



Your Security Rabbits report for March 30, 2022

Source: [Ransom Watch](#)















Ransomware attacks

























| | | | |
|-----------|-------------------------------|-----------|-------------------------------|
| conti | BANQUE CENTRALE DE TUNISIE | lockbit2 | bcad.org |
| cuba | bcintlgroup-com | blackbyte | Credit Risk Management Canada |
| blackbyte | GEBE | blackbyte | MZ Architects |
| lockbit2 | rebuildingt | cuba | trant-co-uk |
| conti | Automobil Holding AS | conti | Azimut Benetti Group |
| lorenz | Biz Retek | conti | Critical Content |
| conti | ITECOR International SA | hiveleak | PHC |
| conti | Royal Brunei Airlines Sdn Bhd | ransomexx | Stago |

Hot topics





Nothing today

News

| | | | |
|---|---|--|--|
|  Security Affairs | \$625M stolen from Axie Infinity 's Ronin bridge, the largest ever crypto hack Threat actors have stolen approximately \$625 million worth of Ethereum and USDC tokens from Axie Infinity 's Ronin network bridge. Threat actors have stolen almost \$625 million in Ethereum and USDC (a U.S. dollar pegged stablecoin) tokens from Axie Infinity's Ronin network bridge. The attack took place on March 23rd, but the cyber heist was [...] The post \$625M stolen from Axie Infinity 's Ronin bridge, the largest ever crypto hack appeared first on Security Affairs. |  Cyware News - Latest Cyber News | 2021 COVID bounce: Malware has returned with a vengeance According to Malwarebytes , there was a 77% increase in malware detections over 2020. Business-focused cyberthreats jumped 143%, while consumer-specific threats rose by 65% to more than 152 million in 2021. |
|  Cyware News - Latest Cyber News | An Ongoing Reply-Chain Hijacking Campaign Drops IcedID Researchers have detected a new conversation hijacking campaign that exploits unpatched Exchange servers to deliver IcedID trojan within the energy, healthcare, pharmaceutical, and legal sectors. It's been almost a year since the disclosure of ProxyShell vulnerabilities in Exchange servers but not many organizations, apparently, couldn't apply the patch. |  Cyware News - Latest Cyber News | Anonymous Hacks 2 Russian Industrial Firms, Leaks 112GB of Data for Ukraine The online hacktivist group Anonymous has claimed responsibility for targeting two Russian companies, MashOil and FID Group, stealing a trove of their data and leaking it online for the public to download. |
|  Blog @Flashpoint | Breach Forums Is Marketing Itself as a Raid Forums Successor Updated March 29, 2022:This post has been updated to reflect the most current understanding of Breach Forums, its user base, and operations. On March 16, just about three weeks after Raid Forums was seized, a threat actor named "pompompurin," previously highly active on Raid Forums, launched an alternative illicit hacking community called Breach Forums. In [...] The post Breach Forums Is Marketing Itself as a Raid Forums Successor appeared first on Flashpoint. |  Cyware News - Latest Cyber News | CISA Warns of Attacks Targeting Internet-connected UPS Devices In a joint advisory with the Department of Energy, the Cybersecurity and Infrastructure Security Agency (CISA) warned U.S. organizations today to secure Internet-connected UPS devices from ongoing attacks. |
|  The Hacker News | CISA Warns of Ongoing Cyber Attacks Targeting Internet-Connected UPS Devices The U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Energy (DoE) are jointly warning of attacks against internet-connected uninterruptible power supply (UPS) devices by means of default usernames and passwords. "Organizations can mitigate attacks against their UPS devices, which provide emergency power in a variety of applications when normal power sources are |  Security Affairs | Compromised WordPress sites launch DDoS on Ukrainian websites Threat actors compromised WordPress sites to deploy a script that was used to launch DDoS attacks, when they are visited, on Ukrainian websites. MalwareHunterTeam researchers discovered the malicious script on a compromised WordPress site, when the users were visiting the website the script launched a DDoS attack against ten Ukrainian sites. The JavaScript was designed [...] The post Compromised WordPress sites launch DDoS on Ukrainian websites appeared first on Security Affairs. |
|  Cyware News - Latest Cyber News | Consistency in password resets helps block credential theft As such, organizations should practice defense in depth. Filtering inbound email and removing phishing messages before they make it into a user's inbox is a critical first step, but that alone is not enough. |  CyberScoop | Coordinated phishing campaign targeted election officials in nine states, according to FBI This kind of activity is likely to continue or increase as the 2022 midterms approach, the FBI said. The post Coordinated phishing campaign targeted election officials in nine states, according to FBI appeared first on CyberScoop. |
|  The Hacker News | Critical SonicOS Vulnerability Affects SonicWall Firewall Appliances SonicWall has released security updates to contain a critical flaw across multiple firewall appliances that could be weaponized by an unauthenticated, remote attacker to execute arbitrary code and cause a denial-of-service (DoS) condition. Tracked as CVE-2022-22274 (CVSS score: 9.4), the issue has been described as a stack-based buffer overflow in the web management interface of SonicOS that |  The Hacker News | Critical Sophos Firewall RCE Vulnerability Under Active Exploitation Cybersecurity firm Sophos on Monday warned that a recently patched critical security vulnerability in its firewall product is being actively exploited in real-world attacks. The flaw, tracked as CVE-2022-1040, is rated 9.8 out of 10 on the CVSS scoring system and impacts Sophos Firewall versions 18.5 MR3 (18.5.3) and older. It relates to an authentication bypass vulnerability in the User Portal |
|  Cyware | Estonian Gets 66 Months for Ransomware Conspiracy Maksim Berezan, 37, was arrested in Latvia and extradited to the US, where he pleaded guilty in April 2021 to conspiracy to commit wire fraud affecting a |  WeLiveSecurity | Europe's quest for energy independence - and how cyber-risks come into play Soaring energy prices and increased geopolitical tensions amid the Russian invasion of Ukraine bring a sharp focus on European energy security The post |

| | | | |
|--|---|---|---|
|  | financial institution and conspiracy to commit access device fraud and computer intrusions. |  | Europe's quest for energy independence - and how cyber-risks come into play appeared first on WeLiveSecurity |
|  | Exchange Servers Speared in IcedID Phishing Campaign The ever-evolving malware shows off new tactics that use email thread hijacking and other obfuscation techniques to provide advanced evasion techniques. |  | FBI joins other intelligence agencies in warning about Russia The assistant director of the bureau's cyber division told lawmakers the FBI was doing its best to provide real-time updates to industry. The post FBI joins other intelligence agencies in warning about Russia appeared first on CyberScoop. |
|  | Hackers Gaining Power of Subpoena Via Fake "Emergency Data Requests" There is a terrifying and highly effective "method" that criminal hackers are now using to harvest sensitive customer data from Internet service providers, phone companies and social media firms. It involves compromising email accounts and websites tied to police departments and government agencies, and then sending unauthorized demands for subscriber data while claiming the information being requested can't wait for a court order because it relates to an urgent matter of life and death. |  | Hackers Gaining Power of Subpoena Via Fake "Emergency Data Requests" - Krebs on Security There is a terrifying and highly effective "method" that criminal hackers are now using to harvest sensitive customer data from Internet service providers, phone companies, and social media firms. |
|  | Hackers steal more than \$600M from Ronin blockchain used to play Axie Infinity It's one of the biggest crypto heists in history. The post Hackers steal more than \$600M from Ronin blockchain used to play Axie Infinity appeared first on CyberScoop. |  | Hackers Steal Over \$600 Million from Axie Infinity Developer's Ronin Bridge The Ronin bridge and Katana Dex have been halted after suffering an exploit for 173,600 Ethereum (ETH) and 25.5 million USD Coin (USDC), worth a combined \$612 million at Tuesday's prices. |
|  | LAPSUS\$ Claims to Have Breached IT Firm Globant; Leaks 70GB of Data The LAPSUS\$ data extortion gang announced their return on Telegram after a week-long "vacation," leaking what they claim is data from software services company Globant. "We are officially back from a vacation," the group wrote on their Telegram channel - which has nearly around 54,000 members as of writing - posting images of extracted data and credentials belonging to the company's DevOps |  | Lockbit Beats Conti and Ryuk in Encryption Speed Test A new study by Splunk has found that modern-day ransomware, such as LockBit, is capable of encrypting around 25,000 files in just one minute. The time window is so small that before an organization realizes the effect, the ransomware would have done its job. |
|  | Log4JShell Used to Swarm VMware Servers with Miners, Backdoors Researchers have found three backdoors and four miners in attacks exploiting the Log4Shell vulnerability, some of which are still ongoing. |  | Log4Shell exploited to infect VMware Horizon servers with backdoors, crypto miners Three backdoors and four miners have been detected in new attacks. |
|  | Mobile security firm Zimperium to be acquired by Steven Mnuchin's private equity group The former Treasury Secretary's Liberty Strategic Capital has made a string of investments in cybersecurity businesses. The post Mobile security firm Zimperium to be acquired by Steven Mnuchin's private equity group appeared first on CyberScoop. |  | Multiple E-commerce Stores Found Being Targeted Since 2020 Active since 2020, the campaign is a work of cybercriminal gangs from China. According to Seguranca Informatica, the campaign has targeted around 617 online stores located in Portugal, France, Spain, Italy, Chile, Mexico, Columbia, among others. |
|  | New Hacking Campaign by Transparent Tribe Hackers Targeting Indian Officials A threat actor of likely Pakistani origin has been attributed to yet another campaign designed to backdoor targets of interest with a Windows-based remote access trojan named CrimsonRAT since at least June 2021. "Transparent Tribe has been a highly active APT group in the Indian subcontinent," Cisco Talos researchers said in an analysis shared with The Hacker News. "Their primary targets have |  | New JSSLoader Variant Uses XLL Files to Evade Detection A new wave of JSSLoader infections, operated by the FIN7 threat group, was observed using XLL files to deliver the malware via malicious Microsoft Excel add-ins. The latest variant comes with some new layers of obfuscation to keep itself hidden from security analysts. Organizations need to have intrusion detection systems or intrusion prevention systems as a part of their security and protection strategy to thwart such threats. |
|  | Privid: A Privacy-Preserving Surveillance Video Analytics System A group of academics has designed a new system known as "Privid" that enables video analytics in a privacy-preserving manner to combat concerns with invasive tracking. "We're at a stage right now where cameras are practically ubiquitous. If there's a camera on every street corner, every place you go, and if someone could actually process all of those videos in aggregate, you can imagine that |  | School of Hard Knocks: Job Fraud Threats Target University Students Employment fraud typically impacts individuals, and the results can be costly. According to the FBI's Internet Crime Complaint center, the average reported loss from this type of scheme is \$3,000. |
|  | Steve Mnuchin's private equity firm buys Zimperium for \$525m Former US Treasury secretary Steve Mnuchin's private equity firm has announced its plans to buy a controlling stake in a mobile cybersecurity company for more than half a billion dollars. |  | Threat actors actively exploit recently fixed Sophos firewall bug Cybersecurity firm Sophos warned that the recently addressed CVE-2022-1040 flaw in Sophos Firewall is actively exploited in attacks. Sophos has recently fixed an authentication bypass vulnerability, tracked as CVE-2022-1040, that resides in the User Portal and Webadmin areas of Sophos Firewall. The CVE-2022-1040 flaw received a CVSS score of 9.8 and impacts Sophos Firewall versions 18.5 MR3 (18.5.3) and [...] The post Threat actors actively exploit recently fixed Sophos firewall bug appeared first on Security Affairs. |
|  | Transparent Tribe APT returns to strike India's government and military The development of custom malware indicates the group is trying to "compromise even more victims." |  | Ukraine destroys five bot farms that were spreading 'panic' among citizens Over 100,000 fake accounts were allegedly used to spread misinformation about Russia's invasion. |
|  | Wyze Cam flaw lets hackers remotely access your saved videos A Wyze Cam internet camera vulnerability allows unauthenticated, remote access to videos and images stored on local memory cards and has remained unfixed for almost three years. |  | Zlib data compressor fixes 17-year-old security bug - patch, errrm, now This code is venerable! Surely all the bugs must be out by now? |

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 |  | This man slept with a Chinese spy and is now giving cybersecurity tips. Please fact check me, @twitter[...] |
|  | 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. |  | The best #Indian #conferences for #womenintech in 2022 #fintech #cybersecurity @Analyticsindiam |

NIST CVE: Critical

Nothing today

Source: [NIST](#)

NIST CVE: High

Nothing today

Source: [NIST](#)

NIST CVE: Medium

Nothing today

Source: [NIST](#)

NIST CVE: Low

Nothing today

Source: [NIST](#)

NIST CVE: Unrated

| | | | |
|----------------|---|----------------|--|
| CVE-2022-27432 | <p>A Cross-Site Request Forgery (CSRF) in Pluck CMS v4.7.15 allows attackers to change the password of any given user by exploiting this feature leading to account takeover.</p> <p>UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-30</p> | CVE-2022-26244 | <p>A stored cross-site scripting (XSS) vulnerability in Hospital Patient Record Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the "special" field.</p> <p>UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-30</p> |
| CVE-2022-28206 | <p>An issue was discovered in MediaWiki through 1.37.1. ImportPlanValidator.php in the FileImporter extension mishandles the check for edit rights.</p> <p>UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-30</p> | CVE-2022-28205 | <p>An issue was discovered in MediaWiki through 1.37.1. The CentralAuth extension mishandles a ttl issue for groups expiring in the future.</p> <p>UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-30</p> |
| CVE-2022-28209 | <p>An issue was discovered in Mediawiki through 1.37.1. The check for the override-antispoof permission in the AntiSpoof extension is incorrect.</p> <p>UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-30</p> | CVE-2022-28202 | <p>An XSS issue was discovered in MediaWiki before 1.35.6, 1.36.x before 1.36.4, and 1.37.x before 1.37.2. The widthheight, widthheightpage, and nbytes properties of messages are not escaped when used in galleries or Special:RevisionDelete.</p> <p>UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-30</p> |
| CVE-2022-26951 | <p>Archer 6.x through 6.10 (6.10.0.0) contains a reflected XSS vulnerability. A remote SAML-unauthenticated malicious Archer user could potentially exploit this vulnerability by tricking a victim application user into supplying malicious HTML or JavaScript code to the vulnerable web application; the malicious code is then reflected back to the victim and gets executed by the web browser in the context of the vulnerable web application.</p> <p>UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-30</p> | CVE-2022-26950 | <p>Archer 6.x through 6.9 P2 (6.9.0.2) is affected by an open redirect vulnerability. A remote unprivileged attacker may potentially redirect legitimate users to arbitrary web sites and conduct phishing attacks. The attacker could then steal the victims' credentials and silently authenticate them to the Archer application without the victims realizing an attack occurred.</p> <p>UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-30</p> |
| CVE-2022-26949 | <p>Archer 6.x through 6.9 SP2 P1 (6.9.2.1) contains an improper access control vulnerability on attachments. A remote authenticated malicious user could potentially exploit this vulnerability to gain access to files that should only be allowed by extra privileges.</p> <p>UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-30</p> | CVE-2022-26947 | <p>Archer 6.x through 6.9 SP3 (6.9.3.0) contains a reflected XSS vulnerability. A remote authenticated malicious Archer user could potentially exploit this vulnerability by tricking a victim application user into supplying malicious HTML or JavaScript code to the vulnerable web application; the malicious code is then reflected back to the victim and gets executed by the web browser in the context of the vulnerable web application.</p> <p>UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-30</p> |
| CVE-2022-24693 | <p>Baicells Nova436Q and Neutrino 430 devices with firmware through QRTB 2.7.8 have hardcoded credentials that are easily discovered, and can be used by remote attackers to authenticate via ssh. (The credentials are stored in the firmware, encrypted by the crypt function.)</p> <p>UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-30</p> | CVE-2022-1163 | <p>Cross-site Scripting (XSS) - Stored in GitHub repository mineweb/minewebcms prior to next.</p> <p>UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-30</p> |
| CVE-2021-41594 | <p>In RSA Archer 6.9.SP1 P3, if some application functions are precluded by the Administrator, this can be bypassed by intercepting the API request at the /api/V2/internal/TaskPermissions/CheckTaskAccess endpoint. If the parameters of this request are replaced with empty fields, the attacker achieves access to the precluded functions.</p> <p>UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-30</p> | CVE-2020-24771 | <p>Incorrect access control in NexusPHP 1.5.beta5.20120707 allows unauthorized attackers to access published content.</p> <p>UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-30</p> |
| CVE-2020-24770 | <p>SQL injection vulnerability in modrules.php in NexusPHP 1.5 allows remote attackers to execute arbitrary SQL commands via the id parameter.</p> <p>UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-30</p> | CVE-2020-24769 | <p>SQL injection vulnerability in takeconfirm.php in NexusPHP 1.5 allows remote attackers to execute arbitrary SQL commands via the classes parameter.</p> <p>UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-30</p> |
| CVE-2022-27815 | <p>SWHKD 1.1.5 unsafely uses the /tmp/swhkd.pid pathname. There can be an information leak or denial of service.</p> <p>UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-30</p> | CVE-2022-27816 | <p>SWHKD 1.1.5 unsafely uses the /tmp/swhks.pid pathname. There can be data loss or a denial of service.</p> <p>UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-30</p> |
| CVE-2022-26948 | <p>The Archer RSS feed integration for Archer 6.x through 6.9 SP1 (6.9.1.0) is affected by an insecure credential storage vulnerability. A malicious attacker may obtain access to credential information to use it in further attacks.</p> <p>UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-30</p> | CVE-2015-3298 | <p>Yubico ykneo-openpgp before 1.0.10 has a typo in which an invalid PIN can be used. When first powered up, a signature will be issued even though the PIN has not been validated.</p> <p>UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-30</p> |
| | | | |

CVE-2018-25032

zlib before 1.2.12 allows memory corruption when deflating (i.e., when compressing) if the input has many distant matches.

UNRATED

Vector: unkown

Created: 2022-03-25

Updated: 2022-03-30

Source: Hybrid Analysis

Top malicious files

| | | | |
|----------------------|---|----------------------|-------------------|
| 100% Threat score | PI-09876542345.exe | 100% Threat score | webPrepare_nl.exe |
| 100% Threat score | Server.exe | 100% Threat score | Server.exe |
| 100% Threat score | KMSTools.exe | 100% Threat score | tmpqu80oezz |
| 100% Threat score | tmpmlcyk5rq | 100% Threat score | tmpazb5rtzm |
| 100% Threat score | tmpf7fpbtdw | 100% Threat score | tmpwhvc3g6c |
| 100% Threat score | tmpokwi8lin | 100% Threat score | hwi_722.exe |
| 100% Threat score | esfdbcv.exe | 100% Threat score | cvdb.dll |
| 100% Threat score | Nodulation.exe | 100% Threat score | palqisidaiu.xlsb |
| 91% Threat score | rundll32.exe | 89% Threat score | s6.dll |
| 84% Threat score | tmp5sahwqb6 | 84% Threat score | OOSU10.exe |
| 80% Threat score | Key2 Vehicle Management.lnk | 80% Threat score | MobiriseSetup.exe |
| 75% Threat score | By_Click_Downloader_Premium_v2.3.25.exe | | |



Source: Hybrid Analysis

Top malicious URL

| | | | |
|----------------------|---|----------------------|---|
| 100% Threat score | http://r.sender.mea-finance.com/mk/un/v2/cvTn4Gr-2l7DUTpLdGmBEUHWsjcyO8N8p6m_b3q7-_6_b_LPVTWTRbDE84YHeNFL77J4XTetU85ZoFCkErjzyM5Y17zKvrCGplOUNbugG9v4mN_mi5Nt8kS4RmwXxUJ-m_avj67wssscOFcmWqNk388w5mso4MgjFPxqzilz8 | 100% Threat score | https://gabrielcarranza |
| 100% Threat score | http://www.meonhanong.com/bins/dd1.jpg | 100% Threat score | http://www.meonhanon |
| 97% Threat score | http://emporiumbrewing.ca/css/MKEFbAtccjpJGr0MZPLu33b/ | 95% Threat score | http://sgtm.eventdecor |
| 90% Threat score | https://pt-luactivation.weebly.com/ | 86% Threat score | https://urldefense.com/v3/_l=20_%3B%21%21J8jlxA%21YzIgSjZMloMNu |
| 86% Threat score | https://urldefense.com/v3/_http://www.hpdocument.com/8f2995fe2c5db215?l=34_%3B%21%21J8jBlt3-xA%21drYwzsMYWXRh6pwz1im59ymGaUGFpc0lUVxPgc6KPdXKjcB9kbQnpVCijM5MZPXVLA%24 | 86% Threat score | https://urldefense.com/v3/_l=34_%3B%21%21J8jlxA%21ceGKI9AUo2h3F |
| 84% Threat score | http://documentarytickletop/Rosseti/tb.php?lcarxdie1648610687652 | 82% Threat score | http://try.eventdecordin |
| 82% Threat score | http://r.sender.mea-finance.com/mk/cl/f/9NAb2ldDDywwqFRi3xa_MZQ6juz3VeulGflnhZhGGZUrYZTLmvsqpphL-KadlKShLedrZlaA7s2nH8ypj7JEMcJe4ibV-W3kS9XwBbDOv9h4OuktSDtjKd5CTLFz81QHpACps9x5ZzZN-VyYfGy2M8HAXwufMSsui97z7DHZJBPMrCabhwoCU8zxuYqROFPHEV5SvCDLnczeztBHF0dIlldmUs0XiKfVCr7wUsgQMPfvId8qj0ZSa58VWF6g | 82% Threat score | http://el.email.eventdec |
| 81% Threat score | http://18.179.111.240/1b1/loader/uploads/QLT0208220167_Zsirkors.bmp | 77% Threat score | http://rei.theflybook.cor |
| 77% Threat score | http://auth.theflybook.com/ | 77% Threat score | http://rover.org/ |
| 75% Threat score | http://r.sender.mea-finance.com/mk/ | 74% Threat score | https://lacapitaldelsol.clatino/ |
| 72% Threat score | https://bit.ly/3IIV6ki | 72% Threat score | https://bit.ly/3LijDhZ |
| 72% Threat score | http://www.thinkfon-tech.de/ | 72% Threat score | http://www.ib-solution.e |
| | | | |










Source: SpamHaus

Top spamming countries

| | |
|---|---|
|  #1 United States of America |  #2 China |
|  #3 Russian Federation |  #4 Mexico |
|  #5 Dominican Republic |  #6 Saudi Arabia |
|  #7 India |  #8 Uruguay |
|  #9 Brazil |  #10 Japan |


Source: SpamHaus

Top spammers

| | |
|--|---|
|  #1 Canadian Pharmacy A long time running pharmacy spam operation. They send tens of millions of spams per day using botnet techniques. Probably based in Eastern Europe, Ukraine/Russia. Host spammed web sites on botnets and on bulletproof Chinese & Russian web hosting. |  #2 PredictLabs / Sphere Digital This operation uses dozens of "hosting" companies as fronts to lease IP addresses which are then used to send spam. Based in Chicago, Illinois and Tangier, Morocco. |
|  #3 Hosting Response / Michael Boehm Snowshoe spam organization that uses large numbers of inexpensive, automated VPS hosting IP addresses and domains in whatever TLD is currently cheapest to send high volumes of spam to extremely dirty, scraped lists. Operates under many business and individual names. Owner or manager of these companies seems to be Michael Boehm and Associates. |  #4 Michael Persaud Long time snowshoe type spammer, raided by FBI then indicted in 2017 on federal wire fraud charges tied to his spamming operations. |
|  #5 RetroCubes Web development, application development, and business training company that spams email appended lists, usually through ESPs that offer automated provisioning and services directed at small businesses. |  #6 Cyber World Internet Services/ e-Insites Bulletproof spam host operating Cyber World Internet Services / e-Insites, and currently spamming using a variety of aliases such as Brand 4 Marketing, Ad Media Plus, Site Traffic Network, RCM Delivery, and eBox. The company is owned or managed by Alvin Slocombe. |
|  #7 RR Media A high volume spam operation based in or run from Huntington Beach, CA, USA. The operation uses a variety of different names. |  #8 Kobeni Solutions High volume snowshoe spam operation based in Florida. The manager or owner of the company seems to be a Yair Shalev / . (Former?) partner-in-spam of ROKSO spammer Darrin Wohl. Son-in-law of ROKSO-listed spammer Dan Abramovich. Sued for fraud by the US FTC in 2014. |
|  #9 Richpro Trade Inc. / Richvestor GmbH Uses botnets or hires botnet spammers to send spam linking back to suspect investment, "quack-health-cures" and other sites that he owns or is an affiliate of. Botnet spamming and hosting sites on hacked servers is fully criminal in much of the world. Managed or owned by a Timo Richert. | |







Source: SpamHaus


Top countries with botnet

| | |
|---|--|
|  #1 China |  #2 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 Japan |
|  #3 Germany |  #4 United Kingdom |
|  #5 Russia |  #6 Netherlands |

| | | | |
|--|--------------|--|---------------|
|  | #7 Singapore |  | #8 Finland |
|  | #9 India |  | #10 Hong Kong |




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

Have I been pwned

Nothing today




Source: [Imperva DDOS Map](#)

Top DDOS attackers

| | |
|---|---------------------|
|  | United States (28%) |
|  | Russia (21%) |
|  | Germany (10%) |

Source: [Imperva DDOS Map](#)

Top DDOS country targets

| | |
|---|---------------------|
|  | Russia (52%) |
|  | Ukraine (19%) |
|  | United States (13%) |

Source: [Imperva DDOS Map](#)

Top DDOS techniques

| | |
|-----|------------------|
| 71% | DDoS |
| 19% | Automated Threat |
| 9% | OWASP |

Source: [Imperva DDOS Map](#)

Top DDOS industry targets

| | |
|-----|--------------------|
| 59% | Financial Services |
| 24% | Business |
| 4% | Computing & IT |