Your Security Rabbits report for March 04, 2022

Source: Ransom Watch

Ransomware attacks

conti Target: A . J . Rose(2022-03-04)

conti Target: Get Fresh Company(2022-03-04)

conti Target: Prima Power(2022-03-04)

conti Target: United McGill Corporation(2022-03-04)

lockbit2 Target: simatelex . com . h . . . (2022-03-03)

conti Target: Caledonian(2022-03-04)

conti Target: Gleason Corporation(2022-03-04)

lockbit2 Target: tovogom(2022-03-04)

snatch Target: Private company #2(2022-03-03)

Hot topics

Nothing today

News

Security Affairs

75% of medical infusion pumps affected by known vulnerabilities

Researchers analyzed more than 200,000 network-connected medical infusion pumps and discovered that over 100,000 of them are vulnerable. Researchers from Palo Alto Networks have analyzed more than 200,000 medical infusion pumps on the networks of hospitals and other healthcare organizations and discovered that 75% are affected by known vulnerabilities that could be exploited by attackers. […] The post 75% of medical infusion pumps affected by known vulnerabilities appeared first on Security Affairs.

Cyware News - Latest Cyber News

Avast researchers warns against joining in DDoS attacks in aid of Ukraine

These DDoS tools collect personal data that can make users identifiable, such as IP address, country code, city, location based on IP address, username, hardware configuration, and system language.

Security Affairs

Cisco fixed two critical flaws in Expressway, TelePresence VCS solutions

Cisco fixed critical flaws in its Expressway Series and TelePresence Video Communication Server (VCS) unified communications products. Cisco announced security patches for a couple of critical vulnerabilities, tracked as CVE-2022-20754 and CVE-2022-20755 (CVSS score of 9.0), in its Expressway Series and TelePresence Video Communication Server (VCS) unified communications products. "Multiple vulnerabilities in the API and […] The post Cisco fixed two critical flaws in Expressway, TelePresence VCS solutions appeared first on Security Affairs.

The Hacker News

Critical Patches Issued for Cisco Expressway Series, TelePresence VCS Products

Cisco this week shipped patches to address a new round of critical security vulnerabilities affecting Expressway Series and Cisco TelePresence Video Communication Server (VCS) that could be exploited by an attacker to gain elevated privileges and execute arbitrary code. The two flaws - tracked as CVE-2022-20754 and CVE-2022-20755 (CVSS scores: 9.0) - relate to an arbitrary file write and a

WeLiveSecurity

ESET Research Podcast: Ukraine's past and present cyberwar

Press play to hear Aryeh Goretsky, Jean-Ian Boutin and Robert Lipovsky discuss how recent malware attacks in Ukraine tie into years of cyberattacks against the country The post ESET Research Podcast: Ukraine's past and present cyberwar appeared first on WeLiveSecurity

Blog â€” Flashpoint

ISIS Attacks, February 2022: Key Trends, Statistics, and Geographic Analysis

The following research is based on information gathered by Flashpoint analysts and data collections. For January's report, click here. Key takeaways: February 2022 ISIS attacks Attacks claimed by ISIS worldwide in February were down at least 15-20 percent from the average monthly tally in the last six months. Although some considerations can be made for […] The post ISIS Attacks, February

Security Affairs

Avast released a free decryptor for the HermeticRansom that hit Ukraine

Avast released a decryptor for the HermeticRansom ransomware used in recent targeted attacks against Ukrainian entities. Avast has released a free decryptor for the HermeticRansom ransomware employed in targeted attacks against Ukrainian systems since February 23. The security firms aim at helping Ukrainians victims in recovering their file for free. The HermeticRansomware was one of […] The post Avast released a free decryptor for the HermeticRansom that hit Ukraine appeared first on Security Affairs.

IT Security Guru

Blackouts hit Ukraine

Several Ukrainian cities are experiencing power outages as the Russian invasion rages on. NetBlocks, a Global internet access tracker, has shared data highlighting widespread internet outages across Mariupol, Sumy and other regions of the country. This comes alongside an increase in bombing campaigns and rocket fire from Russian units. Alp Toker, director of NetBlocks, told […] The post Blackouts hit Ukraine appeared first on IT Security Guru.

Cyware News - Latest Cyber News

Cisco Patches Critical Vulnerabilities in Expressway, TelePresence VCS Products

Cisco this week announced patches that address a couple of critical vulnerabilities in its Expressway Series and TelePresence Video Communication Server (VCS) unified communications products.

IT Security Guru

Cyber attack attempts on Ukraine surge tenfold

A threat actor in support of Russia has compromised at least 30 Ukrainian universities as vulnerability exploit attempts have surged, according to Wordfence. The security firm has generated useful intelligence on the the attacks campaign as it protects over 8300 Ukrainian WordPress sites, including those of private businesses, government, military and police. The attack campaign […] The post Cyber attack attempts on Ukraine surge tenfold appeared first on IT Security Guru.

Cyware News - Latest Cyber News

Google WAF bypassed via oversized POST requests

Researchers at Kloudle found they were able to bypass both Google Cloud Platform (GCP) and Amazon Web Services (AWS) web app firewalls just by making a POST request more than 8KB in size.

Cyware News - Latest Cyber

Log4shell exploits now used mostly for DDoS botnets, cryptominers

According to Barracuda, the past couple of months were characterized by dips and spikes in the targeting of Log4Shell, but the volume of exploitation attempts has remained relatively constant.

2022: Key Trends, Statistics, and Geographic Analysis appeared first on Flashpoint.

Cyware News - Latest Cyber News

Look out for identity theft and fraud crimes as tax season begins

Between October and December 2021, identity theft and fraud cases increased by 11%, led by rapid spikes in instances of fraudulent credit and/or loan account creation, inquiries, and applications.

The Hacker News

New Security Vulnerability Affects Thousands of GitLab Instances

Researchers have disclosed details of a now-patched security vulnerability in GitLab, an open-source DevOps software, that could potentially allow a remote, unauthenticated attacker to recover user-related information. Tracked as CVE-2021-4191 (CVSS score: 5.3), the medium-severity flaw affects all versions of GitLab Community Edition and Enterprise Edition starting from 13.0 and all versions

CyberScoop

Personal data from T-Mobile breach still spreading on dark web, state governments warn

The top law enforcement officials from multiple states are alerting people affected by an August 2021 breach at T-Mobile that their personal data might be circulating in cybercrime forums online. "Information stolen in a massive data breach has fallen into the wrong hands and is circulating on the dark web," New York Attorney General Letitia James said Wednesday in a news release. Officials from California, Florida and several other states issued similar warnings. The T-Mobile breach involved the data of tens of millions of current, former or prospective customers of the wireless company. The stolen data is attractive for identity theft and other financial crimes. The hacker who claimed resp[...]

CyberScoop

Putin's government lists IPs and domains allegedly aiming DDoS traffic at Russia

The Russian government on Wednesday published a list of more than 17,500 IP addresses and 174 internet domains it says are involved in ongoing distributed denial-of-service attacks on Russian domestic targets. The list include the FBI and CIA's home pages, and other sites with top-level domain (TLD) extensions denoting they are registered through countries such as Belarus, Germany, Ukraine and Georgia, as well as the European Union. The Russian government did not publish any proof or evidence backing up its claims about the IP addresses or domains on its list. DDoS incidents can be tough to attribute to any specific actor, and otherwise benign internet domains can be hijacked by attackers to[...]

Cyware News - Latest Cyber News

Researchers Demonstrate New Side-Channel Attack Against Homomorphic Encryption

A group of academics have demonstrated what they say is the "first side-channel attack" on homomorphic encryption that could be exploited to leak data as the encryption process is underway.

Cyware News - Latest Cyber News

Rural Idaho Receives Cybersecurity Boost

According to a new announcement, Boise State University (BSU) has partnered with Stellar Cyber to launch a new program to improve cybersecurity in Idaho's rural and remote communities.

The Hacker News

Russia Releases List of IPs, Domains Attacking Its Infrastructure with DDoS Attacks

As the ongoing Russia-Ukraine conflict continues to escalate, the Russian government on Thursday released a massive list containing 17,576 IP addresses and 166 domains that it said are behind a series of distributed denial-of-service (DDoS) attacks aimed at its domestic infrastructure. Some of the noticeable domains in the listing released by Russia's National Coordination Center for Computer

CyberScoop

Russia's invasion of Ukraine has turned the global internet into a battlefield

Russia and Ukraine are both racing to take control of a key battlefield in the ongoing conflict: the internet. Moves by both countries have open internet advocates worrying that civilians' rights to the global internet and freedom of information are getting caught in the middle. Ukraine failed in one of its attempts to cut Russia off on Wednesday. The Internet Corporation for Assigned Names and Numbers (ICANN) -- a nonprofit that oversees domain and internet protocol systems vital to the global internet -- rejected a request by Ukrainian officials to shut down high-level Russian domains. ICANN noted that it is not able to take unilateral action to disconnect domains. Third-party operators ha[...]

Naked Security

S3 Ep72: AirTag stalking, web server coding woes and Instascams [Podcast + Transcript]

Latest episode - listen now (or read it, if that's your preference)...

IT Security Guru

Telegram now favoured by hacktivists, cybercriminals

As the conflict in Ukraine progresses, Telegram messaging has emerged as a favourite tool for both hacktivists and cybercriminals alike. Research from the cybersecurity company Check Point suggests that there are six times as many groups on the messaging apps since February 24. Some topic-specific groups have grown significantly, some even reaching more

News

Cyware News - Latest Cyber News

MITRE Engage framework provides defense strategies for the cyber defense community

Informed by adversary behavior observed in the real world, MITRE Engage helps chief information security officers (CISOs), cyber defenders, and vendors to implement defense strategies.

Security Affairs

NVIDIA discloses data breach after the recent cyber attack

Chipmaker giant Nvidia confirmed a data breach after the recently disclosed security incident, proprietary information stolen. The chipmaker giant Nvidia was recently the victim of a cyber attack that impacted some of its systems for two days. The security breach is not connected to the ongoing crisis in Ukraine, according to a person familiar with […] The post NVIDIA discloses data breach after the recent cyber attack appeared first on Security Affairs.

Threatpost

Phishing Campaign Targeted Those Aiding Ukraine Refugees

A military email address was used to distribute malicious email macros among EU personnel helping Ukrainians.

Cyware News - Latest Cyber News

Ransomware infections top list of the most common results of phishing attacks

In a new study, eighty-four percent of organizations reported falling victim to a phishing attack last year, Egress said, and of those 59% were infected with ransomware as a result.

The Hacker News

Researchers Demonstrate New Side-Channel Attack on Homomorphic Encryption

A group of academics from the North Carolina State University and Dokuz Eylul University have demonstrated what they say is the "first side-channel attack" on homomorphic encryption that could be exploited to leak data as the encryption process is underway. "Basically, by monitoring power consumption in a device that is encoding data for homomorphic encryption, we are able to read the data as it

Threatpost

Russia Leaks Data From a Thousand Cuts-Podcast

It's not just Ukraine: There's a flood of intel on Russian military, nukes and crooks, says dark-web intel expert Vinny Troia, even with the Conti ransomware gang shuttering its leaking Jabber chat server.

Security Affairs

Russia-Ukraine, who are the soldiers that crowd cyberspace?

While Russia is invading Ukraine, multiple forces are joining in the conflict, especially in the cyber space, let's analyze them The analysis of the current scenario in cyberspace is not easy due to the presence of multiple threat actors and the difficulty of attributing the attacks. Security group CyberKnow shared an interesting analysis about the […] The post Russia-Ukraine, who are the soldiers that crowd cyberspace? appeared first on Security Affairs.

Blog â€“ Flashpoint

Russian APT and Ransomware Groups: Vulnerabilities and Threat Actors Who Exploit Them

A history of cyberattacks Far before Russia launched its full-scale invasion of Ukraine, cybersecurity officials from the Ukrainian government already believed their nation had experienced multiple cyberattacks led by Russian Advanced Persistent Threat (APT) groups. As Russian troops gathered on their borders, numerous Ukrainian government websites as well as several banks were DDoS'd, with the […] The post Russian APT and Ransomware Groups: Vulnerabilities and Threat Actors Who Exploit Them appeared first on Flashpoint.

Threatpost

Securing Data With a Frenzied Remote Workforce-Podcast

Stock the liquor cabinet and take a shot whenever you hear GitLab Staff Security Researcher Mark Loveless say "Zero Trust."

Security Affairs

The Difference Between Human and Machine Identities

As digital transformation is advancing and automation is becoming an essential component of modern enterprises, collaboration between humans and machines is crucial. With this level of interaction, a new identity problem is emerging as machines operate on behalf of humans. Collaboration between humans and machines is a working reality today.

than 250,000 members. […] The post Telegram now favoured by hacktivists, cybercriminals appeared first on IT Security Guru.

Cyware News - Latest Cyber News

[The Linux Foundation's Census of OSS app libraries helps prioritize security work]
The foundation announced released the "Census II of Free and Open Source Software - Application Libraries," which identifies over 1,000 of the most widely deployed open-source application libraries.

CyberScoop

[Treasury Department sanctions alleged Russian cyber-espionage, disinformation sources]
The Biden administration on Thursday sanctioned Russian oligarchs and organizations for their role in spreading disinformation and supporting Russian President Vladimir Putin's war in Ukraine, among them a news agency the Treasury Department says has ties to a Russian cyber-espionage and offensive unit. The sanctions targeted nine employees of InfoRos, a nominal news agency primarily run by the GRU, which controls the Russian military intelligence service and operates its own special forces units. According to the Treasury Department, the GRU's 72nd Main Intelligence Information Center, a unit within Russia's Information Operations Troops, functions as Russia's "military force for conducting[…]

Security Affairs

[Ukrainian WordPress sites under massive complex attacks]
Researchers observed a spike in the attacks against Ukrainian WordPress sites since the beginning of the military invasion of the country. Cyber attacks are an important component of the military strategy against Ukraine, experts observed a spike in the attacks against Ukrainian WordPress sites since the beginning of the military invasion of the country. The […] The post Ukrainian WordPress sites under massive complex attacks appeared first on Security Affairs.

ZDNet | security RSS

[US KleptoCapture force to tackle cryptocurrency use in Russian sanction avoidance]
According to the DoJ, the team will target "efforts" to use cryptocurrency to circumvent sanctions or launder cash.

Along with this comes the […] The post The Difference Between Human and Machine Identities appeared first on Security Affairs.

ZDNet | security RSS

[These are the problems that cause headaches for bug bounty hunters]
A researcher shares his thoughts on the challenges of responsible vulnerability disclosure.

IT Security Guru

[Ukraine's request to block Russia's internet rejected]
As Russia invaded Ukraine, the besieged country asked the Internet Corporation for Assigned Names and Numbers (ICANN) to take away Russia's top-level domains (TLD), such as .ru, .rf, and .su be revoked, as well as the nation's associated Secure Sockets Layer (SSL) certificates. Andrii Nabok, ICANN's Ukrainian representative, and Mykhailo Fedorov, Ukraine's vice prime minister […] The post Ukraine's request to block Russia's internet rejected appeared first on IT Security Guru.

Cyware News - Latest Cyber News

[Update: Personal data from T-Mobile breach still spreading on dark web, state governments warn]
The top law enforcement officials from multiple states are alerting people affected by an August 2021 breach at T-Mobile that their personal data might be circulating in cybercrime forums online.

Cyware News - Latest Cyber News

[West Virginia-based Mon Health Discloses Data Breach Impacting Patients, Employees, and Partners]
The healthcare services provider discovered the incident on December 18, when some of its IT systems were disrupted, but learned of the potential data theft only a couple of weeks later.

Twitter

CVE

CVE-2022-24442 JetBrains YouTrack before 2021.4.40426 was vulnerable to SSTI (Server-Side Template Injection) via FreeMarker templates.

Threat Intel Center

NEW: CVE-2022-24340 In JetBrains TeamCity before 2021.2.1, XXE during the parsing of the configuration file was possible. Severity: CRITICAL

Threat Intel Center

NEW: CVE-2022-24340 In JetBrains TeamCity before 2021.2.1, XXE during the parsing of the configuration file was possible. Severity: CRITICAL

ThreatMeter

CVE-2022-24340 In JetBrains TeamCity before 2021.2.1, XXE during the parsing of the configuration file was possible. (CVSS:0.0) (Last Update:2022-02-25)

CVE

CVE-2022-24340 In JetBrains TeamCity before 2021.2.1, XXE during the parsing of the configuration file was possible.

Remotely Alerts

Severity: | JetBrains YouTrack before 2021.4.40426 w... | CVE-2022-24442 | Link for more:

Kevin Beaumont

ideal time to be a threat actor in cybersecurity

Threat Intel Center

NEW: CVE-2022-24442 JetBrains YouTrack before 2021.4.40426 was vulnerable to SSTI (Server-Side Template Injection) via FreeMarker templates. Severity: CRITICAL

Remotely Alerts

Severity: | In JetBrains TeamCity before 2021.2.1, X... | CVE-2022-24340 | Link for more:

CVE.report

CVE-2022-24340 : In JetBrains TeamCity before 2021.2.1, XXE during the parsing of the configuration file was possible....

Vulmon Vulnerability Feed

CVE-2022-24340 In JetBrains TeamCity before 2021.2.1, XXE during the parsing of the configuration file was possible.

Threat Intel Center

NEW: CVE-2022-24340 In JetBrains TeamCity before 2021.2.1, XXE during the parsing of the configuration file was possible.

Threat Intel Center

NEW: CVE-2022-24442 JetBrains YouTrack before 2021.4.40426 was vulnerable to SSTI (Server-Side Template Injection) via FreeMarker templates. Severity: CRITICAL

Source: NIST

NIST CVE: Critical

CVE-2022-24340

In **JetBrains TeamCity** before 2021.2.1, XXE during the parsing of the configuration file was possible.

🟥

CVE-2022-24442

JetBrains YouTrack before 2021.4.40426 was vulnerable to SSTI (Server-Side Template Injection) via FreeMarker templates.

🟥

CRITICAL Vector: network Created: 2022-02-25 Updated: 2022-03-04

CRITICAL Vector: network Created: 2022-02-25 Updated: 2022-03-04

Source: NIST

NIST CVE: High

CVE-2022-24947

Apache JSPWiki user preferences form is vulnerable to CSRF attacks, which can lead to account takeover. Apache JSPWiki users should upgrade to 2.11.2 or later.

HIGH Vector: network Created: 2022-02-25 Updated: 2022-03-04

CVE-2022-24341

In **JetBrains TeamCity** before 2021.2.1, editing a user account to change its password didn't terminate sessions of the edited user.

HIGH Vector: network Created: 2022-02-25 Updated: 2022-03-04

CVE-2022-24335

JetBrains TeamCity before 2021.2 was vulnerable to a Time-of-check/Time-of-use (TOCTOU) race-condition attack in agent registration via **XML-RPC**.

HIGH Vector: network Created: 2022-02-25 Updated: 2022-03-04

CVE-2022-24327

In **JetBrains** Hub before 2021.1.13890, integration with JetBrains Account exposed an API key with excessive permissions.

HIGH Vector: network Created: 2022-02-25 Updated: 2022-03-04

CVE-2022-24342

In **JetBrains TeamCity** before 2021.2.1, URL injection leading to CSRF was possible.

HIGH Vector: network Created: 2022-02-25 Updated: 2022-03-04

Source: NIST

NIST CVE: Medium

CVE-2022-24948

A carefully crafted user preferences for submission could trigger an XSS vulnerability on **Apache** JSPWiki, related to the user preferences screen, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim. Apache JSPWiki users should upgrade to 2.11.2 or later.

MEDIUM Vector: network Created: 2022-02-25 Updated: 2022-03-04

CVE-2021-38993

IBM AIX 7.1, 7.2, 7.3, and **VIOS** 3.1 could allow a non-privileged local user to exploit a vulnerability in the smbcd daemon to cause a denial of service. IBM X-Force ID: 212962.

MEDIUM Vector: local Created: 2022-02-25 Updated: 2022-03-04

CVE-2022-24337

In **JetBrains TeamCity** before 2021.2, **health** items of pull requests were shown to users who lacked appropriate permissions.

MEDIUM Vector: network Created: 2022-02-25 Updated: 2022-03-04

CVE-2022-24336

In **JetBrains TeamCity** before 2021.2.1, an unauthenticated attacker can cancel running builds via an **XML-RPC** request to the TeamCity server.

MEDIUM Vector: network Created: 2022-02-25 Updated: 2022-03-04

CVE-2022-24343

In **JetBrains YouTrack** before 2021.4.31698, a custom logo could be set by a user who has read-only permissions.

MEDIUM Vector: network Created: 2022-02-25 Updated: 2022-03-04

CVE-2022-24338

JetBrains TeamCity before 2021.2.1 was vulnerable to reflected XSS.

MEDIUM Vector: network Created: 2022-02-25 Updated: 2022-03-04

CVE-2022-24344

JetBrains YouTrack before 2021.4.31698 was vulnerable to stored XSS on the Notification templates page.

MEDIUM Vector: network Created: 2022-02-25 Updated: 2022-03-04

CVE-2022-24612

An authenticated user can upload an XML file containing an XSS via the ITSM module of **EyesOfNetwork** 5.3.11, resulting in a stored XSS.

MEDIUM Vector: network Created: 2022-02-25 Updated: 2022-03-04

CVE-2022-24328

In **JetBrains** Hub before 2021.1.13956, an unprivileged user could perform DoS.

MEDIUM Vector: network Created: 2022-02-25 Updated: 2022-03-04

CVE-2022-24330

In **JetBrains TeamCity** before 2021.2.1, a **redirection** to an external site was possible.

MEDIUM Vector: network Created: 2022-02-25 Updated: 2022-03-04

CVE-2022-24334

In **JetBrains TeamCity** before 2021.2.1, the Agent Push feature allowed selection of any private key on the server.

MEDIUM Vector: network Created: 2022-02-25 Updated: 2022-03-04

CVE-2022-25259

JetBrains Hub before 2021.1.14276 was vulnerable to reflected XSS.

MEDIUM Vector: network Created: 2022-02-25 Updated: 2022-03-04

CVE-2022-24339

JetBrains TeamCity before 2021.2.1 was vulnerable to stored XSS.

MEDIUM Vector: network Created: 2022-02-25 Updated: 2022-03-04

CVE-2022-24347

JetBrains YouTrack before 2021.4.36872 was vulnerable to stored XSS via a project **icon**.

MEDIUM Vector: network Created: 2022-02-25 Updated: 2022-03-04

Source: NIST

NIST CVE: Low

Nothing today

Source: NIST

NIST CVE: Unrated

CVE-2022-0838

Cross-site Scripting (XSS) - Reflected in **GitHub** repository

CVE-2022-0841

OS Command Injection in **GitHub** repository ljharb/npm-lockfile in

	hestiacp/hestiacp prior to 1.5.10.	UNRATED	Vector: unkown	Created: 2022-03-04	Updated: 2022-03-04
CVE-2022-0848	OS Command Injection in **GitHub** repository part-db/part-db prior to 0.5.11.	UNRATED	Vector: unkown	Created: 2022-03-04	Updated: 2022-03-04
	v2.0.3 and v2.0.4.	UNRATED	Vector: unkown	Created: 2022-03-03	Updated: 2022-03-04

Source: Hybrid Analysis

Top malicious files

100% Threat score	Trojan (.) Win32 (.) Chapak (.) gen (.) 2 (.) exe
100% Threat score	oaioimoadmbrlocsm (.) xlsb
100% Threat score	report 826 (.) xlsm
100% Threat score	report 826 (.) xlsm
100% Threat score	Trojan (.) Win32 (.) Chapak (.) gen (.) exe (.) vir
100% Threat score	30714966754_019_00005_SURAGUS GmbH,pdf (.) exe
100% Threat score	30714966754_019_00005_SURAGUS GmbH,pdf (.) exe
100% Threat score	setup_x64 (.) exe
100% Threat score	Client-built (.) exe
92% Threat score	Compliance-Report-383243427-Mar-02 (.) xlsb
87% Threat score	Updater (.) exe
85% Threat score	winrar-x64-611 (.) exe
100% Threat score	2022-03-02_1610 (.) xlsm
100% Threat score	commenti_78 (.) xlsm
100% Threat score	atbswpv0 (.) 3 (.) 0-windows (.) exe
100% Threat score	Server (.) exe
100% Threat score	Server (.) exe
100% Threat score	091222 (.) exe
100% Threat score	keygen (.) exe
100% Threat score	setup (.) exe
100% Threat score	Andale_Loader (.) exe
87% Threat score	1cb583a8967f7c2cd4ba249bbf81d300
85% Threat score	winrar-x32-611 (.) exe

Source: Hybrid Analysis

Top malicious URL

100% Threat score	https://bambaluateatro (.) com/eor/pdf-RD877/index (.) html
93% Threat score	http://113 (.) 70 (.) 122 (.) 225:38721/Mozi (.) m
82% Threat score	http://bjh (.) co/?nr4Y5
77% Threat score	http://www (.) myharrypotterfanfiction (.) site/wp-content/plugins/pdf-poster-pro/pdfjs/web/viewer (.) php?file=http%3A%2F%2Fwww (.) myharrypotterfanfiction (.) site%2Fwp-content%2Fuploads%2F2020%2F05%2Ffinalhp-s-times-gift-word-1 (.) pdf&download=true&print=true&side=false&open=false#page%3D1
77% Threat score	http://dinakconsulting (.) com/
76% Threat score	https://ronemo (.) com/video/P7rjgUnHeTZ/GEfbyr4jnT
74% Threat score	https://granicus (.) com/solution/govmeetings/
72% Threat score	http://www (.) cuponesparaempresas (.) com/
100% Threat score	http://s (.) arcik (.) net/
91% Threat score	http://go (.) tapickot (.) com/0bnl&sa=D&545=040&usg=AFQjCNEBWN7UWBe4sSXxZxr3LAbSgg4tlw
77% Threat score	http://thanos (.) wetransfer (.) net/
77% Threat score	http://linklyhq (.) com/
77% Threat score	http://blog (.) moddedeuros (.) com/
74% Threat score	http://www (.) kellerball (.) com/ (.) th/dec/b3Jpb2wucGVyZWFybmF1QGZpLWdyb3VwLmNvbQ==
72% Threat score	http://www (.) havesino (.) com/
72% Threat score	http://cms-files (.) softonic (.) s3 (.) amazonaws (.) com/b78b07d5-e3e7-42d2-a657-499ed189310c

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 Japan
- #9 Brazil
- #10 Uruguay

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 **Mint Global Marketing / Adgenics / Cabo Networks**
Florida affiliate spammers and bulletproof spam hosters

#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 **Michael Persaud**
Long time snowshoe type spammer, raided by FBI then indicted in 2017 on federal wire fraud charges tied to his spamming operations.

#7 **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 **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 **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 India
- #3 United States of America
- #4 Thailand
- #5 Indonesia
- #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 Hong Kong
- #5 France
- #6 Singapore

#7 Netherlands

#8 Canada

#9 United Kingdom

#10 India

Source: Have I been pwned?

Have I been pwnd

Robinhood (robinhood.com)
In November 2021, the online trading platform Robinhood suffered a data breach after a customer service representative was socially engineered. The incident exposed over 5M customer email addresses and 2M customer names. The data was provided to HIBP by a source who requested it be attributed to "Jarand Moen Romtviet".

Count: 5003937 Created: 2021-11-03 Updated: 2022-03-03

Source: Imperva DDOS Map

Top DDOS attackers

Germany (28%)

United States (21%)

Singapore (9%)

Source: Imperva DDOS Map

Top DDOS country targets

Russia (77%)

Ukraine (16%)

United States (4%)

Source: Imperva DDOS Map

Top DDOS techniques

92%	**DDoS**
5%	**Automated Threat**
3%	**OWASP**

Source: Imperva DDOS Map

Top DDOS industry targets

79%	**Financial Services**
16%	**Business**
1%	**Computing & IT**