Your Security Rabbits report for April 09, 2022

Source: Ransom Watch

Ransomware attacks

lockbit2	ch1	lockbit2	ardeche.fr
lockbit2	genieroute.be	cuba	metagenics
lockbit2	rosagroup.com	conti	Wocklum Group

Hot topics

Nothing today

News

Security Affairs

15 Cybersecurity Measures for the Cloud Era

Which are the most important cybersecurity measures that businesses can take to protect themselves in the cloud era? We are now firmly in the era of cloud data and storage. In fact, it's become quite difficult to find a service that doesn't rely on the cloud in some way. This ubiquity has led to increased [...] The post 15 Cybersecurity Measures for the Cloud Era appeared first on Security Affairs.

Security Affairs

A Mirai-based botnet is exploiting the Spring4Shell vulnerability

Experts warn of a Mirai-based botnet exploiting the recently discovered Spring4Shell vulnerability in attacks in the wild. Trend Micro Threat Research reported that the recently discovered Spring4Shell vulnerability (CVE-2022-22965) is actively exploited by a Mirai-based botnet. Researchers from Chinese cybersecurity firm Qihoo 360 first reported the exploitation of the Spring4Shell by a Mirai-based botnet in early April. [...] The post A Mirai-based botnet is exploiting the Spring4Shell vulnerability appeared first on Security Affairs.

Security Affairs

A Ukrainian man is the third FIN7 member sentenced in the United States

A Ukrainian man was sentenced in the US to 5 years in prison for his criminal activity in the cybercrime group FIN7. Denys Iarmak, a Ukrainian national (32), has been sentenced to five years in prison in the U.S. for high-level hacking activity in the cybercrime group FIN7 (aka Carbanak Group and the Navigator Group). The man [...] The post A Ukrainian man is the third FIN7 member sentenced in the United States appeared first on Security Affairs.

Security Affairs

Anonymous and the IT ARMY of Ukraine continue to target Russian entities

The popular hacking Anonymous and the IT ARMY of Ukraine continue to target Russian government entities and private businesses. This week Anonymous claimed to have hacked multiple private businesses and leaked their data through the DDoSecrets platform. The list of recently compromised businesses includes: Forest - The hacktivists leaked 37,500 emails stolen from the company [...] The post Anonymous and the IT ARMY of Ukraine continue to target Russian entities appeared first on Security Affairs.

The Hacker News

Chinese Hacker Groups Continue to Target Indian Power Grid Assets

China-linked adversaries have been attributed to an ongoing onslaught against Indian power grid organizations, one year after a concerted campaign targeting critical infrastructure in the country came to light. Most of the intrusions involved a modular backdoor named ShadowPad, according to Recorded Future's Insikt Group, a sophisticated remote access trojan which has been dubbed a "masterpiece

Cyware News - Latest Cyber News

Command injection bug patched in Ruby library for converting AsciiDoc files

Developers have issued a patch for a popular Ruby library used to parse and convert AsciiDoc files, to safeguard servers against a newly discovered command injection vulnerability.

CyberScoop

Denial-of-service disrupts Finnish government sites during Zelenskyy speech

The incident also coincided with Finland openly weighing NATO membership and the Finns saying a Russian aircraft violated their airspace. The post Denial-of-service disrupts Finnish government sites during Zelenskyy speech appeared first on CyberScoop.

CyberScoop

DOJ's Sandworm operation raises questions about how far feds can go to disarm botnets

The Department of Justice and FBI announced they used remote access technology to shut down a Sandworm botnet. The post DOJ's Sandworm operation raises questions about how far feds can go to disarm botnets appeared first on CyberScoop.

Cyware News - Latest Cyber News

FIN7 Forays into Ransomware Attack Landscape with New Tools

Mandiant warned against the evil ambitions of the FIN7 group, which has shown strong signs of entering ransomware operations. The group's presence has been reported before attack events from Maze, Darkside, BlackCat, and Ryuk. Recently, it has been observed showing off a novel backdoor and new malicious tools.

ZDNet | security RSS

FIN7 hacking group member sentenced to five years behind bars

He worked as a penetration tester for the criminal outfit.

Cyware News - Latest Cyber News

Finland Government Sites Forced Offline by DDoS Attacks

The websites of Finland's defense and foreign affairs were taken offline today following DDoS attacks. The ministries each confirmed the attacks on Twitter, although the websites now appear to be back up and running.

Threatpost

Google Play Bitten by Sharkbot Info-stealer 'AV Solution'

Google removed six different malicious Android applications targeting mainly users in the U.K. and Italy that were installed about 15,000 times.

The Hacker News

Hackers Exploiting Spring4Shell Vulnerability to Deploy Mirai Botnet Malware

The recently disclosed critical Spring4Shell vulnerability is being actively exploited by threat actors to execute the Mirai botnet malware, particularly in the Singapore region since the start of April 2022. "The

Cyware

Looking Inside Pandora's Box

The threat group uses the double extortion method to increase pressure on the victim. This means that they not only encrypt the victim's files, but also exfiltrate them and threaten to release the data if the victim exploitation allows threat actors to download the Mirai sample to the '/tmp' folder and execute them after permission change using 'chmod,'" Trend Micro researchers Deep Patel, Nitesh

Cyware News - Latest Cyber News

Microsoft dogs Strontium domains to stop attacks on Ukraine

Microsoft this week seized seven internet domains run by Russia-linked threat group Strontium, which was using the infrastructure to target Ukrainian institutions as well as think tanks in the US and EU.

Cyware News - Latest Cyber News

New SolarMarker (Jupyter) Campaign Demonstrates the Malware's Changing Attack Patterns

Researchers have identified a new version of SolarMarker, a malware family known for its infostealing and backdoor capabilities, mainly delivered through search engine optimization (SEO) manipulation to convince users to download malicious documents.

Naked Security

Popular Ruby Asciidoc toolkit patched against critical vuln - get the update now!

A rogue line-continuation character can trick the code into validating just the second half of the line, but executing all of it.

The Hacker News

Researchers Connect BlackCat Ransomware with Past BlackMatter Malware Activity

Cybersecurity researchers have uncovered further links between BlackCat (aka AlphaV) and BlackMatter ransomware families, the former of which emerged as a replacement following international scrutiny last year. "At least some members of the new BlackCat group have links to the BlackMatter group, because they modified and reused a custom exfiltration tool [...] and which has only been observed in

IT Security Guru

Server-Side-Request-Forgery Enabled Administrative Account Takeover on FinTech Platform

Salt Labs has uncovered a Server-Side-Request Forgery on a major FinTech platform, enabling an administrative account takeover. Researchers identified API vulnerabilities allowing them to launch attacks where: Attackers could gain administrative access to the banking platform Attackers could leak users' personal data Attackers could access users' banking details and financial transactions Attackers could perform unauthorised [...] The post Server-Side-Request-Forgery Enabled Administrative Account Takeover on FinTech Platform appeared first on IT Security Guru.

Cyware News - Latest Cyber News

Update: Attack on Ukraine Telecoms Provider Caused by Compromised Employee Credentials

Russian hackers used compromised employee credentials to launch the cyberattack that severely disrupted internet services in Ukraine last week, it has been claimed today.

Cyware News - Latest Cyber News

YouTube Fraudsters Steal $1.7m in Crypto 'Giveaway'

They used footage of tech entrepreneurs and crypto enthusiasts like Elon Musk, Brad Garlinghouse, Michael Saylor, Changpeng Zhao and Cathie Wood to add legitimacy to their efforts.

News - Latest Cyber News

does not pay.

CyberScoop

Microsoft seizes internet domains linked to GRU cyberattacks against Ukraine

Strontium -- a group linked to Russian military intelligence -- was using the domains to target Ukrainian institutions, Microsoft said. The post Microsoft seizes internet domains linked to GRU cyberattacks against Ukraine appeared first on CyberScoop.

Cyware News - Latest Cyber News

Northern Ireland TrustFord Sites Hit by Ransomware Gang

The vehicle dealer group revealed the attack, which is believed to have been committed by the Conti ransomware gang, affected the firm's internal systems. In particular, access to the internet and phones within the business was affected.

Cyware News - Latest Cyber News

Ransomware Forces North Carolina A&T University to Take Systems and Services Offline

North Carolina A&T State University, the largest historically black college in the US, University was recently struck by a ransomware Group called ALPHV, sending university staff into a scramble to restore services last month.

Cyware News - Latest Cyber News

SaintBear Uses New Set of Payloads to Target Ukrainian Organizations

Researchers found the SaintBear actors targeting Ukrainian organizations using macro-embedded documents in its latest campaign that delivers different Elephant payloads. SaintBear has been actively performing cyberespionage campaigns aimed at Ukraine since 2021. For better protection, organizations are recommended to use email gateways, reliable anti-malware, and a firewall.

Cyware News - Latest Cyber News

Snap-on discloses data breach claimed by Conti ransomware gang

American automotive tools manufacturer Snap-on announced a data breach exposing associate and franchisee data after the Conti ransomware gang began leaking the company's data in March.

Cyware News - Latest Cyber News

WonderHero Game Disabled After Hackers Steal $320,000 in Cryptocurrency

The operators of cryptocurrency play-to-earn game WonderHero have disabled the service after hackers stole about $320,000 worth of Binance Coin (BNB). The attack caused the price of WonderHero's own coin, WND, to plummet more than 90%.

Twitter

CVE

CVE-2022-22570 A buffer overflow vulnerability found in the UniFi Door Access Reader Lites (UA Lite) firmware (Version 3.8.28.24 and earlier) allows a malicious actor who has gained access to a network to control all connected UA devices. This vu...

CVE

CVE-2021-35117 An Out of Bounds read may potentially occur while processing an IBSS beacon, in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & ...

SRM IT Risk

IT Risk: Multiple vulnerabilities in Made by Philips Vue PACS (Picture Archiving and Communication Systems for medial) products -3/4 CVE-2020-1938 CVE-2018-12326CVE-2018-11218 CVE-2020-4670 CVE-2018-8014 CVE-2021-33020 CVE-2018-10115 CVE-2021-27501 CVE-2021-33018 CVE-2021-27497

Remotely Alerts

Severity: | A command injection vulnerability found i... | CVE-2021-23247 | Link for more:

vulnonym

Hi, I'm CVE-2021-23247. I was never good with numbers though, so you can call me Diddy Anchovy

CVE

CVE-2021-23247 A command injection vulerability found in quick game engine allows arbitrary remote code in quick app. Allows remote attacke0rs to gain arbitrary code execution in quick game engine

Vulmon Vulnerability Feed

CVE-2021-35117 An Out of Bounds read may potentially occur while processing an IBSS beacon, in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snap...

CVE

CVE-2021-27497 Philips Vue PACS versions 12.2.x.x and prior does not use or incorrectly uses a protection mechanism that provides sufficient defense against directed attacks against the product.

ThreatMeter

CVE-2021-23247 A command injection vulnerability found in quick game engine allows arbitrary remote code in quick app. Allows remote attacke0rs to gain arbitrary code execution in quick game engine (CVSS:0.0) (Last Update:2022-04-01)

Vulmon Vulnerability Feed

CVE-2021-23247 A command injection vulerability found in quick game engine allows arbitrary remote code in quick app. Allows remote attacke0rs to gain arbitrary code execution in quick game engine

CVE.report

CVE-2021-23247 : A command injection vulerability found in quick game engine allows arbitrary remote code in quick app. Allows remote attacke0rs to gain arbitrary code execution in quick game engine...

Selina Cheng

Well-known citizen journalist Siu Wan publicly apologized to his interviewees & sources after devices were taken by national security police, saying they werent sufficiently secure. When taking cybersecurity measures, journalists are taking the responsibility to ensure..

Remotely Alerts

Severity: | Philips Vue PACS versions 12.2.x.x and p... | CVE-2021-27497 | Link for more:

Source: NIST

NIST CVE: Critical

CVE-2022-22570

A buffer overflow vulnerability found in the **UniFi** Door Access **Reader** Lite's (UA Lite) firmware (Version 3.8.28.24 and earlier) allows a malicious actor who has gained access to a network to control all connected UA devices. This vulnerability is fixed in Version 3.8.31.13 and later.

CRITICAL Vector: network Created: 2022-04-01 Updated: 2022-04-09

CVE-2022-26562

An issue in provider/libserver/ECKrbAuth.cpp of Kopano-Core v11.0.2.51 contains an issue which allows attackers to authenticate even if the user account or password is expired.

CRITICAL Vector: network Created: 2022-04-01 Updated: 2022-04-09

CVE-2021-30064

On Schneider Electric ConneXium Tofino **Firewall** TCSEFEA23F3F22 before 03.23, TCSEFEA23F3F20/21, and **Belden** Tofino **Xenon** Security Appliance, an SSH login can succeed with hardcoded default credentials (if the device is in the uncommissioned state).

CRITICAL Vector: network Created: 2022-04-03 Updated: 2022-04-09

CVE-2022-24066

The package simple-git before 3.5.0 are vulnerable to Command Injection due to an incomplete fix of [CVE-2022-24433](https://security.snyk.io/vuln/SNYK-JS-SIMPLEGIT-2421199) which only patches against the git fetch attack vector. A similar use of the --upload-pack feature of git is also supported for git clone, which the prior fix didn't cover.

CRITICAL Vector: network Created: 2022-04-01 Updated: 2022-04-09

CVE-2021-23247

A command injection vulerability found in quick game engine allows arbitrary remote code in quick app. Allows remote attacke0rs to gain arbitrary code execution in quick game engine

CRITICAL Vector: network Created: 2022-04-01 Updated: 2022-04-09

CVE-2021-35117

An Out of Bounds read may potentially occur while processing an IBSS beacon, in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon **Voice** & Music

CRITICAL Vector: network Created: 2022-04-01 Updated: 2022-04-09

CVE-2021-27497

Philips Vue PACS versions 12.2.x.x and prior does not use or incorrectly uses a protection mechanism that provides sufficient defense against directed attacks against the product.

CRITICAL Vector: network Created: 2022-04-01 Updated: 2022-04-09

Source: NIST

NIST CVE: High

CVE-2021-32937

An attacker can gain knowledge of a session temporary working folder where the getfile and putfile commands are used in MDT **AutoSave** versions prior to v6.02.06. An attacker can leverage this knowledge to provide a malicious command to the working directory where the read and write activity can be initiated.

HIGH Vector: network Created: 2022-04-01 Updated: 2022-04-09

CVE-2022-24426

Dell Command | Update, Dell Update, and Alienware Update versions prior to 4.5 contain a Local Privilege Escalation Vulnerability in the Advanced Driver Restore component. A local malicious user could potentially exploit this vulnerability, leading to privilege escalation.

HIGH Vector: local Created: 2022-04-01 Updated: 2022-04-09

CVE-2022-25017

Hitron CHITA 7.2.2.0.3b6-CD devices contain a command injection vulnerability via the Device/DDNS ddnsUsername field.

HIGH Vector: network Created: 2022-04-01 Updated: 2022-04-09

CVE-2019-14839

It was observed that while login into Business-central console, HTTP request discloses sensitive information like username and password when intercepted using some tool like **burp** suite etc.

HIGH Vector: network Created: 2022-04-01 Updated: 2022-04-09

CVE-2021-30062

On Schneider Electric ConneXium Tofino OPCLSM TCSEFM0000 before 03.23 and **Belden** Tofino **Xenon** Security Appliance, crafted OPC packets can bypass the OPC enforcer.

CVE-2021-26624

An local privilege escalation vulnerability due to a "runasroot" command in eScan **Anti-Virus**. This vulnerability is due to invalid arguments and insufficient execution conditions related to "runasroot" command. This vulnerability can induce remote attackers to exploit root privileges by manipulating parameter values.

HIGH Vector: network Created: 2022-04-01 Updated: 2022-04-09

CVE-2022-23155

Dell Wyse **Management Suite** versions 2.0 through 3.5.2 contain an unrestricted file upload vulnerability. A malicious user with admin privileges can exploit this vulnerability in order to execute arbitrary code on the system.

HIGH Vector: network Created: 2022-04-01 Updated: 2022-04-09

CVE-2021-35115

Improper handling of multiple session supported by PVM backend can lead to use after free in Snapdragon Auto, Snapdragon Mobile

HIGH Vector: local Created: 2022-04-01 Updated: 2022-04-09

CVE-2021-30065

On Schneider Electric ConneXium Tofino **Firewall** TCSEFEA23F3F22 before 03.23, TCSEFEA23F3F20/21, and **Belden** Tofino **Xenon** Security Appliance, crafted ModBus packets can bypass the ModBus enforcer. NOTE: this issue exists because of an incomplete fix of CVE-2017-11401.

HIGH Vector: network Created: 2022-04-03 Updated: 2022-04-09

CVE-2021-30063

On Schneider Electric ConneXium Tofino OPCLSM TCSEFM0000 before 03.23 and **Belden** Tofino **Xenon** Security Appliance, crafted OPC packets can cause an OPC enforcer denial of service.

HIGH Vector: network Created: 2022-04-03 Updated: 2022-04-09

CVE-2021-33020

Philips Vue PACS versions 12.2.x.x and prior uses a cryptographic key or password past its expiration date, which diminishes its **safety** significantly by increasing the timing window for cracking attacks against that key.

HIGH Vector: network Created: 2022-04-01 Updated: 2022-04-09

CVE-2021-35106

Possible out of bound read due to improper length calculation of WMI message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon **Voice** & Music, Snapdragon Wearables

HIGH Vector: local Created: 2022-04-01 Updated: 2022-04-09

CVE-2021-35105

Possible out of bounds access due to improper input validation during graphics profiling in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon **Voice** & Music, Snapdragon Wearables

HIGH Vector: local Created: 2022-04-01 Updated: 2022-04-09

HIGH Vector: network Created: 2022-04-03 Updated: 2022-04-09

CVE-2021-35110

Possible buffer overflow to improper validation of hash segment of file while allocating memory in Snapdragon Connectivity, Snapdragon Mobile

HIGH Vector: local Created: 2022-04-01 Updated: 2022-04-09

CVE-2021-35103

Possible out of bound write due to improper validation of number of timer values received from firmware while syncing timers in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking

HIGH Vector: local Created: 2022-04-01 Updated: 2022-04-09

Source: NIST

NIST CVE: Medium

CVE-2022-26565

A cross-site scripting (XSS) vulnerability in **Totaljs** commit 95f54a5 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Page Name text field when creating a new page.

MEDIUM Vector: network Created: 2022-04-01 Updated: 2022-04-09

CVE-2021-30061

On Schneider Electric ConneXium Tofino **Firewall** TCSEFEA23F3F22 before 03.23, TCSEFEA23F3F20/21, and **Belden** Tofino **Xenon** Security Appliance, physically proximate attackers can execute code via a crafted file on a USB stick.

MEDIUM Vector: physical Created: 2022-04-03 Updated: 2022-04-09

CVE-2021-23288

The vulnerability exists due to insufficient validation of input from certain **resources** by the IPP software. The attacker would need access to the local Subnet and an administrator interaction to compromise the system. This issue affects: Intelligent Power Protector versions prior to 1.69.

MEDIUM Vector: adjacent_network Created: 2022-04-01 Updated: 2022-04-09

CVE-2021-30066

On Schneider Electric ConneXium Tofino **Firewall** TCSEFEA23F3F22 before 03.23, TCSEFEA23F3F20/21, and **Belden** Tofino **Xenon** Security Appliance, an arbitrary firmware image can be loaded because firmware signature verification (for a USB stick) can be bypassed. NOTE: this issue exists because of an incomplete fix of CVE-2017-11400.

MEDIUM Vector: physical Created: 2022-04-03 Updated: 2022-04-09

CVE-2020-14479

Sensitive information can be obtained through the handling of serialized data. The issue results from the lack of proper authentication required to query the server

MEDIUM Vector: network Created: 2022-04-01 Updated: 2022-04-09

CVE-2021-23287

The vulnerability exists due to insufficient validation of input of certain **resources** within the IPM software. This issue affects: **Intelligent Power Manager** (IPM 1) versions prior to 1.70.

MEDIUM Vector: network Created: 2022-04-01 Updated: 2022-04-09

Source: NIST

NIST CVE: Low

Nothing today

Source: NIST

NIST CVE: Unrated

CVE-2022-27883

A link following vulnerability in Trend Micro **Antivirus** for Mac 11.5 could allow an attacker to create a specially-crafted file as a symlink that can lead to privilege escalation. Please note that an attacker must at least have low-level privileges on the system to attempt to exploit this vulnerability.

UNRATED Vector: unkown Created: 2022-04-09 Updated: 2022-04-09

CVE-2022-28805

singlevar in lparser.c in Lua through 5.4.4 lacks a certain luaK_exp2anyregup call, leading to a heap-based buffer over-read that might affect a system that compiles untrusted Lua code.

UNRATED Vector: unkown Created: 2022-04-08 Updated: 2022-04-09

CVE-2022-26877

Asana Desktop before 1.6.0 allows remote attackers to exfiltrate local files if they can trick the Asana desktop app into loading a malicious web page.

UNRATED Vector: unkown Created: 2022-04-09 Updated: 2022-04-09

Source: Hybrid Analysis

Top malicious files

100% Threat score	Kerschi WOOFER(Run as admin).exe	100% Threat score	rabbit è¿œæŽ§.exe
100% Threat score	OfficeSetup.exe	100% Threat score	Ø®Ø§Ø§Ø§Ø§Ø§Ø§Ø§Ø§Ø§Ø§Ø§Ø§Ø§Ø§Ø§Øµ.exe
100% Threat score	hitomi_downloader_GUI.exe	100% Threat score	Rock.exe
100% Threat score	malware.exe	100% Threat score	6e44eca9e7f7f73d0d78a6a623e1fcf9
100% Threat score	tmp_92ni_ms	100% Threat score	aScTimeTables.exe
100% Threat score	Setup.exe	100% Threat score	winrar-x32-611.exe
100% Threat score	roz.exe	96% Threat score	hack.exe
87% Threat score	ibisPaint-X-v9-3-2.apk	85% Threat score	STEP-2__INSTALL_SOFTWARE.exe
85% Threat score	GameSetup.exe	83% Threat score	com.pandasecurity.pandaav_3.6.5.apk
81% Threat score	gm.cmd	76% Threat score	ransomware.exe
75% Threat score	Picsart v19.5.4 [Gold]-M.apk	75% Threat score	tmpcab5kfzi

Source: Hybrid Analysis

Top malicious URL

100% Threat score	https://omarrobinson.xyz/new.exe	100% Threat score	http://zani.streghettaincucina.com/index?5472
100% Threat score	https://fmchr.in/images/common/NEACD/Qzqrn0.hta	100% Threat score	http://zani.streghettaincucina.com/index?79703
98% Threat score	http://209.127.19.101/vendredi.vbs	97% Threat score	http://61.53.83.16:44479/Mozi.m
95% Threat score	http://christinadudley.com/public_html/cdudley/sites/default/files/1203427/Zjckk0.hta	91% Threat score	http://45.95.169.143/The420smokeplace.dns/
86% Threat score	http://143.244.180.227/server.exe	84% Threat score	https://mohanimpex.com/include/tempdoc/891250/Ersrr0.hta
84% Threat score	https://mohanimpex.com/include/tempdoc/891250/image.png	84% Threat score	https://mohanimpex.com/include/tempdoc/891250/upload.php
80% Threat score	http://mastersgolf2022.unaux.com/	80% Threat score	https://ammouriarts.com/wp-content/loader/uploads/Voice_message0002110_Rtwpobgv.bmp
73% Threat score	https://osf.io/qyx7v/	73% Threat score	https://lacapitaldelsol.com/anuncio/ver-la-ciudad-perdida-2022-pelicula-completa-en-espanol-hd-gratis/
73% Threat score	https://lacapitaldelsol.com/anuncio/v-e-r-ambulance-plan-de-huida-2022-pelicula-completa-en-espanol-latino-hd/	73% Threat score	https://lacapitaldelsol.com/anuncio/er-cuevana-gratis-fresh-2022-pelicula-completa-en-espanol-y-latino-o-n-l-i-n-e/
73% Threat score	https://lacapitaldelsol.com/anuncio/nueva-hd-online-animales-fantasticos-los-secretos-de-dumbledore-2022-espana-gratis/	73% Threat score	http://bit.ly/3iDkDAO

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 Uruguay

#9 Brazil

#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 Viet Nam

#7 Algeria

#8 Brazil

#9 Pakistan

#10 Venezuela (Bolivarian Republic of)

Source: *SpamHaus*

Top phishing countries

#1 United States

#2 Singapore

#3 Russia

#4 Germany

#5 Netherlands

#6 Australia

#7 Japan

#8 Hong Kong

#9 Canada

#10 United Kingdom

Source: *Have I been pwned?*

Have I been pwnd

Nothing today

Source: Imperva DDOS Map

Top DDOS attackers

Source: Imperva DDOS Map

Top DDOS country targets

Source: Imperva DDOS Map

Top DDOS techniques

Source: Imperva DDOS Map

Top DDOS industry targets