



Your Security Rabbits report for March 18, 2022

Source: [Ransom Watch](#)













Ransomware attacks







lockbit2	Target: draftex . de	lockbit2	Target: www . centralacci . . .
conti	Target: TIG	lockbit2	Target: thionvillenola
everest	Target: South Africa Electricity company	alphv	Target: Noble Oil nobleoil . com
lockbit2	Target: montanarisrl . ne . . .	lockbit2	Target: ifis . com . sg
lockbit2	Target: gezairi . com	lockbit2	Target: ihg . com
lockbit2	Target: lawsdn . com	lockbit2	Target: hilltopconstruc . . .
lockbit2	Target: rosslare . com . hk	lockbit2	Target: specialinc . com
suncrypt	Target: FitFlop Ltd .	lockbit2	Target: finances . gouv . c . . .
lockbit2	Target: aetnabridge . com		

Hot topics

Nothing today

News

 CISA Alerts	AA22-076A: Strengthening Cybersecurity of SATCOM Network Providers and Customers Actions to Take Today: * Use secure methods for authentication. * Enforce principle of least privilege. * Review trust relationships. * Implement encryption. * Ensure robust patching and system configuration audits. * Monitor logs for suspicious activity. * Ensure incident response, resilience, and continuity of operations plans are in place. The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) are aware of possible threats to U.S. and international satellite communication (SATCOM) networks. Successful intrusions into SATCOM networks could create risk in SATCOM network providers' customer env[...]	 Security Affairs	Anonymous continues to support Ukraine against the Russia The collective Anonymous and its affiliated groups continue to target the Russian government and private organizations. The collective Anonymous, and other groups in its ecosystem, continue to target the Russian government and private organizations. Let's summarize the most interesting attacks observed in the last few days. Yesterday Anonymous announced the hack of the website of [...] The post Anonymous continues to support Ukraine against the Russia appeared first on Security Affairs.
 Cyware News - Latest Cyber News	Around 34 Ransomware Variants Detected In Q4 2021 The ransomware landscape witnessed 34 different variants in approximately 722 distinct attacks, with LockBit 2.0, Conti, and PYSA occupying the top three places. In comparison to Q3 2021 data, the attacks on the manufacturing sector have declined while consumer and industrial products rose by 22.2% in Q4. The most affected countries were the U.S., Italy, Germany, France, and Canada.	 Security Affairs	B1txor20 Linux botnet use DNS Tunnel and Log4j exploit Researchers uncovered a new Linux botnet, tracked as B1txor20, that exploits the Log4j vulnerability and DNS tunnel. Researchers from Qihoo 360's Netlab have discovered a new backdoor used to infect Linux systems and include them in a botnet tracked as B1txor20. The malware was first spotted on February 9, 2022, when 360Netlab's honeypot system captured [...] The post B1txor20 Linux botnet use DNS Tunnel and Log4j exploit appeared first on Security Affairs.
 ZDNet security RSS	Cloudflare debuts Friendly Bot validation service Machine learning is already used to "spot your bot."	 Threatpost	Dev Sabotages Popular NPM Package to Protest Russian Invasion In the latest software supply-chain attack, the code maintainer added malicious code to the hugely popular node-ipc library to replace files with a heart emoji and a peacenotwar module.
 The Hacker News	DirtyMoe Botnet Gains New Exploits in Wormable Module to Spread Rapidly The malware known as DirtyMoe has gained new worm-like propagation capabilities that allow it to expand its reach without requiring any user interaction, the latest research has found. "The worming module targets older well-known vulnerabilities, e.g., EternalBlue and Hot Potato Windows privilege escalation," Avast researcher Martin Chlumecky said in a report published Wednesday. "One worm	 Cyware News - Latest Cyber News	DirtyMoe Malware Adopts New Exploits in Wormable Module to Spread Rapidly The malware known as DirtyMoe has gained new worm-like propagation capabilities that allow it to expand its reach without requiring any user interaction, the latest research has found.
 IT Security Guru	Disability service provider suffers cyber-attack The Rehab Group, one of the State's largest disability services provider, been hit with a cyber-attack. The organisation notified the Data Protection Commissioner (DPC) that some of its systems have been compromised. The group informed the Data Protection Commissioner (DPC) that some of its systems have been compromised by malware. In a statement, the group said: [...] The post Disability service provider suffers cyber-attack appeared first on IT Security Guru.	 ZDNet security RSS	Ex CafePress owner fined \$500,000 for 'shoddy' security, covering up data breach When victim accounts were closed after being hacked in one incident, CafePress went so far as to charge them a \$25 fee.
 IT Security Guru	Forrester positions KnowBe4 as a leader in security awareness and training solutions KnowBe4, the provider of the world's largest security awareness training and simulated phishing platform, has been positioned as a Leader in The Forrester Wave(tm): Security Awareness and Training Solutions, Q1 2022 report. Using a 30-criteria evaluation, The Forrester Wave report ranks 11 vendors in the security awareness and training market based on their current offering, [...] The post Forrester positions KnowBe4 as a leader in security awareness and training	 The Hacker News	Google Uncovers 'Initial Access Broker' Working with Conti Ransomware Gang Google's Threat Analysis Group (TAG) took the wraps off a new initial access broker that it said is closely affiliated to a Russian cyber crime gang notorious for its Conti and Diavol ransomware operations. Dubbed Exotic Lily, the financially motivated threat actor has been observed exploiting a now-patched critical flaw in the Microsoft Windows MSHTML platform (CVE-2021-40444) as part of

	<p>solutions appeared first on IT Security Guru.</p>		
 <div>CYWARE SOCIAL Cyware News - Latest Cyber News</div>	<p>Hundreds of GoDaddy-hosted Websites Backdoored in Single Day The backdoor infecting all sites is a 2015 Google search SEO-poisoning tool implanted on the wp-config.php to fetch spam link templates from the C2 that are used to inject malicious pages into search results.</p>	 <div>CYWARE SOCIAL Cyware News - Latest Cyber News</div>	<p>Kwampirs Malware Linked with Shamoon Security experts linked the activities of Shamoon APT with those behind Kwapirs malware. They said both could be from the same group as they have been collaborating, sharing updates, techniques, and codes for years. Organizations should be ready with countermeasures including reliable anti-malware solutions to thwart such threats.</p>
 <div>CYWARE SOCIAL Cyware News - Latest Cyber News</div>	<p>Lapsus\$ gang sends a worrying message to would-be criminals The Lapsus\$ cyber-crime gang, believed to be based in Brazil, until recently was best known for attacks on that country's Ministry of Health and Portuguese media outlets SIC Noticias and Expresso.</p>	 <div>cyberscoop CyberScoop</div>	<p>Lawmakers, experts debate whether fears about evasion of cryptocurrency sanctions are overblown Fear abounds that Russia will use cryptocurrency to skirt U.S. sanctions imposed in response to the invasion of Ukraine. The post Lawmakers, experts debate whether fears about evasion of cryptocurrency sanctions are overblown appeared first on CyberScoop.</p>
 <div>Security Affairs</div>	<p>Microsoft releases open-source tool for checking MikroTik Routers compromise Microsoft released an open-source tool to secure MikroTik routers and check for indicators of compromise for Trickbot malware infections. Microsoft has released an open-source tool, dubbed RouterOS Scanner, that can be used to secure MikroTik routers and check for indicators of compromise associated with Trickbot malware infections. "This analysis has enabled us to develop a [...] The post Microsoft releases open-source tool for checking MikroTik Routers compromise appeared first on Security Affairs.</p>	 <div>threatpost Threatpost</div>	<p>Misconfigured Firebase Databases Exposing Data in Mobile Apps Five percent of the databases are vulnerable to threat actors: It's a gold mine of exploit opportunity in thousands of mobile apps, researchers say.</p>
 <div>IT Security Guru</div>	<p>Mobile apps are exposing your data New research suggests that mobile applications boasting tens of millions of downloads are leaking sensitive user data due to the misconfiguration of back-end cloud databases, according to Check Point. Check Point's three-month study began with a simple query on VirusTotal for mobile apps listed on the malware scanning service that communicates with the Firebase cloud database. [...] The post Mobile apps are exposing your data appeared first on IT Security Guru.</p>	 <div>CYWARE SOCIAL Cyware News - Latest Cyber News</div>	<p>New Botnet Targets Linux Devices Via Log4j Vulnerability New B1txor20 botnet is actively exploiting Log4j flaws in Linux systems to create a bot army that helps hackers install rootkits and steal sensitive records. The bot sends the stolen information, results of any command execution, or any other information to its C2 server in form of a DNS request. The malware possesses many additional features which are either not enabled or have a buggy code, thus, suggesting that it is under development.</p>
 <div>cyberscoop CyberScoop</div>	<p>New details emerge on prolific Conti-linked cybercrime group Google's Threat Analysis Group is calling the hackers Exotic Lily, and it says they employed relatively novel tactics. The post New details emerge on prolific Conti-linked cybercrime group appeared first on CyberScoop.</p>	 <div>IT Security Guru</div>	<p>New ransomware threatens to wipe Windows PCs A relatively new Ransomware, LokiLocker, uses the standard extortion-through-encryption racket but also incorporates disk-wiper functionality. Double extortion soared in popularity last year, with ransomware gangs stealing files before encrypting them to threaten victims with a sensitive data leak if they didn't pay up. BlackBerry Threat Intelligence is warning that LokiLock, first seen in August 2021, [...] The post New ransomware threatens to wipe Windows PCs appeared first on IT Security Guru.</p>
 <div>The Hacker News</div>	<p>New Variant of Russian Cyclops Blink Botnet Targeting ASUS Routers ASUS routers have emerged as the target of a nascent botnet called Cyclops Blink, almost a month after it was revealed the malware abused WatchGuard firewall appliances as a stepping stone to gain remote access to breached networks. According to a new report published by Trend Micro, the botnet's "main purpose is to build an infrastructure for further attacks on high-value targets," given that</p>	 <div>CYWARE SOCIAL Cyware News - Latest Cyber News</div>	<p>New Wipers and Fake AV Updates Target Ukraine Researchers spotted the third wiper malware in use against Ukrainian organizations, which destroys user data and partition information from attached drives while also reporting a new phishing attack. The Ukrainian agency has linked the recent activity with the UAC-0056 group with medium confidence.</p>
 <div>Security Affairs</div>	<p>node-ipc NPM Package sabotage to protest Ukraine invasion The developer behind the popular "node-ipc" NPM package uploaded a destructive version to protest Russia's invasion of Ukraine. RIAEvangelist, the developer behind the popular "node-ipc" NPM package, shipped a new version that wipes Russia, Belarus systems to protest Russia's invasion of Ukraine. The Node-ipc node module allows local and remote inter-process communication with support for Linux. [...] The post node-ipc NPM Package sabotage to protest Ukraine invasion appeared first on Security Affairs.</p>	 <div>IT Security Guru</div>	<p>Phishers exploit Ukraine conflict to solicit crypto In the wake of the Ukraine-Russia conflict, cyber-criminals have begun to impersonate legitimate aid organisations in order to steal financial donations intended for the Ukrainian people. The discovery comes from new research by managed detection and response provider, Expel. The company's security operations centre (SOC) analysed attack vectors and incident trends for its February Attack [...] The post Phishers exploit Ukraine conflict to solicit crypto appeared first on IT Security Guru.</p>
 <div>The Hacker News</div>	<p>Popular NPM Package Updated to Wipe Russia, Belarus Systems to Protest Ukraine Invasion In what's an act of deliberate sabotage, the developer behind the popular "node-ipc" NPM package shipped a new tampered version to condemn Russia's invasion of Ukraine, raising concerns about security in the open-source and the software supply chain. Affecting versions 10.1.1 and 10.1.2 of the library, the alterations introduced by its maintainer RIAEvangelist brought about undesirable behavior</p>	 <div>Krebs on Security</div>	<p>Pro-Ukraine 'Protestware' Pushes Antiwar Ads, Geo-Targeted Malware Researchers are tracking a number of open-source "protestware" projects on GitHub that have recently altered their code to display "Stand with Ukraine" messages for users, or basic facts about the carnage in Ukraine. The group also is tracking several code packages that were recently modified to erase files on computers that appear to be coming from Russian or Belarusian Internet addresses.</p>
 <div>Threatpost</div>	<p>Reporting Mandates to Clear Up Feds' Hazy Look into Threat Landscape - Podcast It's about time, AttackIQ's Jonathan Reiber said about 24H/72H report deadlines mandated in the new spending bill. As it is, visibility into adversary behavior has been muck.</p>	 <div>ZDNet security RSS</div>	<p>Russian Cyclops Blink botnet launches assault against Asus routers The only option available might be a return to factory settings for infected routers.</p>
 <div>SOPHOS Naked Security</div>	<p>S3 Ep74: Cybercrime busts, Apple patches, Pi Day, and disconnect effects [Podcast] Latest episode - listen now!</p>	 <div>CYWARE SOCIAL Cyware News - Latest Cyber News</div>	<p>Sabotaged Version of Popular NPM Package Deletes Files to Protest Against Ukraine War Newer versions of the 'node-ipc' package began deleting all data and overwriting all files on developer's machines, in addition to creating new text files with "peace" messages.</p>
 <div>cyberscoop CyberScoop</div>	<p>Sandworm-linked botnet has another piece of hardware in its sights The CyclopsBlink malware is now targeting internet routers from hardware maker ASUS, Trend Micro researchers said. The post Sandworm-linked botnet has another piece of hardware in its sights appeared first on CyberScoop.</p>	 <div>CYWARE SOCIAL Cyware News - Latest Cyber News</div>	<p>Sandworm-linked CyclopsBlink botnet has another piece of hardware in its sights Botnet activity that drew loud warnings last month from U.S. and U.K. cybersecurity agencies has expanded to a second type of hardware, according to researchers at Trend Micro.</p>
 <div>Security Affairs</div>	<p>SolarWinds Warns of Attacks Targeting Web Help Desk Users SolarWinds warns customers of potential cyberattacks targeting unpatched installs of its Web Help Desk (WHD) product. SolarWinds has published a security advisory to warn customers of the risk of cyberattacks targeting unpatched Web Help Desk (WHD) installs. The WHD is described by SolarWinds as an affordable Help Desk Ticketing and Asset Management Software. SolarWinds declared [...] The post SolarWinds Warns of Attacks Targeting Web Help Desk Users appeared first on Security Affairs.</p>	 <div>The Hacker News</div>	<p>The Golden Hour of Incident Response As a CSIRT consultant, I cannot overemphasize the importance of effectively managing the first hour in a critical incident. Finding out what to do is often a daunting task in a critical incident. In addition, the feeling of uneasiness often prevents an incident response analyst from making effective decisions. However, keeping a cool head and actions planned out is crucial in successfully</p>
			<p>TrickBot Malware Abusing MikroTik Routers as Proxies for Command-and-</p>

These four types of ransomware make up nearly three-quarters of reported incidents

Ransomware causes problems no matter what brand it is, but some forms are noticeably more prolific than others, with four strains of the malware accounting for a combined total of almost 70% of all attacks.

Ukraine SBU arrested a hacker who supported Russia during the invasion

The Security Service of Ukraine (SBU) announced the arrest of a "hacker" who helped Russian Army during the invasion. The Security Service of Ukraine (SBU) announced to have arrested a hacker who provided technical support to Russian troops during the invasion, the man provided mobile communication services inside the Ukrainian territory. The man has broadcasted [...] The post Ukraine SBU arrested a hacker who supported Russia during the invasion appeared first on Security Affairs.

Control

Microsoft on Wednesday detailed a previously undiscovered technique put to use by the TrickBot malware that involves using compromised Internet of Things (IoT) devices as a go-between for establishing communications with the command-and-control (C2) servers. "By using MikroTik routers as proxy servers for its C2 servers and redirecting the traffic through non-standard ports, TrickBot adds

Twitter

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

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.

This man slept with a Chinese spy and is now giving cybersecurity tips. Please fact check me, @twitter[...]

The best #Indian #conferences for #womenintech in 2022 #fintech #cybersecurity @Analyticsindiam

Source: NIST

NIST CVE: Critical

Nothing today

Source: NIST

NIST CVE: High

CVE-2022-26521

Abantecart through 1.3.2 allows remote authenticated administrators to execute arbitrary code by uploading an executable file, because the Catalog>Media Manager>Images settings can be changed by an administrator (e.g., by configuring .php to be a valid image file type).

HIGH Vector: **network** Created: 2022-03-10 Updated: 2022-03-18

CVE-2022-26311

Couchbase Operator 2.2.x before 2.2.3 exposes Sensitive Information to an Unauthorized Actor. Secrets are not redacted in logs collected from **Kubernetes** environments.

HIGH Vector: **network** Created: 2022-03-10 Updated: 2022-03-18

Source: NIST

NIST CVE: Medium

CVE-2022-20058

In preloader (usb), there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, for an attacker who has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06160806; Issue ID: ALPS06160485.

MEDIUM Vector: physical Created: 2022-03-10 Updated: 2022-03-18

CVE-2022-20059

In preloader (usb), there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, for an attacker who has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06160806; Issue ID: ALPS06160781.

MEDIUM Vector: physical Created: 2022-03-10 Updated: 2022-03-18

CVE-2022-20056

In preloader (usb), there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, for an attacker who has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06160806; Issue ID: ALPS06160820.

MEDIUM Vector: physical Created: 2022-03-10 Updated: 2022-03-18

CVE-2022-20060

In preloader (usb), there is a possible permission bypass due to a missing proper image authentication. This could lead to local escalation of privilege, for an attacker who has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06160806; Issue ID: ALPS06137462.

MEDIUM Vector: physical Created: 2022-03-10 Updated: 2022-03-18

CVE-2022-26652

NATS nats-server before 2.7.4 allows Directory Traversal (with write access) via an element in a ZIP archive for **JetStream streams**. nats-streaming-server before 0.24.3 is also affected.

MEDIUM Vector: **network** Created: 2022-03-10 Updated: 2022-03-18

CVE-2022-26104

SAP **Financial Consolidation** - version 10.1, does not perform necessary authorization checks for updating homepage messages, resulting for an unauthorized user to alter the maintenance system message.

MEDIUM Vector: **network** Created: 2022-03-10 Updated: 2022-03-18

CVE-2022-26103

Under certain conditions, SAP **NetWeaver** (Real Time Messaging Framework) - version 7.50, allows an attacker to access information which could lead to information gathering for further exploits and attacks.

MEDIUM Vector: **network** Created: 2022-03-10 Updated: 2022-03-18

Source: NIST

NIST CVE: Low

Nothing today

Source: NIST

NIST CVE: Unrated

CVE-2021-45967

An issue was discovered in Pascom Cloud **Phone** System before 7.20.x. A configuration error between **NGINX** and a backend **Tomcat** server leads to a path traversal in the Tomcat server, exposing unintended

CVE-2021-45966

An issue was discovered in Pascom Cloud **Phone** System before 7.20.x. In the management REST API, /services/apply in exd.pl allows remote

	endpoints. <div>UNRATEDVector: unknown Created: 2022-03-18 Updated: 2022-03-18</div>		attackers to execute arbitrary code via shell metacharacters. <div>UNRATEDVector: unknown Created: 2022-03-18 Updated: 2022-03-18</div>
CVE-2021-45968	An issue was discovered in xmppserver jar in the XMPP Server component of the Jive platform, as used in Pascom Cloud Phone System before 7.20.x (and in other products). An endpoint in the backend Tomcat server of the Pascom allows SSRF, a related issue to CVE-2019-18394. <div>UNRATEDVector: unknown Created: 2022-03-18 Updated: 2022-03-18</div>	CVE-2022-27191	golang .org/x/crypto/ssh before 0.0.0-20220314234659-1baeb1ce4c0b in Go through 1.16.15 and 1.17.x through 1.17.8 allows an attacker to crash a server in certain circumstances involving AddHostKey. <div>UNRATEDVector: unknown Created: 2022-03-18 Updated: 2022-03-18</div>
CVE-2022-26965	In Pluck 4.7.16, an admin user can use the theme upload functionality at /admin.php?action=themeinstall to perform remote code execution. <div>UNRATEDVector: unknown Created: 2022-03-18 Updated: 2022-03-18</div>	CVE-2021-45868	In the Linux kernel before 5.15.3, fs/quota/quota_tree.c does not validate the block number in the quota tree (on disk). This can, for example, lead to a kernel/locking/rwsem.c use-after-free if there is a corrupted quota file. <div>UNRATEDVector: unknown Created: 2022-03-18 Updated: 2022-03-18</div>
CVE-2022-27240	scheme/webauthn.c in Glewlwyd SSO server 2.x before 2.6.2 has a buffer overflow associated with a webauthn assertion. <div>UNRATEDVector: unknown Created: 2022-03-18 Updated: 2022-03-18</div>		

Source: *Hybrid Analysis*

Top malicious files

100% Threat score	HMajCleExt_WDL (.) dll	100% Threat score	pack_0696470 (.) xls
100% Threat score	NEW_OpenVPN_260621 (2) (.) exe	100% Threat score	adjunto_16032022 (.) xls
100% Threat score	uploaded_file~	100% Threat score	sample2 (.) exe
100% Threat score	vbc (.) exe	100% Threat score	6049d38e75426a8f47a03c7a6ededf82fa5e0319b99351175ca20d27e5f62016 (.) exe
100% Threat score	torbrowser-install-win64-11 (.) 0 (.) 7_pt-BR (.) exe	80% Threat score	SABnzbd-3 (.) 5 (.) 3-win-setup (.) exe



Source: *Hybrid Analysis*

Top malicious URL










100% Threat score	https://waitlesscy (.) com/vol-baningletonline
91% Threat score	http://nzpeudg (.) cn/
88% Threat score	http://59 (.) 97 (.) 172 (.) 23:34522/i
85% Threat score	https://mokslogistics (.) com/EM365/
81% Threat score	http://stats (.) update-apps (.) com/installer (.) gif?action=started&browser=ie&browserver=8&ver=1_27_153&bic=C213DA945BE34B09AC9346DF757C3DD9IE&app=33906&appver=0&verifier=1b3421c7a808a70426704d553f04
77% Threat score	http://link (.) cancerdatasci (.) org/
74% Threat score	https://u15645754 (.) ct (.) sendgrid (.) net/ls/click?upn=6IyljN38cI-2FqajTDlajNLtX6WJKVu4vuzGoQycqWw43ekSWwVdkZKDXpqr-2BdH9WpyXcJ_kXggRx
73% Threat score	http://filtplate (.) net/236436ae5f4ea15a97 (.) js

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

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.		

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 Iran (Islamic Republic of)		#10 Pakistan

Top phishing countries

	#1 United States		#2 Germany
	#3 Singapore		#4 Russia
	#5 Netherlands		#6 Hong Kong
	#7 India		#8 Indonesia
	#9 United Kingdom		#10 France

Have I been pwned

Nothing today

Top DDOS attackers

Top DDOS country targets

Source: [Imperva DDOS Map](#)

Top DDOS techniques

Source: [Imperva DDOS Map](#)

Top DDOS industry targets