Your Security Rabbits report for April 06, 2022

Source: Ransom Watch

Ransomware attacks

lockbit2	allcountysurvey[...]	lockbit2	gordoncounty.or[...]
lockbit2	http://www.toot[...]	lockbit2	vgoc.ca
lockbit2	www.rnrinc.com	lockbit2	www.wania.at
ransomexx	Sonae		

Hot topics

Nothing today

News

Security Affairs

A cyber attack forced the wind turbine manufacturer Nordex Group to shut down some of IT systems

Nordex Group, one of the largest manufacturers of wind turbines, was hit by a cyberattack that forced the company to shut down part of its infrastructure. Nordex Group, one of the world's largest manufacturers of wind turbines, was the victim of a cyberattack that forced the company to take down multiple systems. The attack was [...] The post A cyber attack forced the wind turbine manufacturer Nordex Group to shut down some of IT systems appeared first on Security Affairs.

IT Security Guru

Armis Appoints Tom Gol as CTO for Research

Today, Armis announced the appointment of Tom Gol as CTO for Research. He will be reporting directly to Nadir Izrael, Global CTO and Co-founder at Armis. In this role, Tom will lead and oversee all research efforts as the company continues to solidify its place as a security leader and expert in threat and vulnerability research. His team [...] The post Armis Appoints Tom Gol as CTO for Research appeared first on IT Security Guru.

Threatpost

Authorities Fully Behead Hydra Dark Marketplace

The popular underground market traded in drugs, stolen data, forged documents and more -- raking in billions in Bitcoin.

The Hacker News

Block Admits Data Breach Involving Cash App Data Accessed by Former Employee

Block, the company formerly known as Square, has disclosed a data breach that involved a former employee downloading unspecified reports pertaining to its Cash App Investing that contained information about its U.S. customers. "While this employee had regular access to these reports as part of their past job responsibilities, in this instance these reports were accessed without permission after

Cyware News - Latest Cyber News

CISA advises D-Link users to take vulnerable routers offline

CVE-2021-45382 is a Remote Code Execution (RCE) vulnerability that exists in all series H/W revisions D-Link DIR-810L, DIR-820L/LW, DIR-826L, DIR-830L, and DIR-836L routers via the DDNS function in ncc2 binary file.

Cyware News - Latest Cyber News

Coro secures $60M at ~$500M valuation for an all-in, SaaS-based cyber protection platform aimed at SMBs

Alongside this latest round, the company is also disclosing for the first time an additional $20 million raised in the last six months, bringing the total to $80 million in the period.

ZDNet | security RSS

FIN7 hackers evolve operations with ransomware, novel backdoor

Researchers have explored the shift in the sophisticated group's latest tactics.

Security Affairs

Anonymous targets the Russian Military and State Television and Radio propaganda

Anonymous continues to support Ukraine against the Russian criminal invasion targeting the Russian military and propaganda. Anonymous leaked personal details of the Russian military stationed in Bucha where the Russian military carried out a massacre of civilians that are accused of having raped and shot local women and children. Leaked data include names, ranks and [...] The post Anonymous targets the Russian Military and State Television and Radio propaganda appeared first on Security Affairs.

Cyware News - Latest Cyber News

AsyncRAT campaigns feature new version of 3LOSH crypter

The threat actor(s) behind these campaigns have been using 3LOSH to generate the obfuscated code responsible for the initial infection process. The same operator is likely distributing a variety of commodity RATs, such as AsyncRAT and LimeRAT.

Cyware News - Latest Cyber News

Beastmode Botnet Adds New Exploits to its Arsenal

According to Fortinet, BeastMode attempts to infect TOTOLINK routers by exploiting several vulnerabilities. The threat actors added the exploits just a week after the PoCs were publicly released on GitHub.

Security Affairs

CISA adds Spring4Shell flaw to its Known Exploited Vulnerabilities Catalog

The U.S. CISA added the recently disclosed remote code execution (RCE) vulnerability Spring4Shell to its Known Exploited Vulnerabilities Catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added the recently disclosed CVE-2022-22965 (aka Spring4Shell, CVSS score: 9.8) flaw in the Spring Framework, along with three other issues, to its Known Exploited Vulnerabilities Catalog. According to Binding Operational Directive (BOD) [...] The post CISA adds Spring4Shell flaw to its Known Exploited Vulnerabilities Catalog appeared first on Security Affairs.

Cyware News - Latest Cyber News

Colibri Loader combines Task Scheduler and PowerShell in clever persistence technique

Colibri Loader is a relatively new piece of malware that first appeared on underground forums in August 2021 and was advertised to "people who have large volumes of traffic and lack of time to work out the material".

Cyware News - Latest Cyber News

Cyber Threats at Retail Endpoints Giving Way to Data Theft

e-Commerce sites are frequently targeted by cyberattackers and there isn't much attention paid to the cybersecurity measures at brick-and-mortar retailers. Many cybercriminal groups rely on banking trojans to steal customer credit/debit card information or internet banking credentials from the networks of retailers. Online retailers are suggested to review their budgets and allocate an adequate portion to secure themsleves.

The Hacker News

FIN7 Hackers Leveraging Password Reuse and Software Supply Chain Attacks

The notorious cybercrime group known as FIN7 has diversified its initial access vectors to incorporate software supply chain compromise and the use of stolen credentials, new research has revealed. "Data theft extortion or ransomware deployment following FIN7-attributed activity at multiple organizations, as well as technical overlaps, suggests that FIN7 actors have been associated with various

German Authorities Seize Hydra's Servers, Close the Largest Russian-

Naked Security

Firefox 99 is out - no major bugs, but update anyway!
Firefox's four-weekly updates just dropped - here's what you need to know.

Security Affairs

Germany police shut down Hydra Market dark web marketplace
Germany's Federal Criminal Police Office shut down Hydra Market, the Russian-language darknet marketplace specialized in drug dealing. Germany's Federal Criminal Police Office, the Bundeskriminalamt (BKA), announced they have shut down Hydra, one of the world's largest dark web marketplace. The seizure of the Hydra Market is the result of an international investigation conducted by the [...] The post Germany police shut down Hydra Market dark web marketplace appeared first on Security Affairs.

Cyware News - Latest Cyber News

Germany takes down Hydra, world's largest darknet market
Apart from narcotics and money laundering services, which were the main focus, the underground market also offered stolen databases, forged documents, and hacking for hire services.

Naked Security

Google's monthly Android updates patch numerous "get root" holes
Get the update now... if it's available for your phone. Here's how to check.

Cyware News - Latest Cyber News

IPfuscation is Hive's New Technique to Evade Detection
Hive ransomware gang is using a new IPfuscation tactic to hide its payload wherein they hide 64-bit Windows executables in the form of an array of ASCII IPv4 addresses. Additionally, the researchers spotted additional IPfuscation variants using IPv6 instead of IPv4 addresses, UUIDs, and MAC addresses, all operating in almost the same way.

Cyware News - Latest Cyber News

MacOS SUHelper Root Privilege Escalation Vulnerability: A Deep Dive Into CVE-2022-22639
Designated as CVE-2022-22639, the vulnerability could allow root privilege escalation if successfully exploited. After discovering the flaw, we reported it to Apple, hence the release of a patch through the macOS Monterey 12.3 security update.

Threatpost

No-Joke Borat RAT Propagates Ransomware, DDoS
This fresh malware strain extends the functionality of typical trojans with advanced functionality and a series of modules for launching various types of threat activity.

Security Affairs

Russia-linked Armageddon APT targets Ukrainian state organizations, CERT-UA warns
Ukraine CERT-UA spotted a spear-phishing campaign conducted by Russia-linked Armageddon APT targeting local state organizations. Ukraine CERT-UA published a security advisory to warn of spear-phishing attacks conducted by Russia-linked Armageddon APT (aka Gamaredon, Primitive Bear, Armageddon, Winterflounder, or Iron Tilden) targeting local state organizations. The phishing messages have been sent from "vadim_melnik88@i[.]ua," the campaign aims at [...] The post Russia-linked Armageddon APT targets Ukrainian state organizations, CERT-UA warns appeared first on Security Affairs.

IT Security Guru

The Works closes stores after cyber attack
The Works has reported that five of its 526 shops were forced to close last week as hackers gained access to its computer systems and caused issues with its tills. While customers are experiencing longer delivery times for online orders, the company has said that no shoppers' payment details had been compromised. The Works said [...] The post The Works closes stores after cyber attack appeared first on IT Security Guru.

Cyware News - Latest Cyber News

Thwarting Loaders: From SocGholish to BLISTER's LockBit Payload
SocGholish has been around longer than BLISTER, having already established itself well among threat actors for its advanced delivery framework. Reports show that its framework of attack has previously been used by threat actors from as early as 2020.

WeLiveSecurity

We're going on Tor
If better privacy and anonymity sound like music to your ears, you may not need to look much further than Tor Browser. Here's what it's like to surf the dark web using the browser. The post We're going on Tor appeared first on WeLiveSecurity

Blog â€" Flashpoint

Language Darknet Market [Updated]
German authorities announced today that they had taken down the Germany-based servers of Hydra Market--the largest Russian-speaking darknet market--and closed it. They also confiscated 23M Euros (about $25M) in Bitcoin. The steps follow an investigation with the participation of German and U.S. law enforcement, which started in August 2021. According to German authorities, the market [...] The post German Authorities Seize Hydra's Servers, Close the Largest Russian-Language Darknet Market [Updated] appeared first on Flashpoint.

The Hacker News

Germany Shuts Down Russian Hydra Darknet Market; Seizes $25 Million in Bitcoin
Germany's Federal Criminal Police Office, the Bundeskriminalamt (BKA), on Tuesday announced the official takedown of Hydra, the world's largest illegal dark web marketplace that has cumulatively facilitated over $5 billion in Bitcoin transactions to date. "Bitcoins amounting to currently the equivalent of approximately EUR23 million were seized, which are attributed to the marketplace," the BKA

ZDNet | security RSS

GitHub now scans for secret leaks in developer workflows
The new tool aims to protect developers against API and token exposure.

CyberScoop

Hydra market's servers, $25M in bitcoin seized by German police in dark web sting
Narcotics trafficking and money laundering were the main business for Hydra, which researchers say was the largest dark-web market. The post Hydra market's servers, $25M in bitcoin seized by German police in dark web sting appeared first on CyberScoop.

CyberScoop

Legislators rail against potential rollback of flexible DOD cyber powers
U.S. Cyber Command General Paul Nakasone told senators that scaling back his organization's cyber ops authorities would be damaging to its mission. The post Legislators rail against potential rollback of flexible DOD cyber powers appeared first on CyberScoop.

IT Security Guru

New Risk-based Application Access Control aims to solve BYOD and Remote Work Security and Productivity Challenges
Yesterday, Cato Networks introduced its new risk-based application access control for combatting the threat of infiltration posed by remote workers and Bring Your Own Device (BYOD). Now, enterprise policies will be able to consider real-time device context when restricting access to certain capabilities within corporate applications, the internet and cloud resources. "User devices can be [...] The post New Risk-based Application Access Control aims to solve BYOD and Remote Work Security and Productivity Challenges appeared first on IT Security Guru.

IT Security Guru

Nominations for 2022's European Cybersecurity Blogger Awards NOW OPEN!
Now in its ninth successive year, the much-anticipated annual European Cybersecurity Blogger Awards, sponsored by KnowBe4 and Qualys, is now open for nominations. The awards have always been committed to celebrating the cybersecurity industry's most coveted bloggers, vloggers, podcasters and social media influencers. Previous award winners have included renowned blogging and podcast stars such as [...] The post Nominations for 2022's European Cybersecurity Blogger Awards NOW OPEN! appeared first on IT Security Guru.

CyberScoop

Russian attempts to phish Ukrainian targets with 'war crimes' lures unsuccessful so far, official says
Russian cyber attacks on Ukraine continue unabated, official says. The post Russian attempts to phish Ukrainian targets with 'war crimes' lures unsuccessful so far, official says appeared first on CyberScoop.

Cyware News - Latest Cyber News

The Works hit by hackers, UK retailer shuts some stores after problems with payment tills
UK high street retailer The Works was forced to shut some of its stores following a "cyber security incident" which saw hackers gaining unauthorized access to its systems.

The Hacker News

U.S. Treasury Department Sanctions Russia-based Hydra Darknet Marketplace
The U.S. Treasury Department on Tuesday sanctioned Hydra, the same day German law enforcement authorities disrupted the world's largest and longest-running dark web marketplace following a coordinated operation in partnership with U.S. officials. The sanctions are part of an "international effort to disrupt proliferation of malicious cybercrime services, dangerous drugs, and other illegal

Cyware News - Latest Cyber News

Yokogawa Patches Flaws Allowing Disruption, Manipulation of Physical Processes
Japanese automation giant Yokogawa recently patched a series of vulnerabilities in control system products that, according to researchers, can be exploited for the disruption or manipulation of physical processes.

Twitter

Remotely Alerts

Severity: | An XML External Entity (XXE) vulnerabili... | CVE-2021-43142 | Link for more:

vulnonym

Let the annals of the day show that CVE-2021-43142... has been granted the moniker Shafted Chersonese

Threat Intel Center

NEW: CVE-2021-43142 An XML External Entity (XXE) vulnerability exists in wuta jox 1.16 in the readObject method in JOXSAXBeanInput.

Robo Shadow Alerts

Potentially Critical CVE Detected! CVE-2021-43142 An XML External Entity (XXE) vulnerability exists in wuta jox 1.16 in the readObject method in JOXSAXBeanInput.... CVSS: 9.39 #CVE #CyberSecurity

Rashami Desai

@loveasimriaz33 @tweetsrandom_21 @realumarriaz @TheRajivAdatia @MahaCyber1 @cyber @MumbaiPolice my pets request plz look in to the matter because ther are harming me and my family image and its the actual fandom or on purpose m getting harassment. My family is getting dragged and its a harassment @MumbaiPolice @CybercrimeCID

Spiros Margaris

15 Tech Leaders On The #NextBigThing In #Cybersecurity #fintech #blockchain #SaaS #privacy @Shirastweet @m49D4ch3lly @mclynd @missdkingsbury @ChuckDBrooks @digitalcloudgal @Forbes

Threat Intel Center

NEW: CVE-2021-43142 An XML External Entity (XXE) vulnerability exists in wuta jox 1.16 in the readObject method in JOXSAXBeanInput. Severity: CRITICAL

Vulmon Vulnerability Feed

CVE-2021-43142 An XML External Entity (XXE) vulnerability exists in wuta jox 1.16 in the readObject method in JOXSAXBeanInput.

CVE.report

CVE-2021-43142 : An XML External Entity XXE vulnerability exists in wuta jox 1.16 in the readObject method in JOXSAXBeanInput....

CVE

CVE-2021-43142 An XML External Entity (XXE) vulnerability exists in wuta jox 1.16 in the readObject method in JOXSAXBeanInput.

Henrik Fisker

Driving without a driver!! Cybersecurity is important! #Fisker #Love #EVs #ESG #cybersecurity @Twitter

Source: NIST

NIST CVE: Critical

CVE-2021-43142

An XML External Entity (XXE) vulnerability exists in wuta jox 1.16 in the readObject method in JOXSAXBeanInput.

CRITICAL Vector: network Created: 2022-03-30 Updated: 2022-04-06

Source: NIST

NIST CVE: High

CVE-2021-39772

In Bluetooth, there is a possible way to access the a2dp audio control switch due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12LAndroid ID: A-181962322

HIGH Vector: adjacent_network Created: 2022-03-30 Updated: 2022-04-06

CVE-2021-33581

MashZone NextGen through 10.7 GA has an SSRF vulnerability that allows an attacker to **interact** with arbitrary TCP services, by abusing the feature to check the availability of a PPM connection. This occurs in com.idsscheer.ppmmashup.web.webservice.impl.ZPrestoAdminWebService.

HIGH Vector: network Created: 2022-03-30 Updated: 2022-04-06

CVE-2021-33523

MashZone NextGen through 10.7 GA allows a remote authenticated user, with access to the admin console, to upload a new **JDBC** driver that can execute arbitrary commands on the underlying host. This occurs in com.idsscheer.ppmmashup.business.jdbc.DriverUploadController.

HIGH Vector: network Created: 2022-03-30 Updated: 2022-04-06

Source: NIST

NIST CVE: Medium

CVE-2021-45900

Vivoh Webinar Manager before 3.6.3.0 has improper API authentication. When a user logs in to the administration configuration web portlet, a VIVOH_AUTH **cookie** is assigned so that they can be uniquely identified. Certain APIs can be successfully executed without proper authentication. This can let an attacker impersonate as victim and make state changing requests on their behalf.

MEDIUM Vector: network Created: 2022-03-30 Updated: 2022-04-06

Source: NIST

NIST CVE: Low

Nothing today

Source: NIST

NIST CVE: Unrated

CVE-2022-23446

A improper control of a resource through its lifetime in **Fortinet** FortiEDR version 5.0.3 and earlier allows attacker to make the whole

CVE-2021-40374

A stored cross-site scripting (XSS) vulnerability was identified in Apperta Foundation OpenEyes 3.5.1. Updating a patient's details allows remote attackers to inject arbitrary web script or HTML via the

application unresponsive via changing its root directory access permission.

UNRATED Vector: unkown Created: 2022-04-06 Updated: 2022-04-06

CVE-2022-23441

A use of hard-coded cryptographic key vulnerability [CWE-321] in FortiEDR versions 5.0.2, 5.0.1, 5.0.0, 4.0.0 may allow an unauthenticated attacker on the network to disguise as and **forge** messages from other collectors.

UNRATED Vector: unkown Created: 2022-04-06 Updated: 2022-04-06

CVE-2020-29013

An improper input validation vulnerability in the sniffer interface of **FortiSandbox** before 3.2.2 may allow an authenticated attacker to silently halt the sniffer via specifically crafted requests.

UNRATED Vector: unkown Created: 2022-04-06 Updated: 2022-04-06

CVE-2021-45103

An issue was discovered in **HTCondor** 9.0.x before 9.0.10 and 9.1.x before 9.5.1. An attacker can access files stored in S3 cloud storage that a user has asked HTCondor to transfer.

UNRATED Vector: unkown Created: 2022-04-06 Updated: 2022-04-06

CVE-2021-40375

Apperta Foundation OpenEyes 3.5.1 allows remote attackers to view the sensitive information of patients without having the intended level of privilege. Despite OpenEyes returning a Forbidden error message, the contents of a patient's profile are still returned in the server response. This response can be read in an intercepting proxy or by viewing the page source. Sensitive information returned in responses includes patient PII and medication records or history.

UNRATED Vector: unkown Created: 2022-04-06 Updated: 2022-04-06

CVE-2022-26953

Digi Passport Firmware through 1.5.1,1 is affected by a buffer overflow. An attacker can supply a string in the page parameter for reboot.asp endpoint, allowing him to force an overflow when the string is concatenated to the HTML body.

UNRATED Vector: unkown Created: 2022-04-06 Updated: 2022-04-06

CVE-2022-26250

Synaman v5.1 and below was discovered to contain weak file permissions which allows authenticated attackers to escalate privileges.

UNRATED Vector: unkown Created: 2022-04-06 Updated: 2022-04-06

CVE-2022-1234

XSS in **livehelperchat** in **GitHub** repository livehelperchat/livehelperchat prior to 3.97. This vulnerability has the potential to deface websites, result in compromised user accounts, and can run malicious code on web pages, which can lead to a compromise of the useraEUR(tm)s device.

UNRATED Vector: unkown Created: 2022-04-06 Updated: 2022-04-06

Address1 parameter. This JavaScript then executes when the patient profile is loaded, which could be used in a XSS attack.

UNRATED Vector: unkown Created: 2022-04-06 Updated: 2022-04-06

CVE-2022-1248

A vulnerability was found in SAP Information System 1.0 which has been rated as critical. Affected by this issue is the file /SAP_Information_System/controllers/add_admin.php. An unauthenticated attacker is able to create a new admin account for the web application with a simple POST request. Exploit details were disclosed.

UNRATED Vector: unkown Created: 2022-04-06 Updated: 2022-04-06

CVE-2022-26110

An issue was discovered in **HTCondor** 8.8.x before 8.8.16, 9.0.x before 9.0.10, and 9.1.x before 9.6.0. When a user authenticates to an HTCondor daemon via the CLAIMTOBE method, the user can then impersonate any entity when issuing additional commands to that daemon.

UNRATED Vector: unkown Created: 2022-04-06 Updated: 2022-04-06

CVE-2021-45104

An issue was discovered in **HTCondor** 9.0.x before 9.0.10 and 9.1.x before 9.5.1. An attacker who can capture HTCondor network data can interfere with users' jobs and data.

UNRATED Vector: unkown Created: 2022-04-06 Updated: 2022-04-06

CVE-2022-26952

Digi Passport Firmware through 1.5.1,1 is affected by a buffer overflow in the function for building the Location header string when an unauthenticated user is redirected to the authentication page.

UNRATED Vector: unkown Created: 2022-04-06 Updated: 2022-04-06

CVE-2021-30497

Ivanti Avalanche (Premise) 6.3.2 allows remote unauthenticated users to read arbitrary files via Absolute Path Traversal. The imageFilePath parameter processed by the /AvalancheWeb/image endpoint is not verified to be within the scope of the image folder, e.g., the attacker can obtain sensitive information via the C:/Windows/system32/config/system.sav value.

UNRATED Vector: unkown Created: 2022-04-06 Updated: 2022-04-06

CVE-2022-26251

The HTTP interface of **Synaman** v5.1 and below was discovered to allow authenticated attackers to execute arbitrary code and escalate privileges.

UNRATED Vector: unkown Created: 2022-04-06 Updated: 2022-04-06

Source: Hybrid Analysis

Top malicious files

100% Threat score	struts2.exe	100% Threat score	Byrogavr.exe
100% Threat score	Byrogavr.exe	100% Threat score	gbnfgndrr.exe
100% Threat score	435trendrr.exe	100% Threat score	BL 216238068
100% Threat score	989626f5873b0a047184d29d169e3ef2	100% Threat score	Elcomsoft_6.32.1622_portable.exe
100% Threat score	C1.exe	100% Threat score	Fakturierung 2022.21.03_1035.xlsm
100% Threat score	RE P.I-118.exe	100% Threat score	QLOADER.exe
100% Threat score	70060472_DCTAH003_2022_11241651_1_4_1.exe	100% Threat score	i864x__setup__624d5a3742277.exe
100% Threat score	woodie.exe	100% Threat score	123c341cab2c6cc0351b3e9ef77295a8e8ef375a7e3697d62a32d6059e159e15
95% Threat score	RAT.exe	91% Threat score	tmpup0hxrfl
76% Threat score	com.samsung.android.messaging.apk		

Source: Hybrid Analysis

Top malicious URL

100% Threat score	https://lthinfra.in/IN	97% Threat score	http://183.138.154.58:49533/Mozi.m
91% Threat score	http://115.54.105.64:45538/Mozi.m	91% Threat score	http://59.35.93.51:41043/Mozi.m
90% Threat score	http://fahdaldobian.com/	89% Threat score	http://dimenew.com.br/
87% Threat score	http://keepmaildomainupdatedathou.herokuapp.com/	84% Threat score	http://renam30fdomain.com/
82% Threat score	http://kevinconsulting.in/	82% Threat score	http://ct.de/
81% Threat score	https://creditagricole-securipass-web.web.app/ca	77% Threat score	http://sotrabus-mickel.com/
77% Threat score	http://chatbot.cnxloyalty.com/	74% Threat score	http://tmlaug.no/cs-f/?redacted

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 Algeria
#7 Viet Nam	#8 Brazil
#9 Pakistan	#10 Venezuela (Bolivarian Republic of)

Source: SpamHaus

Top phishing countries

#1 United States	#2 Germany
#3 Russia	#4 India
#5 Netherlands	#6 Japan
#7 Belize	#8 Singapore
#9 United Kingdom	#10 Australia

Source: Have I been pwned?

Have I been pwnd

Nothing today

Source: Imperva DDOS Map

Top DDOS attackers

United States (31%)
Germany (13%)
Singapore (6%)

Source: Imperva DDOS Map

Top DDOS country targets

Russia (34%)
United States (18%)
South Korea (14%)

Source: Imperva DDOS Map

Top DDOS techniques

61%	**DDoS**
28%	**Automated Threat**
12%	**OWASP**

Source: Imperva DDOS Map

Top DDOS industry targets

45%	**Financial Services**
21%	**Business**
10%	**Computing & IT**