



Your Security Rabbits report for March 26, 2022

Source: [Ransom Watch](#)

Ransomware attacks

lockbit2	centuryaluminum,,,	lockbit2	ctigas.com
lockbit2	https://century,,,	alphv	Relationships Australia
alphv	VOYAGER DISTRIBUTING COMPANY PTY, LTD.		

Hot topics

Nothing today

News



100s of Russian Building Controllers Can be Remotely Hacked

Jose Bertin, an IT security researcher, has identified critical vulnerabilities in Tekon Avtomatika's building controllers, which, if exploited, can lead to remote hacking of building controllers used by a vast number of Russian organizations.

The Hacker News

The Hacker News

7 Suspected Members of LAPSUS\$ Hacker Gang, Aged 16 to 21, Arrested in U.K.

The City of London Police has arrested seven teenagers between the ages of 16 and 21 for their alleged connections to the prolific LAPSUS\$ extortion gang that's linked to a recent burst of attacks targeting NVIDIA, Samsung, Ubisoft, LG, Microsoft, and Okta. "The City of London Police has been conducting an investigation with its partners into members of a hacking group," Detective Inspector,



Security Affairs

Anonymous leaked 28GB of data stolen from the Central Bank of Russia

Anonymous announced that the affiliate group Black Rabbit World has leaked 28 GB of data stolen from the Central Bank of Russia This week the Anonymous hacker collective claims to have hacked the Central Bank of Russia and stole accessed 35,000 documents. The group of hackers announced that will leak the stolen documents in 48 [...] The post Anonymous leaked 28GB of data stolen from the Central Bank of Russia appeared first on Security Affairs.

The Hacker News

The Hacker News

Another Chinese Hacking Group Spotted Targeting Ukraine Amid Russia Invasion

A Chinese-speaking threat actor called Scarab has been linked to a custom backdoor dubbed HeaderTip as part of a campaign targeting Ukraine since Russia embarked on an invasion last month, making it the second China-based hacking group after Mustang Panda to capitalize on the conflict. "The malicious activity represents one of the first public examples of a Chinese threat actor targeting Ukraine



ZDNet | security RSS

Avast acquires SecureKey Technologies in authentication, identity management push

The Canadian company specializes in digital identity services.



Cyware News - Latest Cyber News

Chinese Threat Actor Scarab Found Targeting Ukraine

The malicious activity by the threat actor dubbed UAC-0026 represents one of the first public examples of a Chinese threat actor targeting Ukraine since the invasion began.



Security Affairs

Chinese threat actor Scarab targets Ukraine, CERT-UA warns

Ukraine CERT (CERT-UA) released details about a campaign that SentinelLabs linked with the suspected Chinese threat actor tracked as Scarab. Ukraine CERT (CERT-UA) published technical details about a malicious activity tracked as UAC-0026, which SentinelLabs associated with China-linked Scarab APT. Scarab APT was first spotted in 2015, but experts believe it has been active since [...] The post Chinese threat actor Scarab targets Ukraine, CERT-UA warns appeared first on Security Affairs.































Security Affairs





Chrome emergency update fixes actively exploited a zero-day bug

Google addresses an actively exploited zero-day flaw with the release of Chrome 99.0.4844.84 for Windows, Mac, and Linux. Google fixed an actively exploited high-severity zero-day vulnerability with the release of Chrome 99.0.4844.84 for Windows, Mac, and Linux. Google has released Chrome 99.0.4844.84 for Windows, Mac, and Linux users to address a high-severity zero-day bug, tracked [...] The post Chrome emergency update fixes actively exploited a zero-day bug appeared first on Security Affairs.

[Conti Ransomware Attacks Persist With an Updated](#)

 <div> Cyware News - Latest Cyber News </div>	<div> Version Despite Leaks The most recent Conti ransomware update introduced a number of new features and changes to the ransomware code. Some of these modifications include new command-line arguments. </div>	 <div> Threatpost </div>	<div> DOJ Indicts Russian Gov't Employees Over Targeting Power Sector The supply-chain attack on the U.S. energy sector targeted thousands of computers at hundreds of organizations, including at least one nuclear power plant. </div>
 <div> Cyware News - Latest Cyber News </div>	<div> Emergency Google Chrome update fixes zero-day used in attacks The zero-day bug fixed (tracked as CVE-2022-1096) is a high severity type confusion weakness in the Chrome V8 JavaScript engine reported by an anonymous security researcher. </div>	 <div> CyberScoop </div>	<div> Estonian man sentenced to prison for role in cyber intrusions, ransomware attacks Maksim Berezan was sentenced to 66 months in federal prison for cybercrimes, including ransomware extortions. The post Estonian man sentenced to prison for role in cyber intrusions, ransomware attacks appeared first on CyberScoop. </div>
 <div> Krebs on Security </div>	<div> Estonian Tied to 13 Ransomware Attacks Gets 66 Months in Prison An Estonian man was sentenced today to more than five years in a U.S. prison for his role in at least 13 ransomware attacks that caused losses of approximately \$53 million. Prosecutors say the accused also enjoyed a lengthy career of "cashing out" access to hacked bank accounts worldwide. </div>	 <div> The Hacker News </div>	<div> FCC Adds Kaspersky and Chinese Telecom Firms to National Security Threat List The U.S. Federal Communications Commission (FCC) on Friday moved to add Russian cybersecurity company Kaspersky Lab to the "Covered List" of companies that pose an "unacceptable risk to the national security" of the country. The development marks the first time a Russian entity has been added to the list that's been otherwise dominated by Chinese telecommunications firms. Also added alongside </div>
 <div> ZDNet security RSS </div>	<div> Frosties NFT operators arrested over \$1.1 million 'rug pull' scam Investors hand over their cryptocurrency. Project developers vanish. </div>	 <div> Threatpost </div>	<div> Google Chrome Zero-Day Bugs Exploited Weeks Ahead of Patch Two separate campaigns from different threat actors targeted users with the same exploit kit for more than a month before the company fixed an RCE flaw found in February. </div>
 <div> The Hacker News </div>	<div> Google Issues Urgent Chrome Update to Patch Actively Exploited Zero-Day Vulnerability Google on Friday shipped an out-of-band security update to address a high severity vulnerability in its Chrome browser that it said is being actively exploited in the wild. Tracked as CVE-2022-1096, the zero-day flaw relates to a type confusion vulnerability in the V8 JavaScript engine. An anonymous researcher has been credited with reporting the bug on March 23, 2022. Type confusion errors, </div>	 <div> IT Security Guru </div>	<div> Honda bug allows hackers to unlock and start your car Multiple researchers disclosed a vulnerability this week that would allow nearby attackers to unlock and even start some Honda and Acura cars. To carry out the attack, threat actors would capture the R signals sent from a key fob to a car, then resending these signals to unlock the car and even start the engine [...] The post Honda bug allows hackers to unlock and start your car appeared first on IT Security Guru. </div>
 <div> Cyware News - Latest Cyber News </div>	<div> Honda Bug Lets Hackers Unlock and Start Vulnerable Car via Replay Attacks This week, multiple researchers disclosed a vulnerability that can be used by a nearby attacker to unlock some Honda and Acura car models, and start their engines wirelessly. </div>	 <div> Cyware News - Latest Cyber News </div>	<div> Honda downplays vulnerability allowing hackers to lock, unlock and start Civics Honda said it has no plans to update its older vehicles after researchers with the University of Massachusetts and cybersecurity firm Cybereason released a proof-of-concept for a replay vulnerability affecting the Honda Civics. </div>
 <div> Cyware News - Latest Cyber News </div>	<div> HTTP request smuggling bug patched in mitmproxy Mitmproxy, an open source, interactive HTTPS proxy service, has patched a dangerous bug that potentially allowed attackers to stage HTTP request smuggling attacks against backend servers. </div>	 <div> CyberScoop </div>	<div> Kaspersky added to FCC list that bans Huawei, ZTE from US networks Kaspersky is the first cybersecurity company and first Russian entity on the FCC's "Covered List," which so far has focused on China. The post Kaspersky added to FCC list that bans Huawei, ZTE from US networks appeared first on CyberScoop. </div>
 <div> Cyware News - Latest Cyber News </div>	<div> New Advisory Released by the CISA, the FBI, and the DOE on Russia Threat Activity Against Energy Sector Organizations This joint Cybersecurity Advisory coauthored by the CISA, the FBI, and the DOE provides information on multiple intrusion campaigns conducted by state-sponsored Russian cyber actors from 2011 to 2018 against Energy Sector organizations. </div>	 <div> Cyware News - Latest Cyber News </div>	<div> Okta says 366 clients had data 'acted upon' in Lapsus\$ hack As many as 366 Okta customers might have had their data 'acted upon' following the LapsusUS\$ cyberattack against the identity security giant's customer support subcontractor. </div>
 <div> Cyware News - Latest Cyber News </div>	<div> Over 100 Building Controllers in Russia Vulnerable to Remote Hacker Attacks The security flaws were discovered by researcher Jose Bertin in a controller made by Russian company Tekon Avtomatika, which specializes in equipment and software for elevators and other building systems. </div>	 <div> Cyware News - Latest Cyber News </div>	<div> QNAP NAS Device Makers Warn of DeadBolt Attacks and Risks Due to a Linux Bug Taiwanese hardware manufacturer QNAP is facing twin threats. While Deadbolt ransomware actors are targeting users, the vendor has also urged customers to stay vigilant of Dirty Pipe. Around 5,000 exposed QNAP NAS devices--out of 130,000 exposed--were targeted by ransomware. Whereas, the flaw exists in all major distros, leading to root access with local access. </div>

 <p>Cyware News - Latest Cyber News</p>	<p>Ransomware infections follow precursor malware A ransomware infection is usually preceded by what Lumu founder and CEO Ricardo Villadiego calls "precursor malware," essentially reconnaissance malicious code that has been around for a while.</p>	 <p>IT Security Guru</p>	<p>Russia preparing to conduct cyberattacks, White House warns 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, BleepingComputer reported this week. With the U.S. imposing strict sanctions against Russia and aiding Ukraine in the war, the White House is expecting the Kremlin to retaliate [...] The post Russia preparing to conduct cyberattacks, White House warns appeared first on IT Security Guru.</p>
 <p>Cyware News - Latest Cyber News</p>	<p>Russian military behind hack of satellite communication devices in Ukraine at war's outset, U.S. officials say U.S. intelligence analysts have concluded that Russian military spy hackers were behind a cyberattack on a satellite broadband service that disrupted Ukraine's military communications at the start of the war last month.</p>	 <p>Cyware News - Latest Cyber News</p>	<p>Storm Cloud Attempting To GIMMICK macOS Users Volexity discovered a newly discovered macOS variant of Gimmick, a malware implant developed by a Chinese group tracked as Storm Cloud. It is targeting organizations across Asia. The samples of the GIMMICK malware are large and complex, which suggests the threat actor behind it seems to be well resourced. Moreover, there is the possibility that Storm Cloud bought this malware from a third-party developer.</p>
 <p>IT Security Guru</p>	<p>Strong Customer Authentication (SCA): what to expect SCA is a new set of rules from the Financial Conduct Authority (FCA) to help protect customers from fraud when they are shopping online, UK Finance explains. With increasing amounts of purchases being made online, these new rules will help to ensure that customers are safe when shopping and their money is better protected. The changes [...] The post Strong Customer Authentication (SCA): what to expect appeared first on IT Security Guru.</p>	 <p>IT Security Guru</p>	<p>Teens arrested amidst Lapsus\$ crackdown City of London police have arrested seven individuals between the ages of 16-21 in connection with the Lapsus\$ ransom attacks, according to the BBC. All of those arrested have been released under investigation. At this time, it is unclear whether the 16 year old alleged ringleader, operating out of his Mother's house, is among these. [...] The post Teens arrested amidst Lapsus\$ crackdown appeared first on IT Security Guru.</p>
 <p>The Hacker News</p>	<p>U.S. Charges 4 Russian Govt. Employees Over Hacking Critical Infrastructure Worldwide The U.S. government on Thursday released a cybersecurity advisory outlining multiple intrusion campaigns conducted by state-sponsored Russian cyber actors from 2011 to 2018 that targeted the energy sector in the U.S. and beyond. "The [Federal Security Service] conducted a multi-stage campaign in which they gained remote access to U.S. and international Energy Sector networks, deployed</p>	 <p>ZDNet security RSS</p>	<p>UK police arrest seven individuals suspected of being hacking group members The youngest suspect is 16 years old.</p>
 <p>Security Affairs</p>	<p>UK police arrested 7 alleged members of Lapsus\$ extortion gang UK police suspect that a 16-year-old from Oxford is one of the leaders of the popular Lapsus\$ extortion group. The City of London Police announced to have arrested seven teenagers suspected of being members of the notorious Lapsus\$ extortion gang, which is believed to be based in South America. "Four researchers investigating the hacking group [...] The post UK police arrested 7 alleged members of Lapsus\$ extortion gang appeared first on Security Affairs.</p>	 <p>Cyware News - Latest Cyber News</p>	<p>US charges 4 Russian govt employees with critical infrastructure hacks The U.S. has indicted four Russian government employees for their involvement in hacking campaigns targeting hundreds of companies and organizations from the global energy sector between 2012 and 2018.</p>

Twitter	
 <p>Rep. Val Demings</p> <p>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</p>	 <p>Dave Rubin</p> <p>This man slept with a Chinese spy and is now giving cybersecurity tips. Please fact check me, @twitter[...]</p>
 <p>Gary Gensler</p> <p>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.</p>	 <p>Spiros Margaritis</p> <p>The best #Indian #conferences for #womenintech in 2022 #fintech #cybersecurity @Analyticsindiam</p>

Source: NIST

NIST CVE: Critical	
<p>CVE-2022-25390</p> <p>DCN Firewall DCME-520 was discovered to contain a remote command execution (RCE) vulnerability via the host parameter in the file /system/tool/ping.php.</p> <div></div>	<p>CVE-2022-25458</p> <p>Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the cmdinput parameter in the exeCommand function.</p> <div> <div>CRITICAL</div> <div>Vector:</div> <div>Created:</div> <div>Updated:</div> </div>

	<div>CRITICAL</div>	Vector: network	Created: 2022-03-18	Updated: 2022-03-26		<div></div>	network	2022-03-18	2022-03-26
CVE-2022-25460	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the endip parameter in the SetPtpServerCfg function.				CVE-2022-25459	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the S1 parameter in the SetSysTimeCfg function.			
	<div>CRITICAL</div>	Vector: network	Created: 2022-03-18	Updated: 2022-03-26		<div>CRITICAL</div>	Vector: network	Created: 2022-03-18	Updated: 2022-03-26

Source: *NIST*

NIST CVE: High

CVE-2022-22593	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Security Update 2022-001 Catalina, macOS Monterey 12.2, macOS Big Sur 11.6.3. A malicious application may be able to execute arbitrary code with kernel privileges.				CVE-2022-22591	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.2. A malicious application may be able to execute arbitrary code with kernel privileges.			
	HIGH	Vector: local	Created: 2022-03-18	Updated: 2022-03-26		HIGH	Vector: local	Created: 2022-03-18	Updated: 2022-03-26
CVE-2022-22633	A memory corruption issue was addressed with improved state management. This issue is fixed in watchOS 8.5, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, macOS Monterey 12.3. Opening a maliciously crafted PDF file may lead to an unexpected application termination or arbitrary code execution.				CVE-2022-22620	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Monterey 12.2.1, iOS 15.3.1 and iPadOS 15.3.1, Safari 15.3 (v. 16612.4.9.1.8 and 15612.4.9.1.8). Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited..			
	HIGH	Vector: local	Created: 2022-03-18	Updated: 2022-03-26		HIGH	Vector: network	Created: 2022-03-18	Updated: 2022-03-26
CVE-2022-22627	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.6.5, macOS Monterey 12.3, Security Update 2022-003 Catalina. Processing a maliciously crafted AppleScript binary may result in unexpected application termination or disclosure of process memory.				CVE-2022-25389	DCN Firewall DCME-520 was discovered to contain an arbitrary file download vulnerability via the path parameter in the file /audit/log/log_management.php.			
	HIGH	Vector: local	Created: 2022-03-18	Updated: 2022-03-26		HIGH	Vector: network	Created: 2022-03-18	Updated: 2022-03-26

Source: *NIST*

NIST CVE: Medium

CVE-2022-22652	The GSMA authentication panel could be presented on the lock screen . The issue was resolved by requiring device unlock to interact with the GSMA authentication panel. This issue is fixed in iOS 15.4 and iPadOS 15.4. A person with physical access may be able to view and modify the carrier account information and settings from the lock screen.			
	MEDIUM	Vector: physical	Created: 2022-03-18	Updated: 2022-03-26

Source: *NIST*

NIST CVE: Low

Nothing today

Source: *NIST*

NIST CVE: Unrated

CVE-2021-44226	Razer Synapse before 3.7.0228.022817 allows privilege escalation because it relies on %PROGRAMDATA%\Razer\Synapse3\Service\bin				CVE-2022-27254	The remote keyless system on Honda Civic 2018 vehicles sends the same RF signal for each door-			
----------------	---	--	--	--	----------------	--	--	--	--

even if %PROGRAMDATA%\Razer has been created by any unprivileged user before Synapse is installed. The unprivileged user may have placed Trojan horse DLLs there.

UNRATED

Vector:
unkown

Created:
2022-03-23

Updated:
2022-03-26

open request, which allows for a replay attack, a related issue to CVE-2019-20626.

UNRATED

Vector:
unkown

Created:
2022-03-23

Updated:
2022-03-26

CVE-2022-1071 User after free in mrb_vm_exec in **GitHub** repository mruby/mruby prior to 3.2.

UNRATED

Vector:
unkown

Created:
2022-03-26

Updated:
2022-03-26

Source: Hybrid Analysis

Top malicious files

100% Threat score	Eclipse Logger.exe	100% Threat score	tmp3pcz871q
100% Threat score	stub1.exe	100% Threat score	image logger.exe
100% Threat score	c.exe	100% Threat score	Install.exe
100% Threat score	tmpphza2cf_	100% Threat score	ul4.exe
100% Threat score	tmpn099j4nj	100% Threat score	Doc_2403.xls
99% Threat score	kotcka.exe	96% Threat score	tmppvbujsxv
92% Threat score	com.pas.webcam_7695_apps.evozi.com.apk	91% Threat score	Power meter stopper.1.0.exe
85% Threat score	abelssoft FileFusion 2022 Giveaway.exe	85% Threat score	tmpm0wet02o
85% Threat score	Sandboxie-Plus-x64-v1.0.15.exe	81% Threat score	Video Downloader_v1.8.5_apkpure.com.apk
75% Threat score	Deep_Learning_with_Python_2nd_Edition_(Final_Rele_17992678_(z-lib.org).pdf	74% Threat score	FFMPEGMJPEG.dll











Source: Hybrid Analysis

Top malicious URL

100% Threat score	https://financialtimes365.com/user/finance.asp	100% Threat score	http://120.193.91.197:36142/i
100% Threat score	http://seventyseven.ph/wm-x/?00dL6LN-T0dVlo4G	100% Threat score	http://95.106.165.81:36271/Mozi.m
100% Threat score	http://vitalpharma.al/le-e/?03q-d7z66tBsY4dJ3vI	100% Threat score	http://alencarsantana.com.br/rj-a/?00msnzgpd-iPqvRBq
100% Threat score	https://www.colfincas.com/	100% Threat score	http://bryan-conklin.com/uploads/1/3/0/6/130605453/757ff1.pdf
100% Threat score	http://www.colfincas.com/	100% Threat score	http://61.52.159.124:58364/Mozi.m
100% Threat score	http://42.232.9.111:49578/Mozi.m	100% Threat score	http://27.36.133.247:36317/bin.sh










100% Threat score	http://27.153.132.143:40274/i	100% Threat score	http://sounddesignmasters.com/
100% Threat score	https://teenbeanjs.com/cloud/javascript.asp	100% Threat score	http://221.13.149.157:47211/bin.sh
97% Threat score	http://188.166.89.189/lmaoWTF/loligang.spc	95% Threat score	http://beautiful.stagingyour.site/
95% Threat score	http://usamediarights.org/vpp	95% Threat score	http://synacksolution.com/
95% Threat score	http://usamediarights.org/jdr	93% Threat score	http://81.163.12.211:43066/Mozi.m
92% Threat score	http://cpcalendars.theshadiwale.com/	90% Threat score	http://182.121.15.134:45388/Mozi.m
88% Threat score	http://188.166.89.189/lmaoWTF/loligang.mips	88% Threat score	http://27.215.81.82:45021/bin.sh
85% Threat score	https://ukrbaget.com.ua/xe-s/?085Xmm-30aWKq0kQ	82% Threat score	http://zypher.net/maps
82% Threat score	http://usamediarights.org/xrr	82% Threat score	http://usamediarights.org/index.html
82% Threat score	http://usamediarights.org/rlt	77% Threat score	https://humingbot.io/cdn/js.asp
77% Threat score	http://sisterologyblog.com/uploads/1/3/0/6/130604805/130604805.html	77% Threat score	http://lighttheory.us/
77% Threat score	http://usamediarights.org/fzn	77% Threat score	http://usamediarights.org/shujuku
72% Threat score	http://usamediarights.org/windows	72% Threat score	http://usamediarights.org/pjj
72% Threat score	http://usamediarights.org/rlz	72% Threat score	http://usamediarights.org/sitemap.html
72% Threat score	http://usamediarights.org/xrf	72% Threat score	http://www.ontariobrokers.info/
72% Threat score	http://matongo-tours.com/uploads/1/3/0/2/130271004/130271004.html	72% Threat score	http://yallywood.net/

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

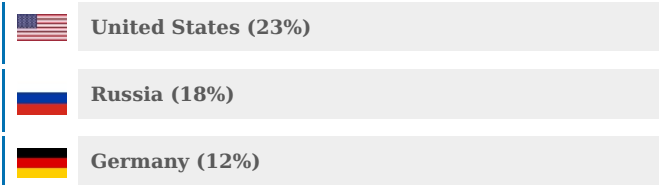
Source: [Have I been pwned?](#)

Have I been pwnd

Nothing today

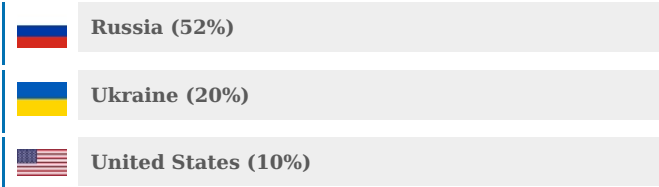
Source: [Imperva DDOS Map](#)

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

