Security Rabbits

Your Security Rabbits report for March 22, 2022

Source: Ransom Watch

Ransomware attacks

lockbit2	apec-capital,co,,,
hiveleak	Centerline Communication Llc
stormous	Core Design
alphv	BERITASATUMEDIA,COM
lockbit2	sete,co,u
stormous	Aurora hacked data
stormous	Company ENOS PROPERTIES
hiveleak	Polynt Group
conti	OCA Global

Hot topics

Nothing today

News

Cyware News - Latest Cyber News

Are cybercriminals really using fake QR codes to steal your financial information?
In January 2022, the FBI issued a PSA warning people of a new trend: cybercriminals are allegedly taking advantage of QR codes to redirect victims to malicious sites that can steal their credentials and financial information.

Threatpost

Bridgestone Hit as Ransomware Torches Toyota Supply Chain
A ransomware attack struck Bridgestone Americas, weeks after another Toyota supplier experienced the same and a third reported some kind of cyber hit.

Cyware News - Latest Cyber News

Caketap Rootkit by UNC2891 Targets Banks Customers
The LightBasin threat actor is using the new Unix rootkit Caketap against servers running Oracle Solaris. Caketap can hide network files, processes, and connections, and install hooks into system functions for remote commands and configurations. The group has mostly targeted Oracle Solaris-based systems with TINYSHELL and SLAPSTICK backdoors.

Cyware News - Latest Cyber News

Facebook phish claims "Someone tried to log into your account"
The mail itself combines a fairly clean design with minimal messaging. There's a tendency with some phish attempts to overstuff the mail with all manner of nonsense to look more convincing.

Cyware News - Latest Cyber News

Fake Esports voting sites looking to phish Steam users
A Steam user receives an unsolicited message from a stranger. It may be sent via Steam's own messenger service, or it could be in a Discord channel. The scammer presents the "offer" as a way to help a fellow Steam enthusiast out.

Cyware News - Latest Cyber News

GoDaddy Managed Hosting Service Targeted via Backdoor Infection
The Wordfence Incident Response team alerted nearly 300 websites hosted on GoDaddy's Managed WordPress service that were infected with a common backdoor. The backdoor payload is a 2015 Google search SEO-poisoning tool. Website admins are suggested to remove the backdoor and spam search engine results.

IT Security Guru

Hackers target luxury hotels in Macau
Luxury hotels in Macau were the target of malicious spear-phishing campaigns for nearly 3 months, according to research from security researchers at Trellix. The cybersecurity firm has attributed the campaign to the aptly named DarkHotel group, building on research published by Zscaler in December 2021. DarkHotel is believed to have been access since 2007, with […] The post Hackers target luxury hotels in Macau appeared first on IT Security Guru.

IT Security Guru

Hubspot breach spreads to BlockFi, Swan Bitcoin
Hubspot, a widely used Customer Relationship Management (CRM) platform, was hacked on Friday by a threat actor accessing an employee account. The hacker then used the account to target 30 as yet unnamed cryptocurrency stakeholders, with BlockFi and Swan Bitcoin confirming that they suffered a breach. As Hubspot is a third party vendor, the hacker […] The post Hubspot

Cyware News - Latest Cyber News

Attackers Targeting Unpatched SolarWinds WHD Instances
In the wake of new attacks, SolarWinds urged customers to remove their Web Help Desk instances from their publicly accessible infrastructure. An attacker may take advantage of unpatched WHD instances (CVE-2021-35251) for getting access to environmental details about the installation. SolarWinds recommends all its customers use WHD with an externally facing implementation to remove it from the internet.

Threatpost

Browser-in-the-Browser Attack Makes Phishing Nearly Invisible
Can we trust web browsers to protect us, even if they say "https?" Not with the novel BitB attack, which fakes popup SSO windows to phish away credentials for Google, Facebook and Microsoft, et al.

Threatpost

Conti Ransomware V. 3, Including Decryptor, Leaked
The latest is a fresher version of the ransomware pro-Ukraine researcher ContiLeaks already released, but it's reportedly clunkier code.

Threatpost

Facestealer Trojan Hidden in Google Play Plunders Facebook Accounts
The trojanized Craftsart Cartoon Photo Tools app is available in the official Android app store, but it's actually spyware capable of stealing any and all information from victims' social-media accounts.

Cyware News - Latest Cyber News

Gh0stCringe Targets Weakly Configured Microsoft SQL, MySQL Servers
AhnLab found a malware threat dubbed Gh0stCringe targeting Oracle's open-source MySQL and Microsoft's SQL Server by abusing weak user credentials. Moreover, researchers have identified multiple malware samples--such as KingMiner and Vollgar CoinMiner--on the targeted servers. Experts say frequently patching exposed servers and using additional security layers such as firewalls further help fend off such attacks.

Security Affairs

Hacker leaked a new version of Conti ransomware source code on Twitter
A Ukrainian security researcher has leaked more source code from the Conti ransomware operation to protest the gang's position on the conflict. Hacker leaked a new version of the Conti ransomware source code on Twitter as retaliation of the gang's support to Russia The attack against the Conti ransomware and the data leak is retaliation […] The post Hacker leaked a new version of Conti ransomware source code on Twitter appeared first on Security Affairs.

Cyware News - Latest Cyber News

How a Vulnerability in Third-Party Technology Is Leaving Many IP Cameras and Surveillance Systems Vulnerable
A large number of IP cameras and surveillance systems used in enterprise networks were recently discovered to be vulnerable to remote code execution and information leakage due to CVE-2021-28372.

Cyware News - Latest Cyber News

Influx of Trojanized Apps on Google Play Store
Dr.Web disclosed numerous trojanized apps on Google Play Store prompting potential victims to take action, such as depositing money for trading or signing up for expensive subscriptions, benefitting the scammers eventually. The detected malicious apps include SecretVideoRecorder, FakeAntiVirus, KeyStroke, WapSniff, FreeAndroidSpy, SilentInstaller, etc. Android users are

breach spreads to BlockFi, Swan Bitcoin appeared first on IT Security Guru.

Cyware News - Latest Cyber News

[Iranian hackers leak Mossad chief's personal information]
Iranian hackers on Wednesday published a video on an anonymous Telegram channel featuring personal photos and documents allegedly obtained from a phone used by the wife of Mossad Director David Barnea.

Security Affairs

[Lapsus$ extortion gang leaked the source code for some Microsoft projects]
The Lapsus$ extortion group claims to have hacked Microsoft 's internal Azure DevOps server and leaked the source code for some projects. Microsoft recently announced that is investigating claims that the Lapsus$ cybercrime gang breached their internal Azure DevOps source code repositories and stolen data. On Sunday, the Lapsus$ gang announced to have compromised Microsoft's Azure DevOps [...] The post Lapsus$ extortion gang leaked the source code for some Microsoft projects appeared first on Security Affairs.

Cyware News - Latest Cyber News

[Microsoft Investigating Claim of Breach by Extortion Gang]
Earlier this month the group said on its Telegram channel that it was seeking employees inside technology companies who would be willing to work with them, including Microsoft.

The Hacker News

[New Browser-in-the Browser (BITB) Attack Makes Phishing Nearly Undetectable]
A novel phishing technique called browser-in-the-browser (BitB) attack can be exploited to simulate a browser window within the browser in order to spoof a legitimate domain, thereby making it possible to stage convincing phishing attacks. According to penetration tester and security researcher, who goes by the handle mrd0x on Twitter, the method takes advantage of third-party single sign-on (

The Hacker News

[New Dell BIOS Bugs Affect Millions of Inspiron, Vostro, XPS, Alienware Systems]
Five new security weaknesses have been disclosed in Dell BIOS that, if successfully exploited, could lead to code execution on vulnerable systems, joining the likes of firmware vulnerabilities recently uncovered in Insyde Software's InsydeH2O and HP Unified Extensible Firmware Interface (UEFI). Tracked as CVE-2022-24415, CVE-2022-24416, CVE-2022-24419, CVE-2022-24420, and CVE-2022-24421, the

Cyware News - Latest Cyber News

[Payment fraud attack rate across fintech ballooned 70% in 2021]
According to Sift, these rising attacks were aimed primarily at alternative payments like digital wallets, which saw a 200% increase in payment fraud, along with payments service providers (+169%), and cryptocurrency exchanges (+140%).

Cyware News - Latest Cyber News

[Russian Hackers Abuse MFA Flaw for Lateral Movement - Warns FBI]
The FBI said that the hackers gained access to an NGO cloud by abusing default MFA protocols. They enrolled their own device into the organization's Duo MFA.

Security Affairs

[Serpent backdoor targets French entities with high-evasive attack chain]
A new email campaign aimed at French entities leverages the Chocolatey Windows package manager to deliver the Serpent backdoor. Proofpoint researchers uncovered a targeted attack leveraging an open-source package installer Chocolatey to deliver a backdoor tracked as Serpent. The campaign targeted French entities in the construction, real estate, and government industries. Experts believe the attacks were [...] The post Serpent backdoor targets French entities with high-evasive attack chain appeared first on Security Affairs.

ZDNet | security RSS

[Ukraine warns of InvisiMole attacks tied to state-sponsored Russian hackers]
InvisiMole has been collaborating with the Gamaredon APT for years.

Naked Security

[Web vendor CafePress fined $500,000 for giving cybersecurity a low value]
Just because you're the victim of a cybercrime doesn't let you off your cybersecurity obligations

Cyware News - Latest Cyber News

[Windows zero-day flaw giving admin rights gets unofficial patch, again]
A Windows local privilege escalation zero-day vulnerability that Microsoft has failed to fully address for several months now, allows users to gain administrative privileges in Windows 10, Windows 11, and Windows Server.

recommended to avoid APK downloads from unknown sources.

Security Affairs

[Italy's data privacy watchdog investigates how Kaspersky manages Italian users' data]
Italy's data privacy watchdog launched an investigation into the "potential risks" associated with the use of Russian antivirus software Kaspersky. Italy's data privacy watchdog has launched an investigation into potential risks associated with the use of the Kaspersky antivirus. The Italian authority aims at verifying how the Russian company processes the data of Italian users [...] The post Italy's data privacy watchdog investigates how Kaspersky manages Italian users' data appeared first on Security Affairs.

Security Affairs

[Lapsus$ gang claims to have hacked Microsoft source code repositories]
Microsoft is investigating claims that the Lapsus$ hacking group breached its internal Azure DevOps source code repositories. Microsoft announced that is investigating claims that the Lapsus$ cybercrime gang breached their internal Azure DevOps source code repositories and stolen data. Over the last months, the gang compromised other prominent companies such as NVIDIA, Samsung, Ubisoft, Mercado [...] The post Lapsus$ gang claims to have hacked Microsoft source code repositories appeared first on Security Affairs.

CyberScoop

[Microsoft investigating hacking group's claims of successful breach]
Cybercrime organization Lapsus$ posted suspicious screenshots. Microsoft officials said they are "aware of the claims and are investigating." The post Microsoft investigating hacking group's claims of successful breach appeared first on CyberScoop.

ZDNet | security RSS

[New Conti ransomware source code leaked]
The individual responsible is targeting Conti after the group announced its loyalty to Russia during the invasion of Ukraine.

ZDNet | security RSS

[Okta says breach evidence posted by Lapsus$ hackers linked to January 'security incident']
Okta claims there is no proof of current malicious activity on its networks.

Security Affairs

[Russia-linked InvisiMole APT targets state organizations of Ukraine]
Ukraine CERT (CERT-UA) warns of spear-phishing attacks conducted by UAC-0035 group (aka InvisiMole) on state organizations of Ukraine. The Government Team for Response to Computer Emergencies of Ukraine (CERT-UA) warns of spear-phishing messages conducted by UAC-0035 group (aka InvisiMole) against Ukrainian state bodies. The messages use an archive named "501_25_103.zip", which contains a shortcut file. Upon opening [...] The post Russia-linked InvisiMole APT targets state organizations of Ukraine appeared first on Security Affairs.

WeLiveSecurity

[Sandworm: A tale of disruption told anew]
As the war rages, the APT group with a long resume of disruptive cyberattacks enters the spotlight again The post Sandworm: A tale of disruption told anew appeared first on WeLiveSecurity

ZDNet | security RSS

[Suspected DarkHotel APT resurgence targets luxury Chinese hotels]
Hospitality firms in Macao, China, are bearing the brunt of targeted cyberattacks.

CyberScoop

[Venezuelan leftists took to Twitter in attempt to swing Colombian presidential election]
An account had more than 144,000 followers before Twitter suspended it. The post Venezuelan leftists took to Twitter in attempt to swing Colombian presidential election appeared first on CyberScoop.

CyberScoop

[White House issues call to action in light of new intelligence on Russian cyberthreat]
\Russia has taken "preparatory actions" including probing websites for vulnerabilities, presidential adviser Anne Neuberger said. The post White House issues call to action in light of new intelligence on Russian cyberthreat appeared first on CyberScoop.

Blog â€" Flashpoint

[Your Data, Their Gain: How Threat Actors Leverage Tax Season to Commit Fraud]
In 2020, the IRS identified over US$2.3 billion in tax fraud schemes, including tax return fraud. And in 2021, we identified 113 breaches which resulted in more than 69 million exposed records, including tax information, documents, and other sensitive data; this year, we've already identified 15 breaches and 3 million exposed records. This number is [...] The post Your Data, Their Gain: How Threat Actors Leverage Tax Season to Commit Fraud appeared first on Flashpoint.

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-2022-22720

Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

CRITICAL Vector: network Created: 2022-03-14 Updated: 2022-03-22

CVE-2022-23943

Out-of-bounds Write vulnerability in mod_sed of **Apache** HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

CRITICAL Vector: network Created: 2022-03-14 Updated: 2022-03-22

CVE-2022-22721

If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects **Apache** HTTP Server 2.4.52 and earlier.

CRITICAL Vector: network Created: 2022-03-14 Updated: 2022-03-22

Source: NIST

NIST CVE: High

CVE-2022-22719

A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects **Apache** HTTP Server 2.4.52 and earlier.

HIGH Vector: network Created: 2022-03-14 Updated: 2022-03-22

CVE-2022-0778

The BN_mod_sqrt() function, which computes a modular **square** root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain **elliptic** curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - TLS clients consuming server certificates - TLS servers consuming client certificates - **Hosting** providers taking certificates or private keys from customers - Certificate authorities parsing **certification** requests from subscribers - Anything else which parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the **OpenSSL** 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

HIGH Vector: network Created: 2022-03-15 Updated: 2022-03-22

Source: NIST

NIST CVE: Medium

Nothing today

Source: NIST

NIST CVE: Low

Nothing today

Source: NIST

NIST CVE: Unrated

CVE-2022-0386

A post-auth SQL injection vulnerability in the **Mail** Manager potentially allows an authenticated attacker to execute code in **Sophos** UTM before version 9.710.

UNRATED Vector: unkown Created: 2022-03-22 Updated: 2022-03-22

CVE-2022-0652

Confd log files contain local users', including rootaEUR(tm)s, SHA512crypt password hashes with insecure access permissions. This allows a local attacker to attempt off-line brute-force attacks against these password hashes in **Sophos** UTM before version 9.710.

UNRATED Vector: unkown Created: 2022-03-22 Updated: 2022-03-22

CVE-2022-1034

There is a Unrestricted Upload of File vulnerability in **ShowDoc** v2.10.3 in **GitHub** repository star7th/showdoc prior to 2.10.4.

UNRATED Vector: unkown Created: 2022-03-22 Updated: 2022-03-22

CVE-2022-27607

Bento4 1.6.0-639 has a heap-based buffer over-read in the AP4_HvccAtom class, a different issue than CVE-2018-14531.

UNRATED Vector: unkown Created: 2022-03-21 Updated: 2022-03-22

CVE-2022-24775

guzzlehttp/psr7 is a PSR-7 HTTP message library. Versions prior to 1.8.4 and 2.1.1 are vulnerable to improper header parsing. An attacker could sneak in a new line character and pass untrusted values. The issue is patched in 1.8.4 and 2.1.1. There are currently no known workarounds.

UNRATED Vector: unkown Created: 2022-03-21 Updated: 2022-03-22

Source: Hybrid Analysis

Top malicious files

100% Threat score	SW2010-2014,Activator,GUI,2014,2,SSQ,exe	100% Threat score	XK097543456789008765,exe
100% Threat score	STOREWEL INQ LIST,jpg,exe	100% Threat score	FTrader,exe
100% Threat score	0d8bc09abccf43b95242bbbc865d24d27b8e692f04633d56656fb72595c72b61,exe	100% Threat score	kein,apk
100% Threat score	KaonTeam BL219v4,exe	95% Threat score	foto,PDF,exe
85% Threat score	DVA5Setup,exe	79% Threat score	f1aea4880886b5c7749508ecc9f4472da07adfc27c4fc2546cb44255c76e5c81,exe
75% Threat score	Uninstall,exe	71% Threat score	Wireless Hacking 101,pdf

Source: Hybrid Analysis

Top malicious URL

100% Threat score	https://serialms,com/	100% Threat score	http://main,d2bv07yzwiuc4x,amplifyapp,com/
100% Threat score	http://www,igametalent,com/	100% Threat score	https://bit,ly/3CPztxf
95% Threat score	http://123,8,77,49:37627/Mozi,m	95% Threat score	http://christ-michael,net/die-ukraine-und-der-krieg-der-alle-kriege-beendet/
94% Threat score	http://14,138,109,129:3763/i	94% Threat score	https://bit,ly/368aeul
94% Threat score	http://123,14,252,174:38387/Mozi,m	94% Threat score	http://98,0,239,142:45802/i
94% Threat score	http://116,212,156,134:36567/Mozi,m	93% Threat score	http://219,155,238,45:43423/bin,sh
93% Threat score	http://120,86,145,111:59330/Mozi,m	93% Threat score	http://213,248,132,39:53891/i
93% Threat score	http://219,154,125,228:36000/i	93% Threat score	http://58,53,75,38:37519/bin,sh
93% Threat score	http://123,14,41,100:58784/Mozi,m	93% Threat score	http://103,119,78,151:35184/Mozi,m
92% Threat score	http://www,bptdmaluku,com/pengaduan/	89% Threat score	https://u25644684,ct,sendgrid,net/ls/click?upn=qcXd7y-2Bot3SUHNietiJx3Xhz1zgEXlLJ1-2B2x-2BaNyYp5gxWYxq5x2FcnHfIRV7l1LYstpQBPwxMvzdSzFpLjmU2QNoFzmY48E1O1yMg0ozRBMA0qn-2BIsvBG7tjKnFwbdLCwOlSyTQf-2FAvvffOyZ4DmS1fTYXGLeZcKbj-2F8KwxgDLxOzonD3jGL1vEvxHZpZLalQVYtFxSO55EEHUBz3-2FexGl2PGKzFFDi8kbti9xzIUa7l2WaLiYkwrDVerr1Ppm0vTw6psWiCQSvy2lM5xGA-3D-3DNNEt_F-2Flw29EQ3IrxNy2FT0NkcH9HgW9v8Zfhv4o4GB62oaDu66nX0VBCBSfIAjpDFff0CoxPFeucmEQeJltLEm6kXGtasQdaSuFjsfNDAqsuNa2BV8dW1McwEeHebKcTp7sKm5AA1vrKjBOEknrXcSF4MUI9mQUGVGH99prpyxI0V-2F8F5fxocNWE-2BMGVIe78tChGm9JDC7JJOk61t04bfwYY5ma25VoJxl3Ilb5op9M8oLHQ-2FhUPrq7qDs2-2BctEiDxJ3jo8HJA-2FYUWMZyB8894Tc0ujncgG-2BUEc9FGVp9qEP-2BgbN-2FlTX-2FvKZeK43b-2FJvVl2ywzxlyGQ6E-2BDwCOCcOo6qn7m4WyqbdKKckOfw5pJlt2pnMDG5TG6L5savUoLUXYJbh52mh37WJH0vViYUc4oTHh0ZBgqmBy-22Fu3rXEDVBWEZr7nGUu3hbjJFf63jqbp83P8rjMci-2FqpQGtowX4dMVWEb-2FFqYBXqx5Cz8T55pwyt0aqynzmSDjDjJX579Eiu3AZpjjhr1nI76lIu6Snyz1ME0-2Be5AIUl5N6huVrz319hvReECoqJSbDIYlxRaAfLh7ONQzyYXKFHirokAYwGY6ckGBAxJbxq6Y-2FNp7XfiTugBzDNTFfeL7vza0bahlL1rOyhsH5Jz0thJY7c5YRUyhYKour0tLzT7RdRXnMXJoBDiSE3TlC9OB-2F8FWX-2Ff9SXwqOIgv9HwI1GyxMHcTPEAt9WGKtjNSM4fRPNTy2M4FTzPHCD30wbLyk-2BzGJnMPSsh0Gu35wQ7X03I-2B4bEAjkv9CLnMFPUJXFlMphXiLvcxtllrHBxHQfWs34z7xV9dQ0JOUVqlLxTDsbiQ-3D
88% Threat score	http://182,127,110,88:35382/Mozi,m	88% Threat score	http://117,201,197,186:35362/Mozi,m
85% Threat score	https://onlinetinyurl,com/	83% Threat score	http://www,uundz,de/intern/Keyvi3_3,4,9,0,zip
82% Threat score	http://www,maineemploymentlawyerblog,com/first-circuit-permits-worker-to-sue-kansas-company-in-massachusetts-for-unpaid-commission/	82% Threat score	http://text8282,xyz/
82% Threat score	http://pussy-cheat,com/	82% Threat score	http://jobcenterkenya,com/job-scam-alert-career-point-kenya/
82% Threat score	http://stealer,stih,nl/	81% Threat score	http://mbfbank,to/a/%23/
78% Threat score	https://bit,ly/36jFPJg	77% Threat score	http://minato-council-communicator,web,app/
77% Threat score	http://www,cheshuntcomp,com/	75% Threat score	http://kobkoblianchreb,shop/
74% Threat score	http://clt1426789,bmetrack,com/	72% Threat score	http://spacekeys,net/
72% Threat score	http://www,besthappybuds,net/	72% Threat score	http://www,oreadybags,com/

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 Venezuela (Bolivarian Republic of)

Source: SpamHaus

Top phishing countries

- #1 United States
- #2 Singapore
- #3 Germany
- #4 Russia
- #5 Netherlands
- #6 United Kingdom
- #7 Bulgaria
- #8 India

- #9 Italy
- #10 Brazil

Source: Have I been pwned?

Have I been pwnd

Nothing today

Source: Imperva DDOS Map

Top DDOS attackers

- **United States (27%)**
- **Russia (14%)**
- **Germany (11%)**

Source: Imperva DDOS Map

Top DDOS country targets

- **Russia (55%)**
- **Ukraine (17%)**
- **United States (12%)**

Source: Imperva DDOS Map

Top DDOS techniques

77%	**DDoS**
17%	**Automated Threat**
7%	**OWASP**

Source: Imperva DDOS Map

Top DDOS industry targets

59%	**Financial Services**
21%	**Business**
6%	**Law & Government**