



Your Security Rabbits report for March 02, 2022

Source: [Ransom Watch](#)

Ransomware attacks

clop	Target: ALEXIM . COM (2022-03-02)	clop	Target: BOLTONUSA . COM (2022-03-02)
clop	Target: CAPCARPET . COM (2022-03-02)	clop	Target: DUTTONFIRM . COM (2022-03-02)
clop	Target: EDAN . COM (2022-03-02)	conti	Target: HOL-MAC Corp . (2022-03-02)
clop	Target: JBINSTANTLAWN . NET (2022-03-02)	clop	Target: MCH-GROUP . COM (2022-03-02)
clop	Target: MTMRECOGNITION . COM (2022-03-02)	clop	Target: SLIMSTOCK . COM (2022-03-02)
clop	Target: SSMSJUSTICE . COM (2022-03-02)	lockbit2	Target: www . elitecorp . c . . . (2022-03-02)
lockbit2	Target: www . haeny . com(2022-03-02)	lockbit2	Target: www . tccm . com(2022-03-02)
lockbit2	Target: www . wimmog . ch(2022-03-02)		

Hot topics











Even more intelligence sources

Security Rabbits will now report DDOS statistics.

This has been automatically added to your Security Rabbits report. Feel free to customize your Security Rabbits report if you want to change the order or disable this feature.

--
JL Dupont

News

 CyberScoop	Biden pushes to strengthen children's privacy in State of the Union address President Joe Biden urged Congress to strengthen children's privacy protections in his State of the Union address Tuesday, following growing concerns about the potential mental health impact online platforms cause children -- an issue that Congress has repeatedly hauled in tech giants to address in hearings in recent months. A fact sheet released prior to the speech grouped the initiative into four distinct calls to action: banning targeted advertising for children, prioritizing safety design standards for online platforms, stopping discriminatory algorithmic decision-making and investing at least \$5 million in fiscal year 2023 toward research on social media's effects on mental health. "The[...]"	 The Hacker News	Break into Ethical Hacking with 18 Advanced Online Courses for just \$42.99 It is predicted that 3.5 million jobs will be unfilled in the field of cybersecurity by the end of this year. Several of these jobs pay very well, and in most cases, you don't even need a college degree to get hired. The most important thing is to have the skills and certifications. The All-In-One 2022 Super-Sized Ethical Hacking Bundle helps you gain both, with 18 courses covering all aspects
 Security Affairs	China-linked APT used Daxin, one of the most sophisticated backdoor even seen Daxin is the most advanced backdoor in the arsenal of China-linked threat actors designed to avoid the detection of sophisticated defense systems. Symantec researchers discovered a highly sophisticated backdoor, named Daxin, which is being used by China-linked threat actors to avoid advanced threat detection capabilities. The malicious code was likely designed for long-running espionage campaigns [...] The post China-linked APT used Daxin, one of the most sophisticated backdoor even seen appeared first on Security Affairs.	 Cyware News - Latest Cyber News	Chrome Skype extension with nine million installs found to be leaking user info Security researcher Wladimir Palant discovered a "trivial" bug in the Skype-for-Chrome extension that allowed websites to ascertain information about user accounts that should typically be off-limits.
 The Hacker News	Conti Ransomware Gang's Internal Chats Leaked Online After Siding With Russia Days after the Conti ransomware group broadcasted a pro-Russian message pledging its allegiance to Vladimir Putin's ongoing invasion of Ukraine, an anonymous security researcher using the Twitter handle @ContiLeaks has leaked the syndicate's internal chats. The file dump, published by malware research group VX-Underground, is said to contain 13 months of chat logs between affiliates and	 Krebs on Security	Conti Ransomware Group Diaries, Part I: Evasion A Ukrainian security researcher this week leaked several years of internal chat logs and other sensitive data tied to Conti, an aggressive and ruthless Russian cybercrime group that focuses on deploying its ransomware to companies with more than \$100 million in annual revenue. The chat logs offer a fascinating glimpse into the challenges of running a sprawling criminal enterprise with more than 100 salaried employees. The records also provide insight into how Conti has dealt with its own internal breaches and attacks from private security firms and foreign governments.
 IT Security Guru	Conti ransomware group suffers another leak A Ukrainian researcher retaliating to Conti siding with Ukraine has dealt another devastating blow to the ransomware operation. More internal conversations have been leaked, alongside the source for their ransomware, administrative panels and more. The Ukrainian researcher, who uses the Twitter handle @ContiLeaks leaked 393 JSON files containing over 60,000 internal messages on Sunday. The messages [...] The post Conti ransomware group suffers another leak appeared first on IT Security Guru.	 The Hacker News	Critical Bugs Reported in Popular Open Source PJSIP SIP and Media Stack As many as five security vulnerabilities have been disclosed in the PJSIP open-source multimedia communication library that could be abused by an attacker to trigger arbitrary code execution and denial-of-service (DoS) in applications that use the protocol stack. The weaknesses were identified and reported by JFrog's Security Research team, following which the project maintainers released
 Cyware News - Latest Cyber	Critical GitLab vulnerability could allow attackers to steal runner registration tokens The vulnerability affects all versions from 12.10 to 14.6.4, all versions starting from 14.7 to 14.7.3, and all versions starting from 14.8 to 14.8.1, according to a security advisory from GitLab.	 The Hacker News	Critical Security Bugs Uncovered in VoIPmonitor Monitoring Software Critical security vulnerabilities have been uncovered in VoIPmonitor software that, if successfully exploited, could allow unauthenticated attackers to escalate privileges to the administrator level and execute arbitrary commands. Following responsible disclosure by researchers from Kerbit, an Ethiopia-based penetration-testing and vulnerability research firm, on December 15, 2021, the

<div>News</div>		<div>issues</div>
<div> <div> <div>CYWARE</div> <div>SOCIAL</div> <div>Cyware News - Latest Cyber News</div> </div> </div>	<div> Cyberstarts raises new \$200 million fund for cyber security investments The new "opportunity" fund would invest up to \$15 million per round in companies in its seed funds for Series A and B funding rounds, Cyberstarts founder Gili Raanan told Reuters. </div>	<div> <div> <div>threatpost</div> <div>Threatpost</div> </div> </div> <div> Daxin Espionage Backdoor Ups the Ante on Chinese Malware Via node-hopping, the espionage tool can reach computers that aren't even connected to the internet. </div>
<div> <div> <div>CYWARE</div> <div>SOCIAL</div> <div>Cyware News - Latest Cyber News</div> </div> </div>	<div> Euro Police Bust Gang Linked to Migrant Smugglers European police forces are claiming another win after busting a suspected cybercrime gang that used the dark web to distribute counterfeit ID documents for migrant smugglers. </div>	<div> <div> <div>The Hacker News</div> <div>The Hacker News</div> </div> </div> <div> Hackers Begin Weaponizing TCP Middlebox Reflection for Amplified DDoS Attacks Distributed denial-of-service (DDoS) attacks leveraging a new amplification technique called TCP Middlebox Reflection have been detected for the first time in the wild, six months after the novel attack mechanism was presented in theory. "The attack [...] abuses vulnerable firewalls and content filtering systems to reflect and amplify TCP traffic to a victim machine, creating a powerful DDoS </div>
<div> <div> <div>IT SECURITY GURU</div> <div>IT Security Guru</div> </div> </div>	<div> Hackers steal employee and internal data from Nvidia Nvidia has admitted that employee and internal data was stolen in an apparent ransomware attack last week. The chip behemoth initially gave little away, announcing only that its "business and commercial activities continue uninterrupted" while the attack was investigated. A new statement provided more information: "Shortly after discovering the incident, we further hardened our network, [...] The post Hackers steal employee and internal data from Nvidia appeared first on IT Security Guru. </div>	<div> <div> <div>CYWARE</div> <div>SOCIAL</div> <div>Cyware News - Latest Cyber News</div> </div> </div> <div> Hundreds of eBike phishing sites abuse Google Ads to push scams A large-scale campaign involving over 200 phishing and scam sites has tricked users into giving their personal data to fake investments schemes impersonating genuine brands. </div>
<div> <div> <div>cyberscoop</div> <div>CyberScoop</div> </div> </div>	<div> In response to Russia threat, US cybersecurity firms offer free services, data, threat intel 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 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, [...] </div>	<div> <div> <div>eset</div> <div>WeLiveSecurity</div> </div> </div> <div> IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine ESET researchers uncover a new wiper that attacks Ukrainian organizations and a worm component that spreads HermeticWiper in local networks The post IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine appeared first on WeLiveSecurity </div>
<div> <div> <div>Security Affairs</div> </div> </div>	<div> IsaacWiper, the third wiper spotted since the beginning of the Russian invasion IsaacWiper, a new data wiper was used against an unnamed Ukrainian government network after Russia's invasion of Ukraine. ESET researchers uncovered a new data wiper, tracked as IsaacWiper, that was used against an unnamed Ukrainian government network after Russia's invasion of Ukraine. The wiper was first spotted on February 24 within an organization that was [...] The post IsaacWiper, the third wiper spotted since the beginning of the Russian invasion appeared first on Security Affairs. </div>	<div> <div> <div>threatpost</div> <div>Threatpost</div> </div> </div> <div> RCE Bugs in WhatsApp, Other Hugely Popular VoIP Apps: Patch Now! The flaws are in the ubiquitous open-source PJSIP multimedia communication library, used by the Asterisk PBX toolkit that's found in a massive number of VoIP implementations. </div>
<div> <div> <div>The Hacker News</div> <div>The Hacker News</div> </div> </div>	<div> Second New 'IsaacWiper' Data Wiper Targets Ukraine After Russian Invasion A new data wiper malware has been observed deployed against an unnamed Ukrainian government network, a day after destructive cyber attacks struck multiple entities in the country preceding the start of Russia's military invasion. Slovak cybersecurity firm ESET dubbed the new malware "IsaacWiper," which it said was detected on February 24 in an organization that was not affected by HermeticWiper </div>	<div> <div> <div>cyberscoop</div> <div>CyberScoop</div> </div> </div> <div> Security experts say Ukraine's request to shut down Russian domains could hurt civilians Ukrainian officials sent an urgent request Monday to the nonprofit that stewards domain and IP systems key to the global internet, but security experts are warning that it's not as simple as it looks. Ukraine asked the Internet Corporation for Assigned Names and Numbers (ICANN) to shut down Russian top-level domains -- such as those with the .ru country code -- in response to Russia's use of the internet as a key attack surface for both information operations and cyberattacks. ICANN has not yet responded to the request, Andrii Nabok, head of the expert group for the development of fixed broadband at Ukraine's Ministry of Digital Transformation and Ukraine's representative to ICANN, confirmed[...] </div>
<div> <div> <div>CYWARE</div> <div>SOCIAL</div> <div>Cyware News - Latest Cyber News</div> </div> </div>	<div> SMS PVA Part 2: Underground Service for Cybercriminals SMS verification has become the standard for verifying the users behind accounts for online platforms. But because of new services like SMS PVA, cybercriminals can now bypass this method. </div>	<div> <div> <div>The Hacker News</div> <div>The Hacker News</div> </div> </div> <div> TeaBot Android Banking Malware Spreads Again Through Google Play Store Apps An Android banking trojan designed to steal credentials and SMS messages has been observed once again sneaking past Google Play Store protections to target users of more than 400 banking and financial apps, including those from Russia, China, and the U.S. "TeaBot RAT capabilities are achieved via the device screen's live streaming (requested on-demand) plus the abuse of Accessibility Services </div>
<div> <div> <div>ZDNet</div> <div>ZDNet security RSS</div> </div> </div>	<div> TeaBot Android Banking Trojan continues its global conquest with new upgrades The RAT has is now targeting over 400 applications. </div>	<div> <div> <div>CYWARE</div> <div>SOCIAL</div> <div>Cyware News - Latest Cyber News</div> </div> </div> <div> Threat Actors to Shift Focus Back to Consumers In comparison to organizations, consumers are less secure, have fewer resources, and sometimes miss having a reliable antivirus solution. </div>
<div> <div> <div>The Hacker News</div> <div>The Hacker News</div> </div> </div>	<div> TrickBot Malware Gang Upgrades its AnchorDNS Backdoor to AnchorMail Even as the TrickBot infrastructure closed shop, the operators of the malware are continuing to refine and retool their arsenal to carry out attacks that culminated in the deployment of Conti ransomware. IBM Security X-Force, which discovered the revamped version of the criminal gang's AnchorDNS backdoor, dubbed the new, upgraded variant AnchorMail. AnchorMail "uses an email-based [</div>	<div> <div> <div>ZDNet</div> <div>ZDNet security RSS</div> </div> </div> <div> Ukraine asks cryptocurrency firms to block Russian users The request comes at a time when economic sanctions are sending shockwaves through the Russian banking system. </div>
<div> <div> <div>threatpost</div> <div>Threatpost</div> </div> </div>	<div> Ukraine Hit with Novel 'FoxBlade' Trojan Hours Before Invasion Microsoft detected cyberattacks launched against Ukraine hours before Russia's tanks and missiles began to pummel the country last week. </div>	<div> <div> <div>Security Affairs</div> </div> </div> <div> Ukrainian researcher leaked the source code of Conti Ransomware A Ukrainian researcher leaked the source for the Conti ransomware and components for the control panels. Recently 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. He was able to access the database XMPP chat server of the Conti group. Clearly, the [...] The post Ukrainian researcher leaked the source code of Conti Ransomware appeared first on Security Affairs. </div>
<div> <div> <div>cyberscoop</div> <div>CyberScoop</div> </div> </div>	<div> US chip maker Nvidia says hackers breached company, stole data Hackers stole employee user logins and proprietary company data from Nvidia last week, the U.S. chip maker said Tuesday, but added that it has not seen evidence of a ransomware attack. A ransomware group known as Lapsus\$ claims to be leaking Nvidia data. "We have no evidence of ransomware being deployed on the NVIDIA environment or that this is related to the Russia-Ukraine conflict," a company spokesperson said. "We are aware that the threat </div>	<div> <div> <div>CYWARE</div> <div>SOCIAL</div> <div>Cyware</div> </div> </div> <div> Vulnerabilities in Lansweeper could lead to JavaScript, SQL injections Cisco Talos recently discovered multiple vulnerabilities in the Lansweeper IT asset management solution that could allow an attacker to inject JavaScript or SQL code on the targeted device. </div>

actor took employee credentials and some NVIDIA proprietary information from our systems and has begun leaking it online." The spokesperson did not answer questions about a Telegraph report that the incident partially shut down operations for two days. [...]

News - Latest Cyber News

CYWARE SOCIAL
Cyware News - Latest Cyber News

What Does TrickBot's Shutdown Imply?

After months of inactivity, operators behind the TrickBot malware botnet appear to went offline with their server infrastructure. Its TTPs were becoming highly detectable. Going by experts, the decline in the volume of the Trickbot campaigns is accompanied by the fact that its operators are working with Emotet malware. Organizations must equip themselves with reliable threat intel solutions to stay ahead of the curve.

CYWARE SOCIAL
Cyware News - Latest Cyber News

Xenomorph Trojan Spreading via Play Store to Target European Banks

A new banking trojan called Xenomorph was found distributing via Google Play Store in the form of fake performance-boosting apps, targeting European banks. It comes with a modular engine that abuses accessibility services, which may allow advanced capabilities. Experts recommend using an anti-malware app in smartphones and monitoring app behavior after installations.

Twitter

Open Source CVEs

(CVE-2022-0717): Out-of-bounds Read in mruby/mruby. Disclosed by , fixed by mruby maintainers... #opensource #CVE #bugbounty #security #vulnerability

Remotely Alerts

Severity: | Out-of-bounds Read in GitHub repository ... | CVE-2022-0717 | Link for more:

CVE.report

CVE-2022-0717 : Out-of-bounds Read in GitHub repository mruby/mruby prior to 3.2....

ThreatMeter

CVE-2022-0717 Out-of-bounds Read in GitHub repository mruby/mruby prior to 3.2. (CVSS:0.0) (Last Update:2022-02-23)

Tribe Security Inc.

CVE-2022-0717 #TribeSecure #CyberAwareness

Threat Intel Center

NEW: CVE-2022-0717 Out-of-bounds Read in GitHub repository mruby/mruby prior to 3.2.

Ursula von der Leyen

I met President @Zourabichvili S to discuss the current crisis. The EU stands by Georgia and supports its sovereignty and resilience in these difficult times. We are ready to step up our cooperation, including on cyber security, strategic communication and hybrid threats.

CVE

CVE-2022-0717 Out-of-bounds Read in GitHub repository mruby/mruby prior to 3.2.

Threat Intel Center

NEW: CVE-2022-0717 Out-of-bounds Read in GitHub repository mruby/mruby prior to 3.2. Severity: CRITICAL

vulnonym

V

My real name is CVE-2022-0717 but all my friends call me Lucid Turkey

CVE Analysis

CVE-2022-0717 #HarsiaInfo

Hernan Espinoza

CVEnew: CVE-2022-0717 Out-of-bounds Read in GitHub repository mruby/mruby prior to 3.2.

Vulmon Vulnerability Feed

CVE-2022-0717 Out-of-bounds Read in GitHub repository mruby/mruby prior to 3.2. Vulnerability Notification:




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: Hybrid Analysis

Top malicious URL

95% Threat score	http://117 (.) 217 (.) 146 (.) 43:58153/bin (.) sh	95% Threat sc
---------------------	---	------------------

91% Threat score	http://integrotech (.) com/	90% Threat sc
89% Threat score	https://siasky (.) net/IACmoXQBAWis818aRGvW636-EvGA2xtefltrjXsFdDhchQ/#ant (.) bert%40francotyp (.) com	88% Threat sc
88% Threat score	http://115 (.) 61 (.) 116 (.) 150:38640/Mozi (.) m	87% Threat sc
83% Threat score	http://mail (.) appraisal-hub (.) com/	82% Threat sc
79% Threat score	https://u25742990 (.) ct (.) sendgrid (.) net/ls/click?upn=qg2tCndjIB0ubEeeulEn8Www15B4B1zMsQLFECBsqq0a42Y-2B2dzezGFMh-2FsbytkfmKojXj7MPaoYYmw59scLrh85dbXlP3t0l5YKAwopzpT8-3DirV9_jOoM0syUzZRWRHQwR4YnLr1VYuoYEJv0LltMAgSs45SU-2FfnP2VX-2FNoC-2F-2Fz3XilyreVRBbbe2cNV-2FpD7UoHYmQlrmfTGx5Ce62e8b6-2B8iicMcORHkvfkUi8YYIL1Z7vCRgRH-2FBCasj9Ujbmrfir-2BwQOyht-2BzFuXzllsArcREq0lsOwyfQlvtjWwD6HzF39PWgu7TaqvqEmUVEcc14vnOGxHbQrCRN2JW3E2vUGZGywdmMx3F2ggQMvfaosn1Z4uxtXtc-2FvVARjp1aWHRakmyh8RLoe6Afp-2By16q3zpNqWhXWs1I8ihLMM93KLTQmD5384iMO1jUHLSo95GDRE-2BPDK4jwaVyeN0Fa5hyPFAZ51En35WQldgKy2kUUT3DYYPbaEDEFmz4-2FskOczyvC1jlTkFFvg2YsKDOgx0XC-2B00nFF2-2FQI-2BFwWR17qBMkRlbyhw0DG0FZjKS6yJbdfMFu0KhjUXJQg2lnlMqskElJqPClRr2Xmgc0kMM5kKK70Cib65mqRJP8vOAfsDGUsDj4S0CnDL1ONQKuwFAzoURZV-2FAQIFexMeR4WhLC87jACfC2lw5AyH9B49DdlgjRUo-2FoYSsMMeLYCWHYTDs60iuC3h3RHtbfOug6tU8naBV8buMGO-2FiSVCZOWdNnrndyWD3p8rxaOiZ4seCVLinnFf2Zyslwg72ltyBAh-2BG-2B8igrK8uW8gCMSPqSA46VGw0QNOVLkvZ9rTPp4RLGr90-2FFkwppa7B-2BWJnRo1L3pBdv7KVFgNKDoMxOrbZ5QwASqHvN-2FsD7y7sjjKs-2FviNot25W91bUX5LZpK0LvCeLgVY6itDduKaj17Fpf1sxqxy-2FRujt-2BTrvpX-2BKJmZgkA9nlg0g1dxGSYow-3D	79% Threat sc
77% Threat score	http://reueu (.) smtpgaze (.) com/tracking/qaR9ZGLkZQVIZmV1ZwDmAGpjAGt1AvM5qzS4qaR9ZQbkHj	77% Threat sc
77% Threat score	http://tracking (.) slcpackf (.) xyz/tracking/unsubscribe?d=Fivd2-0UifPmycPmra1STh35v_jX6XwZbwKR9bWP8CMwFVy6Ux4CHa5yOHvtDSqNPEhT-LNGornhcupTDFjcljyQUR8r2qnjKjM9Eta7bK0	77% Threat sc
77% Threat score	https://www (.) bptdmaluku (.) com/	77% Threat sc
74% Threat score	http://iranaks (.) org/	74% Threat score
72% Threat score	http://et-envue (.) com/	72% Threat sc

Source: *NIST*

NIST CVE: Critical	
CVE-2022-0717	Out-of-bounds Read in GitHub repository mruby/mruby prior to 3.2. CRITICAL Vector: network Created: 2022-02-23 Updated: 2022-03-02

Source: *NIST*

NIST CVE: High	
CVE-2022-0654	Exposure of Sensitive Information to an Unauthorized Actor in GitHub repository fgribreau/node-request-retry prior to 7.0.0. HIGH Vector: network Created: 2022-02-23 Updated: 2022-03-02
CVE-2022-0736	Insecure Temporary File in GitHub repository mlflow/mlflow prior to 1.23.1. HIGH Vector: network Created: 2022-02-23 Updated: 2022-03-02
CVE-2022-22336	IBM Sterling External Authentication Server and IBM Sterling Secure Proxy 6.0.3.0, 6.0.2.0, and 3.4.3.2 could allow a remote user to consume resources causing a denial of service due to a resource leak. HIGH Vector: network Created: 2022-02-23 Updated: 2022-03-02
CVE-2022-0729	Use of Out-of-range Pointer Offset in GitHub repository vim/vim prior to 8.2.4440. HIGH Vector: network Created: 2022-02-23 Updated: 2022-03-02

Source: *NIST*

NIST CVE: Medium	
CVE-2022-0719	Cross-site Scripting (XSS) - Reflected in GitHub repository microweber/microweber prior to 1.3. MEDIUM Vector: network Created: 2022-02-23 Updated: 2022-03-02
CVE-2022-22333	IBM Sterling Secure Proxy 6.0.3.0, 6.0.2.0, and 3.4.3.2 and IBM Sterling External Authentication Server are vulnerable a buffer overflow, due to the Jetty based GUI in the Secure Zone not properly validating the sizes of the form content and/or HTTP headers submitted. A local attacker positioned inside the Secure Zone could submit a specially crafted HTTP request to disrupt service. IBM X-Force ID: 219133. MEDIUM Vector: adjacent_network Created: 2022-02-23 Updated: 2022-03-02
CVE-2022-0724	Insecure Storage of Sensitive Information in GitHub repository microweber/microweber prior to 1.3. MEDIUM Vector: network Created: 2022-02-23 Updated: 2022-03-02
CVE-2022-0476	Denial of Service in GitHub repository radareorg/radare2 prior to 5.6.4. MEDIUM Vector: local Created: 2022-02-23 Updated: 2022-03-02
CVE-2022-0727	Improper Access Control in GitHub repository chocobozzz/peertube prior to 4.1.0. MEDIUM Vector: network Created: 2022-02-23 Updated: 2022-03-02
CVE-2022-0721	Insertion of Sensitive Information Into Debugging Code in GitHub repository microweber/microweber prior to 1.3. MEDIUM Vector: network Created: 2022-02-23 Updated: 2022-03-02









NIST CVE: Low

Nothing today








NIST CVE: Unrated


CVE-2022-22303	An exposure of sensitive system information to an unauthorized control sphere vulnerability [CWE-497] in FortiManager versions prior to 7.0.2, 6.4.7 and 6.2.9 may allow a low privileged authenticated user to gain access to the FortiGate users credentials via the config conflict file. UNRATED Vector: unkown Created: 2022-03-02 Updated: 2022-03-02	CVE-2021-44166	An improper access control vulnerability [CWE-284] in FortiToken Mobile (Android) external push notification 5.1.0 and below may allow a remote attacker having already obtained a user's password to access the protected system during the 2FA procedure, even though the deny button is clicked by the legitimate user. UNRATED Vector: unkown Created: 2022-03-02 Updated: 2022-03-02
CVE-2022-22301	An improper neutralization of special elements used in an OS Command vulnerability [CWE-78] in FortiAP-C console 5.4.0 through 5.4.3, 5.2.0 through 5.2.1 may allow an authenticated attacker to execute unauthorized commands by running CLI commands with specifically crafted arguments. UNRATED Vector: unkown Created: 2022-03-02 Updated: 2022-03-02	CVE-2021-45860	An integer overflow in DTSSStreamReader::findFrame() of tsMuxer git-2678966 allows attackers to cause a Denial of Service (DoS) via a crafted file. UNRATED Vector: unkown Created: 2022-03-02 Updated: 2022-03-02
CVE-2022-25051	An Off-by-one Error occurs in cmr113_decode of rtl_433 21.12 when decoding a crafted file. UNRATED Vector: unkown Created: 2022-03-02 Updated: 2022-03-02	CVE-2022-0577	Exposure of Sensitive Information to an Unauthorized Actor in GitHub repository scrapy/scrapy prior to 2.6.1. UNRATED Vector: unkown Created: 2022-03-02 Updated: 2022-03-02
CVE-2022-24407	In Cyrus SASL 2.1.17 through 2.1.27 before 2.1.28, plugins/sql.c does not escape the password for a SQL INSERT or UPDATE statement. UNRATED Vector: unkown Created: 2022-02-24 Updated: 2022-03-02	CVE-2022-25050	rtl_433 21.12 was discovered to contain a stack overflow in the function somfy_iohc_decode(). This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted file. UNRATED Vector: unkown Created: 2022-03-02 Updated: 2022-03-02
CVE-2021-45861	There is an Assertion `num <= INT_BIT` failed at BitStreamReader::skipBits in /bitStream.h:132 of tsMuxer git-c6a0277. UNRATED Vector: unkown Created: 2022-03-02 Updated: 2022-03-02	CVE-2021-45863	tsMuxer git-2678966 was discovered to contain a heap-based buffer overflow via the function HevcUnit::updateBits in hevc.cpp. UNRATED Vector: unkown Created: 2022-03-02 Updated: 2022-03-02
CVE-2021-45864	tsMuxer git-c6a0277 was discovered to contain a segmentation fault via DTSSStreamReader::findFrame in dtsStreamReader.cpp. UNRATED Vector: unkown Created: 2022-03-02 Updated: 2022-03-02		

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

Top spammers

 #1 Canadian Pharmacy A long time running pharmacy spam operation. They send tens of millions of spams per day using botnet techniques. Probably based in Eastern Europe, Ukraine/Russia. Host spammed web sites on botnets and on bulletproof Chinese & Russian web hosting.	 #2 PredictLabs / Sphere Digital This operation uses dozens of "hosting" companies as fronts to lease IP addresses which are then used to send spam. Based in Chicago, Illinois and Tangier, Morocco.
 #3 Hosting Response / Michael Boehm Snowshoe spam organization that uses large numbers of inexpensive, automated VPS hosting IP addresses and domains in whatever TLD is currently cheapest to send high volumes of spam to extremely dirty, scraped lists. Operates under many business and individual names. Owner or manager of these companies seems to be Michael Boehm and Associates.	 #4 Mint Global Marketing / Adgenics / Cabo Networks Florida affiliate spammers and bulletproof spam hosts
 #5 RetroCubes Web development, application development, and business training company that spams email appended lists, usually through ESPs that offer automated provisioning and services directed at small businesses.	 #6 Michael Persaud Long time snowshoe type spammer, raided by FBI then indicted in 2017 on federal wire fraud charges tied to his spamming operations.
 #7 Cyber World Internet Services/ e-Insites Bulletproof spam host operating Cyber World Internet Services / e-Insites, and currently spamming using a variety of aliases such as Brand 4 Marketing, Ad Media Plus, Site Traffic Network, RCM Delivery, and eBox. The company is owned or managed by Alvin Slocombe.	 #8 RR Media A high volume spam operation based in or run from Huntington Beach, CA, USA. The operation uses a variety of different names.



#9 **Kobeni Solutions**

High volume snowshoe spam operation based in Florida. The manager or owner of the company seems to be a Yair Shalev / . (Former?) partner-in-spam of ROKSO spammer Darrin Wohl. Son-in-law of ROKSO-listed spammer Dan Abramovich. Sued for fraud by the US FTC in 2014.










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

Source: [Hybrid Analysis](#)

Top malicious files

100% Threat score	roblox-script-exploit-FULL-2022 (.) exe	100% Threat score	kReg (.) exe
100% Threat score	rlleoevod (.) xlsb	100% Threat score	IDM6 (.) 40_Patch (.) exe
100% Threat score	Client (.) exe	100% Threat score	Change of Address (.) xlsx
100% Threat score	New Address and payment details (.) xlsx	100% Threat score	5_protected (.) exe
100% Threat score	Client_protected (.) exe	100% Threat score	MicrosoftToolkit (.) exe
98% Threat score	payment (.) xlsx	95% Threat score	ICBCSetupIntegration_64 (.) msi
76% Threat score	fixdamage (.) exe	74% Threat score	AWB_spedizione_ricevuta_20222002987773000000 (.) xlsx

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