Your Security Rabbits report for March 20, 2022

Source: Ransom Watch

Ransomware attacks

lockbit2	connectcec,com	lockbit2	danubius-exim,r,,,
conti	MJH Life Sciences	conti	PFC USA
conti	BAUKING	conti	bChannels Ltd,
lockbit2	denro,ca	lockbit2	jewelry,org,hk
lockbit2	pla-pumpen	lockbit2	montanarisrl,ne,,,

Hot topics

Nothing today

News

Security Affairs

Avoslocker ransomware gang targets US critical infrastructure
The Federal Bureau of Investigation (FBI) reported that AvosLocker ransomware is being used in attacks targeting US critical infrastructure. The Federal Bureau of Investigation (FBI) published a joint cybersecurity advisory warning of AvosLocker ransomware attacks targeting multiple US critical infrastructure. The advisory was published in coordination with the US Treasury Department and the Financial Crimes Enforcement Network […] The post Avoslocker ransomware gang targets US critical infrastructure appeared first on Security Affairs.

Security Affairs

Crooks claims to have stolen 4TB of data from TransUnion South Africa
TransUnion South Africa discloses a data breach, threat actors who stolen sensitive data, demanded a ransom payment not to release stolen data. TransUnion South Africa announced that threat actors compromised a company server based in South Africa using stolen credentials. Threat actors have stolen company data and demanded a ransom payment not to release stolen […] The post Crooks claims to have stolen 4TB of data from TransUnion South Africa appeared first on Security Affairs.

Security Affairs

Emsisoft releases free decryptor for the victims of the Diavol ransomware
Cybersecurity firm Emsisoft released a free decryptor that allows the victims of the Diavol ransomware to recover their files without paying a ransom. Cybersecurity firm Emsisoft has released a free decryption tool to help Diavol ransomware victims recover their files without paying a ransom. In January, the FBI officially linked the Diavol ransomware operation to the infamous TrickBot […] The post Emsisoft releases free decryptor for the victims of the Diavol ransomware appeared first on Security Affairs.

Security Affairs

Exotic Lily initial access broker works with Conti gang
Google's Threat Analysis Group (TAG) uncovered a new initial access broker, named Exotic Lily, that is closely affiliated with the Conti ransomware gang. Google's Threat Analysis Group (TAG) researchers linked a new initial access broker, named Exotic Lily, to the Conti ransomware operation. Initial access brokers play an essential role in the cybercrime ecosystem, they provide access to previously […] The post Exotic Lily initial access broker works with Conti gang appeared first on Security Affairs.

Cyware News - Latest Cyber News

Got Milk? After Supplier Hit by Cyberattack, a NH School District Is Short
The school district said they were informed of the cyberattack on the dairy company. In a statement, the superintendent said the school anticipates milk shortages in the coming weeks.

Cyware News - Latest Cyber News

NRA Confirms It Got Pwned by Cybercriminals
A ransomware gang calling itself "Grief" bragged to the digital underworld last October about compromising the gun lobby's servers and stealing sensitive internal documents.

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

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.

CRITICAL Vector: network Created: 2022-03-13 Updated: 2022-03-20

CVE-2021-25007

The MOLIE **WordPress** plugin through 0.5 does not validate and escape a post parameter before using in a SQL statement, leading to an SQL Injection

CRITICAL Vector: network Created: 2022-03-14 Updated: 2022-03-20

CVE-2021-25003

The WPCargo Track & Trace **WordPress** plugin before 6.9.0 contains a file which could allow unauthenticated attackers to write a PHP file anywhere on the web server, leading to RCE

CRITICAL Vector: network Created: 2022-03-14 Updated: 2022-03-20

Source: NIST

NIST CVE: High

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).

HIGH Vector: network Created: 2022-03-13 Updated: 2022-03-20

CVE-2021-24959

The WP Email Users **WordPress** plugin through 1.7.6 does not escape the data_raw parameter in the weu_selected_users_1 AJAX action, available to any authenticated users, allowing them to perform SQL injection attacks.

HIGH Vector: network Created: 2022-03-14 Updated: 2022-03-20

CVE-2022-24575

GPAC 1.0.1 is affected by a stack-based buffer overflow through MP4Box.

HIGH Vector: local Created: 2022-03-14 Updated: 2022-03-20

Source: NIST

NIST CVE: Medium

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.

MEDIUM Vector: network Created: 2022-03-13 Updated: 2022-03-20

CVE-2022-24574

GPAC 1.0.1 is affected by a NULL pointer dereference in gf_dump_vrml_field.isra ().

MEDIUM Vector: local Created: 2022-03-14 Updated: 2022-03-20

CVE-2021-24897

The Add Subtitle **WordPress** plugin through 1.1.0 does not sanitise or escape the sub-title field (available only with classic editor) when output in the page, which could allow users with a role as low as contributor to perform Cross-Site Scripting attacks

MEDIUM Vector: network Created: 2022-03-14 Updated: 2022-03-20

CVE-2021-24895

The Cybersoldier **WordPress** plugin before 1.7.0 does not sanitise and escape the URL settings before outputting it in an attribute, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed

MEDIUM Vector: network Created: 2022-03-14 Updated: 2022-03-20

CVE-2021-24995

The HTML5 **Responsive** FAQ **WordPress** plugin through 2.8.5 does not properly sanitise and escape some of its settings, which could allow a high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed

MEDIUM Vector: network Created: 2022-03-14 Updated: 2022-03-20

CVE-2021-24950

The **Insight** Core **WordPress** plugin through 1.0 does not have any authorisation and CSRF checks in the insight_customizer_options_import (available to any authenticated user), does not validate user input before passing it to unserialize(), nor sanitise and escape it before outputting it in the response. As a result, it could allow users with a role as low as Subscriber to perform PHP Object Injection, as well as Stored Cross-Site Scripting attacks

MEDIUM Vector: network Created: 2022-03-14 Updated: 2022-03-20

CVE-2021-25026

The **Patreon WordPress** plugin before 1.8.2 does not sanitise and escape the field "Custom Patreon Page name", which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed

MEDIUM Vector: network Created: 2022-03-14 Updated: 2022-03-20

CVE-2021-24692

The Simple **Download Monitor WordPress** plugin before 3.9.5 allows users with a role as low as Contributor to download any file on the web server (such as wp-config.php) via a path traversal vector.

MEDIUM Vector: network Created: 2022-03-14 Updated: 2022-03-20

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.

MEDIUM Vector: network Created: 2022-03-13 Updated: 2022-03-20

CVE-2022-24576

GPAC 1.0.1 is affected by Use After Free through MP4Box.

MEDIUM Vector: local Created: 2022-03-14 Updated: 2022-03-20

CVE-2021-24982

The Child Theme Generator **WordPress** plugin through 2.2.7 does not sanitise escape the parade parameter before outputting it back, leading to a Reflected Cross-Site Scripting in the admin dashboard

MEDIUM Vector: network Created: 2022-03-14 Updated: 2022-03-20

CVE-2021-24966

The **Error Log Viewer WordPress** plugin through 1.1.1 does not validate the path of the log file to clear, allowing high privilege users to clear arbitrary files on the web server, including those outside of the **blog** folder

MEDIUM Vector: network Created: 2022-03-14 Updated: 2022-03-20

CVE-2021-24996

The IDPay for **Contact Form 7 WordPress** plugin through 2.1.2 does not sanitise and escape the idpay_error parameter before outputting it back in the page leading to a Reflected Cross-Site Scripting

MEDIUM Vector: network Created: 2022-03-14 Updated: 2022-03-20

CVE-2021-25006

The MOLIE **WordPress** plugin through 0.5 does not escape the course_id parameter before outputting it back in the admin dashboard, leading to a Reflected Cross-Site Scripting issue

MEDIUM Vector: network Created: 2022-03-14 Updated: 2022-03-20

CVE-2021-24940

The Persian **Woocommerce WordPress** plugin through 5.8.0 does not escape the s parameter before outputting it back in an attribute in the admin dashboard, which could lead to a Reflected Cross-Site Scripting issue

MEDIUM Vector: network Created: 2022-03-14 Updated: 2022-03-20

Source: NIST

NIST CVE: Low

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."

LOW Vector: network Created: 2022-03-13 Updated: 2022-03-20

Source: NIST

NIST CVE: Unrated

CVE-2022-24126

A buffer overflow in the NRSessionSearchResult parser in Bandai Namco FromSoftware Dark Souls III through 2022-03-19 allows remote attackers to execute arbitrary code via matchmaking servers, a different vulnerability than CVE-2021-34170.

UNRATED Vector: unkown Created: 2022-03-20 Updated: 2022-03-20

CVE-2022-23989

In **Stormshield Network Security** (SNS) before 3.7.25, 3.8.x through 3.11.x before 3.11.13, 4.x before 4.2.10, and 4.3.x before 4.3.5, a flood of connections to the SSLVPN service might lead to saturation of the **loopback** interface. This could result in the blocking of almost all network traffic, making the **firewall** unreachable. An attacker could exploit this via forged and properly timed traffic to cause a denial of service.

UNRATED Vector: unkown Created: 2022-03-15 Updated: 2022-03-20

CVE-2021-45010

A path traversal vulnerability in the file upload functionality in tinyfilemanager.php in Tiny **File Manager** before 2.4.7 allows remote attackers (with valid user accounts) to upload malicious PHP files to the webroot, leading to code execution.

UNRATED Vector: unkown Created: 2022-03-15 Updated: 2022-03-20

CVE-2022-24125

The matchmaking servers of Bandai Namco FromSoftware Dark Souls III through 2022-03-19 allow remote attackers to send arbitrary push requests to clients via a RequestSendMessageToPlayers request. For example, ability to send a push message to hundreds of thousands of machines is only restricted on the client side, and can thus be bypassed with a modified client.

UNRATED Vector: unkown Created: 2022-03-20 Updated: 2022-03-20

Source: Hybrid Analysis

Top malicious files

100% Threat score	,exe
100% Threat score	FLiNG,exe
100% Threat score	MC5_STORE,EXE
100% Threat score	StartGame,exe
100% Threat score	Server,exe
100% Threat score	41_defense_debug,exe
100% Threat score	5e_defense_timegap,exe
100% Threat score	Server,exe
95% Threat score	The-Darkness_97137,exe
90% Threat score	JtqFQW
80% Threat score	TX16Wx Software Sampler 3,5,0m x64,msi
71% Threat score	CSHFware,dll

100% Threat score	vbc,exe
100% Threat score	FearlessFighter,exe
100% Threat score	setup,exe
100% Threat score	CypherRat,exe
100% Threat score	CCleaner,v5,91,9537,exe
100% Threat score	58_defense_debug,exe
100% Threat score	41_defense_timegap,exe
100% Threat score	Server,exe
93% Threat score	Adobe Photoshop 3,0,exe
85% Threat score	avidemux_2,8,0_win64,exe
80% Threat score	Audials Play Pro â€“ Radio & Podcasts v9,11,4-0-g66acdf20a Premium Mod Apk {CracksHash},apk

Source: Hybrid Analysis

Top malicious URL

100% Threat score	https://nutsabouteducation,org/caseypattersonent,com/outlook,office,com/
100% Threat score	http://117,201,195,61:54878/Mozi,m
97% Threat score	http://37,29,92,173:42634/Mozi,m
93% Threat score	http://59,99,46,43:52887/Mozi,m
93% Threat score	http://222,142,200,28:44777/bin,sh
93% Threat score	http://222,141,90,50:42130/Mozi,m
93% Threat score	http://59,97,173,173:51126/Mozi,m
93% Threat score	http://45,224,170,124:51553/Mozi,m
93% Threat score	http://221,14,207,239:45532/Mozi,m

100% Threat score	http://sollicitoque,sam118,com/
100% Threat score	http://222,134,174,101:42930/i
97% Threat score	http://www,diapers,com,sg/GOO,N-Japan-Versi
93% Threat score	http://cpanel,bitsnbrain,com/
93% Threat score	http://222,141,74,169:38185/bin,sh
93% Threat score	http://115,55,56,13:37565/i
93% Threat score	http://182,116,68,117:60607/Mozi,m
93% Threat score	http://115,56,131,210:39038/i
93% Threat score	http://58,255,214,42:43905/Mozi,m

93% Threat score	http://222,142,200,28:44777/i
93% Threat score	http://58,243,19,43:46688/Mozi,m
93% Threat score	http://117,194,173,227:34030/bin,sh
92% Threat score	http://login,039304,com/e2c5e6/ac97641f-a840-4d14-90c4-e3476aaeb458/?
88% Threat score	http://45,120,16,238:42986/mozi,m
88% Threat score	http://222,141,93,235:51521/i
88% Threat score	http://117,215,202,94:59749/Mozi,m
87% Threat score	http://mangapro,top/
82% Threat score	http://r,marketing,atmata,sa/mk/cl/f/C__iX8GT1Mak349-LHWUIRw3-8ngmtYI9XJ2mP8IpEuofmG6lLBK3QijQdH-c8Ik_ExpgpYTinZC3ZuNPrg5yWfViAOoyfdB9b29H7ve7o13M8vOx6RFiZ2dnP8QoF-iISirWVBTdHWC6AQr0YTo8fnCgxS4EYHkoFihhxM1K63qcGZ32yNEKYaz8uXt-iIbL1avZCsebbI0EGCThoFsuzuEm8pYOaYvR8XBMwsuA-xLZtx5IQ%20Enter%20another%20short%20URL,,,
77% Threat score	http://thenewcontext,milanoschool,org/
77% Threat score	http://es,adminsub,net/tcp-udp-port-finder/back/138
72% Threat score	http://zecdz,smtpgaze,com/tracking/qaR9ZGLkAwpkBQN4Amx5ZwplZGDjBPM5qzS4qaR9ZQblZQH
72% Threat score	http://qzsnc,smtpgaze,com/tracking/qaR9ZGLkAGxkZwN2ZQV5AwpjBQN5AvM5qzS4qaR9ZQb2ID

93% Threat score	http://27,206,82,80:40127/Mozi,m
93% Threat score	http://117,215,255,215:51876/bin,sh
93% Threat score	http://182,127,101,108:45210/i
89% Threat score	https://transfer,sh/get/yrRWO4/Ngame%20v%
88% Threat score	http://123,5,147,68:55412/bin,sh
88% Threat score	http://103,121,174,110:42626/Mozi,m
88% Threat score	http://117,195,81,58:41123/bin,sh
83% Threat score	http://117,195,89,153:60527/i
77% Threat score	http://manufacturing-conf,com/
77% Threat score	http://www,surveymonkey,com/tr/v1/te/akU_2BQc2vAhAsa_2B264x
77% Threat score	http://kyndryl,box,com/
72% Threat score	http://nhatminhist,com/
72% Threat score	http://ewnyj,smtpgaze,com/tracking/qaR9ZGLk

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 Uruguay
- #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 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 Indonesia

#5 Thailand

#6 Algeria

#7 Viet Nam

#8 Brazil

#9 Pakistan

#10 Iran (Islamic Republic of)

Source: SpamHaus

Top phishing countries

#1 United States

#2 Singapore

#3 Russia

#4 Hong Kong

#5 Germany

#6 Netherlands

#7 Belgium

#8 Australia

#9 France

#10 Indonesia

Source: Have I been pwned?

Have I been pwnd

ZAP-Hosting (zap-hosting.com)
In November 2021, web host ZAP-Hosting suffered a data breach that exposed over 60GB of data containing 746k unique email addresses. The breach also contained support chat logs, IP addresses, names, purchases, physical addresses and phone numbers.

Count: 746682 Created: 2021-11-22 Updated: 2022-03-19

Source: Imperva DDOS Map

Top DDOS attackers

United States (24%)

Russia (14%)

Singapore (11%)

Source: Imperva DDOS Map

Top DDOS country targets

Russia (62%)

Ukraine (18%)

United States (7%)

Source: Imperva DDOS Map

Top DDOS techniques

81% **DDoS**

13% **Automated Threat**

5%	**OWASP**

Source: Imperva DDOS Map

Top DDOS industry targets

65%	**Financial Services**
23%	**Business**
4%	**Computing & IT**