Your Security Rabbits report for March 25, 2022

Hot topics

Nothing today

Source: Ransom Watch

Ransomware attacks

lockbit2	alaliengineerin...	hiveleak	Pollmann
lockbit2	standard-furnit...	lockbit2	buffingtonl
alphv	Davis Law Group, P.C. - dlgva.com	lockbit2	guazzini.it
lockbit2	japoauto.com	alphv	North View Escrow Corp
lockbit2	onedoc.ch/fr/ce...	hiveleak	Passero Associates
lockbit2	serilization-se...	lockbit2	stt-logistique....

News

The Hacker News

23-Year-Old Russian Hacker Wanted by FBI for Running Marketplace of Stolen Logins
A 23-year-old Russian national has been indicted in the U.S. and added to the Federal Bureau of Investigation's (FBI) Cyber Most Wanted List for his alleged role as the administrator of Marketplace A, a cyber crime forum that sold stolen login credentials, personal information, and credit card data. Igor Dekhtyarchuk, who first appeared in hacker forums in 2013 under the alias "floraby," has

Blog â€" Flashpoint

All About LAPSUS$: What We Know About the Extortionist Group [Updated]
Updated March 24, 2022: The City of London Police arrested seven individuals today, March 24, in connection with the extortionist group LAPSUS$, allegedly responsible for carrying out several high-profile attacks in recent weeks. Police revealed that all of the individuals arrested were between the ages of 16 and 21; no names are yet to be [...] The post All About LAPSUS$: What We Know About the Extortionist Group [Updated] appeared first on Flashpoint.

Cyware News - Latest Cyber News

Bad Actors Trying to Capitalize on Current Events via Shameless Email Scams
This attack starts with an IRS impersonation email that contains a ZIP attachment called "W-9 form.zip". The email is sent to the target, and a password is provided within the body of the email for convenient extraction.

Threatpost

Chinese APT Combines Fresh Hodur RAT with Complex Anti-Detection
Mustang Panda's already sophisticated cyberespionage campaign has matured even further with the introduction of a brand-new PlugX RAT variant.

WeLiveSecurity

Crypto malware in patched wallets targeting Android and iOS devices
ESET Research uncovers a sophisticated scheme that distributes trojanized Android and iOS apps posing as popular cryptocurrency wallets The post Crypto malware in patched wallets targeting Android and iOS devices appeared first on WeLiveSecurity

CyberScoop

Dual North Korean hacking efforts found attacking Google Chrome vulnerability
The hacking attempts are just the latest in the multiple ongoing campaigns from the North Korean government. The post Dual North Korean hacking efforts found attacking Google Chrome vulnerability appeared first on CyberScoop.

Security Affairs

Experts explained how to hack a building controller widely adopted in Russia
A researcher discovered critical flaws that can be exploited by remote attackers to hack a building controller popular in Russia. A researcher has identified critical vulnerabilities that can allegedly be exploited to remotely hack a building controller predominantly used by organizations in Russia. Researcher Jose Bertin discovered critical flaws affecting a controller made by Russian [...]

CISA Alerts

AA22-083A: Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector
Actions to Take Today to Protect Energy Sector Networks: * Implement and ensure robust network segmentation between IT and ICS networks. * Enforce MFA to authenticate to a system. * Manage the creation of, modification of, use of--and permissions associated with--privileged accounts. This joint Cybersecurity Advisory (CSA)--coauthored by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Energy (DOE)--provides information on multiple intrusion campaigns conducted by state-sponsored Russian cyber actors from 2011 to 2018 and targeted U.S. and international Energy Sector organizations. CISA, the [...]

Security Affairs

Anonymous targets western companies still active in Russia, including Auchan, Leroy Merlin e Decathlon
Anonymous launches its offensive against Wester companies still operating in Russia, it 'DDoSed' Auchan, Leroy Merlin e Decathlon websites. Since the start of the Russian invasion of Ukraine on February 24, Anonymous has declared war on Russia and launched multiple cyber-attacks against Russian entities, including Russian government sites, state-run media websites, and energy firms. Anonymous recently declared war on all companies that [...] The post Anonymous targets western companies still active in Russia, including Auchan, Leroy Merlin e Decathlon appeared first on Security Affairs.

CyberScoop

Bigger demands, bigger payouts are the trend in ransomware, report says
Palo Alto Networks' Unit 42 says that in the cases it worked, the average demand was up 144% and average payment was up 78%. The post Bigger demands, bigger payouts are the trend in ransomware, report says appeared first on CyberScoop.

The Hacker News

Chinese APT Hackers Targeting Betting Companies in Southeast Asia
A Chinese-speaking advanced persistent threat (APT) has been linked to a new campaign targeting gambling-related companies in South East Asia, particularly Taiwan, the Philippines, and Hong Kong. Cybersecurity firm Avast dubbed the campaign Operation Dragon Castling, describing its malware arsenal as a "robust and modular toolset." The ultimate motives of the threat actor are not immediately

CyberScoop

DOJ unseals charges against Russians in attempted hacks of infrastructure, including Trisis case
One indictment alleges hacking attempts on industrial control systems, and the other involves a separate spree from 2012-17. The post DOJ unseals charges against Russians in attempted hacks of infrastructure, including Trisis case appeared first on CyberScoop.

Cyware News - Latest Cyber News

Elden Ring exploit traps players in infinite death loop
A little over a week ago, players of Elden Ring complained that their sessions were being invaded by "hackers". Invading people's games is a normal feature of the title, but being put into an endless death loop, not so much.

The Hacker News

Experts Uncover Campaign Stealing Cryptocurrency from Android and iPhone Users
Researchers have blown the lid off a sophisticated malicious scheme primarily targeting Chinese users via copycat apps on Android and iOS that mimic legitimate digital wallet services to siphon cryptocurrency funds. "These malicious apps were able to steal victims' secret seed phrases by impersonating

The post Experts explained how to hack a building controller widely adopted in Russia appeared first on Security Affairs.

Cyware News - Latest Cyber News

Heap overflow vulnerability in Sound Exchange libsox library

The vulnerability specifically exists in the way the Sound Exchange libsox library handles NIST Speech Header Resources (SPHERE) files, which are used for speech recognition.

Cyware News - Latest Cyber News

Internet crime in 2021: Investment fraud losses soar

The number of complaints received by the FBI IC3 in 2021 (847,376) has surpassed that of complaints in 2020 (791,790), and the total monetary loss suffered by victims ($6.9 Billion) has far outstripped losses suffered in 2020 ($4.2 Billion).

Threatpost

Just-Released Dark Souls Game, Elden Ring, Includes Killer Bug

A patch fixes exploit hidden in Elden Ring that traps PC players in a 'death loop.'

Cyware News - Latest Cyber News

Lawsuit claims Kronos breach exposed data for 'millions'

A class-action lawsuit was filed against Ultimate Kronos Group for alleged negligence leading to the exposure of millions of workers' info during a ransomware attack and private cloud breach in December.

Threatpost

Microsoft Azure Developers Awash in PII-Stealing npm Packages

A large-scale, automated typosquatting attack saw 200+ malicious packages flood the npm code repository, targeting popular Azure scopes.

Cyware News - Latest Cyber News

Microweber developers resolve XSS vulnerability in CMS software

These shortcomings meant it was possible for attackers to upload an XSS payload, providing it contained a file whose name ended with 'html' - a category that includes far more than just simple .html files.

ZDNet | security RSS

Mustang Panda hacking group takes advantage of Ukraine crisis in new attacks

Just as criminals seized on the pandemic, this group is trying to capitalize on Russia's invasion of Ukraine.

The Hacker News

North Korean Hackers Exploited Chrome Zero-Day to Target Fintech, IT, and Media Firms

Google's Threat Analysis Group (TAG) on Thursday disclosed that it acted to mitigate threats from two distinct government-backed attacker groups based in North Korea that exploited a recently-uncovered remote code execution flaw in the Chrome web browser. The campaigns, once again "reflective of the regime's immediate concerns and priorities," are said to have targeted U.S. based organizations

IT Security Guru

Ransomware payments peaked in 2021

Ransomware payments reached all-time highs last year, with related data leaks and ransom demands also surging, according to Palo Alto Networks. The stats were compiled from cases worked on by the security vendor's Unit 42 security consulting business. The 2022 Unit 42 Ransomware Threat Report published by Palo Alto Networks today claimed the average ransomware payment reached [...] The post Ransomware payments peaked in 2021 appeared first on IT Security Guru.

Blog â€" Flashpoint

Russia's Efforts to Control the Flow of Information at Home Shows the Limits of Censorship in the Digital Age

Erecting Russia's digital iron curtain As its war against Ukraine rages on, Russia is attempting to block, throttle, fine, and/or censor nearly all "Western" social media platforms, as well as other key information sources. These internet blocks and bans affect information going in and out of Russia, which theoretically prevents information about the conflict from [...] The post Russia's Efforts to Control the Flow of Information at Home Shows the Limits of Censorship in the Digital Age appeared first on Flashpoint.

CyberScoop

Strengthening industrial cybersecurity

Dragos' analysis and recommendations to combat global threat activity targeting industrial environments. The post Strengthening industrial cybersecurity appeared first on CyberScoop.

CyberScoop

The international surge to help keep Ukraine's frontlines connected

Donations of modems, routers and other equipment are flooding in from around the world. The post The international surge to help keep Ukraine's frontlines connected appeared first on CyberScoop.

Threatpost

Top 3 Attack Trends in API Security - Podcast

Bots & automated attacks have exploded, with attackers and developers alike in love with APIs, according to a new Cequence Security report. Hacker-in-residence Jason Kent explains the latest.

Naked Security

UK police arrest 7 hacking suspects - have they bust the LAPSUS$ gang?

Seven alleged hackers have been arrested in the UK. But who are they, and which hacking crew are they from?

Coinbase, imToken, MetaMask, Trust Wallet, Bitpie, TokenPocket, or OneKey," said Lukas Stefanko

Threatpost

HubSpot Data Breach Ripples Through Crytocurrency Industry

~30 crypto companies were affected, including BlockFi, Swan Bitcoin and NYDIG, providing an uncomfortable reminder about how much data CRM systems snarf up.

WeLiveSecurity

Is a nation-state digital deterrent scenario so far-fetched?

Why has the conflict in Ukraine not caused the much anticipated global cyber-meltdown? The post Is a nation-state digital deterrent scenario so far-fetched? appeared first on WeLiveSecurity

Cyware News - Latest Cyber News

Lapsus$ Infiltrates High Profile Victims Through Employee Accounts

The Lapsus$ group, also tracked as DEV-0537, deploys the RedLine password stealer to get access to session tokens and passwords. It buys session tokens and credentials from underground forums. These credentials are used to access VPN, RDP, and VDI systems.

Cyware News - Latest Cyber News

Many Critical Flaws Patched in Delta Electronics Energy Management System

At least 30 vulnerabilities were found in the past year in the DIAEnergie industrial energy management system made by Delta Electronics. The company says it has created patches for all of them.

Threatpost

Microsoft Help Files Disguise Vidar Malware

Attackers are hiding interesting malware in a boring place, hoping victims won't bother to look.

Cyware News - Latest Cyber News

MixMode raises $45 million to automate cyberattack detection for organizations

MixMode announced that it has raised $45 million in a Series B funding round led by the growth equity firm PSG, with participation from existing investor Entrada Ventures.

CyberScoop

NATO, G-7 leaders promise bulwark against retaliatory Russian cyberattacks

The pledges follow the Biden administration saying that Russia's calculus on digital assaults had changed. The post NATO, G-7 leaders promise bulwark against retaliatory Russian cyberattacks appeared first on CyberScoop.

CyberScoop

Okta breach leads to questions on disclosure, reliance on third-party vendors

Security experts questioned how long it took Okta to disclose the Lapsus$ breach and worried about a domino effect. The post Okta breach leads to questions on disclosure, reliance on third-party vendors appeared first on CyberScoop.

IT Security Guru

Researchers trace LAPSUS$ hacks to English teenager

Cybersecurity researchers investigating the ultra-prolific LAPSUS$ group have traced the attacks to a 16 year old living at his mother's house near Oxford, England. In a shocking turn of events, the four researchers investigating the attacks have said they believe the teenager is the mastermind behind the operation. LAPSUS$ has gained significant notoriety in the [...] The post Researchers trace LAPSUS$ hacks to English teenager appeared first on IT Security Guru.

Naked Security

S3 Ep75: Okta hack, CryptoRom, OpenSSL, and CafePress [Podcast]

Latest episode - listen now!

Threatpost

Tax-Season Scammers Spoof Fintechs, Including Stash, Public

Threat actors are impersonating such wildly popular personal-finance apps (which are used more than social media or streaming services) to try to fool people into giving up their credentials.

CyberScoop

The long, bumpy road to cyber incident reporting legislation -- and the one still ahead

The legislation eventually garnered widespread support on its way to becoming law, but much remains unresolved. The post The long, bumpy road to cyber incident reporting legislation -- and the one still ahead appeared first on CyberScoop.

Threatpost

UK Cops Collar 7 Suspected Lapsus$ Gang Members

London Police can't say if they nabbed the 17-year-old suspected mastermind & multimillionaire - but researchers say they've been tracking an Oxford teen since mid-2021.

Cyware News - Latest Cyber News

Ukrainian Enterprises Targeted with New DoubleZero Wiper Malware

DoubleZero wipe files use two techniques, overwriting their content with zero blocks of 4096 bytes (using FileStream.Write) or using API-calls NtFileOpen, NtFsControlFile (code: FSCTL_SET_ZERO_DATA).

Security Affairs

US indicted 4 Russian government employees for attacks on critical infrastructure

The U.S. has indicted four Russian government employees for their involvement in attacks on entities in critical infrastructure. The U.S. has indicted four Russian government employees for their role in cyberattacks targeting hundreds of companies and organizations in the energy sector worldwide between 2012 and 2018. "The Department of Justice unsealed two indictments today charging […] The post US indicted 4 Russian government employees for attacks on critical infrastructure appeared first on Security Affairs.

Cyware News - Latest Cyber News

Western Digital My Cloud OS update fixes critical vulnerability

The flaw, tracked as CVE-2022-23121, was exploited by the NCC Group's EDG team members and relied on the open-source service named "Netatalk Service" that was included in My Cloud OS.

ZDNet | security RSS

Vidar spyware is now hidden in Microsoft help files

The malware is being spread through an interesting phishing tactic.

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: Have I been pwned?

Have I been pwnd

Nothing today

Source: Imperva DDOS Map

Top DDOS attackers

- **United States (24%)**
- **Russia (19%)**
- **Singapore (11%)**

Source: Imperva DDOS Map

Top DDOS country targets

- **Russia (54%)**
- **Ukraine (21%)**
- **United States (9%)**

Source: Hybrid Analysis

Top malicious URL

100% Threat score	https://pgeobrot,live/
100% Threat score	http://222,140,219,155:59875/bin,sh
100% Threat score	http://61,52,53,145:53974/bin,sh
100% Threat score	http://61,3,154,217:38385/Mozi,m
100% Threat score	https://pgeobrot,live/091c23
100% Threat score	http://171,125,46,8:55208/Mozi,a
100% Threat score	http://115,63,133,130:55274/Mozi,m
98% Threat score	http://107,175,17,147/m-i,p-s,GHOUL
96% Threat score	http://179,43,175,171/qelh/CL,exe
100% Threat score	http://61,52,93,131:35985/Mozi,m
100% Threat score	http://117,26,220,195:40472/i
100% Threat score	http://27,46,45,202:43475/Mozi,m
100% Threat score	http://60,170,181,138:64946/Mozi,m
100% Threat score	http://45,224,169,58:54522/Mozi,a
100% Threat score	http://182,113,203,248:44768/Mozi,m
100% Threat score	http://182,121,41,18:46440/Mozi,m
97% Threat score	http://45,14,224,68/bins/aeneas,mips
95% Threat score	https://loadmaster,net/

95% Threat score	http://www.thegenesis.in/
95% Threat score	https://eventsquid.events/
89% Threat score	https://www.thegenesis.in/
89% Threat score	https://www.dropbox.com/s/0kl5ypie623n067/totolink
86% Threat score	http://177.84.221.109:35811/bin.sh
77% Threat score	http://peck.vaccable.co/
72% Threat score	http://www.la-matelote.com/
95% Threat score	http://www.canva.com/design/DAE74t1N9ko/BWYBLshIFvJkJhFhEzmXrg/view
95% Threat score	https://bit.ly/3tBhgRk#fuckyou%40fuck.com
89% Threat score	https://www.enoc-contractor.com/
89% Threat score	https://soundsoftravellingwell.cathaypacific.com/
84% Threat score	https://protect-eu.mimecast.com/s/5M6DC19zmCBj45ySLSAUN?domain=qs32210eui3910op473144.efraga.com.br
72% Threat score	http://3g52iv.bestellbar-ohne-rezept.sbs/

Source: NIST

NIST CVE: Critical

CVE-2022-25448

Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the day parameter in the openSchedWifi function.

CRITICAL Vector: network Created: 2022-03-18 Updated: 2022-03-25

CVE-2022-25455

Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the list parameter in the SetIpMacBind function.

CRITICAL Vector: network Created: 2022-03-18 Updated: 2022-03-25

CVE-2022-25450

Tenda AC6 V15.03.05.09_multi was discovered to contain a stack overflow via the list parameter in the SetVirtualServerCfg function.

CRITICAL Vector: network Created: 2022-03-18 Updated: 2022-03-25

CVE-2022-25457

Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the ntpserver parameter in the SetSysTimeCfg function.

CRITICAL Vector: network Created: 2022-03-18 Updated: 2022-03-25

CVE-2022-25446

Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the schedstarttime parameter in the openSchedWifi function.

CRITICAL Vector: network Created: 2022-03-18 Updated: 2022-03-25

CVE-2022-25445

Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the time parameter in the PowerSaveSet function.

CRITICAL Vector: network Created: 2022-03-18 Updated: 2022-03-25

CVE-2022-25452

Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the URLs parameter in the saveParentControlInfo function.

CRITICAL Vector: network Created: 2022-03-18 Updated: 2022-03-25

CVE-2022-25438

Tenda AC9 v15.03.2.21 was discovered to contain a remote command execution (RCE) vulnerability via the SetIPTVCfg function.

CRITICAL Vector: network Created: 2022-03-18 Updated: 2022-03-25

CVE-2022-25428

Tenda AC9 v15.03.2.21 was discovered to contain a stack overflow via the deviceId parameter in the saveparentcontrolinfo function.

CRITICAL Vector: network Created: 2022-03-18 Updated: 2022-03-25

CVE-2022-25439

Tenda AC9 v15.03.2.21 was discovered to contain a stack overflow via the list parameter in the SetIpMacBind function.

CRITICAL Vector: network Created: 2022-03-18 Updated: 2022-03-25

CVE-2022-25437

Tenda AC9 v15.03.2.21 was discovered to contain a stack overflow via the list parameter in the SetVirtualServerCfg function.

CRITICAL Vector: network Created: 2022-03-18 Updated: 2022-03-25

CVE-2022-25427

Tenda AC9 v15.03.2.21 was discovered to contain a stack overflow via the schedendtime parameter in the openSchedWifi function.

CRITICAL Vector: network Created: 2022-03-18 Updated: 2022-03-25

CVE-2022-25431

Tenda AC9 v15.03.2.21 was discovered to contain multiple stack overflows via the NPTR, V12, V10 and V11 parameter in the Formsetqosband function.

CRITICAL Vector: network Created: 2022-03-18 Updated: 2022-03-25

CVE-2022-25449

Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the deviceId parameter in the saveParentControlInfo function.

CRITICAL Vector: network Created: 2022-03-18 Updated: 2022-03-25

CVE-2022-25451

Tenda AC6 V15.03.05.09_multi was discovered to contain a stack overflow via the list parameter in the setstaticroutecfg function.

CRITICAL Vector: network Created: 2022-03-18 Updated: 2022-03-25

CVE-2022-25454

Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the loginpwd parameter in the SetFirewallCfg function.

CRITICAL Vector: network Created: 2022-03-18 Updated: 2022-03-25

CVE-2022-25447

Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the schedendtime parameter in the openSchedWifi function.

CRITICAL Vector: network Created: 2022-03-18 Updated: 2022-03-25

CVE-2022-25456

Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the security_5g parameter in the WifiBasicSet function.

CRITICAL Vector: network Created: 2022-03-18 Updated: 2022-03-25

CVE-2022-25453

Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the time parameter in the saveParentControlInfo function.

CRITICAL Vector: network Created: 2022-03-18 Updated: 2022-03-25

CVE-2022-25429

Tenda AC9 v15.03.2.21 was discovered to contain a buffer overflow via the time parameter in the saveparentcontrolinfo function.

CRITICAL Vector: network Created: 2022-03-18 Updated: 2022-03-25

CVE-2022-25441

Tenda AC9 v15.03.2.21 was discovered to contain a remote command execution (RCE) vulnerability via the vlanid parameter in the SetIPTVCfg function.

CRITICAL Vector: network Created: 2022-03-18 Updated: 2022-03-25

CVE-2022-25434

Tenda AC9 v15.03.2.21 was discovered to contain a stack overflow via the firewallen parameter in the SetFirewallCfg function.

CRITICAL Vector: network Created: 2022-03-18 Updated: 2022-03-25

CVE-2022-25435

Tenda AC9 v15.03.2.21 was discovered to contain a stack overflow via the list parameter in the SetStaticRoutecfg function.

CRITICAL Vector: network Created: 2022-03-18 Updated: 2022-03-25

CVE-2022-25440

Tenda AC9 v15.03.2.21 was discovered to contain a stack overflow via the ntpserver parameter in the SetSysTimeCfg function.

CRITICAL Vector: network Created: 2022-03-18 Updated: 2022-03-25

CVE-2022-25433

Tenda AC9 v15.03.2.21 was discovered to contain a stack overflow via the urls parameter in the saveparentcontrolinfo function.

CRITICAL Vector: network Created: 2022-03-18 Updated: 2022-03-25

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-2022-26629

An Access Control vulnerability exists in SoroushPlus+ **Messenger** 1.0.30 in the **Lock Screen** Security Feature function due to insufficient permissions and privileges, which allows a malicious attacker bypass the lock screen function.

UNRATED Vector: unkown Created: 2022-03-24 Updated: 2022-03-25

CVE-2022-22688

Improper neutralization of special elements used in a command ('Command Injection') vulnerability in File service functionality in **Synology DiskStation Manager** (DSM) before 6.2.4-25556-2 allows remote authenticated users to execute arbitrary commands via unspecified vectors.

UNRATED Vector: unkown Created: 2022-03-25 Updated: 2022-03-25

CVE-2022-22687

Buffer copy without checking size of input ('Classic Buffer Overflow') vulnerability in Authentication functionality in **Synology DiskStation Manager** (DSM) before 6.2.3-25426-3 allows remote attackers to execute arbitrary code via unspecified vectors.

UNRATED Vector: unkown Created: 2022-03-25 Updated: 2022-03-25

CVE-2018-25032

zlib 1.2.11 allows memory corruption when deflating (i.e., when compressing) if the input has many distant matches.

UNRATED Vector: unkown Created: 2022-03-25 Updated: 2022-03-25

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.

🇺🇸 #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.

🇺🇸 #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.

🇺🇸 #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.

🇩🇪 #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.

🇺🇸 #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.

🇺🇸 #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.

🇺🇸 #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.

🇺🇸 #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.

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 Netherlands
- #4 Germany
- #5 Singapore
- #6 United Kingdom
- #7 France
- #8 Hong Kong
- #9 Turkey
- #10 Brazil

Source: Hybrid Analysis

Top malicious files

100% Threat score	Server,exe	100% Threat score	BANK DETAILS,exe
100% Threat score	a3ERPSII,exe	100% Threat score	9407b4a736fe6f81101adb5a2e66bdd35171d9f15e756fd90a50a3e86a35d71d,vbs
100% Threat score	RDPCheck,exe	100% Threat score	1887d44bd913b81d9943f4b5637e01b057d20d757b23cd6ea3da239827a9cd95,exe
100% Threat score	12559af5c2c626b4e492751a8235076667926d41d6a29d1792e8ce65164fc42c,exe	100% Threat score	762276d9ce6d04d1f95c4dd8ec742e7d73cd88a307b815d0154a23d32515107d,exe
100% Threat score	8435fa985a445994ae3b8134721302ecd6dbfa29d1052eb8471721649ab1b522,exe	100% Threat score	æœ¨é©¬CVE-2022-24086,exe,bin
100% Threat score	84a2887b7e85c116b8b5fcf2c410ef356f1c328a3cc0505817e46d48a0a52a17,exe	100% Threat score	HSBC Customer Information,com
100% Threat score	f_00114a,pdf	100% Threat score	tmpmvzda3bu
100% Threat score	tmpbsbt5oo3	100% Threat score	Server,exe
100% Threat score	IBankWizSetup,exe	100% Threat score	d601bf3abee70a794408898d9eb1bb90b06b64db0302dedb77197c08bfdb8f0b,exe
100% Threat score	Server,exe	100% Threat score	677e22ac06a74d6db2d3d5fb3b5334aed5b5f5ac65ba8d72d1d85030dcda49c1
100% Threat score	843a557c49c0837e5555d2f48fad9e9844b55482908233dc411008cc82d29fd9,exe	100% Threat score	Firefox Setup 89,0,2,exe
85% Threat score	ChromeSetup,exe	82% Threat score	cb5c2d2be9a81f5ab856413ff208687ae1faa3a8e23f7f4ba792377021d35ed6,dll
81% Threat score	72a206dfebdf674f2c0205eccc90ea1e2b7a4e2b10abc3052908e9ba4a862a76,dll	77% Threat score	ManAndMachine,exe
75% Threat score	PotPlayerSetup64,exe	75% Threat score	tmpflo0v6qx
75% Threat score	Pi_setup_14thJan2020,exe	75% Threat score	IDMan,exe

Source: Imperva DDOS Map

Top DDOS techniques

78%	**DDoS**
15%	**Automated Threat**
7%	**OWASP**

Source: Imperva DDOS Map

Top DDOS industry targets

59%	**Financial Services**
23%	**Business**
4%	**Computing & IT**