



## Your Security Rabbits report for April 11, 2022

Source: [Ransom Watch](#)













### Ransomware attacks


cllop	JDAVIDTAXLAW.COM	lockbit2	tokyo-plant.co,...
cllop	THENOC.NET	cllop	SSMSJUSTICE.COM
lockbit2	ruthtaubman.com	cllop	OAKDELL.COM
conti	MARTINELLI GINETTO	cllop	FAIR-RITE.COM
conti	Eminox	cllop	DRIVEANDSHINE.COM
lockbit2	farmaciastatuto...	lockbit2	groupemeunier.c...
cllop	JBINSTANTLAWN.NET	cllop	AFJCONSULTING.NET
lockbit2	lerros.com	lockbit2	lo
cllop	ORBITELECTRIC.COM	conti	Snap-on Incorporated
cllop	DRC-LAW.COM	cllop	CAPCARPET.COM
cllop	ALTERNATIVETECHS.COM		

### Hot topics














*Nothing today*

### News

 CYWARE SOCIAL Cyware News - Latest Cyber News	<a href="#">Accounts Deceivable: Email Scam Costliest Type of Cybercrime</a> The huge payoffs and low risks associated with BEC scams have attracted criminals worldwide. Some flaunt their ill-gotten riches on social media, posing in pictures next to Ferraris, Bentleys, and stacks of cash.	 CYWARE SOCIAL Cyware News - Latest Cyber News	<a href="#">Analyzing the Exploitation of Spring4Shell Vulnerability in Weaponizing and Executing the Mirai Botnet Malware</a> Trend Micro Threat Research observed active exploitation of the Spring4Shell vulnerability assigned as CVE-2022-22965, which allows malicious actors to weaponize and execute the Mirai botnet malware.
 Security Affairs	<a href="#">Apr 03 - Apr 09 Ukraine - Russia the silent cyber conflict</a> This post provides a timeline of the events related to the Russian invasion of Ukraine from the cyber security perspective. Below is the timeline of the events related to the ongoing invasion of Ukraine that occurred in the previous weeks: April 8 - Anonymous and the IT ARMY of Ukraine continue to target Russian entities [...] The post Apr 03 - Apr 09 Ukraine - Russia the silent cyber conflict appeared first on Security Affairs.	 Security Affairs	<a href="#">Dependency Review GitHub Action prevents adding known flaws in the code</a> Dependency Review GitHub Action scans users' pull requests for dependency changes and will raise an error if any new dependencies have existing flaws. GitHub announced Dependency Review GitHub Action which scans users' pull requests for dependency changes and will raise an error if any new dependencies have existing flaws that can be exploited in supply [...] The post Dependency Review GitHub Action prevents adding known flaws in the code appeared first on Security Affairs.
 CYWARE SOCIAL Cyware News - Latest Cyber News	<a href="#">Eavesdropping scam: A new scam call tactic</a> Hiya has detected the newest scam call tactic, the eavesdropping scam. The new scam aims to get users to call back by leaving vague voicemail messages where an unknown voice is heard talking about the potential victim.	 CYWARE SOCIAL Cyware News - Latest Cyber News	<a href="#">Ensign unveils cybersecurity employment scheme for individuals with autism</a> The collaboration aimed to create career opportunities by identifying and training suitable individuals for the industry, said the cybersecurity vendor in a statement Friday.
 IT Security Guru	<a href="#">Fraudsters stole PS58m with RATs in 2021</a> 2021 saw victims of Remote Access Tool (RAT)scams lost PS58m in 2021, official UK police figures show. RAT scams involve scammers taking control of a victims device, typically in order to access bank accounts. Some 20,144 victims fell for this type of scam in 2021, averaging around PS2800 stolen per incident. Typically, RAT attacks begin [...] The post Fraudsters stole PS58m with RATs in 2021 appeared first on IT Security Guru.	 CYWARE SOCIAL Cyware News - Latest Cyber News	<a href="#">Hackers use Conti's leaked ransomware to attack Russian companies</a> For the past month, a hacking group known as NB65 has been breaching Russian entities, stealing their data, and leaking it online, warning that the attacks are due to Russia's invasion of Ukraine.
 CYWARE SOCIAL Cyware News - Latest Cyber News	<a href="#">Human activated risk still a pain point for organizations</a> Egress announced the results of a report, which revealed that 56% of IT leaders say that their non-technical staff is only 'somewhat' prepared, or 'not at all' prepared, for a security attack.	 IT Security Guru	<a href="#">Microsoft announces new Autopatch feature</a> Microsoft announced last week that it will make generally available a feature dubbed "Autopatch" included in Windows Enterprise E3 in July 2022. Lior Bela, senior product marketing manager at Microsoft, said in a post last week: "This service will keep Windows and Office software on enrolled endpoints up-to-date automatically, at no additional cost. The second [...] The post Microsoft announces new Autopatch feature appeared first on IT Security Guru.
 The Hacker News	<a href="#">Microsoft's New Autopatch Feature to Help Businesses Keep Their Systems Up-to-Date</a> Microsoft last week announced that it intends to make generally available a feature called Autopatch as part of Windows Enterprise E3 in July 2022. "This service will keep Windows and Office software on enrolled endpoints up-to-date automatically, at no additional cost," said Lior Bela, senior product marketing manager at Microsoft, in a post last week. "The second Tuesday of every month	 CYWARE SOCIAL Cyware News - Latest Cyber	<a href="#">Raspberry Pi removes default user to hinder brute-force attacks</a> An update to Raspberry Pi OS Bullseye has removed the default 'pi' user to make it harder for attackers to find and compromise Internet-exposed Raspberry Pi devices using default credentials.

	will be	News	
 Security Affairs	<b>Securing Easy Appointments and earning CVE-2022-0482</b> Easy Appointments contained a very dangerous Broken Access Control vulnerability tracked as CVE-2022-0482 that was exposing PII. Another day, another threat to your data. The recently discovered CVE-2022-0482 is a Broken Access Control vulnerability affecting Easy Appointments, a popular open-source web app written in PHP, used by thousands of sites to manage their online bookings. [...] The post Securing Easy Appointments and earning CVE-2022-0482 appeared first on Security Affairs.		

Twitter

 TDCT	CVE-2022-0452: La vulnerabilidad permite que un atacante remoto comprometa un sistema vulnerable.	 TDCT	Mltiples vulnerabilidades en Microsoft Edge: CVE-2022-0459 CVE-2022-23262 CVE-2022-23263 CVE-2022-0452 CVE-2022-0453 CVE-2022-0454 CVE-2022-0455 CVE-2022-0456 CVE-2022-0457 CVE-2022-0458
 RedPacket Security	Google Chrome Safe Browsing code execution   CVE-2022-0452 -	 SRM IT Risk	IT Risk: Microsoft.Multiple Vulnerabilities in Edge (Chromium-based) -2/3 CVE-2022-0462 CVE-2022-0470 CVE-2022-0469 CVE-2022-0468 CVE-2022-0467 CVE-2022-0466 CVE-2022-0465 CVE-2022-0464 CVE-2022-0463 CVE-2022-0461 CVE-2022-0452 CVE-2022-0452 CVE-2022-0460 CVE-2022-0459 CVE-2022-0458 CVE-2022-0457 CVE-2022-0456 CVE-2022-0455 CVE-2022-0454
 kawn	#microsoftupdate #securityupdate #Edge Microsoft Edge Stable Channel (Version 98.0.1108.43) CVE 22 CVE-2022-0452 CVE-2022-0470 CVE-2022-23261 CVE-2022-23263	 SRM IT Risk	IT Risk: Google.Multiple Vulnerabilities in Chrome -2/3 CVE-2022-0462 CVE-2022-0470 CVE-2022-0469 CVE-2022-0468 CVE-2022-0467 CVE-2022-0466 CVE-2022-0465 CVE-2022-0464 CVE-2022-0463 CVE-2022-0461 CVE-2022-0452 CVE-2022-0460 CVE-2022-0459 CVE-2022-0458
 SRM IT Risk	IT Risk: -2/3 CVE-2022-0469 CVE-2022-0468 CVE-2022-0467 CVE-2022-0466 CVE-2022-0465 CVE-2022-0464 CVE-2022-0463 CVE-2022-0461 CVE-2022-0452 CVE-2022-0460 CVE-2022-0459 CVE-2022-0458 CVE-2022-0457 CVE-2022-0456 CVE-2022-0455 CVE-2022-0454	 manabu2111	27Google Chrome98 - PC Watch @pc_watch (CVE-2022-0452High)
 SRM IT Risk	IT Risk: Microsoft.Edge (Chromium-based) -2/2 CVE-2022-0467 CVE-2022-0466 CVE-2022-0465 CVE-2022-0464 CVE-2022-0463 CVE-2022-0461 CVE-2022-0452 CVE-2022-0460 CVE-2022-0459 CVE-2022-0458 CVE-2022-0457 CVE-2022-0456 CVE-2022-0455 CVE-2022-0454 CVE-2022-0453	 vigilance on	Vigil@nce #Vulnerability of Chrome: multiple vulnerabilities. Identifiers: #CVE-2022-0789, #CVE-2022-0790, #CVE-2022-0791. #alert
 RedPacket Security	Google Chrome Cast UI code execution   CVE-2022-0790 -	 CVE report	CVE-2022-0790 : Use after free in Cast UI in Google Chrome prior to 99.0.4844.51 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially perform a sandbox escape via a crafted HTML page....
 Watcher.Guru	JUST IN: Florida police have arrested a cybersecurity expert who allegedly stole \$576,000 in #cryptocurrency from a client's hardware wallet after promising to set up a security system.		

Source: NIST

NIST CVE: Critical

CVE-2022-0790	Use after free in Cast UI in <b>Google Chrome</b> prior to 99.0.4844.51 allowed a remote attacker who convinced a user to <b>engage</b> in specific user interaction to potentially perform a sandbox escape via a crafted HTML page. <b>CRITICAL</b> Vector: <b>network</b> Created: 2022-04-05 Updated: 2022-04-11	CVE-2022-0452	Use after free in <b>Safe</b> Browsing in <b>Google Chrome</b> prior to 98.0.4758.80 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. <b>CRITICAL</b> Vector: <b>network</b> Created: 2022-04-05 Updated: 2022-04-11
---------------	---	---------------	---

Source: NIST

NIST CVE: High

CVE-2022-28390	ems_usb_start_xmit in drivers/net/can/usb/ems_usb.c in the <b>Linux</b> kernel through 5.17.1 has a double free. <b>HIGH</b> Vector: <b>local</b> Created: 2022-04-03 Updated: 2022-04-11	CVE-2022-0800	Heap buffer overflow in Cast UI in <b>Google Chrome</b> prior to 99.0.4844.51 allowed a remote attacker who convinced a user to <b>engage</b> in specific user interaction to potentially exploit heap corruption via a crafted HTML page. <b>HIGH</b> Vector: <b>network</b> Created: 2022-04-05 Updated: 2022-04-11
CVE-2022-0610	Inappropriate implementation in Gamepad API in <b>Google Chrome</b> prior to 98.0.4758.102 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. <b>HIGH</b> Vector: <b>network</b> Created: 2022-04-05 Updated: 2022-04-11	CVE-2022-0799	Insufficient policy enforcement in Installer in <b>Google Chrome</b> on <b>Windows</b> prior to 99.0.4844.51 allowed a remote attacker to perform local privilege escalation via a crafted offline installer file. <b>HIGH</b> Vector: <b>network</b> Created: 2022-04-05 Updated: 2022-04-11
CVE-2022-28389	mcba_usb_start_xmit in drivers/net/can/usb/mcba_usb.c in the <b>Linux</b> kernel through 5.17.1 has a double free. <b>HIGH</b> Vector: <b>local</b> Created: 2022-04-03 Updated: 2022-04-11	CVE-2022-0797	Out of bounds memory access in Mojo in <b>Google Chrome</b> prior to 99.0.4844.51 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. <b>HIGH</b> Vector: <b>network</b> Created: 2022-04-05 Updated: 2022-04-11
CVE-2022-0470	Out of bounds memory access in V8 in <b>Google Chrome</b> prior to 98.0.4758.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. <b>HIGH</b> Vector: <b>network</b> Created: 2022-04-05 Updated: 2022-04-11	CVE-2022-0795	Type confusion in <b>Blink</b> Layout in <b>Google Chrome</b> prior to 99.0.4844.51 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. <b>HIGH</b> Vector: <b>network</b> Created: 2022-04-05 Updated: 2022-04-11
CVE-2022-0457	Type confusion in V8 in <b>Google Chrome</b> prior to 98.0.4758.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. <b>HIGH</b> Vector: <b>network</b> Created: 2022-04-05 Updated: 2022-04-11	CVE-2022-28388	usb_8dev_start_xmit in drivers/net/can/usb/usb_8dev.c in the <b>Linux</b> kernel through 5.17.1 has a double free. <b>HIGH</b> Vector: <b>local</b> Created: 2022-04-03 Updated: 2022-04-11

CVE-2022-0805	Use after free in Browser Switcher in <b>Google Chrome</b> prior to 99.0.4844.51 allowed a remote attacker who convinced a user to <b>engage</b> in specific user interaction to potentially exploit heap corruption via user interaction.  <b>HIGH</b> Vector: <b>network</b> Created: 2022-04-05 Updated: 2022-04-11
CVE-2022-0796	Use after free in Media in <b>Google Chrome</b> prior to 99.0.4844.51 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  <b>HIGH</b> Vector: <b>network</b> Created: 2022-04-05 Updated: 2022-04-11
CVE-2022-0791	Use after free in Omnibox in <b>Google Chrome</b> prior to 99.0.4844.51 allowed a remote attacker who convinced a user to <b>engage</b> in specific user interactions to potentially exploit heap corruption via user interactions.  <b>HIGH</b> Vector: <b>network</b> Created: 2022-04-05 Updated: 2022-04-11
CVE-2022-0794	Use after free in WebShare in <b>Google Chrome</b> prior to 99.0.4844.51 allowed a remote attacker who convinced a user to <b>engage</b> in specific user interaction to potentially exploit heap corruption via a crafted HTML page.  <b>HIGH</b> Vector: <b>network</b> Created: 2022-04-05 Updated: 2022-04-11

Source: *NIST*

**NIST CVE: Medium**

CVE-2021-36826	Authenticated (subscriber or higher <b>user role</b> if allowed to access projects) Stored Cross-Site Scripting (XSS) vulnerability in <b>weDevs</b> WP Project Manager (WordPress plugin) versions <= 2.4.13.  <b>MEDIUM</b> Vector: <b>network</b> Created: 2022-04-04 Updated: 2022-04-11
CVE-2022-0807	Inappropriate implementation in Autofill in <b>Google Chrome</b> prior to 99.0.4844.51 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.  <b>MEDIUM</b> Vector: <b>network</b> Created: 2022-04-05 Updated: 2022-04-11
CVE-2022-0802	Inappropriate implementation in Full <b>screen</b> mode in <b>Google Chrome</b> on <b>Android</b> prior to 99.0.4844.51 allowed a remote attacker to <b>hide</b> the contents of the Omnibox (URL bar) via a crafted HTML page.  <b>MEDIUM</b> Vector: <b>network</b> Created: 2022-04-05 Updated: 2022-04-11
CVE-2022-0803	Inappropriate implementation in Permissions in <b>Google Chrome</b> prior to 99.0.4844.51 allowed a remote attacker to tamper with the contents of the Omnibox (URL bar) via a crafted HTML page.  <b>MEDIUM</b> Vector: <b>network</b> Created: 2022-04-05 Updated: 2022-04-11

Source: *NIST*

**NIST CVE: Low**

*Nothing today*

Source: *NIST*

**NIST CVE: Unrated**

CVE-2021-43009	A Cross Site Scripting (XSS) vulnerability exists in <b>OpServices OpMon</b> through 9.11 via the search parameter in the request URL.  <b>UNRATED</b> Vector: <b>unkown</b> Created: 2022-04-08 Updated: 2022-04-11
CVE-2021-32162	A Cross-site request forgery (CSRF) vulnerability exists in <b>Webmin</b> 1.973 through the <b>File Manager</b> feature.  <b>UNRATED</b> Vector: <b>unkown</b> Created: 2022-04-11 Updated: 2022-04-11
CVE-2021-32159	A Cross-site request forgery (CSRF) vulnerability exists in <b>Webmin</b> 1.973 via the Upload and Download feature.  <b>UNRATED</b> Vector: <b>unkown</b> Created: 2022-04-11 Updated: 2022-04-11
CVE-2022-27961	A cross-site scripting (XSS) vulnerability at /ofcms/company-c-47 in OFCMS v1.1.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Comment text box.  <b>UNRATED</b> Vector: <b>unkown</b> Created: 2022-04-10 Updated: 2022-04-11
CVE-2021-32161	A Cross-Site Scripting (XSS) vulnerability exists in <b>Webmin</b> 1.973 through the <b>File Manager</b> feature.  <b>UNRATED</b> Vector: <b>unkown</b> Created: 2022-04-11 Updated: 2022-04-11
CVE-2021-32158	A Cross-Site Scripting (XSS) vulnerability exists in <b>Webmin</b> 1.973 via

CVE-2022-0607	Use after free in GPU in <b>Google Chrome</b> prior to 98.0.4758.102 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  <b>HIGH</b> Vector: <b>network</b> Created: 2022-04-05 Updated: 2022-04-11
CVE-2022-0798	Use after free in MediaStream in <b>Google Chrome</b> prior to 99.0.4844.51 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension.  <b>HIGH</b> Vector: <b>network</b> Created: 2022-04-05 Updated: 2022-04-11
CVE-2022-0459	Use after free in <b>Screen</b> Capture in <b>Google Chrome</b> prior to 98.0.4758.80 allowed a remote attacker who had compromised the renderer process and convinced a user to <b>engage</b> in specific user interaction to potentially exploit heap corruption via a crafted HTML page.  <b>HIGH</b> Vector: <b>network</b> Created: 2022-04-05 Updated: 2022-04-11
CVE-2022-0605	Use after free in Webstore API in <b>Google Chrome</b> prior to 98.0.4758.102 allowed an attacker who convinced a user to install a malicious extension and convinced a user to enage in specific user interaction to potentially exploit heap corruption via a crafted HTML page.  <b>HIGH</b> Vector: <b>network</b> Created: 2022-04-05 Updated: 2022-04-11

CVE-2022-0806	Data leak in <b>Canvas</b> in <b>Google Chrome</b> prior to 99.0.4844.51 allowed a remote attacker who convinced a user to <b>engage</b> in <b>screen</b> sharing to potentially leak cross-origin data via a crafted HTML page.  <b>MEDIUM</b> Vector: <b>network</b> Created: 2022-04-05 Updated: 2022-04-11
CVE-2022-0455	Inappropriate implementation in Full <b>Screen</b> Mode in <b>Google Chrome</b> on <b>Android</b> prior to 98.0.4758.80 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.  <b>MEDIUM</b> Vector: <b>network</b> Created: 2022-04-05 Updated: 2022-04-11
CVE-2022-0804	Inappropriate implementation in Full <b>screen</b> mode in <b>Google Chrome</b> on <b>Android</b> prior to 99.0.4844.51 allowed a remote attacker to <b>hide</b> the contents of the Omnibox (URL bar) via a crafted HTML page.  <b>MEDIUM</b> Vector: <b>network</b> Created: 2022-04-05 Updated: 2022-04-11

CVE-2022-26588	A Cross-Site Request Forgery (CSRF) in <b>IceHrm</b> 31.0.0.OS allows attackers to delete arbitrary users or achieve account takeover via the app/service.php URI.  <b>UNRATED</b> Vector: <b>unkown</b> Created: 2022-04-08 Updated: 2022-04-11
CVE-2021-32156	A cross-site request forgery (CSRF) vulnerability exists in <b>Webmin</b> 1.973 via the Scheduled <b>Cron</b> Jobs feature.  <b>UNRATED</b> Vector: <b>unkown</b> Created: 2022-04-11 Updated: 2022-04-11
CVE-2022-27476	A cross-site scripting (XSS) vulnerability at /admin/goods/update in <b>Newbee-Mall</b> v1.0.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the goodsName parameter.  <b>UNRATED</b> Vector: <b>unkown</b> Created: 2022-04-10 Updated: 2022-04-11
CVE-2021-32160	A Cross-Site Scripting (XSS) vulnerability exists in <b>Webmin</b> 1.973 through the Add Users feature.  <b>UNRATED</b> Vector: <b>unkown</b> Created: 2022-04-11 Updated: 2022-04-11
CVE-2021-32157	A Cross-Site Scripting (XSS) vulnerability exists in <b>Webmin</b> 1.973 via the Scheduled <b>Cron</b> Jobs feature.  <b>UNRATED</b> Vector: <b>unkown</b> Created: 2022-04-11 Updated: 2022-04-11
CVE-2022-1289	A denial of service vulnerability was found in tildearrow Furnace. It has been <b>classified</b> as problematic. This is due to an incomplete fix of CVE-2022-1211. It is possible to initiate the attack remotely but it requires

	<div>the Upload and Download feature.</div> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-11</div>	<div>user interaction. The issue got fixed with the patch 0eb02422d5161767e9983bdaa5c429762d3477ce.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>
CVE-2022-27883	<div>A link following vulnerability in Trend Micro <b>Antivirus</b> for Mac 11.5 could allow an attacker to create a specially-crafted file as a symlink that can lead to privilege escalation. Please note that an attacker must at least have low-level privileges on the system to attempt to exploit this vulnerability.</div> <div>UNRATEDVector: unknownCreated: 2022-04-09Updated: 2022-04-11</div>	<div>CVE-2022-1287A vulnerability <b>classified</b> as critical was found in School Club Application System 1.0. This vulnerability affects a request to the file /scas/classes/Users.php?f=save_user. The manipulation with a POST request leads to privilege escalation. The attack can be initiated remotely and does not require authentication. The exploit has been disclosed to the public and may be used.</div> <div>UNRATEDVector: unknownCreated: 2022-04-09Updated: 2022-04-11</div>
CVE-2022-1288	<div>A vulnerability, which was <b>classified</b> as problematic, has been found in School Club Application System 1.0. This issue affects access to /scas/admin/. The manipulation of the parameter page with the input %22%3E%3Cimg%20src=x%20onerror=alert(1)%3E leads to a reflected cross site scripting. The attack may be initiated remotely and does not require any form of authentication. The exploit has been disclosed to the public and may be used.</div> <div>UNRATEDVector: unknownCreated: 2022-04-09Updated: 2022-04-11</div>	CVE-2022-27129
CVE-2022-27131	<div>An arbitrary file upload vulnerability at /zbzedit/php/zbz.php in zbzcms v1.0 allows attackers to execute arbitrary code via a crafted PHP file.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>	<div>CVE-2022-27128An incorrect access control issue at /admin/run_ajax.php in zbzcms v1.0 allows attackers to arbitrarily add administrator accounts.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>
CVE-2022-26877	<div>Asana Desktop before 1.6.0 allows remote attackers to exfiltrate local files if they can trick the Asana desktop app into loading a malicious web page.</div> <div>UNRATEDVector: unknownCreated: 2022-04-09Updated: 2022-04-11</div>	<div>CVE-2022-0936Cross-site Scripting (XSS) - Stored in <b>GitHub</b> repository autolab/autolab prior to 2.8.0.</div> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-11</div>
CVE-2022-27295	<div><b>D-Link</b> DIR-619 Ax v1.00 was discovered to contain a stack overflow in the function formAdvanceSetup. This vulnerability allows attackers to cause a Denial of Service (DoS) via the webpage parameter.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>	<div>CVE-2022-27291<b>D-Link</b> DIR-619 Ax v1.00 was discovered to contain a stack overflow in the function formdumpeasysetup. This vulnerability allows attackers to cause a Denial of Service (DoS) via the config.save_network_enabled parameter.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>
CVE-2022-27292	<div><b>D-Link</b> DIR-619 Ax v1.00 was discovered to contain a stack overflow in the function formLanguageChange. This vulnerability allows attackers to cause a Denial of Service (DoS) via the nextPage parameter.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>	<div>CVE-2022-27290<b>D-Link</b> DIR-619 Ax v1.00 was discovered to contain a stack overflow in the function formSetWanDhcpplus. This vulnerability allows attackers to cause a Denial of Service (DoS) via the curTime parameter.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>
CVE-2022-27289	<div><b>D-Link</b> DIR-619 Ax v1.00 was discovered to contain a stack overflow in the function formSetWanL2TP. This vulnerability allows attackers to cause a Denial of Service (DoS) via the curTime parameter.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>	<div>CVE-2022-27286<b>D-Link</b> DIR-619 Ax v1.00 was discovered to contain a stack overflow in the function formSetWanNonLogin. This vulnerability allows attackers to cause a Denial of Service (DoS) via the curTime parameter.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>
CVE-2022-27287	<div><b>D-Link</b> DIR-619 Ax v1.00 was discovered to contain a stack overflow in the function formSetWanPPPoE. This vulnerability allows attackers to cause a Denial of Service (DoS) via the curTime parameter.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>	<div>CVE-2022-27288<b>D-Link</b> DIR-619 Ax v1.00 was discovered to contain a stack overflow in the function formSetWanPPTP. This vulnerability allows attackers to cause a Denial of Service (DoS) via the curTime parameter.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>
CVE-2022-27293	<div><b>D-Link</b> DIR-619 Ax v1.00 was discovered to contain a stack overflow in the function formWlanSetup. This vulnerability allows attackers to cause a Denial of Service (DoS) via the webpage parameter.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>	<div>CVE-2022-27294<b>D-Link</b> DIR-619 Ax v1.00 was discovered to contain a stack overflow in the function formWlanWizardSetup. This vulnerability allows attackers to cause a Denial of Service (DoS) via the webpage parameter.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>
CVE-2022-22563	<div><b>Dell EMC Powerscale OneFS</b> 8.2.x - 9.2.x omit security-relevant information in /etc/master.passwd. A high-privileged user can exploit this vulnerability to not record information identifying the source of account information changes.</div> <div>UNRATEDVector: unknownCreated: 2022-04-08Updated: 2022-04-11</div>	<div>CVE-2022-26851<b>Dell</b> PowerScale OneFS, 8.2.2-9.3.x, contains a predictable file name from observable state vulnerability. An unprivileged network attacker could potentially exploit this vulnerability, leading to data loss.</div> <div>UNRATEDVector: unknownCreated: 2022-04-08Updated: 2022-04-11</div>
CVE-2022-26854	<div><b>Dell</b> PowerScale OneFS, versions 8.2.x-9.2.x, contain risky cryptographic algorithms. A remote unprivileged malicious attacker could potentially exploit this vulnerability, leading to full system access</div> <div>UNRATEDVector: unknownCreated: 2022-04-08Updated: 2022-04-11</div>	<div>CVE-2022-26855<b>Dell</b> PowerScale OneFS, versions 8.2.x-9.3.0.x, contains an incorrect default permissions vulnerability. A local malicious user could potentially exploit this vulnerability, leading to a denial of service.</div> <div>UNRATEDVector: unknownCreated: 2022-04-08Updated: 2022-04-11</div>
CVE-2022-26852	<div><b>Dell</b> PowerScale OneFS, versions 8.2.x-9.3.x, contain a predictable seed in pseudo-random number generator. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to an account compromise.</div> <div>UNRATEDVector: unknownCreated: 2022-04-08Updated: 2022-04-11</div>	<div>CVE-2022-24428<b>Dell</b> PowerScale OneFS, versions 8.2.x, 9.0.0.x, 9.1.0.x, 9.2.0.x, 9.2.1.x, and 9.3.0.x, contain an improper preservation of privileges. A remote filesystem user with a local account could potentially exploit this vulnerability, leading to an escalation of file privileges and information disclosure.</div> <div>UNRATEDVector: unknownCreated: 2022-04-08Updated: 2022-04-11</div>
CVE-2021-36288	<div><b>Dell</b> VNX2 for File version 8.1.21.266 and earlier, contain a path traversal vulnerability which may lead unauthenticated users to read/write restricted files</div> <div>UNRATEDVector: unknownCreated: 2022-04-08Updated: 2022-04-11</div>	<div>CVE-2021-36293<b>Dell</b> VNX2 for File version 8.1.21.266 and earlier, contain a privilege escalation vulnerability. A local malicious admin may potentially exploit vulnerability and gain elevated privileges.</div> <div>UNRATEDVector: unknownCreated: 2022-04-08Updated: 2022-04-11</div>
CVE-2021-36290	<div><b>Dell</b> VNX2 for File version 8.1.21.266 and earlier, contain a privilege escalation vulnerability. A local malicious admin may potentially exploit vulnerability and gain privileges.</div> <div>UNRATEDVector: unknownCreated: 2022-04-08Updated: 2022-04-11</div>	<div>CVE-2021-36287<b>Dell</b> VNX2 for file version 8.1.21.266 and earlier, contain an unauthenticated remote code execution vulnerability which may lead unauthenticated users to execute commands on the system.</div> <div>UNRATEDVector: unknownCreated: 2022-04-08Updated: 2022-04-11</div>
CVE-2022-1286	<div>heap-buffer-overflow in mrb_vm_exec in mruby/mruby in <b>GitHub</b> repository mruby/mruby prior to 3.2. Possible arbitrary code execution if</div>	<div>CVE-2022-27269InHand Networks InRouter 900 Industrial 4G Router before v1.0.0.r11700 was discovered to contain a remote code execution (RCE) vulnerability via the component config_ovpn. This vulnerability is</div>

	<div>being exploited.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>		<div>triggered via a crafted packet.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>
CVE-2022-27268	<div>InHand Networks InRouter 900 Industrial 4G Router before v1.0.0.r11700 was discovered to contain a remote code execution (RCE) vulnerability via the component get_cgi_from_memory. This vulnerability is triggered via a crafted packet.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>	CVE-2022-27270	<div>InHand Networks InRouter 900 Industrial 4G Router before v1.0.0.r11700 was discovered to contain a remote code execution (RCE) vulnerability via the component ipsec_secrets. This vulnerability is triggered via a crafted packet.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>
CVE-2022-27271	<div>InHand Networks InRouter 900 Industrial 4G Router before v1.0.0.r11700 was discovered to contain a remote code execution (RCE) vulnerability via the component python-lib. This vulnerability is triggered via a crafted packet.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>	CVE-2022-27276	<div>InHand Networks InRouter 900 Industrial 4G Router before v1.0.0.r11700 was discovered to contain a remote code execution (RCE) vulnerability via the function sub_10F2C. This vulnerability is triggered via a crafted packet.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>
CVE-2022-27274	<div>InHand Networks InRouter 900 Industrial 4G Router before v1.0.0.r11700 was discovered to contain a remote code execution (RCE) vulnerability via the function sub_12028. This vulnerability is triggered via a crafted packet.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>	CVE-2022-27273	<div>InHand Networks InRouter 900 Industrial 4G Router before v1.0.0.r11700 was discovered to contain a remote code execution (RCE) vulnerability via the function sub_12168. This vulnerability is triggered via a crafted packet.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>
CVE-2022-27275	<div>InHand Networks InRouter 900 Industrial 4G Router before v1.0.0.r11700 was discovered to contain a remote code execution (RCE) vulnerability via the function sub_122D0. This vulnerability is triggered via a crafted packet.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>	CVE-2022-27272	<div>InHand Networks InRouter 900 Industrial 4G Router before v1.0.0.r11700 was discovered to contain a remote code execution (RCE) vulnerability via the function sub_1791C. This vulnerability is triggered via a crafted packet.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>
CVE-2022-27280	<div>InHand Networks InRouter 900 Industrial 4G Router before v1.0.0.r11700 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the web_exec parameter at /apply.cgi.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>	CVE-2022-27277	<div>InHand Networks InRouter 900 Industrial 4G Router before v1.0.0.r11700 was discovered to contain an arbitrary file deletion vulnerability via the function sub_17C08.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>
CVE-2022-27279	<div>InHand Networks InRouter 900 Industrial 4G Router before v1.0.0.r11700 was discovered to contain an arbitrary file read via the function sub_177E0.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>	CVE-2022-27960	<div>Insecure permissions configured in the user_id parameter at SysUserController.java of <b>OFCMS</b> v1.1.4 allows attackers to access and arbitrarily modify users' <b>personal</b> information.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>
CVE-2022-27958	<div>Insecure permissions configured in the userid parameter at /user/getuserprofile of FEBS-Security v1.0 allows attackers to access and arbitrarily modify users' <b>personal</b> information.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>	CVE-2022-27477	<div><b>Newbee-Mall</b> v1.0.0 was discovered to contain an arbitrary file upload via the Upload function at /admin/goods/edit.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>
CVE-2022-1276	<div>Out-of-bounds Read in mrb_get_args in <b>GitHub</b> repository mruby/mruby prior to 3.2. Possible arbitrary code execution if being exploited.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>	CVE-2022-26180	<div><b>qdPM</b> 9.2 allows Cross-Site Request Forgery (CSRF) via the index.php/myAccount/update URI.</div> <div>UNRATEDVector: unknownCreated: 2022-04-08Updated: 2022-04-11</div>
CVE-2022-28363	<div>Reprise <b>License Manager</b> 14.2 is affected by a reflected cross-site scripting vulnerability (XSS) in the /goform/login_process username parameter via GET. No authentication is required.</div> <div>UNRATEDVector: unknownCreated: 2022-04-09Updated: 2022-04-11</div>	CVE-2022-28364	<div>Reprise <b>License Manager</b> 14.2 is affected by a reflected cross-site scripting vulnerability (XSS) in the /goform/rmswitchr_process file parameter via GET. Authentication is required.</div> <div>UNRATEDVector: unknownCreated: 2022-04-09Updated: 2022-04-11</div>
CVE-2022-28365	<div>Reprise <b>License Manager</b> 14.2 is affected by an Information Disclosure vulnerability via a GET request to /goforms/r/minfo. No authentication is required. The information disclosed is associated with software versions, process IDs, network configuration, hostname(s), system architecture, and file/directory details.</div> <div>UNRATEDVector: unknownCreated: 2022-04-09Updated: 2022-04-11</div>	CVE-2022-1290	<div>Stored XSS in "Name", "Group Name" &amp; "Title" in <b>GitHub</b> repository polonel/trudesk prior to v1.2.0. This allows attackers to execute malicious scripts in the user's browser and it can lead to session hijacking, sensitive data exposure, and worse.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>
CVE-2022-1045	<div>Stored XSS viva .svg file upload in <b>GitHub</b> repository polonel/trudesk prior to v1.2.0.</div> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-11</div>	CVE-2022-28893	<div>The SUNRPC subsystem in the <b>Linux</b> kernel through 5.17.2 can call xs_xprt_free before ensuring that sockets are in the intended state.</div> <div>UNRATEDVector: unknownCreated: 2022-04-11Updated: 2022-04-11</div>
CVE-2022-1291	<div>XSS vulnerability with default `onCellHtmlData` function in <b>GitHub</b> repository hhurz/tableexport.jquery.plugin prior to 1.25.0. Transmitting cookies to third-party servers. Sending data from secure sessions to third-party servers</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>	CVE-2022-24820	<div><b>XWiki</b> Platform is a generic wiki platform offering <b>runtime</b> services for applications built on top of it. A guest user without the right to view pages of the wiki can still list <b>documents</b> by rendering some velocity documents. The problem has been patched in XWiki versions 12.10.11, 13.4.4, and 13.9-rc-1. There is no known workaround for this problem.</div> <div>UNRATEDVector: unknownCreated: 2022-04-08Updated: 2022-04-11</div>
CVE-2022-24819	<div><b>XWiki</b> Platform is a generic wiki platform offering <b>runtime</b> services for applications built on top of it. A guest user without the right to view pages of the wiki can still list <b>documents</b> related to users of the wiki. The problem has been patched in XWiki versions 12.10.11, 13.4.4, and 13.9-rc-1. There is no known workaround for this problem.</div> <div>UNRATEDVector: unknownCreated: 2022-04-08Updated: 2022-04-11</div>	CVE-2022-27126	<div>zbczms v1.0 was discovered to contain a SQL injection vulnerability via the art parameter at /include/make.php.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>
CVE-2022-27127	<div>zbczms v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /php/ajax.php.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>	CVE-2022-27125	<div>zbczms v1.0 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the neirong parameter at /php/ajax.php.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>
CVE-2022-27133	<div>zbczms v1.0 was discovered to contain an arbitrary file deletion vulnerability via /include/up.php.</div> <div>UNRATEDVector: unknownCreated: 2022-04-10Updated: 2022-04-11</div>		



Top malicious files











100% Threat score	tmp9msg6bgl	100% Threat score	4_5954289857399360616.ps1
100% Threat score	jmf-2_1_1e-windows-i586.exe	99% Threat score	oHuqdP31
98% Threat score	æ, éÿ³ v5.0 â®%œâ"ç%œ^.apk	98% Threat score	cammark.xlsx
96% Threat score	yy.apk	91% Threat score	a5d1dab8e3d5baae8c4b10e1554c9d208956e81bbba4b98a19c073b9f5ca4af0
91% Threat score	e40528fe3e56507a421827f2b2ba350d30924523231b0e231737c032e1869179	91% Threat score	acdb39c2d15e4917e643006b1874fb167f715e3940567fd1c9966fa4b57934d5
91% Threat score	5b410e8885bb1d0a4e182cbe0101e17784aa620ab1cd14cf1b4f3f3cff74ae0	90% Threat score	e0c53e4df2a7aadf32301df87312d2e4e3cc1236052b0fb82bb4094ecb3fd392
87% Threat score	b18a907fd8dbf909343f0a5f4224b88da464671ae19a43fffe7ffa7159d5ff6f	86% Threat score	758ae09ff029ee963bddeba9f3e89feedf44521a1a6fb26c16970b22d32c2031
85% Threat score	TeleTraderWorkstation_11_4_0_3993.exe	85% Threat score	expcommander.exe
85% Threat score	INV-010971.html	84% Threat score	1a1ba512c8ecb8ad79d7e65e95f5095b25ad5569566a1dcdd3d714616440b606
84% Threat score	7c12fd3d7cb4fe88e2e19b175286c771f475ca0de686b1ad892300f14af1e27f	84% Threat score	8aa73463f3e15f4ebb3067a65436cd014f41c5d33d305a88b9fdaabd501164c2
83% Threat score	4e611c6a1e17aedb850a92bc2628b9460ca33f265bc4a95349caac5a1e7ee629	83% Threat score	po885737.xlsx
83% Threat score	789c7786a23835544c58fcd7b3a6582fbf5a8d540fa803eac37069d1e3d65613	81% Threat score	DU_stk_UWMV3 4.0.2_ROCKMODS.NET.apk
71% Threat score	Sn3[1].bin		

Top malicious URL










100% Threat score	http://vnwoei.naveicoipg.online/	100% Threat score	https://www.travellers-autobarnrv.com/new/m9E2A5lQQ
100% Threat score	http://comcomputerbg.com/cgi-sys/suspendedpage.cgi	100% Threat score	http://www.nzservers.net/
100% Threat score	http://vm2rjonq.naveicoipg.online/ACMS/0hUxr3Lx/police0?mid=h1o5cYfJ	100% Threat score	http://outlet.bgschool.bg/wp-content/plugins/ml-slider/php/cgi/updatebilling.php
100% Threat score	http://adjjvazj.naveicoipg.online/	100% Threat score	http://twleqqnwl.naveicoipg.online/
93% Threat score	http://39.77.171.100:33032/bin.sh	92% Threat score	http://192.227.196.135/246/vbc.exe
92% Threat score	http://136.144.41.109/AXZ.exe	91% Threat score	http://112.30.98.129:46557/Mozi.m
90% Threat score	http://naveicoipc.tech/ACMS/0Mogk1Cs/topAccounts?uid=3490blxl	87% Threat score	http://45.143.146.151/770/vbc.exe
85% Threat score	https://www.campusconindigital.org/moodle311/oWZgMvUttcPDFNn/	84% Threat score	https://www.defsalabs.com/videos/i1Dde2yztONF5Nmhs
80% Threat score	http://vm2rjonq.naveicoipg.online/	80% Threat score	http://123fisd.naveicoipg.online/ACMS/0mFCUPf/temp0ttuq=qcnvoiek
80% Threat score	http://cecomtp3.naveicoipg.online/ACMS/0o0WQher/ttt3?qwe=v0OSWog5	80% Threat score	http://olsnvolqwe.naveicoipg.online/
80% Threat score	http://inx.lv/F3Qq	80% Threat score	http://123fisd.naveicoipg.online/
80% Threat score	http://aosm8cts.naveicoipg.online/	80% Threat score	http://jvnquetbon.naveicoipg online/
79% Threat score	http://cecomtp3.naveicoipg.online/	79% Threat score	http://aosm8cts.naveicoipg.online/ACMS/0ucLxIjP/toyota tid=CN2xsRPI
79% Threat score	http://twleqqnwl.naveicoipg.online/ACMS/0y0fMbUp/supportTemplate7?cid=yypwjelnblw	78% Threat score	http://adjjvazj.naveicoipg.online/ACMS/0ucLxIjP/toyotaT tid=2uiSmhx2

78% Threat score	<a href="https://14dqr.trk.elasticemail.com/tracking/click?d=2oPAzDYMVuP_2KRMjnI9Nogebnue-0HiTEJuQwaZjCltydT4g1nka2Aeg-0agfAUZwAa5qEINRjEsYuuI0BWgA6u-SqzTbWfrnd0RsVG1FOOevABsVazUTn6YJEluTjHL_4ctwYNFG-62xnRuMFFwgwoqKI9tc6ObIv8aYKadY9WeWlFvZofWlrgWrQTD3DGg2#c2FsZnVnaG9tQHNhaWlUy29tLnNh">https://14dqr.trk.elasticemail.com/tracking/click?d=2oPAzDYMVuP_2KRMjnI9Nogebnue-0HiTEJuQwaZjCltydT4g1nka2Aeg-0agfAUZwAa5qEINRjEsYuuI0BWgA6u-SqzTbWfrnd0RsVG1FOOevABsVazUTn6YJEluTjHL_4ctwYNFG-62xnRuMFFwgwoqKI9tc6ObIv8aYKadY9WeWlFvZofWlrgWrQTD3DGg2#c2FsZnVnaG9tQHNhaWlUy29tLnNh</a>	75% Threat score	<a href="http://vnwoei.naveicoipg.online/ACMS/0s4AtPuk/wwwTe cid=nnwoieopq">http://vnwoei.naveicoipg.online/ACMS/0s4AtPuk/wwwTe cid=nnwoieopq</a>
75% Threat score	<a href="https://app.getresponse.com/click.html?x=a62b&amp;lc=SZTpZj&amp;mc=r0&amp;s=BtPsp59&amp;u=MGtl&amp;z=Eh3OtEV">https://app.getresponse.com/click.html?x=a62b&amp;lc=SZTpZj&amp;mc=r0&amp;s=BtPsp59&amp;u=MGtl&amp;z=Eh3OtEV</a>	75% Threat score	<a href="http://www.57su.com/">http://www.57su.com/</a>
75% Threat score	<a href="http://www.34ou.org/">http://www.34ou.org/</a>	73% Threat score	<a href="https://qatariship.com/">https://qatariship.com/</a>
73% Threat score	<a href="http://outlet.bgschool.bg/">http://outlet.bgschool.bg/</a>	73% Threat score	<a href="https://blog.deallink.com.br/sera-que-as-transacoes-de-m desacelerar-com-a-guerra/">https://blog.deallink.com.br/sera-que-as-transacoes-de-m desacelerar-com-a-guerra/</a>

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			
	<b>#1 Canadian Pharmacy</b> 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.		
	<b>#3 Hosting Response / Michael Boehm</b> 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.		
	<b>#5 RetroCubes</b> 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.		
	<b>#7 RR Media</b> A high volume spam operation based in or run from Huntington Beach, CA, USA. The operation uses a variety of different names.		
	<b>#9 Richpro Trade Inc. / Richvestor GmbH</b> 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.		
	<b>#2 PredictLabs / Sphere Digital</b> 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.		
	<b>#4 Michael Persaud</b> Long time snowshoe type spammer, raided by FBI then indicted in 2017 on federal wire fraud charges tied to his spamming operations.		
	<b>#6 Cyber World Internet Services/ e-Insites</b> 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.		
	<b>#8 Kobeni Solutions</b> 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.		

Source: SpamHaus

Top countries with botnet			
	#1 China		#2 India
	#3 United States of America		#4 Indonesia
	#5 Thailand		#6 Viet Nam
	#7 Algeria		#8 Brazil
	#9 Pakistan		#10 Venezuela (Bolivarian Republic of)

Source: SpamHaus

Top phishing countries

	#1 United States		#2 Russia
	#3 Japan		#4 Germany
	#5 Singapore		#6 Australia
	#7 Hong Kong		#8 Belgium
	#9 Indonesia		#10 Netherlands




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

Have I been pwnd

Nothing today




Source: [Imperva DDOS Map](#)

Top DDOS attackers

	United States (26%)
	Germany (11%)
	Hong Kong (9%)

Source: [Imperva DDOS Map](#)

Top DDOS country targets

	Russia (30%)
	United States (21%)
	China (14%)

Source: [Imperva DDOS Map](#)

Top DDOS techniques

55%	DDoS
35%	Automated Threat
10%	OWASP

Source: [Imperva DDOS Map](#)

Top DDOS industry targets

41%	Financial Services
24%	Business
9%	Computing & IT