



Your Security Rabbits report for March 14, 2022

Source: [Ransom Watch](#)

Ransomware attacks

everest Target: News(2022-03-14)

Hot topics

Nothing today

News



Security
Affairs

Anonymous sent a message to Russians: "remove Putin"

Anonymous has published a new message for Russian citizens inviting them to remove Putin that is sacrificing them and killing Ukrainians. The hacker collective Anonymous has published a new message for Russians inviting them to wake up and remove Putin, who is responsible for war crimes against Ukrainian. Putin is killing a defenseless population, it [...] The post Anonymous sent a message to Russians: "remove Putin" appeared first on Security Affairs.



Security
Affairs

Brazilian trojan impacting Portuguese users and using the same capabilities seen in other Latin American threats

Brazilian trojan impacting Portuguese users and using the same capabilities seen in other Latin American threats Introduction A new variant of a Brazilian trojan has impacted Internet end users in Portugal since last month (February 2022). Although there are no significant differences and sophistication in contrast to other well-known trojans such as Maxtrilha, URSA, and Javali, an analysis [...] The post Brazilian trojan impacting Portuguese users and using the same capabilities seen in other Latin American threats appeared first on Security Affairs.



Cyware
News -
Latest Cyber
News

Emotet Trojan Shows Strong Resurgence as it Reboots Itself

In November 2021, the Emotet trojan reportedly made a strong comeback with the help of TrickBot. Since that time, the trojan has matured with new functions and modules to target more organizations. According to Black Lotus Labs' telemetry, the trojan has infected approximately 130,000 systems across 179 countries in the last 4 months.



Cyware
News -
Latest Cyber
News

Fake Valorant cheats on YouTube infect you with RedLine stealer

The campaign spotted by ASEC targets the gaming community of Valorant, a free first-person shooter for Windows, offering a link to download an auto-aiming bot on the video description.



Security
Affairs

Mar 06- Mar 12 Ukraine - Russia the silent cyber conflict

This post provides a timeline of the events related to the Russia invasion of Ukraine from the cyber security perspective. March 12 - Russian Internet watchdog Roskomnadzor is going to ban Instagram



CyberScoop

Political fallout in cybercrime circles upping the threat to Western targets

Political motivations might be making the cybercrime underground a more dangerous place, researchers say. The post Political

Russian Internet watchdog Roskomnadzor is going to ban Instagram in Russia to prevent the spreading of info related to the Ukraine invasion. March [...] The post Mar 06- Mar 12 Ukraine - Russia the silent cyber conflict appeared first on Security Affairs.

fallout in cybercrime circles upping the threat to Western targets appeared first on CyberScoop.



Researchers Disclose New Variant of Spectre Attack

Dubbed Spectre-BHI (Branch History Injection), the new speculative injection attack was first demonstrated by VuSec researchers in collaboration with Intel. It's a variant of Spectre-BTI (Branch Target Injection) discovered in 2017.

The Hacker News

The Hacker News

Researchers Find New Evidence Linking Kwampirs Malware to Shamoon APT Hackers

New findings released last week showcase the overlapping source code and techniques between the operators of Shamoon and Kwampirs, indicating that they "are the same group or really close collaborators." "Research evidence shows identification of co-evolution between both Shamoon and Kwampirs malware families during the known timeline," Pablo Rincon Crespo of Cylera Labs said. "If Kwampirs is



Security Affairs

Russia-Ukraine cyber conflict poses critical infrastructure at risk

While the Russia-Ukraine cyber conflict goes on, nation-state actors, crooks, and hacktivists continue to pose critical infrastructure at risk. Critical infrastructure is a privileged target for almost any kind of threat actor, the ongoing Russia-Ukraine cyber conflict is posing them at risk. Ongoing attacks could cause severe damages to multiple sectors, including transportation, communication, financial [...] The post Russia-Ukraine cyber conflict poses critical infrastructure at risk appeared first on Security Affairs.



Cyware News - Latest Cyber News

Russian defense firm Rostec shuts down website after DDoS attack

"We had to briefly close the website. The attack has been repelled, and now the website is functioning again and all information about the corporation is available in full," Rostec told Interfax.



Naked Security

S3 Ep73: Ransomware with a difference, dirty Linux pipes, and much more [Podcast + Transcript]

Latest episode - listen now!



Cyware News - Latest Cyber News

Suspected Ransomware Attack with Custom-Made Tool

Most notably, they used an altered version of Ligolo--Sockbot--a reverse tunneling tool that is available on GitHub. Along with it, they used another custom tool to dump credentials from LSASS.



Security Affairs

The hidden C2: Lampion trojan release 212 is on the rise and using a C2 server for two years

The hidden C2: Lampion trojan release 212 is on the rise and using a C2 server for two years. Lampion trojan is one of the most active banking trojans impacting Portuguese Internet end users since 2019. This piece of malware is known for the usage of the Portuguese Government Finance & Tax (Autoridade Tributaria e Aduaneira) email [...] The post The hidden C2: Lampion trojan release 212 is on the rise and using a C2 server for two years appeared first on Security Affairs.



IT Security Guru

UK announces digital identity security legislation

The UK government has announced plans to introduce new legislation, aiming to improve the security of digital identity solutions. The rules are designed to enhance trust in digital identities and scaling down reliance on physical documents such as passports and driving licenses. The UK's Department for Digital, Culture, Media and Sport (DCMS) made the announcement [...] The post UK announces digital identity security legislation appeared first on IT Security Guru.



IT Security Guru

Ukraine's "IT Army" hit with info-stealing malware

Security researchers have warned pro-Ukrainian actors of employing DDoS tools to attack Russia, as they may be ridden with info-stealing malware. In late February, Ukrainian vice prime minister, Mykhailo Fedorov, called for a volunteer "IT army" of

hackers to DDoS Russian targets. Cisco Talos has claimed that many cyber criminals are attempting to exploit the outpouring of [...] The post Ukraine's "IT Army" hit with info-stealing malware appeared first on IT Security Guru.

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



Dave Rubin

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



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.



Spiros Margaris

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

CVE-2022-26533

Alist v2.1.0 and below was discovered to contain a cross-site scripting (XSS) vulnerability via /i/:data/ipa.plist.

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: unknown	Created: 2022-03-13	Updated: 2022-03-14
---------	-----------------	---------------------	---------------------

CVE-2022-26276

An issue in index.php of OneNav v0.9.14 allows attackers to perform directory traversal.

UNRATED	Vector: unknown	Created: 2022-03-12	Updated: 2022-03-14
---------	-----------------	---------------------	---------------------

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: unknown	Created: 2022-03-13	Updated: 2022-03-14
---------	-----------------	---------------------	---------------------

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: unknown	Created: 2022-03-13	Updated: 2022-03-14
---------	-----------------	---------------------	---------------------

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: unknown	Created: 2022-03-12	Updated: 2022-03-14
---------	-----------------	---------------------	---------------------

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: unknown	Created: 2022-03-13	Updated: 2022-03-14
---------	-----------------	---------------------	---------------------

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?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: unknown	Created: 2022-03-13	Updated: 2022-03-14
---------	-----------------	---------------------	---------------------

CVE-2022-26966

An issue was discovered in the **Linux** kernel before 5.16.12. drivers/net/usb/sr9700.c allows attackers to obtain sensitive information from heap memory via crafted **frame** lengths from a device.

UNRATED	Vector: unknown	Created: 2022-03-12	Updated: 2022-03-14
---------	-----------------	---------------------	---------------------

CVE-2022-0880

Cross-site Scripting (XSS) - Stored in **GitHub** repository star7th/showdoc prior to 2.10.2.

UNRATED	Vector: unknown	Created: 2022-03-13	Updated: 2022-03-14
---------	-----------------	---------------------	---------------------

UNRATED

Vector: unknown
Created: 2022-03-13
Updated: 2022-03-14

unknown 12 14

CVE-2022-0341

Cross-site Scripting (XSS) - Stored in **GitHub** repository vanessa219/vditor prior to 3.8.12.

UNRATED

Vector: unknown
Created: 2022-03-14
Updated: 2022-03-14

CVE-2022-0926

File upload filter bypass leading to stored XSS in **GitHub** repository microweber/microweber prior to 1.2.12.

UNRATED

Vector: unknown
Created: 2022-03-12
Updated: 2022-03-14

CVE-2022-0930

File upload filter bypass leading to stored XSS in **GitHub** repository microweber/microweber prior to 1.2.12.

UNRATED

Vector: unknown
Created: 2022-03-12
Updated: 2022-03-14

CVE-2022-26967

GPAC 2.0 allows a heap-based buffer overflow in gf_base64_encode. It can be triggered via MP4Box.

UNRATED

Vector: unknown
Created: 2022-03-12
Updated: 2022-03-14

CVE-2022-26981

Liblouis through 3.21.0 has a buffer overflow in compilePassOpcode in compileTranslationTable.c (called, indirectly, by tools/lou_checktable.c).

UNRATED

Vector: unknown
Created: 2022-03-13
Updated: 2022-03-14

CVE-2022-24696

Mirametrix **Glance** before 5.1.1.42207 (released on 2018-08-30) allows a local attacker to elevate privileges. NOTE: this is unrelated to products from the glance.com and glance.net websites.

UNRATED

Vector: unknown
Created: 2022-03-13
Updated: 2022-03-14

CVE-2021-46709

phpLiteAdmin through 1.9.8.2 allows XSS via the index.php numberOfRows parameter (aka num or number).

UNRATED

Vector: unknown
Created: 2022-03-13
Updated: 2022-03-14

CVE-2022-0937

Stored xss in **showdoc** through file upload in **GitHub** repository star7th/showdoc prior to 2.10.4.

UNRATED

Vector: unknown
Created: 2022-03-14
Updated: 2022-03-14

CVE-2022-0938

Stored XSS via file upload in **GitHub** repository star7th/showdoc prior to v2.10.4.

UNRATED

Vector: unknown
Created: 2022-03-14
Updated: 2022-03-14

CVE-2021-43954

The DefaultRepositoryAdminService class in **Fisheye** and **Crucible** before version 4.8.9 allowed remote attackers, who have 'can add repository permission', to enumerate the existence of internal network and filesystem **resources** via a Server-Side Request Forgery (SSRF) vulnerability.

UNRATED

Vector: unknown
Created: 2022-03-14
Updated: 2022-03-14

CVE-2022-24128

Timescale TimescaleDB 1.x and 2.x before 2.5.2 may allow privilege escalation during extension installation.

UNRATED

Vector: unknown
Created: 2022-03-13
Updated: 2022-03-14

CVE-2022-0929

XSS on dynamic_text module in **GitHub** repository microweber/microweber prior to 1.2.11.







UNRATED

Vector: unknown
Created: 2022-03-12
Updated: 2022-03-14










Top malicious files			
100% Threat score	Uzsakymo specifikacijos (.) exe	100% Threat score	OperaSetup (.) exe
100% Threat score	CockpitSimulator v0 (.) 9 (.) 101 (.) exe	100% Threat score	IncomeInstaller (.) exe
100% Threat score	Uzsakymo specifikacijos (.) exe	100% Threat score	GoogleEarthProSetup (.) exe
100% Threat score	Vibory (.) exe	100% Threat score	ok-14032022 (.) xlsx
100% Threat score	Sophia (.) exe	100% Threat score	JuniperSetupClientInstaller (.) exe
97% Threat score	Ponudba izdelkov_35675387 (.) xlsx	96% Threat score	PO16213 (.) xlsx
95% Threat score	AcademyOESetup (.) exe	85% Threat score	Xjnnpfmtmgzsjdtbismbqwngwvhuqbxdfh (.) exe
85% Threat score	PIME-G6Win10-1 (.) 2 (.) 0-beta-setup (.) exe	85% Threat score	winrar-x64-610it (.) exe
83% Threat score	c0g5j7hkn7e5qpqwekd78us5l (.) docx	75% Threat score	AvramisGoldIndicator (AGI) (.) exe
72% Threat score	(.) SecureMessageAtt (.) html		

Top malicious URL			
100% Threat score	http://updatesgarmin (.) com/c/X5oK7bz/	100% Threat score	http://seasonunwaveringnatural (.) shop/
91% Threat score	http://d9abm3muima3c (.) cloudfront (.) net/installer/25236277/5953625062450	88% Threat score	http://compmasipokick (.) tk/?rTvgEu
77% Threat score	http://www (.) e4u (.) com (.) pk/	77% Threat score	http://google (.) lpetkov (.) net/
77% Threat score	http://www (.) globetravel-bg (.) com/	77% Threat score	http://service-client-3dff5edeb9f2 (.) intercom-mail (.) com/
77% Threat score	http://google (.) lpetkov (.) net/	75% Threat score	http://d2qrgzarndv7em (.) cloudfront (.) net/installer/0301026734/891084
74% Threat score	http://www (.) omed (.) bg/	72% Threat score	http://bit-pazar (.) eu/

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

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 Japan

Source: [SpamHaus](#)

Top phishing countries	
 #1 United States	 #2 Germany
 #3 Russia	 #4 Singapore
 #5 Netherlands	 #6 Finland
 #7 Australia	 #8 Hong Kong
 #9 Ukraine	 #10 Japan

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

Have I been pwnd

Nothing today

Source: [Imperva DDOS Map](#)

Top DDOS attackers

Top DDOS country targets

Top DDOS techniques

Top DDOS industry targets