



Your Security Rabbits report for March 09, 2022

Source: [Ransom Watch](#)

Ransomware attacks

Nothing today

Hot topics

Samsung Galaxy source code has been stolen!

Source code used by Samsung for encryption has been stolen by the Lapsus\$ hacking group.

Lapsus\$ is the hacking group that hacked Nvidia a few days ago.

Full story here: <https://www.theverge.com/2022/3/7/22965220/samsung-hack-lapsus-galaxy-source-code-confirmed-nvidia>

--
JL Dupont

News



"Dirty Pipe" Linux kernel bug lets anyone write to any file
Even read-only files can be written to, leading to a dangerously general purpose elevation-of-privilege attack.



Against backdrop of Russian-Ukraine war, researchers witness flurry of nation-aligned hacking
Hackers believed to be associated with the governments of Russia, Belarus and China are targeting Ukraine, Poland and European governments, researchers say, ranging from espionage attempts to phishing campaigns and coinciding with the intensification of the Russian assault on Ukraine. Shane Huntley, the director of Google's Threat Analysis Group (TAG), said in a blog post Monday that the group has observed well-known Russian military hacking group Fancy Bear (also known as APT28) conducting several large credential phishing campaigns targeting UkrNet, a Ukrainian media company. Two recent campaigns, he said, involved newly created Blogspot domains as initial landing pages, which then redirect[...]



Chinese APT41 Hackers Broke into at Least 6 U.S. State Governments: Mandiant
APT41, the state-sponsored threat actor affiliated with China, breached at least six U.S. state government networks between May 2021 and February 2022 by retooling its attack vectors to take advantage of vulnerable internet-facing web applications. The exploited vulnerabilities included "a zero-day vulnerability in the USAHERDS application (CVE-2021-44207) as well as the now infamous zero-day in



CISA Adds 95 Flaws to Its Catalog, Urges For Quick Action
The CISA added more than 60 flaws affecting Cisco and Microsoft products. All the Cisco vulnerabilities are rated critical as they can be abused by cybercriminals to run arbitrary code and for privilege escalation. Most vulnerabilities have a due date of March 24. The cybersecurity agency recommends all entities fix all security issues added to its known vulnerabilities catalog.



Critical RCE Bugs Found in Pascom Cloud Phone System Used by Businesses
Researchers have disclosed three security vulnerabilities affecting Pascom Cloud Phone System (CPS) that could be combined to achieve a full pre-authenticated remote code execution of affected systems. Kerbit security researcher Daniel Eshetu said the shortcomings, when chained together, can lead to "an unauthenticated attacker gaining root on these devices." Pascom Cloud Phone System is an



DDoS Attacks Fuel Pandemonium
A threat actor launched an attack using DanaBot against the webmail server belonging to the Ukrainian Ministry of Defense. The malware was



Access:7 flaws impact +150 device models from over 100 manufacturers
Many IoT and medical devices are affected by seven serious flaws, collectively tracked as Access:7, in widely used Axeda platform. Researchers from medical device cybersecurity company CyberMDX have discovered seven serious flaws, collectively tracked as Access:7, in the widely used Axeda platform of IIoT solutions provider PTC. "Access:7 could enable hackers to remotely execute malicious [...] The post Access:7 flaws impact +150 device models from over 100 manufacturers appeared first on Security Affairs.



Bug in the Linux Kernel Allows Privilege Escalation, Container Escape
A missing check allows unprivileged attackers to escape containers and execute arbitrary commands in the kernel.



Chinese phishing accounts are targeting EU diplomats
A group with ties to China tracked as TA416 but widely known as Mustang Panda has targeted European diplomats since August 2020. The most recent activity employs refreshed lures to coincide with the Russian invasion of Ukraine. A new report by Proofpoint found that TA416 leads cyber-espionage campaigns against the EU, focusing on long-term goals [...] The post Chinese phishing accounts are targeting EU diplomats appeared first on IT Security Guru.



CISA urges to fix actively exploited Firefox zero-days by March 21
The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added recently disclosed Firefox zero-days to its Known Exploited Vulnerabilities Catalog. The Cybersecurity and Infrastructure Security Agency (CISA) added two critical security vulnerabilities in Mozilla Firefox, tracked as CVE-2022-26485 and CVE-2022-26486, to its Known Exploited Vulnerabilities Catalog. The US agency has ordered federal civilian agencies to address both issues by [...] The post CISA urges to fix actively exploited Firefox zero-days by March 21 appeared first on Security Affairs.











Critical Security Patches Issued by Microsoft, Adobe and Other Major Software Firms
Microsoft's Patch Tuesday update for the month of March has been made officially available with 71 fixes spanning across its software products such as Windows, Office, Exchange, and Defender, among others. Of the total 71 patches, three are rated Critical and 68 are rated Important in severity. While none of the vulnerabilities are listed as actively exploited, three of them are publicly known














FIDO authentication standard could signal the passing of passwords
The FIDO authentication standard could eventually bypass passwords, or at least augment them, as government and industry turns to more

<div>News - Latest Cyber News</div>	<div>utilized to deploy another second-stage malware.</div>	<div>News - Latest Cyber News</div>	<div>effective authentication technologies.</div>
<div>cyberscoop</div> <div>CyberScoop</div>	<div>FinCEN warns ransomware proceeds could be part of Russia sanctions evasion</div> <div>As banks and other financial institutions work to honor the U.S. sanctions against Russia and monitor for efforts to evade them, the feds are warning that ransomware proceeds could be in the mix. The Treasury Department's Financial Crimes Enforcement Network (FinCEN) issued guidance this week on the responsibility that private institutions have for detecting "sanctions evasion activity" and reporting it under the Bank Secrecy Act and other laws. The alert comes as federal lawmakers have expressed concern about the use of crypto to evade sanctions, and Bloomberg is reporting that the Biden administration is preparing an executive order on the topic this week. At least one big player in the cr[...]</div>	<div>CYWARE SOCIAL</div> <div>Cyware News - Latest Cyber News</div>	<div>Fraud detection and prevention costs merchants more than fraud itself</div> <div>European merchants spent nearly EUR7 billion (~\$7.7 billion) on fraud detection and prevention in 2021 alone - more than three times the value lost to fraud in the same year, CMSPI estimates.</div>
<div>CYWARE SOCIAL</div> <div>Cyware News - Latest Cyber News</div>	<div>Fresh flaws in Facebook Canvas earn bug bounty hunter a second payday</div> <div>Facebook's attempt at addressing the bug last year was found to be deficient. Researchers found three new flaws: a race conditions issue, a security bypass, and an issue involving encrypted parameters.</div>	<div>The Hacker News</div> <div>The Hacker News</div>	<div>Google Buys Cybersecurity Firm Mandiant for \$5.4 Billion</div> <div>Google is officially buying threat intelligence and incident response company Mandiant in an all-cash deal approximately valued at \$5.4 billion, the two technology firms announced Tuesday. Mandiant is expected to be folded into Google Cloud upon the closure of the acquisition, which is slated to happen later this year, adding to the latter's growing portfolio of security offerings such as</div>
<div>cyberscoop</div> <div>CyberScoop</div>	<div>Google has 'definitive agreement' to buy Mandiant for \$5.4B</div> <div>Mandiant, one of the cybersecurity industry's marquee names in threat intelligence and incident response, is being acquired by Google, the two companies said Tuesday. Google has a "definitive agreement" for an all-cash transaction worth about \$5.4 billion, the tech giant said in a news release. Mandiant will join the Google Cloud unit, specifically, with the goal of boosting its security offerings, the companies said. Existing Mandiant customers, meanwhile, will benefit from the reach of Google Cloud's lineup of products, partners and services, said Phil Venables, the chief information security officer for Google Cloud. But there are "a lot of decisions yet to be made about the precise struc[...]</div>	<div>Security Affairs</div> <div>Security Affairs</div>	<div>Google TAG: Russia, Belarus-linked APTs targeted Ukraine</div> <div>Google TAG observed Russian, Belarusian, and Chinese threat actors targeting Ukraine and European government and military orgs. Google Threat Analysis Group (TAG), which focuses on the analysis of nation-state threat actors, revealed to have blocked attacks against hundreds of Ukrainians conducted by Belarus and Russian state-sponsored hackers. The attacks have been attributed to the Russia-linked [...] The post Google TAG: Russia, Belarus-linked APTs targeted Ukraine appeared first on Security Affairs.</div>
<div>CYWARE SOCIAL</div> <div>Cyware News - Latest Cyber News</div>	<div>Google Warns of Russian Hackers Targeing Ukrainians, European Allies via Phishing Attacks</div> <div>A broad range of threat actors, including Fancy Bear, Ghostwriter, and Mustang Panda, have launched phishing campaigns against Ukraine, Poland, and other European entities amid Russia's invasion of Ukraine.</div>	<div>The Hacker News</div> <div>The Hacker News</div>	<div>Google: Russian Hackers Target Ukrainians, European Allies via Phishing Attacks</div> <div>A broad range of threat actors, including Fancy Bear, Ghostwriter, and Mustang Panda, have launched phishing campaigns against Ukraine, Poland, and other European entities amid Russia's invasion of Ukraine. Google's Threat Analysis Group (TAG) said it took down two Blogspot domains that were used by the nation-state group FancyBear (aka APT28) - which is attributed to Russia's GRU military</div>
<div>Krebs on Security</div> <div>Krebs on Security</div>	<div>Internet Backbone Giant Lumen Shuns .RU</div> <div>Lumen Technologies, an American company that operates one of the largest Internet backbones and carries a significant percentage of the world's Internet traffic, said today it will stop routing traffic for organizations based in Russia. Lumen's decision comes just days after a similar exit by backbone provider Cogent, and amid a news media crackdown in Russia that has already left millions of Russians in the dark about what is really going on with their president's war in Ukraine.</div>	<div>CYWARE SOCIAL</div> <div>Cyware News - Latest Cyber News</div>	<div>March 2022 Patch Tuesday: Microsoft fixes RCEs in RDP client, Exchange Server</div> <div>Microsoft's March 2022 Patch Tuesday introduced patches for 71 CVE-numbered vulnerabilities, including three previously unknown "critical" ones and three "important" ones that were already public.</div>
<div>threatpost</div> <div>Threatpost</div>	<div>Microsoft Addresses 3 Zero-Days & 3 Critical Bugs for March Patch Tuesday</div> <div>The computing giant patched 71 security vulnerabilities in an uncharacteristically light scheduled update, including its first Xbox bug.</div>	<div>Security Affairs</div> <div>Security Affairs</div>	<div>Microsoft March 2022 Patch Tuesday updates fix 89 vulnerabilities</div> <div>Microsoft March 2022 Patch Tuesday security updates address 89 vulnerabilities in multiple products, including 3 zero-days. Microsoft March 2022 Patch Tuesday security updates address 89 vulnerabilities in multiple products, including Microsoft Windows components, Azure and Azure DevOps, Azure Sphere, Internet Explorer and Edge (EdgeHTML), Exchange Server, Office and Office Services and Web Apps, SharePoint Server, [...] The post Microsoft March 2022 Patch Tuesday updates fix 89 vulnerabilities appeared first on Security Affairs.</div>
<div>CYWARE SOCIAL</div> <div>Cyware News - Latest Cyber News</div>	<div>Millions of APC Smart UPS Devices Can Be Remotely Hacked, Damaged</div> <div>UPS products made by Schneider Electric subsidiary APC are affected by critical vulnerabilities that can be exploited to remotely hack and damage devices, according to security company Armis.</div>	<div>The Hacker News</div> <div>The Hacker News</div>	<div>New 16 High-Severity UEFI Firmware Flaws Discovered in Millions of HP Devices</div> <div>Cybersecurity researchers on Tuesday disclosed 16 new high-severity vulnerabilities in various implementations of Unified Extensible Firmware Interface (UEFI) firmware impacting multiple HP enterprise devices. The shortcomings, which have CVSS scores ranging from 7.5 to 8.8, have been uncovered in HP's UEFI firmware. The variety of devices affected includes HP's laptops, desktops, point-of-sale</div>
<div>CYWARE SOCIAL</div> <div>Cyware News - Latest Cyber News</div>	<div>PROPHET SPIDER Exploits Citrix ShareFile Vulnerability to Deliver Webshell</div> <div>At the start of 2022, CrowdStrike found PROPHET SPIDER exploiting CVE-2021-22941 vulnerability impacting Citrix ShareFile Storage Zones Controller to compromise a Microsoft IIS web server.</div>	<div>Security Affairs</div> <div>Security Affairs</div>	<div>Ragnar Locker ransomware group breached at least 52 organizations across 10 critical infrastructure sectors</div> <div>The US FBI warns that the Ragnar Locker ransomware gang has breached the networks of at least 52 organizations from multiple US critical infrastructure sectors. The US Federal Bureau of Investigation (FBI) and CISA published a flash alert to warn that the Ragnar Locker ransomware gang has breached the networks of at least 52 organizations across [...] The post Ragnar Locker ransomware group breached at least 52 organizations across 10 critical infrastructure sectors appeared first on Security Affairs.</div>
<div>The Hacker News</div> <div>The Hacker News</div>	<div>Samsung Confirms Data Breach After Hackers Leak Galaxy Source Code</div> <div>Samsung on Monday confirmed a security breach that resulted in the exposure of internal company data, including the source code related to its Galaxy smartphones. "According to our initial analysis, the breach involves some source code relating to the operation of Galaxy devices, but does not include the personal information of our consumers or employees," the electronics giant told Bloomberg.</div>	<div>Security Affairs</div> <div>Security Affairs</div>	<div>Samsung data breach: Lapsus\$ gang stole Galaxy devices' source code</div> <div>Samsung confirmed that threat actors had access to the source code of its Galaxy smartphones in recent security breach. Samsung this week disclosed a data breach, threat actors had access to internal company data, including the source code of Galaxy models. Last week the Lapsus\$ ransomware gang claimed to have stolen a huge trove of sensitive data [...] The post Samsung data breach: Lapsus\$ gang stole Galaxy devices' source code appeared first on Security Affairs.</div>
<div>cyberscoop</div>			<div>The Cyberspace Solarium Commission pushed some major policies into law. So what now?</div>

	<p>Sharp rise in SMB cyberattacks by Russia and China</p> <p>There has been a sharp rise in activity from countries with consistently high levels of both attempted and successful attacks originating within their borders -- Russia and China.</p>	<p>CyberScoop</p> <p>A little more than a year removed from its role in advancing some of the most significant cybersecurity legislation ever enacted, the Cyberspace Solarium Commission is transforming into version 2.0 of itself. With some of its key recommendations now law -- such as the creation of the Office of the National Cyber Director in the White House -- the remnant of the congressionally created panel is turning its attention to tracking how those ideas are implemented, while studying some of the issues it didn't get to fully examine before releasing its final report. Those areas of study include protecting the water, maritime transport and health care sectors, as well as strengthening the federal and [...]</p>
 <p>Threatpost</p>	<p>The Uncertain Future of IT Automation</p> <p>While IT automation is growing, big challenges remain. Chris Hass, director of information security and research at Automox, discusses how the future looks.</p>	 <p>IT Security Guru</p> <p>TLStorm: Armis finds Three Critical Zero-Days in APC Smart-UPS devices that could impact over 7 in 10 organisations worldwide</p> <p>Armis, unified asset visibility and security company, announced the discovery of three zero-day vulnerabilities in APC Smart-UPS devices that can allow attackers to gain remote access. If exploited, these vulnerabilities, collectively known as TLStorm, allow threat actors to disable, disrupt, and even destroy APC Smart-UPS devices and attached assets, researchers have warned. Uninterruptible [...] The post TLStorm: Armis finds Three Critical Zero-Days in APC Smart-UPS devices that could impact over 7 in 10 organisations worldwide appeared first on IT Security Guru.</p>
 <p>Security Affairs</p>	<p>Ukraine's CERT-UA warns of phishing attacks against Ukrainian citizens</p> <p>Ukraine's CERT-UA warned citizens of new phishing attacks launched through compromised email accounts belonging to Indian entities. Ukraine's Computer Emergency Response Team (CERT-UA) is warning of new phishing attacks targeting Ukrainian citizens through compromised email accounts belonging to three different Indian entities. The attacks were aimed at stealing sensitive information from compromised accounts. The malicious [...] The post Ukraine's CERT-UA warns of phishing attacks against Ukrainian citizens appeared first on Security Affairs.</p>	 <p>Understanding US Defense Department's relaxed cybersecurity protocols under CMMC 2.0</p> <p>The DoD announced plans to release CMMC 2.0, with promises to streamline the certification process and ease security regulations for contractors and sub-contractors handling low-priority information.</p>
 <p>IC3.gov News</p>	<p>Unearned payments reported via IRS Form 1099</p>	 <p>Update: Samsung confirms Galaxy source code breach but says no customer information was stolen</p> <p>Samsung has now confirmed in a statement, without naming the hacking group, that there was a security breach, but it asserted that no personal information of customers was compromised.</p>
 <p>Threatpost</p>	<p>Zero-Click Flaws in Widely Used UPS Devices Threaten Critical Infrastructure</p> <p>The 'TLStorm' vulnerabilities, found in APC Smart-UPS products, could allow attackers to cause both cyber and physical damage by taking down critical infrastructure.</p>	

Twitter

 <p>Robo Shadow Alerts</p>	<p>Potentially Critical CVE Detected! CVE-2021-4039 Description: A command injection vulnerability in the web interface of the Zyxel NWA-1100-NH... CVSS: 9.48 #CVE #CyberSecurity #DataBreach</p>	 <p>CVE</p> <p>CVE-2021-4039 A command injection vulnerability in the web interface of the Zyxel NWA-1100-NH firmware could allow an attacker to execute arbitrary OS commands on the device.</p>
 <p>Threat Intel Center</p>	<p>NEW: CVE-2021-4039 A command injection vulnerability in the web interface of the Zyxel NWA-1100-NH firmware could allow an attacker to execute arbitrary OS commands on the device. Severity: CRITICAL</p>	 <p>Threat Intel Center</p> <p>NEW: CVE-2021-4039 A command injection vulnerability in the web interface of the Zyxel NWA-1100-NH firmware could allow an attacker to execute arbitrary OS commands on the device. Severity: CRITICAL</p>
 <p>Remotely Alerts</p>	<p>Severity: A command injection vulnerability in the... CVE-2021-4039 Link for more:</p>	 <p>Threat Intel Center</p> <p>NEW: CVE-2021-4039 A command injection vulnerability in the web interface of the Zyxel NWA-1100-NH firmware could allow an attacker to execute arbitrary OS commands on the device. Severity: CRITICAL</p>
 <p>RedPacket Security</p>	<p>Zyxel NWA-1100-NH command execution CVE-2021-4039 -</p>	 <p>ThreatMeter</p> <p>CVE-2021-4039 A command injection vulnerability in the web interface of the Zyxel NWA-1100-NH firmware could allow an attacker to execute arbitrary OS commands on the device. (CVSS:0.0) (Last Update:2022-03-01)</p>
 <p>vulnonym</p>	<p>My real name is CVE-2021-4039 but all my friends call me Unearthly Scup Rail</p>	 <p>Threat Intel Center</p> <p>NEW: CVE-2021-4039 A command injection vulnerability in the web interface of the Zyxel NWA-1100-NH firmware could allow an attacker to execute arbitrary OS commands on the device.</p>
 <p>CVE.report</p>	<p>CVE-2021-4039 : A command injection vulnerability in the web interface of the Zyxel NWA-1100-NH firmware could allow an attacker to execute arbitrary OS commands on the device....</p>	

Source: NIST

NIST CVE: Critical

CVE-2021-4039	<p>A command injection vulnerability in the web interface of the Zyxel NWA-1100-NH firmware could allow an attacker to execute arbitrary OS commands on the device.</p>
CRITICAL	<p>Vector: network</p> <p>Created: 2022-03-01</p> <p>Updated: 2022-03-09</p>

NIST CVE: High

CVE-2021-43619	Trusted Firmware M 1.4.x through 1.4.1 has a buffer overflow issue in the Firmware Update partition. In the IPC model, a psa_fwu_write caller from SPE or NSPE can overwrite stack memory locations. <div><div>HIGH</div>Vector: localCreated: 2022-03-01Updated: 2022-03-09</div>	CVE-2022-0777	Weak Password Recovery Mechanism for Forgotten Password in GitHub repository microweber/microweber prior to 1.3. <div><div>HIGH</div>Vector: networkCreated: 2022-03-01Updated: 2022-03-09</div>
----------------	---	---------------	--

NIST CVE: Medium

CVE-2021-44747	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Linux Security whereby the Fmlib component used in certain F-Secure products can crash while scanning fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service of the Anti-Virus engine. <div><div>MEDIUM</div>Vector: networkCreated: 2022-03-01Updated: 2022-03-09</div>	CVE-2022-0776	Cross-site Scripting (XSS) - DOM in GitHub repository hakimel/reveal.js prior to 4.3.0. <div><div>MEDIUM</div>Vector: networkCreated: 2022-03-01Updated: 2022-03-09</div>
----------------	--	---------------	---

NIST CVE: Low

Nothing today

NIST CVE: Unrated

CVE-2022-0881	Insecure Storage of Sensitive Information in GitHub repository chocobozzz/peertube prior to 4.1.1. <div><div>UNRATED</div>Vector: unkownCreated: 2022-03-09Updated: 2022-03-09</div>	CVE-2022-25943	The installer of WPS Office for Windows versions prior to v11.2.0.10258 fails to configure properly the ACL for the directory where the service program is installed. <div><div>UNRATED</div>Vector: unkownCreated: 2022-03-09Updated: 2022-03-09</div>
---------------	--	----------------	--

Top malicious files

100% Threat score	GoogleUpdate (.) exe	100% Threat score	3f052dcdd51d6e08fd7cc2bf9e60516120f66b241d6deb5f91c1669f554bbb26 (.) exe
100% Threat score	Priva_Metaupdaloader_Setup (.) exe	100% Threat score	RQF030922 (.) exe
100% Threat score	zhumuintl (.) exe	95% Threat score	20% 1x1"1œ1Y11Y1"1"1Y BIBMI BM20220209 2022 (.) 03 (.) 09_12 (.) 36 (.) 18_11P41±1P%o1P1@ (.) exe
90% Threat score	All-In-One Toolbox vv8 (.) 2 (.) 2 [Modded] (.) apk	89% Threat score	winge (.) exe
85% Threat score	thailand_pass (.) bat	85% Threat score	install (.) exe
80% Threat score	setup (.) exe	74% Threat score	POPULAIRE (.) exe










Top malicious URL

84% Threat score	http://www (.) pochontas895 (.) com/	83% Threat score	http://54 (.) 83 (.) 187 (.) 122/
82% Threat score	http://mocah (.) org/	77% Threat score	http://rosebudsawservice (.) com (.) au/
77% Threat score	http://go (.) identiv (.) com/	77% Threat score	http://gqzfc (.) smtpgaze (.) com/tracking/qaR9ZGLkZwp3AwDmZmplBQDmZQN4ZPM5qzS4qaR9ZQbjID
74% Threat score	https://bafybeieyo3hevfau6ja4qoncx7put4o64jc4z2wuz3qfipdhekytdmqn4 (.) ipfs (.) dweb (.) link/w2 (.) html	72% Threat score	http://www (.) tw-echen (.) com/
72% Threat score	http://figura (.) team/portfolio/projekt-konstrukji-wiaty-stalowej/		




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 Japan	 #10 Uruguay

Top spammers

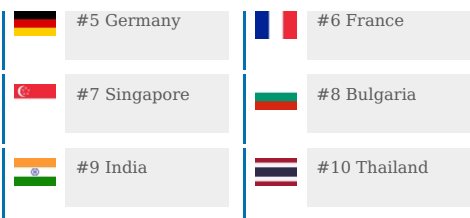
 #1 Canadian Pharmacy A long time running pharmacy spam operation. They send tens of millions of spams per day using botnet techniques. Probably based in Eastern Europe, Ukraine/Russia. Host spammed web sites on botnets and on bulletproof Chinese & Russian web hosting.	 #2 PredictLabs / Sphere Digital 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 Mint Global Marketing / Adgenics / Cabo Networks Florida affiliate spammers and bulletproof spam hosters
 #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 Michael Persaud Long time snowshoe type spammer, raided by FBI then indicted in 2017 on federal wire fraud charges tied to his spamming operations.
 #7 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.	 #8 RR Media A high volume spam operation based in or run from Huntington Beach, CA, USA. The operation uses a variety of different names.
 #9 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.	

Top countries with botnet

 #1 China	 #2 India
 #3 United States of America	 #4 Thailand
 #5 Indonesia	 #6 Algeria
 #7 Viet Nam	 #8 Brazil
 #9 Iran (Islamic Republic of)	 #10 Pakistan

Top phishing countries

 #1 United States	 #2 Iran
 #3 Russia	 #4 Netherlands



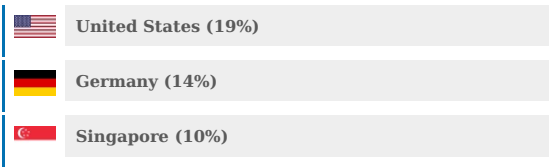
Source: [Have I been pwnd?](#)

Have I been pwnd

Nothing today

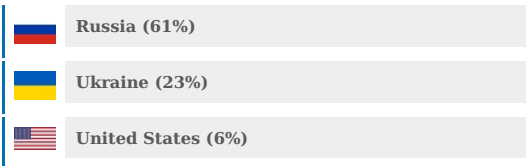
Source: [Imperva DDOS Map](#)

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

