



## Your Security Rabbits report for March 01, 2022

### Hot topics

*Nothing today*




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

### Have I been pwnd

*Nothing today*




Source: [Imperva DDOS Map](#)

### Top DDOS attackers

	United States (29%)
	Germany (18%)
	Singapore (6%)

Source: [Imperva DDOS Map](#)

### Top DDOS country targets

	United States (25%)
	Russia (22%)
	Australia (8%)

Source: [Imperva DDOS Map](#)

### Top DDOS techniques

55%	Automated Threat
26%	DDoS
19%	OWASP

Source: [Imperva DDOS Map](#)

### Top DDOS industry targets

40%	Financial Services
14%	Food & Beverages
12%	Computing & IT

### News

**cyberscoop**  
CyberScoop

**'Most advanced' China-linked backdoor ever, Daxin, raises alarms for cyber-espionage investigators**  
A backdoor in use as recently as November 2021 is the "most advanced piece of malware" ever seen from China-linked spies, according to researchers at Symantec. The cybersecurity company said Monday that the backdoor, dubbed Daxin, is part of "a long-running espionage campaign against select governments and other critical infrastructure targets," most of them being of strategic interest to China. The malware "appears to be optimized for use against hardened targets, allowing the attackers to burrow deep into a target's network and exfiltrate data without raising suspicions," the researchers said. "This isn't really comparable to any other strains of China-linked malware in our opinion. It's o[...]"

**The Hacker News**



















**100 Million Samsung Galaxy Phones Affected with Flawed Hardware Encryption Feature**  
A group of academics from Tel Aviv University have disclosed details of now-

**eset**  
WeLiveSecurity









**#ShieldsUp - Now is the time to double-check cybersecurity processes and operations**  
As the conflict in Ukraine heightens the risk of cyberattacks globally, what can organizations do to improve their resiliency? The post #ShieldsUp - Now is the time to double-check cybersecurity processes and operations appeared first on WeLiveSecurity






Anonymous hacks Russian TV channels & EV charging station with pro-Ukraine

<div> <div>The Hacker News</div> </div>	<p>patched "severe" design flaws affecting about 100 million Android-based Samsung smartphones that could have resulted in the extraction of secret cryptographic keys. The shortcomings are the result of an analysis of the cryptographic design and implementation of Android's hardware-backed Keystore in Samsung's Galaxy S8,</p>	<div> <div>CYWARE SOCIAL</div> <div>Cyware News - Latest Cyber News</div> </div>	<p>messages</p> <p>Anonymous, along with other hacktivist groups is carrying out different types of cyberattacks against the Russian government, media, businesses, and financial institutions.</p>
<div> <div>Security Affairs</div> </div>	<p><b>Anonymous hit Russian Nuclear Institute and leak stolen data</b></p> <p>Anonymous and other hacker groups that responded to the call to war against Russia continue to launch cyberattacks on gov organizations and businesses. Anonymous and numerous hacker groups linked to the popular collective continue to launch cyber attacks against Russian and Belarussian government organizations and private businesses. In the last few days massive DDoS attacks [...] The post Anonymous hit Russian Nuclear Institute and leak stolen data appeared first on Security Affairs.</p>	<div> <div>cyberscoop</div> <div>CyberScoop</div> </div>	<p><b>Backbone is everything, don't be owned by your infrastructure: Lessons from Ukraine for America</b></p> <p>After weeks and months of saber-rattling, Russia has brutally invaded Ukraine. Bullying autocracies are reaching back and executing old playbooks -- in this instance exceptionally audaciously -- and around the globe they will be looking to see how allied democracies react and respond to Russia's military aggression. For both attacker and defender, cyber domain will figure prominently. Indeed, it already has. Consider "intelligence preparation of the battlefield," or IPB. It's what military professionals do to scope the lay of the land -- both physical and virtual -- before taking on their target full bore. And it's what Russia had been doing in and to Ukraine before launching fuller-scale op[...]</p>
<div> <div>cyberscoop</div> <div>CyberScoop</div> </div>	<p><b>Belarusian hackers launch another attack, adding to chaotic hacktivist activity around Ukraine</b></p> <p>A group of Belarusian hackers and IT specialists claimed Sunday that they'd attacked the Belarusian Railways in an attempt to "slow down the transfer of occupying forces and give the Ukrainians more time to repel the attack," according to a Google translation of the message posted to the group's Telegram channel. The hackers -- who call themselves the Cyber Partisans and have targeted Belarus' autocratic government and its leader, Alexander Lukashenko, dating back to September 2020 -- said Sunday their hack "paralyzed" some railway operations in the Belarussian capital of Minsk and in Orsha, an eastern Belarusian city between Moscow and Minsk. Some railway operations were switched to manual mo[...]</p>	<div> <div>CYWARE SOCIAL</div> <div>Cyware News - Latest Cyber News</div> </div>	<p><b>Camera Maker Axis Suffers Service Outage Following Cyberattack</b></p> <p>The Swedish camera giant said it got alerts from its cybersecurity and intrusion detection system on Sunday before it shut down all public-facing services globally to limit the impact of the attack.</p>
<div> <div>The Hacker News</div> <div>The Hacker News</div> </div>	<p><b>China-linked Daxin Malware Targeted Multiple Governments in Espionage Attacks</b></p> <p>A previously undocumented espionage tool has been deployed against selected governments and other critical infrastructure targets as part of a long-running espionage campaign orchestrated by China-linked threat actors since at least 2013. Broadcom's Symantec Threat Hunter team characterized the backdoor, named Daxin, as a technologically advanced malware, allowing the attackers to carry out a</p>	<div> <div>The Hacker News</div> <div>The Hacker News</div> </div>	<p><b>CISA adds recently disclosed Zimbra bug to its Exploited Vulnerabilities Catalog</b></p> <p>The U.S. Cybersecurity and Infrastructure Security Agency (CISA) expanded its Known Exploited Vulnerabilities Catalog to include a recently disclosed zero-day flaw in the Zimbra email platform citing evidence of active exploitation in the wild. Tracked as CVE-2022-24682 (CVSS score: 6.1), the issue concerns a cross-site scripting (XSS) vulnerability in the Calendar feature in Zimbra</p>
<div> <div>Security Affairs</div> </div>	<p><b>CISA and FBI warn of potential data wiping attacks spillover</b></p> <p>US CISA and the FBI warned US organizations that data wiping attacks targeting Ukraine entities could spill over to targets worldwide. The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) published a joint cybersecurity advisory to warn US organizations of data wiping attacks targeting Ukraine that could hit targets worldwide. [...] The post CISA and FBI warn of potential data wiping attacks spillover appeared first on Security Affairs.</p>	<div> <div>The Hacker News</div> <div>The Hacker News</div> </div>	<p><b>CISA Warns of High-Severity Flaws in Schneider and GE Digital's SCADA Software</b></p> <p>The U.S. Cybersecurity and Infrastructure Security Agency (CISA) last week published an industrial control system (ICS) advisory related to multiple vulnerabilities impacting Schneider Electric's Easergy medium voltage protection relays. "Successful exploitation of these vulnerabilities may disclose device credentials, cause a denial-of-service condition, device reboot, or allow an attacker to</p>
<div> <div>CYWARE SOCIAL</div> <div>Cyware News - Latest Cyber News</div> </div>	<p><b>Conti ransomware's internal chats leaked after siding with Russia</b></p> <p>A Ukrainian security researcher has leaked over 60,000 internal messages belonging to the Conti ransomware operation after the gang sided with Russia over the invasion of Ukraine.</p>	<div> <div>CYWARE SOCIAL</div> <div>Cyware News - Latest Cyber News</div> </div>	<p><b>Cybercrime getting more destructive, remote workers in the crosshairs</b></p> <p>Fortinet's intel from the H2 2021 reveals an increase in the automation and speed of attacks demonstrating more advanced persistent cybercrime strategies that are more destructive and unpredictable.</p>
<div> <div>CYWARE SOCIAL</div> <div>Cyware News - Latest Cyber News</div> </div>	<p><b>DeadBolt Ransomware Eyeing ASUSTOR Devices</b></p> <p>Deadbolt ransomware hackers crippled the networks of Asustor NAS drives users and attempted to extort 0.03 BTC for the release of a decryption key. Multiple reports indicate that the AS6102T, AS6602T, AS5304T, AS5304T, and AS-6210T-4K models are unaffected. Meanwhile, ASUSTOR is planning to release a recovery firmware that users may use to gain access to their NAS devices. This update won't recover the encrypted files unless users have backups.</p>	<div> <div>CYWARE SOCIAL</div> <div>Cyware News - Latest Cyber News</div> </div>	<p><b>Defense Contractors Under Attack Using New SockDetour Backdoor</b></p> <p>The backdoor is associated with an APT campaign named TiltedTemple (aka DEV-0322). Recently, four defense contractors were targeted and one was compromised.</p>
<div> <div>CYWARE SOCIAL</div> <div>Cyware News - Latest Cyber News</div> </div>	<p><b>Electron Bot Leverages Microsoft App Store to Pierce Social Media Accounts</b></p> <p>An SEO poisoning bot has been taking over social media accounts and masquerading as the Temple Run game. The bot targets multiple social media accounts such as Facebook, Google, and SoundCloud.</p>	<div> <div>cyberscoop</div> <div>CyberScoop</div> </div>	<p><b>Facebook, Twitter, Google move to intercept Russian propaganda, disinformation about Ukraine</b></p> <p>In recent days, social media companies have gotten more active in stemming the flow of official Russian propaganda, as well tackling sneakier efforts to spread disinformation about Ukraine. The steps follow pressure from policymakers in the U.S. and elsewhere for social media companies to counter narratives from Russia as it conducts its military offense. Meta, the parent company of Facebook and Instagram, said Monday that it had removed about 40 accounts based out of Russia and Ukraine posing as legitimate news sources, which were pushing the narrative that the West had betrayed Ukraine and that Ukraine was a failed state. It also said it had taken steps to counter hacking threats to Facebo[...]</p>
<div> <div>Security Affairs</div> </div>	<p><b>FoxBlade malware targeted Ukrainian networks hours before Russia's invasion</b></p> <p>Microsoft revealed that Ukrainian entities were targeted with a previous undetected malware, dubbed FoxBlade, several hours before the invasion. The Microsoft Threat Intelligence Center (MSTIC) continues to investigate the attacks that are targeting Ukrainian networks and discovered that entities in Ukraine were targeted with a previously undetected malware, dubbed FoxBlade, several hours before Russia's invasion. [...] The post FoxBlade malware targeted Ukrainian networks hours before Russia's invasion appeared first on Security Affairs.</p>	<div> <div>ZDNet</div> <div>ZDNet   security RSS</div> </div>	<p><b>Google TAG removes fraudulent 'influence' operations linked to Belarus, Moldova, Ukraine</b></p> <p>The tech giant has also tackled thousands of YouTube channels connected to China.</p>
<div> <div>CYWARE SOCIAL</div> <div>Cyware News - Latest Cyber News</div> </div>	<p><b>How prepared are organizations to face email-based ransomware attacks?</b></p> <p>A Proofpoint report reveals that attackers were more active in 2021, with findings uncovering that 78% of organizations saw email-based ransomware attacks in 2021, while 77% faced BEC attacks.</p>	<div> <div>IT Security GURU</div> <div>IT Security Guru</div> </div>	<p><b>How the CISO has adapted to protect the hybrid workforce</b></p> <p>Many organisations have been considering a network transformation initiative to support the adoption of SaaS, cloud-based applications, and an increasingly remote workforce. Given the connectivity needs of a remote workforce - and knowing a hybrid workforce is here to stay - many IT teams have had to make sudden changes in the way workers connect [...] The post How the CISO has adapted to protect the hybrid workforce appeared first on IT Security Guru.</p>
<div> <div>cyberscoop</div> <div>CyberScoop</div> </div>	<p><b>In response to Russia threat, U.S. cybersecurity firms offer free services, data, threat intel</b></p> <p>U.S. cybersecurity companies are offering products and services for free to help cyberdefenders at home and abroad during Russia's invasion of Ukraine. As of Monday, a crowdsourced list on GitHub listed more than a dozen experts, nonprofits and companies available for security assistance. Among the firms is</p>		<p><b>Instagram scammers as busy as ever: passwords and 2FA codes at risk</b></p>

 Threatpost	<p>GreyNoise, which announced Thursday it had upgraded all Ukrainian email accounts to include full enterprise access to its products. "In terms of our offer to support defenders in Ukraine, we've been in contact with dozens of different groups to help them get set up on our tools and leverage our data, as well as connect them with others in the InfoSec community doing the same," Dan Maier, [...]</p>	 Naked Security	<p>Instagram scams don't seem to be dying out - we're seeing more variety and trickiness than ever...</p>
 IT Security Guru	<p><b>Microsoft Accounts Targeted by Russian-Themed Credential Harvesting</b> Malicious emails warning Microsoft users of "unusual sign-on activity" from Russia are looking to capitalizing on the Ukrainian crisis.</p>	 The Hacker News	<p><b>Microsoft Finds FoxBlade Malware Hit Ukraine Hours Before Russian Invasion</b> Microsoft on Monday disclosed that it detected a new round of offensive and destructive cyberattacks directed against Ukraine's digital infrastructure hours before Russia launched its first missile strikes last week. The intrusions involved the use of a never-before-seen malware package dubbed FoxBlade, according to the tech giant's Threat Intelligence Center (MSTIC), noting that it added new</p>
 Security Affairs	<p><b>Moscow exchange hit with cyberattack</b> Hackers endorsed by Kyiv officials have claimed responsibility for a cyberattack on the Moscow Stock Exchange. The website for the Moscow Stock Exchange was offline and inaccessible on Monday. The Ukraine IT Army posted a message on Telegram claiming that it had taken only five minutes to take down the website. The hackers claiming responsibility are [...] The post Moscow exchange hit with cyberattack appeared first on IT Security Guru.</p>	 Cyware News - Latest Cyber News	<p><b>Ransomware anatomy: Dual cyberattacks on provider call for vulnerability review</b> A new report by Sophos shed light on two simultaneous ransomware attacks against a healthcare provider organization by different threat groups, pointing to the need for vulnerability management.</p>
 IT Security Guru	<p><b>Researcher leaked Conti's internal chat messages in response to its support to Russia</b> A Ukrainian researcher leaked tens of thousands of internal chat messages belonging to the Conti ransomware operation. A Ukrainian researcher leaked 60,694 messages internal chat messages belonging to the Conti ransomware operation after the announcement of the group of its support to Russia. Researchers from cybersecurity firm Hold Security confirmed that the researcher was able to access [...] The post Researcher leaked Conti's internal chat messages in response to its support to Russia appeared first on Security Affairs.</p>	 IT Security Guru	<p><b>Russian state media hacked</b> The international hacking organisation Anonymous have claimed responsibility for taking down Russian media sites. Among those affected were the state-owned news agency TASS and daily newspaper Kommersant, having been temporarily taken offline on Monday, while St Petersburg-based news outlet Fontanka's content was replaced with a message that read, "This is not our war, let's stop [...]" The post Russian state media hacked appeared first on IT Security Guru.</p>
 IT Security Guru	<p><b>Starlink activated to keep Ukraine's internet running</b> In response to several Russian cyberattacks on the country, Ukraine's Vice Prime Minister and Minister of Digital Transformation Mykhailo Fedorov requested help from SpaceX and Tesla billionaire Elon Musk. Responding on Twitter, Musk confirmed "Starlink service is now active in Ukraine. More terminals en route." SpaceX's low-earth-orbit (LEO), high speed, low latency internet service, which [...] The post Starlink activated to keep Ukraine's internet running appeared first on IT Security Guru.</p>	 CyberScoop	<p><b>Suspected cyberattack on parts supplier forces Toyota to shut down Japan plants</b> Toyota said Monday that it was suspending operations at all 14 of its plants in Japan after a domestic supplier of parts, Kojima Industries Corp., was hit by a suspected cyberattack. Toyota described it as a "system failure" at Kojima in a short statement posted online. A Kojima spokesperson told ABC News that the company was working to fix the problem, which essentially blocked the company's computers from communicating with Toyota. "We are not sure yet if it is a cyberattack, but we suspect it might be one," the spokesperson said. As of Monday morning, U.S. Eastern time, Kojima's website was unreachable. There was no information available about the suspected attackers or their methods. The[...]</p>
 IT Security Guru	<p><b>Toyota hit with ransomware attack, stops production</b> Toyota, the worlds largest car maker has stopped production at all of its plants in Japan following a ransomware attack, reports suggest. Toyota announced it would suspend 28 production lines at 14 factories on Tuesday, planning to resume on Wednesday, according to Nikkei. The report claimed that the cyberattack targeted Kojima Industries, a plastic parts [...] The post Toyota hit with ransomware attack, stops production appeared first on IT Security Guru.</p>	 Security Affairs	<p><b>Toyota Motors halted production due to a cyber attack on a supplier</b> Japanese carmaker Toyota Motors was forced to stop car production due to a cyberattack against one of its suppliers. Japanese carmaker Toyota Motors was forced to halt its production due to a cyber attack that suffered by one of its suppliers, Kojima Industries. "It is true that we have been hit by some kind of [...] The post Toyota Motors halted production due to a cyber attack on a supplier appeared first on Security Affairs.</p>
 Threatpost	<p><b>Toyota to Close Japan Plants After Suspected Cyberattack</b> The plants will shut down on Tuesday, halting about a third of the company's global production. Toyota doesn't know how long the 14 plants will be unplugged.</p>	 ZDNet   security RSS	<p><b>Ukraine security agencies warn of Ghostwriter threat activity, phishing campaigns</b> CERT-UA warns of misinformation, phishing, and active assaults against Ukrainian organizations.</p>
 Threatpost	<p><b>Ukraine-Russia Cyber Warzone Splits Cyber Underground</b> A pro-Ukraine Conti member spilled 13 months of the ransomware group's chats, while cyber actors are rushing to align with both sides.</p>	 Cyware News - Latest Cyber News	<p><b>UNC2596 Deploys Cuba Ransomware via Microsoft Exchange Server Vulnerabilities</b> According to Mandiant, UNC2596 has been launching such campaigns since August 2021. It has targeted utility providers, government agencies, and organizations that support non-profits and healthcare entities.</p>
 Cyware News - Latest Cyber News	<p><b>Update: Nvidia allegedly hacked its hackers, stole its data back</b> Lapsus\$ said that Nvidia hacked it back. The group supposedly left one of its virtual machines enrolled in Nvidia's mobile device management program, which gave Nvidia a backdoor into its systems.</p>	 Cyware News - Latest Cyber News	<p><b>Vulnerabilities spotted in Gerbv could lead to code execution, information disclosure</b> Cisco Talos recently discovered multiple vulnerabilities in the Gerbv file viewing software that could allow an attacker to execute arbitrary remote code or disclose sensitive information.</p>

Twitter

 Governor Roy Cooper	<p>The Russian invasion of Ukraine is elevating the threat of cyber attacks on businesses and government agencies. Today I instructed my Joint Cybersecurity Task Force to increase outreach and assistance. - RC</p>	 The Hacker News	<p>Researchers detail severe flaws in hardware-backed #encryption on nearly 100 million #Android-based #Samsung Galaxy S8, S9, S10, S20 and S21 smartphones that could be exploited to extract secret cryptographic keys. Details: #infosec #cybersecurity #tech</p>
 Suzanne Smalley	<p>Today I begin my new job @CyberScoopNews covering intelligence and disinformation, among other topics. I couldn't be more excited to dive in. Now more than ever cybersecurity is of vital importance and I am privileged to be covering it. @US_CYBERCOM @WHNSC @NSAGov @ODNIGov @CIA</p>	 Jacques Poitras	<p>BREAKING: Cyber NB, the provinces marquee industry organization set up to promote the growong cybersecurity sector, is shutting down. Acting CEO Jeremy Depow says theres no money to pay rent tomorrow or meet payroll on Thursday.</p>
 Shannon Morse	<p>I was today years old when I learned that my cybersecurity channel isn't allowed to take cybersecurity sponsors for core topic videos. Is this what happens when your channel grows? People deem your videos untrustworthy if they're sponsored? Thanks I hate it.</p>	 Governor Roy Cooper	<p>Today, Gov. Cooper was briefed by state agencies on cybersecurity and the best ways to keep our state safe. Its important to be vigilant of phishing emails, ransomware attacks and cyberattacks following recent world events. The best way to prevent attacks is by paying attention.</p>
	<p>Defense and cybersecurity stocks climb amid Russias invasion of Ukraine</p>	 Brian hEoghanin (Brian)	<p>Anyone know the impacts of the financial sanctions against Russia will have on Russian cyber security firms and companies that use them in the West. For example, enterprises who use Kaspersky AV, will they be able to pay for the SW &amp; download updates? Or who use Group IB??</p>

			
	'Online banking systems down for a number of days... oil supplies cut off... and more sinister stuff around attacking email systems within political parties.' Cyber security expert Richard Bingley on what a cyber threat from Russia could look like.		What are the challenges facing women in Cybersecurity field? #GirlsInICTKe #CyberSecurity
	With the childcare responsibility still predominantly placed on women, a rigid work setting can create obstacles for women who want work-life balance but also want to climb the corporate ladder. #GirlsInICTKe #CyberSecurity		

Source: *NIST*

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-2021-35036	A command injection vulnerability in the <b>web interface</b> of the <b>Zyxel</b> NWA-1100-NH firmware could allow an attacker to execute arbitrary OS commands on the device.  UNRATED Vector: unkown Created: 2022-03-01 Updated: 2022-03-01	CVE-2021-4039	A command injection vulnerability in the <b>web interface</b> of the <b>Zyxel</b> NWA-1100-NH firmware could allow an attacker to execute arbitrary OS commands on the device.  UNRATED Vector: unkown Created: 2022-03-01 Updated: 2022-03-01
CVE-2022-25022	A cross-site scripting (XSS) vulnerability in <b>Htmly</b> v2.8.1 allows attackers to excute arbitrary web scripts HTML via a crafted payload in the content field of a <b>blog</b> post.  UNRATED Vector: unkown Created: 2022-03-01 Updated: 2022-03-01	CVE-2022-25020	A cross-site scripting (XSS) vulnerability in <b>Pluxml</b> v5.8.7 allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the thumbnail path of a <b>blog</b> post.  UNRATED Vector: unkown Created: 2022-03-01 Updated: 2022-03-01
CVE-2021-42767	A directory traversal vulnerability in the Apoc <b>plugins</b> in <b>Neo4J</b> Graph database 4.0.0 through 4.3.6 allows attackers to read local files.  UNRATED Vector: unkown Created: 2022-03-01 Updated: 2022-03-01	CVE-2021-44961	A memory leakage flaw exists in the class PerimeterGenerator of Slic3r libslic3r 1.3.0 and Master Commit b1a5500. A Specially crafAn out-of-bounds read vulnerability exists in the GCode::extrude() functionality of Slic3r libslic3r 1.3.0 and Master Commit b1a5500. A specially crafted stl file could lead to information disclosure. An attacker can provide a malicious file to trigger this vulnerability.ted stl files can exhaust available memory.  UNRATED Vector: unkown Created: 2022-03-01 Updated: 2022-03-01
CVE-2021-42951	A Remote Code Execution (RCE) vulnerability exists in Algorithmia MSOL all versions before <b>October</b> 10 2021 of SaaS. Users can register for an account and are allocated a set number of credits to try the product. Once users authenticate, they can proceed to create a new, specially crafted Algorithm and subsequently launch remote code execution with their desired result.  UNRATED Vector: unkown Created: 2022-03-01 Updated: 2022-03-01	CVE-2022-24446	An issue was discovered in <b>Zoho ManageEngine</b> Key Manager <b>Plus</b> 6.1.6. A user, with the level Operator, can see all SSH servers (and user information) even if no SSH server or user is associated to the operator.  UNRATED Vector: unkown Created: 2022-03-01 Updated: 2022-03-01
CVE-2021-44962	An out-of-bounds read vulnerability exists in the GCode::extrude() functionality of Slic3r libslic3r 1.3.0 and Master Commit b1a5500. A specially crafted stl file could lead to information disclosure. An attacker can provide a malicious file to trigger this vulnerability.  UNRATED Vector: unkown Created: 2022-03-01 Updated: 2022-03-01	CVE-2022-26332	Cipi 3.1.15 allows Add Server stored XSS via the /api/servers name field.  UNRATED Vector: unkown Created: 2022-03-01 Updated: 2022-03-01
CVE-2022-0776	Cross-site Scripting (XSS) - DOM in <b>GitHub</b> repository hakimel/reveal.js prior to 4.3.0.  UNRATED Vector: unkown Created: 2022-03-01 Updated: 2022-03-01	CVE-2020-12775	Hicos citizen certificate client-side component does not filter special characters for command parameters in specific web URLs. An unauthenticated remote attacker can exploit this vulnerability to perform command injection attack to execute arbitrary system command, disrupt system or terminate service.  UNRATED Vector: unkown Created: 2022-03-01 Updated: 2022-03-01
CVE-2022-25096	Home Owners Collection Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter in /members/view_member.php.  UNRATED Vector: unkown Created: 2022-02-26 Updated: 2022-03-01	CVE-2022-25018	<b>Pluxml</b> v5.8.7 was discovered to allow attackers to execute arbitrary code via crafted PHP code inserted into static pages.  UNRATED Vector: unkown Created: 2022-03-01 Updated: 2022-03-01
CVE-2022-22262	ROG Live Service's function for deleting temp files created by installation has an improper link resolution before file access vulnerability. Since this function does not validate the path before deletion, an unauthenticated local attacker can create an unexpected	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

	symbolic link to system file path, to delete arbitrary system files and disrupt system service. <div>UNRATEDVector: unkownCreated: 2022-03-01Updated: 2022-03-01</div>		from SPE or NSPE can overwrite stack memory locations. <div>UNRATEDVector: unkownCreated: 2022-03-01Updated: 2022-03-01</div>
CVE-2022-0777	Weak Password Recovery Mechanism for Forgotten Password in <b>GitHub</b> repository microweber/microweber prior to 1.3. <div>UNRATEDVector: unkownCreated: 2022-03-01Updated: 2022-03-01</div>		

Source: Hybrid Analysis

Top malicious files

100% Threat score	New payment details and address update (.) xlsxm	100% Threat score	Detroit_anim (.) exe
100% Threat score	detroit_img (.) exe	100% Threat score	primusmarkets4setup (.) exe
100% Threat score	Detroit (.) exe	100% Threat score	PO#202203-012 (.) xlsx
100% Threat score	000249746c90d568c62516f5df2f1d541c0a3e5a6d8b92702037bde4a931afe3	100% Threat score	http kreator (.) exe
100% Threat score	tmpaee4knrf	100% Threat score	Service-Interrupt-474637778 (.) xlsx
100% Threat score	tmpgtjlho3o	100% Threat score	HiddenSky (.) exe
100% Threat score	def_mal_onlybentor (.) exe	100% Threat score	def_mal2_onlybentor (.) exe
100% Threat score	GDA3 (.) 99 (.) free (.) exe	100% Threat score	2022-03-01_1339 (.) xlsxm
100% Threat score	Specification and drawing (.) pub	100% Threat score	name (.) exe
94% Threat score	xmrig (.) exe	85% Threat score	SecureW2win (.) exe
85% Threat score	Wolow Companion Setup (.) exe	85% Threat score	Chorus_DIMENSION-D_1_0_2_2321 (.) exe
85% Threat score	Zahlungsschreiben 2022 (.) 01 (.) 03_1013 (.) xlsxm	84% Threat score	00D1ED4049DB2CD84B735813BEAF785A3770F9E72BFE3684B5CEA1ECF1B4BE98
80% Threat score	Cab-bourg (.) htm	72% Threat score	AJANCAM (.) Data (.) Migration32 (.) exe


Source: Hybrid Analysis

Top malicious URL

98% Threat score	http://youlanda (.) org/	97% Threat score	http://104 (.) 237 (.) 126 (.) 133:56690/i
93% Threat score	http://39 (.) 89 (.) 8 (.) 2:39482/i	93% Threat score	http://117 (.) 222 (.) 162 (.) 142:39570/i
93% Threat score	http://117 (.) 196 (.) 23 (.) 206:47926/bin (.) sh	93% Threat score	http://125 (.) 47 (.) 247 (.) 157:54358/Mozi (.) m
93% Threat score	http://125 (.) 41 (.) 143 (.) 183:39303/bin (.) sh	93% Threat score	http://182 (.) 126 (.) 114 (.) 235:39893/bin (.) sh
93% Threat score	http://201 (.) 150 (.) 180 (.) 58:48407/i	93% Threat score	http://117 (.) 194 (.) 175 (.) 65:39925/i
93% Threat score	http://37 (.) 232 (.) 77 (.) 59:56656/mozi (.) a	88% Threat score	http://182 (.) 119 (.) 224 (.) 233:37295/i
88% Threat score	http://219 (.) 140 (.) 9 (.) 44:43947/bin (.) sh	82% Threat score	http://sarprassikk (.) com/apm/ecd/1jV/R1l/OJGsUD9 (.) zip
82% Threat score	http://kbzq (.) amlakhamed (.) ir/	79% Threat score	https://app (.) box (.) com/s/k8upfbuyy1jnpu3pydnkfvly5iogw87g
74% Threat score	http://qaz (.) im/load/YKFKBd/58dRKD	74% Threat score	https://r20 (.) rs6 (.) net/tn (.) jsp?f=001JAEOW67sLJJ1q0tXl7HTs2LqqL5NWFk2HrjzJwAxxFjaDyXP7xi15Axjd7DTt19diDd91MbP1o-s1lqs8LGfeSH1FdQGy71Ko7KWigR76RyHy6K4AmiYBUGH45wtPnsHupgCQP_hedGug4bfbNdR_KhQkd188HhCnT6gKvffvr0_RqkuXBy6H9Mk6YXK0-OoktS8IQv_B73tudurxwYDplAw%3D&c=HdaunmMpJCbDSgQCpjftnfuWsNpHYhaPrdjtQOmOivUqF7YMZ9TUGMVL1y3MazTn2scy9S77dW4aZosBkevbVEiRbqfDhjCq%3D%3D
73% Threat score	http://www (.) temari (.) fr/	72% Threat score	http://icmindustrie (.) zohosites (.) com/
72%	http://hu-taexr14t (.) artboxq (.) com/?#ygmdventures (.)		










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 Japan
	#9 Brazil		#10 Uruguay

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>#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>#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>#4 Mint Global Marketing / Adgenics / Cabo Networks</b> Florida affiliate spammers and bulletproof spam hosts
	<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>#6 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>#7 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 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 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 Thailand
	#5 Indonesia		#6 Algeria
	#7 Viet Nam		#8 Brazil
	#9 Pakistan		#10 Iran (Islamic Republic of)

Source: SpamHaus

### Top phishing countries

	#1 United States		#2 Germany
	#3 Singapore		#4 Russia
	#5 Netherlands		#6 France
	#7 South Africa		#8 Japan

			
	#9 Hong Kong		#10 United Kingdom