Security Rabbits

Your Security Rabbits report for March 27, 2022

Source: Ransom Watch

Ransomware attacks

clop	ALEXIM,COM	clop	ALTERNATIVETECHS,COM
clop	BOLTONUSA,COM	clop	CAPCARPET,COM
clop	DUTTONFIRM,COM	clop	EDAN,COM
clop	ENPRECIS,COM	conti	Hochschild Mining
clop	JBINSTANTLAWN,NET	clop	MCH-GROUP,COM
clop	SWIRESPO,COM	lockbit2	aquazzura,
lockbit2	aquazzura,co	hiveleak	Konradin Mediengruppe GmbH
lockbit2	microflex-servi,,,		

Hot topics

Nothing today

News

Security Affairs

CISA adds 66 new flaws to the Known Exploited Vulnerabilities Catalog

The US Cybersecurity and Infrastructure Security Agency (CISA) added 66 new flaws to its Known Exploited Vulnerabilities Catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added 15 vulnerabilities to its Known Exploited Vulnerabilities Catalog.i According to Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities, FCEB agencies have to address the […] The post CISA adds 66 new flaws to the Known Exploited Vulnerabilities Catalog appeared first on Security Affairs.

Security Affairs

FCC adds Kaspersky to Covered List due to unacceptable risks to national security

The Federal Communications Commission (FCC) added Kaspersky to its Covered List because it poses unacceptable risks to U.S. national security. The Federal Communications Commission (FCC) added multiple Kaspersky products and services to its Covered List saying that they pose unacceptable risks to U.S. national security. "The Federal Communications Commission's Public Safety and Homeland Security Bureau […] The post FCC adds Kaspersky to Covered List due to unacceptable risks to national security appeared first on Security Affairs.

Cyware News - Latest Cyber News

Kaspersky named first Russian company on security risk list

The U.S. placed internet-security provider AO Kaspersky Lab on a list of companies deemed a threat to national security, for the first time adding a Russian entity to a list dominated by Chinese telecommunications firms.

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-2022-26620

Akeo Consulting **Rufus** Executable 3.17.1846 and Rufus Portable Executable 3.17p were discovered to allow attackers to execute arbitrary code or escalate privileges via placing a crafted x86 DLL in the same directory as other executables.

UNRATED	Vector: unkown	Created: 2022-03-27	Updated: 2022-03-27

CVE-2022-26205

Marky commit 3686565726c65756e was discovered to contain a remote code execution (RCE) vulnerability via the Display text fields. This vulnerability allows attackers to execute arbitrary code via injection of a crafted payload.

UNRATED	Vector: unkown	Created: 2022-03-27	Updated: 2022-03-27

CVE-2022-26200

Technitium Installer v4.4 was discovered to allow attackers to execute arbitrary code or escalate privileges via placing a crafted DLL in the same directory as the current installer.

UNRATED	Vector: unkown	Created: 2022-03-27	Updated: 2022-03-27

CVE-2021-25220

BIND 9.11.0 -> 9.11.36 9.12.0 -> 9.16.26 9.17.0 -> 9.18.0 BIND Supported Preview Editions: 9.11.4-S1 -> 9.11.36-S1 9.16.8-S1 -> 9.16.26-S1 Versions of BIND 9 earlier than those shown - back to 9.1.0, including Supported Preview Editions - are also believed to be affected but have not been tested as they are EOL. The cache could become poisoned with incorrect records leading to queries being made to the wrong servers, which might also result in false information being returned to clients.

UNRATED	Vector: unkown	Created: 2022-03-23	Updated: 2022-03-27

CVE-2022-26198

Notable v1.8.4 does not filter text editing, allowing attackers to execute arbitrary code via a crafted payload injected into the Title text field.

UNRATED	Vector: unkown	Created: 2022-03-27	Updated: 2022-03-27

Source: Hybrid Analysis

Top malicious files

100% Threat score	Bfhk(1),exe	100% Threat score	SafeHandleMinusOneIsInval,exe
100% Threat score	Firefox Installer,exe	100% Threat score	Adguard 7,9,3855 multiple trial,exe
100% Threat score	Ñ‡Ð¸Ñ, Ð½Ð° cs go,exe	100% Threat score	aTube_Catcher,exe
100% Threat score	aTube_Catcher,exe	100% Threat score	GenshinXYZ Loader,exe
100% Threat score	vbc,exe	100% Threat score	Massscan_GUI,exe
100% Threat score	SkyBlade,exe	100% Threat score	Firefox Setup 42,0,exe
100% Threat score	Firefox Setup 98,0,2,exe	90% Threat score	BTSync-1,3,109,exe
85% Threat score	Ant Download Manager PRO,exe	82% Threat score	teamtanks,exe
75% Threat score	SerenityGameLib,dll	75% Threat score	MovaviVideoEditorPlusSetupC,exe
75% Threat score	Install_FSUIPC7,exe	71% Threat score	OpenVPN-2,5,6-I601-amd64,msi

Source: Hybrid Analysis

Top malicious URL

100% Threat score	http://182,121,202,251:54018/Mozi,m	98% Threat score	http://212,193,30,29/WW/file5,exe
97% Threat score	http://115,54,145,128:56026/Mozi,m	95% Threat score	https://wesleyvirgin,com/100kperday/money5,mp4
93% Threat score	http://117,196,58,36:55352/Mozi,m	89% Threat score	https://sourceforge,net/software/compare/Azure-Cosmos-DB-vs-Google-Cloud-Firestore-vs-Amazon-DocumentDB/
88% Threat score	http://123,9,198,49:50595/Mozi,m	88% Threat score	http://177,52,167,30:41844/Mozi,a

86% Threat score	https://urldefense.com/v3/__http:/account-maintenance.com/3373d6967bbad519?l=20__%3B%21%21J8jBlt3-xA%21Z94kSbbiybdTzMifvbL6e3KyrZ4wc5hupddQkyPXLUlaIsDlB_qnQTENAWx-U8JZoIU%24
82% Threat score	http://mail.seekmyjob.com/
77% Threat score	http://freeonlineradioapptab.com/
74% Threat score	https://cutt.ly/fSA9hdo
74% Threat score	http://www.bit.co.mz/
74% Threat score	https://www.mediafire.com/file/ssxk3zkc34crfxl/Notorious_Installer.exe/file
74% Threat score	https://clck.ru/eSSqh?d1n9m
72% Threat score	http://bit.do/Aramexksa
72% Threat score	http://www.qatarmaster.com.qa/

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 United States of America
- #3 India
- #4 Indonesia
- #5 Thailand
- #6 Algeria
- #7 Viet Nam
- #8 Brazil

- #9 Pakistan
- #10 Venezuela (Bolivarian Republic of)

Source: SpamHaus

Top phishing countries

- #1 United States
- #2 Russia
- #3 Germany
- #4 Singapore
- #5 Netherlands
- #6 France
- #7 Spain
- #8 Japan
- #9 Bulgaria
- #10 United Kingdom

Source: Have I been pwned?

Have I been pwnd

Nothing today

Source: Imperva DDOS Map

Top DDOS attackers

- **United States (24%)**
- **Russia (19%)**
- **Germany (12%)**

Source: Imperva DDOS Map

Top DDOS country targets

- **Russia (54%)**
- **Ukraine (19%)**
- **United States (10%)**

Source: Imperva DDOS Map

Top DDOS techniques

73%	**DDoS**
20%	**Automated Threat**
8%	**OWASP**

Source: Imperva DDOS Map

Top DDOS industry targets

61%	**Financial Services**
22%	**Business**
6%	**Computing & IT**