Security Rabbits

Your Security Rabbits report for March 23, 2022

Source: Ransom Watch

Ransomware attacks

lockbit2	lazpiur,com
conti	Sav-Rx Prescription Services
alphv	inibsa,com | inibsadental,com | inibsa,net 2TB FULL DATA
vicesociety	Griggsville-Perry High School
lockbit2	edukgroup,com
hiveleak	Ministry For Foreign Affairs Of The Republic Of Indonesia
hiveleak	Rotoplas
hiveleak	Dayton T, Brown, Inc
hiveleak	School District Of Janesville
lockbit2	ca,daiyafoods,c,,,
conti	WELCOME HOTELS
stormous	Satz Kontor GmbH data
vicesociety	ICEHOTEL
hiveleak	GomeA
conti	Anac
hiveleak	Otto DÃƒÂ¶rner GmbH & Co, KG
conti	Sanoh America Inc,
hiveleak	Centurion Stone
hiveleak	UCSI University

Hot topics

Nothing today

News

Krebs on Security

'Spam Nation' Villain Vrublevsky Charged With Fraud

Pavel Vrublevsky, founder of the Russian payment technology firm ChronoPay and the antagonist in my 2014 book "Spam Nation," was arrested in Moscow this month and charged with fraud. Russian authorities allege Vrublevsky operated several fraudulent SMS-based payment schemes, and facilitated money laundering for Hydra, the largest Russian darknet market. But according to information obtained by KrebsOnSecurity, it is equally likely Vrublevsky was arrested thanks to his propensity for carefully documenting the links between Russia's state security services and the cybercriminal underground.

Security Affairs

Anonymous hacked Nestle and leaked 10 GB of sensitive

The popular Anonymous hacktivist collective announced to have hacked Nestle and leaked 10 GB of sensitive data because the food and beverage giant continued to operate in Russia. The popular Anonymous hacktivist collective recently declared war on all companies that decided to continue to operate in Russia by paying taxes to the Russian government. Nestle […] The post Anonymous hacked Nestle and leaked 10 GB of sensitive appeared first on Security Affairs.

IT Security Guru

AvosLocker ransomware hits critical infrastructure

Several US authorities issued an alert warning of the threat to critical national infrastructure (CNI) providers from the AvosLocker ransomware group. The group is a ransomware-as-a-service affiliate operation known for targeting financial services, manufacturing and government entities, as well as other sectors, the report indicated. AvosLocker seems to be geographically indiscriminate, with some victims hailing […] The post AvosLocker ransomware hits critical infrastructure appeared first on IT Security Guru.

CyberScoop

Cyber company Okta is latest potential victim cited by Lapsus$ hackers

The financially motivated group of malicious hackers posted screenshots that Okta said could be related to "activity" detected in January. The post Cyber company Okta is latest potential victim cited by Lapsus$ hackers appeared first on CyberScoop.

Threatpost

FIDO: Here's Another Knife to Help Murder Passwords

After years of promising a passwordless future - really, any day now! - FIDO is proposing tweaks to WebAuthn that could put us out of password misery. Experts aren't so sure.

IT Security Guru

LAPSUS$ claims to have breached Okta

The ultra-prolific ransomware group LAPSUS$ are now claiming to have breached Okta, an authentication services provider. The report comes after the hackers posted what they claim to be screenshots of Okta's internal company environment. Thousands of companies rely on Okta to manage access to their networks and applications, making the possibility of a breach especially […] The

Security Affairs

A new wave of DeadBolt Ransomware attacks hit QNAP NAS devices

Internet search engine Censys reported a new wave of DeadBolt ransomware attacks targeting QNAP NAS devices. Internet search engine Censys reported that QNAP devices were targeted in a new wave of DeadBolt ransomware attacks. Since January, DeadBolt ransomware operators are targeting QNAP NAS devices worldwide, its operators claim the availability of a zero-day exploit that […] The post A new wave of DeadBolt Ransomware attacks hit QNAP NAS devices appeared first on Security Affairs.

Cyware News - Latest Cyber News

Another Source Code Leak for Conti Ransomware

New source code for the Russian-based Conti ransomware operation has been leaked on Twitter--as revenge for the ongoing war--by the Ukrainian researcher named Conti Leaks. The source code leak is a Visual Studio solution that can be decompiled easily, thus allowing anyone to compile the code and the decryptor. The recent leak shall help the security community to better understand Conti ransomware operations.

Cyware News - Latest Cyber News

BlackMatter Affiliates Propagate BlackCat Ransomware

Researchers analyzed two recent ransomware attacks by BlackCat and BlackMatter and discovered overlaps in their TTPs. However, one of the representatives of BlackCat had already claimed that the ransomware is not the rebranding of BlackMatter. BlackCat could be playing an important role in helping several groups come together and work as a team.

Cyware News - Latest Cyber News

FBI: AvosLocker Ransomware is Actively Targeting U.S. Critical Infrastructure

The FBI issued a joint cybersecurity advisory against AvosLocker ransomware operations aimed at crippling the networks of U.S. critical infrastructure. It has targeted multiple sectors including financial services, critical manufacturing sectors, and government facilities as well. The advisory provides multiple countermeasures to stay protected from AvosLocker ransomware attacks.

Cyware News - Latest Cyber News

Hundreds of HP printer models vulnerable to remote code execution

HP has published security advisories for three critical-severity vulnerabilities affecting hundreds of its LaserJet Pro, Pagewide Pro, OfficeJet, Enterprise, Large Format, and DeskJet printer models.

Threatpost

Lapsus$ Data Kidnappers Claim Snatches From Microsoft, Okta

Lapsus$ shared screenshots of internal Okta systems and 40Gb of purportedly stolen Microsoft data on Bing, Bing Maps and Cortana.

post LAPSUS$ claims to have breached Okta appeared first on IT Security Guru.

Security Affairs

Lapsus$ extortion gang claims to have stolen sensitive data from Okta

The Lapsus$ extortion group claims to have stolen sensitive data from the identity and access management giant Okta solutions. The gang announced the alleged hack through its Telegram channel and shared a series of screenshots as proof of the hack. Some of the images published by the threat actors appear to be related to the company's [...] The post Lapsus$ extortion gang claims to have stolen sensitive data from Okta appeared first on Security Affairs.

Cyware News - Latest Cyber News

McAfee Enterprise's security service edge business is now called Skyhigh Security

At the start of this year, Symphony Technology Group (STG) announced Trellix was the new name for the business unit that resulted from the merger of McAfee Enterprise and FireEye last October.

IT Security Guru

New attack technique makes phishing near undetectable

A new phishing technique dubbed browser-in-the-browser (BitB) attack allows threat actors to simulate a browser window within a browser, spoofing a legitimate domain and initiating a convincing phishing attack. A penetration tester and security researcher, known as mrd0x on Twitter, explained how the method takes advantage of third-party single sign-on (SSO) options on websites such as [...] The post New attack technique makes phishing near undetectable appeared first on IT Security Guru.

IT Security Guru

Okta confirms hack, 2.5% of customers affected

Okta has confirmed that they were hacked by LAPSUS$ ransomware group. LAPSUS$ ransomware posted screenshots which they claimed were of Okta's internal company environment yesterday. Today, the authentication services provider has updated a blog post confirming the breach: "After a thorough analysis of these claims, we have concluded that a small percentage of customers -- [...] The post Okta confirms hack, 2.5% of customers affected appeared first on IT Security Guru.

The Hacker News

Over 200,000 MicroTik Routers Worldwide Are Under the Control of Botnet Malware

Vulnerable routers from MikroTik have been misused to form what cybersecurity researchers have called one of the largest botnet-as-a-service cybercrime operations seen in recent years. According to a new piece of research published by Avast, a cryptocurrency mining campaign leveraging the new-disrupted Glupteba botnet as well as the infamous TrickBot malware were all distributed using the same

CyberScoop

Private equity firm that created Trellix spins off another cyber business, Skyhigh Security

Skyhigh is essentially the last piece of the puzzle created by Symphony Technology Group's shakeup of several big cybersecurity brands. The post Private equity firm that created Trellix spins off another cyber business, Skyhigh Security appeared first on CyberScoop.

Threatpost

Russia Lays Groundwork for Cyberattacks on US Infrastructure - White House

"Evolving intelligence" shows Russia amping up for cyber-war in response to Ukraine-related sanctions, the White House said -- but researchers warn that many orgs are not prepared.

Threatpost

Serpent Backdoor Slithers into Orgs Using Chocolatey Installer

An unusual attack using an open-source Python package installer called Chocolatey, steganography and Scheduled Tasks is stealthily delivering spyware to companies.

Security Affairs

Three critical RCE flaws affect hundreds of HP printer models

Three critical RCE flaws affect hundreds of HP LaserJet Pro, Pagewide Pro, OfficeJet, Enterprise, Large Format, and DeskJet printer models. HP issued a security bulletin warning of a buffer overflow vulnerability, tracked as CVE-2022-3942 (CVSS score 8.4), that could lead to remote code execution on vulnerable devices. "Certain HP Print products and Digital Sending products may [...] The post Three critical RCE flaws affect hundreds of HP printer models appeared first on Security Affairs.

The Hacker News

U.S. Government Warns Companies of Potential Russian Cyber Attacks

The U.S. government on Monday once again cautioned of potential cyber attacks from Russia in retaliation for economic sanctions imposed by the west on the country following its military assault on Ukraine last month. "It's part of Russia's playbook," U.S. President Joe Biden said in a statement, citing "evolving intelligence that the Russian Government is exploring options." The development

Cyware News - Latest Cyber News

Update: Okta now says Lapsus$ may have accessed customer info

Okta's chief security officer David Bradbury revealed: "a small percentage of customers - approximately 2.5% - have potentially been impacted and whose data may have been viewed or acted upon."

The Hacker News

Wazuh Offers XDR Functionality at a Price Enterprises Will Love -- Free!

Back in 2018, Palo Alto Networks CTO and co-founder Nir Zuk coined a new term to describe the way that businesses needed to approach cybersecurity in the years to come. That term, of course, was extended detection and response (XDR). It described a unified cybersecurity infrastructure that brought endpoint threat detection, network analysis and visibility (NAV), access management, and more under

The Hacker News

LAPSUS$ Hackers Claim to Have Breached Microsoft and Authentication Firm Okta

Microsoft and authentication services provider Okta said they are investigating claims of a potential breach alleged by the LAPSUS$ extortionist gang. The development, which was first reported by Vice and Reuters, comes after the cyber criminal group posted screenshots and source code of what it said were the companies' internal projects and systems on its Telegram channel. The leaked 37GB

The Hacker News

Microsoft and Okta Confirm Breach by LAPSUS$ Extortion Group

Microsoft on Tuesday confirmed that the LAPSUS$ extortion-focused hacking crew had gained "limited access" to its systems, as authentication services provider Okta revealed that nearly 2.5% of its customers have been potentially impacted in the wake of the breach. "No customer code or data was involved in the observed activities," Microsoft's Threat Intelligence Center (MSTIC) said, adding that

The Hacker News

New Variant of Chinese Gimmick Malware Targeting macOS Users

Researchers have disclosed details of a newly discovered macOS variant of a malware implant developed by a Chinese espionage threat actor known to strike attack organizations across Asia. Attributing the attacks to a group tracked as Storm Cloud, cybersecurity firm Volexity characterized the new malware, dubbed Gimmick, a "feature-rich, multi-platform malware family that uses public cloud

ZDNet | security RSS

Okta: Lapsus$ attackers had access to support engineer's laptop

Updated: Okta says that the shared screenshots were sourced from a support engineer's laptop.

Cyware News - Latest Cyber News

Over 40,000 London Voters Have Personal Data Leaked to Strangers

A follow-up message asked the recipient to delete the erroneously sent email and explained that any of the information accidentally leaked was in any case available on a public electoral register.

Cyware News - Latest Cyber News

Public Postal Service of Greece Suffers Outage Due to Ransomware Attack

ELTA, the state-owned provider of postal services in Greece, has disclosed a ransomware incident detected on Sunday that is still keeping most of the organization's services offline.

Cyware News - Latest Cyber News

Scottish mental health charity "devastated" by heartless RansomEXX ransomware attack

SAMH (the Scottish Association for Mental Health) helps provide care and support for adults and young people suffering from issues with their mental health, and campaigns to influence positive social change.

ZDNet | security RSS

Social engineering attacks to dominate Web3, the metaverse

Researchers offer their thoughts on the most prevalent threats faced by emerging technologies.

Cyware News - Latest Cyber News

Top Russian Meat Producer Hit with Windows BitLocker Encryption Attack

The point of compromise was VetIS, a state information system used by veterinary services and companies engaging in the field, making it likely a supply chain compromise, although more clarification is needed.

Cyware News - Latest Cyber News

Update: Microsoft confirms they were hacked by Lapsus$ extortion group

In a new blog post published tonight, Microsoft has confirmed that one of their employee's accounts was compromised by Lapsus$, providing limited access to source code repositories.

The Hacker News

Use This Definitive RFP Template to Effectively Evaluate XDR solutions

A new class of security tools is emerging that promises to significantly improve the effectiveness and efficiency of threat detection and response. Emerging Extended Detection and Response (XDR) solutions aim to aggregate and correlate telemetry from multiple detection controls and then synthesize response actions. XDR has been referred to as the next step in the evolution of Endpoint

Cyware News - Latest Cyber News

White House shares checklist to counter Russian cyberattacks

The White House is urging U.S. organizations to shore up their cybersecurity defenses after new intelligence suggests that Russia is preparing to conduct cyberattacks in the near future.

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-2021-39720

Product: AndroidVersions: Android kernelAndroid ID: A-207433926References: N/A

CRITICAL Vector: network Created: 2022-03-16 Updated: 2022-03-23

Source: NIST

NIST CVE: High

CVE-2021-39714

In ion_buffer_kmap_get of ion.c, there is a possible use-after-free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-205573273References: Upstream kernel

HIGH Vector: local Created: 2022-03-16 Updated: 2022-03-23

Source: NIST

NIST CVE: Medium

CVE-2021-39715

In __show_regs of process.c, there is a possible leak of kernel memory and addresses due to log information disclosure. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-178379135References: Upstream kernel

MEDIUM Vector: local Created: 2022-03-16 Updated: 2022-03-23

CVE-2021-39718

In ProtocolStkProactiveCommandAdapter::Init of protocolstkadapter.cpp, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-205035540References: N/A

MEDIUM Vector: local Created: 2022-03-16 Updated: 2022-03-23

CVE-2021-39712

In TBD of TBD, there is a possible user after free vulnerability due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-176918884References: N/A

MEDIUM Vector: local Created: 2022-03-16 Updated: 2022-03-23

CVE-2021-39717

In iaxxx_btp_write_words of iaxxx-btp.c, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-198653629References: N/A

MEDIUM Vector: local Created: 2022-03-16 Updated: 2022-03-23

CVE-2021-39721

In TBD of TBD, there is a possible out of bounds write due to memory corruption. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-195726151References: N/A

MEDIUM Vector: local Created: 2022-03-16 Updated: 2022-03-23

Source: NIST

NIST CVE: Low

Nothing today

Source: NIST

NIST CVE: Unrated

CVE-2022-27666

In the **Linux** kernel before 5.16.15, there is a buffer overflow in ESP transformation in net/ipv4/esp4.c and net/ipv6/esp6.c via a large message.

UNRATED Vector: unkown Created: 2022-03-23 Updated: 2022-03-23

CVE-2022-1033

Unrestricted Upload of File with Dangerous Type in **GitHub** repository crater-invoice/crater prior to 6.0.6.

UNRATED Vector: unkown Created: 2022-03-23 Updated: 2022-03-23

Source: Hybrid Analysis

Top malicious files

100% Threat score	6a2178639dbebae9ba303db01fe4a9ed980c493f9e21a0425206f325b025fe9e
100% Threat score	downloadcenterproductitoppc
100% Threat score	9c815841be71a4aafec48f38dcb04b94fcf7b13a21ffbb834f77951ed615f9c4.dll
100% Threat score	EasyAntiCheat.exe
100% Threat score	XYplorer_22.90_Install.exe
100% Threat score	uuimeqat.xlsb

100% Threat score	IMG_520004534320005600.exe
100% Threat score	vbc.exe
85% Threat score	fembob.exe
83% Threat score	ejemplo.pdf
80% Threat score	setup_biomechanicstoolbar_v1-2.exe
75% Threat score	z.xlsb

Source: Hybrid Analysis

Top malicious URL

100% Threat score	https://fsm-gov.com/
100% Threat score	http://grupoitplus.com.bo/redirect/
100% Threat score	http://112.248.247.21:47020/Mozi.m
100% Threat score	http://file-coin-coin-10.com/files/6039_1
97% Threat score	http://omuwuj.com/TEPB3bl
97% Threat score	http://221.14.171.95:41569/Mozi.m
93% Threat score	http://27.41.38.207:55032/Mozi.a
93% Threat score	http://61.53.35.73:47485/Mozi.m
93% Threat score	http://222.139.49.245:59960/Mozi.m
93% Threat score	http://189.85.34.135:48012/bin.sh
93% Threat score	http://116.179.192.139:60457/Mozi.m
93% Threat score	http://125.47.251.239:41376/Mozi.m
93% Threat score	http://58.253.13.145:42274/Mozi.m
93% Threat score	http://222.137.141.227:47829/Mozi.a
93% Threat score	http://112.248.62.88:45294/Mozi.m
93% Threat score	http://140.255.8.88:49686/i
93% Threat score	http://1.10.146.29:41489/Mozi.a
93% Threat score	http://112.31.67.95:45431/Mozi.m
93% Threat score	http://182.116.123.242:49262/mozi.m
93% Threat score	http://114.226.220.97:56922/Mozi.a
93% Threat score	http://42.230.99.75:50265/bin.sh
93% Threat score	http://222.137.82.31:35830/Mozi.a
93% Threat score	http://27.36.143.194:36317/Mozi.m
90% Threat score	http://file-coin-coin-10.com/files/6258_1
90% Threat score	http://file-coin-coin-10.com/files/5429_1647629465_1977.exe
87% Threat score	http://inx.lv/h3ip?l4j
84% Threat score	http://allanschwartzrnan.com/
82% Threat score	http://www.sct.org.uk/
77% Threat score	http://link.eu.marcusevans-conferences.com/ls/click?upn=YRsiXMKwPYSz4cCvR11uND6em5VM-2F-2BxuxAJFY5oAOJwsiox2PcN13a0971Ei9V8XgsgDpvlUQ9U-2BQoI-2FypPyXoF5xzR3cezN-2F1bMs0vtRgI-3DsQ4H_zuFOo-2Bcle2th-2F9kAZ1hn7lXJUA9wxFuAe9ZIWtDwCB5RbpPEWbdPgbOpUdH3Zcg05yXiBJAbTbgbtcBZDMoo-2BvBV2l-2FKiFzwilb3-2BLXstHc3owQi-2B3Urux6jpg-2FX471K6z21iLHvmk4Ak7gKddENYpIDIExO3PcJ1hswykdLXHjmoDDzS3fop1MeNwcUEOdokpQciV4eCqN-2BjL8dJRfh-2BRGBushB3BN9gIq8lWdDELBvqQ1Y4ojED8b0bo6UU0-2FyQrQosI1Dz4R-2FYnM-2BcUf0j80bB-2FYxEruv29riQxGWQ3Kji3dtJVVS3M2495iA34w4ZMj2iUvPZO0OVLsc4uPlSuom0rNIdn6OpqhILox0Ov3Ixy3vjys0DlDgjdeCKId-2Bi0mGoP5mTq63wcnZWENeUGzK-2BUeWth-2F20H-2FemVkVYbAfZQQGKueYO8JmXxcnUfUdFBYKhb7BjJbrEPnlraiQYhKyX6i24rKE6Ox3eDSTmJtLiY0ahDQwnaGkjc03pwig-2BFYqSQ0C5o5FP3jSGDDUjNKCw4CcxkR0Id90754SgroP3J65bk6V4-2FdY-2BhU0EJEF30yHM3t5-2FszzbP-2BewWAke6txd6sIbTK2apaBR3iht7injzVgS-2FKAVDv0sbECoOu9VUYBYkJt5iQ65hCB8okn9QURddxAlonQPVj-2F8lTRvgg-2FzBv7gr2lYzQIr5bH0bi4xXCMwEf7y-2F7jUZZw60WUiIm3qUTVnz556-2FrAn3yZ52NVC8800l41MfLra0Wsr5ob1YUIiHH-2FmbbnDZYoQLu6BsnsixOL22nRqkgWxN89BWmXzEfp7-2BJkF1BMCEin41lDv0XlWOwtbuikn8vlf5L-2FMJ2LmPqZAt0uKdRzI-2B7JKbLY6nQ-2FVKBXxZa7pGzxXX-2BgVsSB-2FvOSbcycLT-2BRuLKCLxXKxI2u4Rx7JCbHLhPABG3NDgHAppUBmnpKOQRGw0JF0PxM7y-2FAFiGphx8UCdKKnKQ2bmfSRT4ZfelEj8hjRPU-3D
74% Threat score	https://storageapi.fleek.co/651c73d5-af7 bucket/index_gen_dsav.html
72% Threat score	http://zdtym.smtpgaze.com/tracking/qaR9ZGLkAmtmZQRlZGt0BGZjAmRmAvM5qzS4qaR9ZQbjGt
72% Threat score	https://alumco.mx/poeboybwf/taoaofia/r uja=joe.lee%40nortonrosefulbright.com
72% Threat score	https://alumco.mx/poeboybwf/taoaofia/refluxction/wemohood/parcelangeny/?uja=gdpr%40robertwalters.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 United States of America

#3 India

#4 Indonesia

#5 Thailand

#6 Algeria

#7 Viet Nam

#8 Brazil

#9 Pakistan

#10 Venezuela (Bolivarian Republic of)

Source: SpamHaus

Top phishing countries

#1 United States

#2 Russia

#3 Germany

#4 Netherlands

#5 Singapore

#6 India

#7 France

#8 United Kingdom

#9 Australia

#10 Canada

Source: Have I been pwned?

Have I been pwnd

Nothing today

Source: Imperva DDOS Map

Top DDOS attackers

United States (29%)

- **Russia (16%)**
- **Germany (12%)**

Source: Imperva DDOS Map

Top DDOS country targets

- **Russia (58%)**
- **Ukraine (18%)**
- **United States (13%)**

Source: Imperva DDOS Map

Top DDOS techniques

75%	**DDoS**
15%	**Automated Threat**
10%	**OWASP**

Source: Imperva DDOS Map

Top DDOS industry targets

63%	**Financial Services**
24%	**Business**
4%	**Computing & IT**