XEFI / Neocyber(2022-03-12)
lockbit2	Target: snteseccion30sa . . . (2022-03-12)	lockbit2	Target: orientalaromati . . . (2022-03-12)
alphv	Target: inibsa . com inibsadental . com inibsa . net(2022-03-12)	lockbit2	Target: etg . digital(2022-03-12)
lockbit2	Target: cachibi . co(2022-03-12)	arvinclub	Target: bedfordshire . police . uk(2022-03-12)
everest	Target: SPERONI SpA(2022-03-11)	lockbit2	Target: sysmac . com . sg(2022-03-11)
lockbit2	Target: tingtong . com . cn(2022-03-11)	lockbit2	Target: weber-betonpump . . (2022-03-11)
lockbit2	Target: fer(2022-03-10)	lockbit2	Target: bioskin . sg(2022-03-10)
conti	Target: Great HealthWorks(2022-03-09)	lockbit2	Target: bridgestoneamer . . . (2022-03-09)
conti	Target: TST Logistics(2022-03-09)	conti	Target: Aluminerie Alouette(2022-03-09)
lockbit2	Target: hamm(2022-03-08)	conti	Target: Myron Corp . (2022-03-08)
everest	Target: XEFI(2022-03-08)		

Hot topics

Nothing today

News



Attackers use website contact forms to spread BazarLoader malware

Threat actors are spreading the BazarLoader malware via website contact forms to evade detection, researchers warn. Researchers from cybersecurity firm Abnormal Security observed threat actors spreading the BazarLoader/BazarBackdoor malware via website contact forms. TrickBot operation has recently arrived at the end of the journey, according to AdvIntel some of its top members move under the Conti ransomware gang, [...] The post Attackers use website contact forms to spread BazarLoader malware appeared first on Security Affairs.



LockBit ransomware group claims to have hacked Bridgestone Americas

LockBit ransomware gang claimed to have hacked Bridgestone Americas, one of the largest manufacturers of tires. LockBit ransomware gang claimed to have compromised the network of Bridgestone Americas, one of the largest manufacturers of tires, and stolen data from the company. The Bridgestone Americas family of enterprises includes more than 50 production facilities and 55,000 [...] The post LockBit ransomware group claims to have hacked Bridgestone Americas appeared first on Security Affairs.



New Exploit Bypasses Existing Spectre-V2 Mitigations in Intel, AMD, Arm CPUs

Researchers have disclosed a new technique that could be used to circumvent existing hardware mitigations in modern processors from Intel, AMD, and Arm, and stage speculative execution attacks such as Spectre to leak sensitive information from host memory. Attacks like Spectre are designed to break the isolation between different applications by taking advantage of an optimization technique



Russian Internet watchdog Roskomnadzor is going to ban Instagram Russian Internet watchdog Roskomnadzor is going to ban Instagram in Russia to prevent the spreading of info related to the Ukraine invasion. Russia will ban Instagram, the decision was announced by Russian Internet watchdog Roskomnadzor. Officially the Russian Internet watchdog Roskomnadzor explained that the decision is the response of Meta that the posting of information [...] The post Russian Internet watchdog Roskomnadzor is going to ban Instagram appeared first on Security Affairs.

Twitter



Rep. Val Demings

Last night we passed the federal budget to keep us SAFE. I voted to strengthen Americas military and provide strong resources for: - Securing our border - Homeland security grants that protect communities & houses of worship - Cybersecurity - Coast Guard and port security



Gary Gensler

Join us in now at our Investor Advisory Committee Meeting. Todays agenda includes a panel on artificial intelligence and robo-advising and a discussion on cybersecurity disclosures.



Dave Rubin

This man slept with a Chinese spy and is now giving cybersecurity tips. Please fact check me, @twitter[...]



Spiros Margaritis

The best #Indian #conferences for #womenintech in 2022 #fintech #cybersecurity @Analyticsindiam

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-2021-36368

**** DISPUTED **** An issue was discovered in **OpenSSH** before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot **determine** whether FIDO authentication is going to confirm that the user wishes to **connect** to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is "this is not an authentication bypass, since nothing is being bypassed."

UNRATED	Vector: unknwn	Created: 2022-03-13	Updated: 2022-03-13
---------	----------------	---------------------	---------------------

CVE-2021-45887

An issue was discovered in PONTON X/P **Messenger** before 3.11.2. Due to path traversal in private/SchemaSetUpload.do for uploaded ZIP files, an executable script can be uploaded by web application administrators, giving the attacker remote code execution on the underlying server via an imgs/* .jsp URI.

UNRATED	Vector: unknwn	Created: 2022-03-13	Updated: 2022-03-13
---------	----------------	---------------------	---------------------

CVE-2021-45888

An issue was discovered in PONTON X/P **Messenger** before 3.11.2. The navigation tree that is shown on the left side of every page of the web application is vulnerable to XSS: it allows injection of JavaScript into its nodes. Creating such nodes is only possible for users who have the role Configuration Administrator or Administrator.

UNRATED	Vector: unknwn	Created: 2022-03-13	Updated: 2022-03-13
---------	----------------	---------------------	---------------------

CVE-2021-45886

An issue was discovered in PONTON X/P **Messenger** before 3.11.2. Anti-CSRF tokens are globally valid, making the web application vulnerable to a weakened version of CSRF, where an arbitrary token of a low-privileged user (such as operator) can be used to confirm actions of higher-privileged ones (such as xpadmin).

UNRATED	Vector: unknwn	Created: 2022-03-13	Updated: 2022-03-13
---------	----------------	---------------------	---------------------

CVE-2021-45889

An issue was discovered in PONTON X/P **Messenger** before 3.11.2. Several functions are vulnerable to reflected XSS, as demonstrated by private/index.jsp?partners/ShowNonLocalPartners.do?localID= or private/index.jsp or private/index.jsp?database/databaseTab.jsp or private/index.jsp?activation/activationMainTab.jsp or private/index.jsp?communication/serverTab.jsp or private/index.jsp?emailNotification/notificationTab.jsp.

UNRATED	Vector: unknwn	Created: 2022-03-13	Updated: 2022-03-13
---------	----------------	---------------------	---------------------

CVE-2022-23960

Certain Arm **Cortex** and Neoverse processors through 2022-03-08 do not properly restrict cache speculation, aka Spectre-BHB. An attacker can leverage the shared branch history in the Branch History Buffer (BHB) to influence mispredicted branches. Then, cache allocation can allow the attacker to obtain sensitive information.

UNRATED	Vector: unknwn	Created: 2022-03-13	Updated: 2022-03-13
---------	----------------	---------------------	---------------------

Source: *Hybrid Analysis*

Top malicious files

100% Threat score n3xviruz (.) exe

100% Threat score GhostCosmeticsFree (.) exe

100% Threat score tkraw_Protected99 (.) exe

100% Threat score arm

100% Threat score	sec-request_0311 (.) xlsb	100% Threat score	carlos-arana-bossa-n-62S7Lajvu7 (.) exe
100% Threat score	13 (.) exe	100% Threat score	WeMod-8 (.) 0 (.) 7 (.) exe
100% Threat score	Macro Flooding Tool (Blue) (.) exe	100% Threat score	kswapd0
100% Threat score	Brave Browser (.) exe	99% Threat score	File_Manager_File Explorer_Premium_v1 (.) 17 (.) 1_Mod_AOSP_No_Google_Apk4all (.) com (.) apk
98% Threat score	onions1337 (.) x86	96% Threat score	n3xxviruz (.) exe
90% Threat score	111 (.) exe	85% Threat score	ChromeStandaloneSetup64 (.) exe
85% Threat score	AxisRadarTrackingForPtzSetup (.) exe	85% Threat score	FontLab-7-Win64-Install-7649 (.) exe
85% Threat score	T8 RGB keyboard Driver(English) (.) exe	85% Threat score	windows10manager (.) exe
85% Threat score	OCTGN-Setup-3 (.) 4 (.) 362 (.) 0 (.) msi	85% Threat score	setup (.) exe
81% Threat score	Extra Lives_v1 (.) 14_mod_apkdone (.) com (.) apk	75% Threat score	GRUNDIG Finder (.) exe
73% Threat score	enemybotmips		





Source: *Hybrid Analysis*




Top malicious URL

97% Threat score	http://222 (.) 137 (.) 164 (.) 247:45173/Mozi (.) m	97% Threat score	http://119 (.) 112 (.) 250 (.) 113:55216/i
93% Threat score	http://117 (.) 215 (.) 211 (.) 19:37667/Mozi (.) m	93% Threat score	http://makosoft (.) hu/out_1 (.) exe
93% Threat score	http://220 (.) 133 (.) 159 (.) 3:40747/i	88% Threat score	http://113 (.) 90 (.) 171 (.) 71:50981/i
87% Threat score	http://coiningsparkmine (.) com/	82% Threat score	http://runpen (.) dothome (.) co (.) kr/20 (.) 06 (.) 2019_701 (.) 82 (.) doc
82% Threat score	http://favoacew (.) com/Xwr	82% Threat score	http://runpen (.) dothome (.) co (.) kr/20 (.) 06 (.) 2019_673 (.) 81 (.) doc
77% Threat score	http://edt (.) csoonline (.) com/c/1293nwNzT1Xc7qB4XhGxpPd4cuz0S	77% Threat score	http://www (.) unclaimedassets2022 (.) click/d8b4Q2395uAp8612O_P51obU103z15UacD6bfbGvGEsvZ6cda9Rm5J10x_5ElJwD/movable-murderers?mc_phishing_protection_id=28047-c8mmbcidu815i9djsiu0
77% Threat score	http://worksolutionsrome (.) org/~terryh/20 (.) 06 (.) 2019_430 (.) 22 (.) xls	77% Threat score	http://fapdrop (.) com/
74% Threat score	https://www (.) bleachbit (.) org/download/file/t?file=BleachBit-4 (.) 4 (.) 2-setup (.) exe	72% Threat score	http://lemonstre (.) fr/
72% Threat score	http://foodline (.) site/	72% Threat score	http://reboot (.) pro/index (.) php?showtopic=7739&page=31

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 Brazil
	#9 Japan		#10 Uruguay

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 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 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 Thailand
	#5 Indonesia		#6 Algeria
	#7 Viet Nam		#8 Iran (Islamic Republic of)
	#9 Brazil		#10 Pakistan

Source: [SpamHaus](#)

Top phishing countries

	#1 United States		#2 Germany
	#3 Singapore		#4 Russia
	#5 Netherlands		#6 Japan



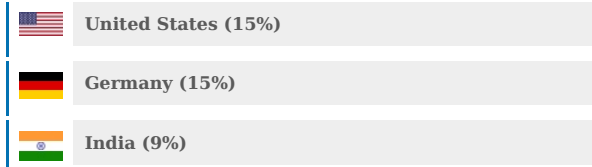
Source: [Have I been pwned?](#)

Have I been pwned

Nothing today

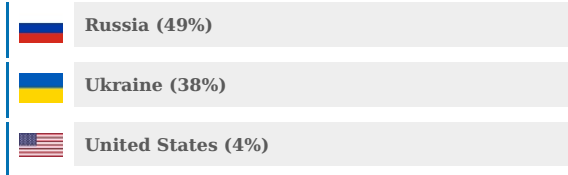
Source: [Imperva DDOS Map](#)

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

