Your Security Rabbits report for March 21, 2022

Source: Ransom Watch

Ransomware attacks

alphv	Abrams & Bayliss LLP	lockbit2	besp-oak.com
midas	Bigmtransport	lockbit2	chicagosteelgro...
alphv	HAVI Logistic | havilog.com | PART 1	lockbit2	ismea.it
lockbit2	onglesdor.com	lockbit2	rh-europe.com
lockbit2	STUDIO PEREGO S...	lockbit2	tomlinsonelectr...
lockbit2	zabel-group.de	lockbit2	bbst-clp.de
lockbit2	meritresources	lockbit2	museum-dingolfi...
ransomexx	Scottish Association for Mental Health	arvinclub	stormous

Hot topics

Nothing today

News

The Hacker News

'CryptoRom' Crypto Scam Abusing iPhone Features to Target Mobile Users
Social engineering attacks leveraging a combination of romantic lures and cryptocurrency fraud have been luring unsuspecting victims into installing fake apps by taking advantage of legitimate iOS features like TestFlight and Web Clips. Cybersecurity company Sophos, which has named the organized crime campaign "CryptoRom," characterized it as a wide-ranging global scam. "This style of

Security Affairs

DirtyMoe modules expand the bot using worm-like techniques
The DirtyMoe botnet continues to evolve and now includes a module that implements wormable propagation capabilities. In June 2021, researchers from Avast warned of the rapid growth of the DirtyMoe botnet (PurpleFox, Perkiler, and NuggetPhantom), which passed from 10,000 infected systems in 2020 to more than 100,000 in the first half of 2021. Experts defined DirtyMoe as a [...] The post DirtyMoe modules expand the bot using worm-like techniques appeared first on Security Affairs.

CyberScoop

For Magecart groups and other credit-card skimmers, old and new opportunities abound
The entry points for Magecart and other e-commerce skimmers are changing, but the attackers are getting more clever, too. The post For Magecart groups and other credit-card skimmers, old and new opportunities abound appeared first on CyberScoop.

IT Security Guru

More Conti group source code leaked
A Ukrainian security researcher has released further source code from the Conti ransomware group in retaliation for their siding with Russia over the ongoing Russia-Ukraine conflict. Conti is a prolific ransomware operation run by Russia-based threat actors. The group has been involved in developing numerous malware families, and is considered one of the most active [...] The post More Conti group source code leaked appeared first on IT Security Guru.

Cyware News - Latest Cyber News

New Phishing toolkit lets anyone create fake Chrome browser windows
A phishing kit has been released that allows red teamers and wannabe cybercriminals to create effective single sign-on phishing login forms using fake Chrome browser windows.

Cyware News - Latest Cyber News

Western Digital app bug gives elevated privileges in Windows, macOS
Western Digital's EdgeRover desktop app for both Windows and Mac are vulnerable to local privilege escalation and sandboxing escape bugs that could allow the disclosure of sensitive information or denial of service (DoS) attacks.

Security Affairs

Anonymous leaked data stolen from Russian pipeline company Transneft
Anonymous hacked Omega Company, the in-house R&D unit of Transneft, the Russian oil pipeline giant, and leaked stolen data. Anonymous collective claims it has hacked Omega Company, which is the in-house R&D unit of Transneft, the Russia-based state-controlled oil pipeline company. Transneft is the largest oil pipeline company in the world, the hacktivists have stolen [...] The post Anonymous leaked data stolen from Russian pipeline company Transneft appeared first on Security Affairs.

Security Affairs

EU and US agencies warn that Russia could attack satellite communications networks
FBI, CISA, and the European Union Aviation Safety Agency (EASA) warn of possible threats to international satellite communication (SATCOM) networks. Satellite communication (SATCOM) networks are critical infrastructure for modern society, US and EU agencies warn of possible threats to them. Victor Zhora, Chief Digital Transformation Officer at the State Service of Special Communication and Information [...] The post EU and US agencies warn that Russia could attack satellite communications networks appeared first on Security Affairs.

Security Affairs

Mar 13- Mar 19 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. Below is the timeline of the events related to the previous weeks: March 18 - China-linked threat actors are targeting the government of Ukraine Google's TAG team revealed that China-linked APT groups are targeting Ukraine [...] The post Mar 13- Mar 19 Ukraine - Russia the silent cyber conflict appeared first on Security Affairs.

The Hacker News

New Backdoor Targets French Entities via Open-Source Package Installer
Researchers have exposed a new targeted email campaign aimed at French entities in the construction, real estate, and government sectors that leverages the Chocolatey Windows package manager to deliver a backdoor called Serpent on compromised systems. Enterprise security firm Proofpoint attributed the attacks to a likely advanced threat actor based on the tactics and the victimology patterns

The Hacker News

South Korean DarkHotel Hackers Targeted Luxury Hotels in Macau
Luxury hotels in the Chinese special administrative region of Macau were the target of a malicious spear-phishing campaign from the second half of November 2021 and through mid-January 2022. Cybersecurity firm Trellix attributed the campaign with moderate confidence to a suspected South Korean advanced persistent threat (APT) tracked as DarkHotel, building on research previously published by

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 Margaris

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

Source: NIST

NIST CVE: Critical

CVE-2022-0169

The Photo **Gallery** by 10Web **WordPress** plugin before 1.6.0 does not validate and escape the bwg_tag_id_bwg_thumbnails_0 parameter before using it in a SQL statement via the bwg_frontend_data AJAX **action** (available to unauthenticated and authenticated users), leading to an unauthenticated SQL injection

CRITICAL Vector: network Created: 2022-03-14 Updated: 2022-03-21

CVE-2021-42171

Zenario CMS 9.0.54156 is vulnerable to File Upload. The web server can be compromised by uploading and executing a web-shell which can run commands, browse system files, browse local resources, attack other servers, and exploit the local vulnerabilities, and so forth.

CRITICAL Vector: network Created: 2022-03-14 Updated: 2022-03-21

Source: NIST

NIST CVE: High

CVE-2022-0165

The **Page Builder KingComposer WordPress** plugin through 2.9.6 does not validate the id parameter before redirecting the user to it via the kc_get_thumbn AJAX **action** available to both unauthenticated and authenticated users

HIGH Vector: network Created: 2022-03-14 Updated: 2022-03-21

Source: NIST

NIST CVE: Medium

CVE-2022-0230

The Better **WordPress Google** XML Sitemaps WordPress plugin through 1.4.1 does not sanitise and escape its logs when outputting them in the admin dashboard, which could allow unauthenticated users to perform Stored Cross-Site Scripting attacks against admins

MEDIUM Vector: network Created: 2022-03-14 Updated: 2022-03-21

CVE-2022-0147

The **Cookie** Information | Free GDPR Consent Solution **WordPress** plugin before 2.0.8 does not escape user data before outputting it back in attributes in the admin dashboard, leading to a Reflected Cross-Site Scripting issue

MEDIUM Vector: network Created: 2022-03-14 Updated: 2022-03-21

CVE-2021-41952

Zenario CMS 9.0.54156 is vulnerable to Cross Site Scripting (XSS) via **upload file** to *.SVG. An attacker can send malicious files to victims and steals victim's **cookie** leads to account takeover. The person viewing the image of a contact can be victim of XSS.

MEDIUM Vector: network Created: 2022-03-14 Updated: 2022-03-21

CVE-2022-0248

The **Contact Form Submissions WordPress** plugin before 1.7.3 does not sanitise and escape additional fields in contact form requests before outputting them in the related submission. As a result, unauthenticated attacker could perform Cross-Site Scripting attacks against admins viewing the malicious submission

MEDIUM Vector: network Created: 2022-03-14 Updated: 2022-03-21

CVE-2021-44964

Use after free in garbage **collector** and finalizer of lgc.c in Lua interpreter 5.4.0~5.4.3 allows attackers to perform Sandbox Escape via a crafted script file.

MEDIUM Vector: local Created: 2022-03-14 Updated: 2022-03-21

Source: NIST

NIST CVE: Low

Nothing today

Source: NIST

NIST CVE: Unrated

CVE-2022-25505

Taocms v3.0.2 was discovered to contain a SQL injection vulnerability via the id parameter in \include\Model\Category.php.

UNRATED Vector: unkown Created: 2022-03-21 Updated: 2022-03-21

CVE-2022-25481

ThinkPHP Framework v5.0.24 was discovered to be configured without the PATHINFO parameter. This allows attackers to access all system environment parameters from index.php.

UNRATED Vector: unkown Created: 2022-03-21 Updated: 2022-03-21

Source: Hybrid Analysis

Top malicious files

100% Threat score	4Shared Cracker V1.exe
100% Threat score	reversal.exe
100% Threat score	TestSightDeveloperSetup_11.1.5.exe
85%	Offline eBIRForms Package v7.9.2.1 setup.exe
100% Threat score	Overwatch-Setup.exe
100% Threat score	MicrosoftEdgeSetupBeta.exe
100% Threat score	Battle.net-Setup.exe
81%	0e57826ed0c7004cae9e1a27b5a4ac987f64ee1dd7c1c7ad9d09b56c197bd9b2.dll

Threat score	
75% Threat score	aaasdadasdasd1339140669990398045.jar

Threat score	

Source: Hybrid Analysis

Top malicious URL

100% Threat score	http://lmkss.com/
93% Threat score	http://42.233.149.135:38319/Mozi.m
93% Threat score	http://123.4.183.195:51553/i
87% Threat score	http://orfo.info/
82% Threat score	http://swisscouncil.swiss/
82% Threat score	http://r.email.fintech.global/mk/cl/f/uwKmEDcLTPdfkihJK5mCGRdMTA9QrJ9gp5POCkw1wqYtcHSqb2-FcXyGHae3aCktzvg8y4ke6txHk0-Ov9qFz0voKoSnf8bzXjjDMv 8eUtgEhThIPghpIx5X3tjrKz2RUJ6S0myPVbpQ7nzGcm8upZ3Fcvfr6RDCAGlQ
77% Threat score	http://www.caillou.com.tr/
74% Threat score	https://www.hiphopleakers.com/video-of-man-fingering-lover-while-on-a-flight-goes-viral/
71% Threat score	https://info.trustquay.com/hs/manage-preferences/unsubscribe? languagePreference=en&d=VndxFr6SZs8PVPbTTN4kzXwYW43SMZw49r51hW3K8hyN43T2PMW4NY1xq15gBJzW766Lwj73QmL8W5XFZwr57JyBSN9lLNgnX1dq lQaT7BwpZAz16YpOrHCFuNJxz4WwFHoRxR-Hz3kBwxRDQR0df9uJGe1771t7eCm1LW1x5PnhPN5YZ-MZWLLJqZdjSRQ&_hsmi=20742
71% Threat score	https://info.trustquay.com/hs/manage-preferences/unsubscribe? languagePreference=en&d=VnkYQD6SZs8PW1cVpNC3T3qGLW3zdYT54kFl1WW45LLf03T2BQ7W4tct2N3K8hyNW43T2PM4NY1xqW17f7hv7vpM8sW9gwknc6TZ8C5W5tmtqF7v1G _HFZdJY3RH5wYLFQ3vkLYcXOHjHg3xb1SJHK7rFG7ACZo8OudLBY824F864ZFqH6PnEy0gd5zoTp9U6eNfVsq_wGioIOwrhpemd7683Jma_fidUGc&_hsmi=207426943

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 Russia

#3 Germany

#4 Singapore

#5 Netherlands

#6 Hong Kong

#7 Japan

#8 India

#9 France

#10 Bulgaria

Source: Have I been pwned?

Have I been pwnd

Nothing today

Source: Imperva DDOS Map

Top DDOS attackers

United States (27%)

Russia (13%)

Singapore (10%)

Source: Imperva DDOS Map

Top DDOS country targets

Russia (58%)

Ukraine (17%)

United States (8%)

Source: Imperva DDOS Map

Top DDOS techniques

78% **DDoS**

16% **Automated Threat**

5% **OWASP**

Source: Imperva DDOS Map

Top DDOS industry targets

63%	**Financial Services**
21%	**Business**
6%	**Computing & IT**