



Your Security Rabbits report for February 25, 2022

Hot topics

Ukraine, of course

As we said in January, there's a cyber-war going on. Today's target is Ukraine. Tomorrow's target could be your country.

What can you do?

- Assume the worst. **What is your remediation plan** if your critical systems are down?
- Have an up-to-date backup of your data and critical systems. Also, make sure you have an **offline** copy.
- If you don't have any **DDOS protection**, check how you can have one ready quickly.

--

JL Dupont

News



CISA Alerts

AA22-055A : Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks

Actions to Take Today to Protect Against Malicious Activity * Search for indicators of compromise. * Use antivirus software. * Patch all systems. * Prioritize patching known exploited vulnerabilities. * Train users to recognize and report phishing attempts. * Use multi-factor authentication. Note: this advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK(r)) framework, version 10. See the ATT&CK for Enterprise for all referenced threat actor tactics and techniques. The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the U.S. Cyber Command Cyber National[...]



Security
Affairs

CISA adds two Zabbix flaws to its Known Exploited Vulnerabilities Catalog

US CISA added two flaws impacting Zabbix infrastructure monitoring tool to its Known Exploited Vulnerabilities Catalog. US Cybersecurity and Infrastructure Security Agency (CISA) added two new vulnerabilities impacting the Zabbix infrastructure monitoring tool to its Known Exploited Vulnerabilities Catalog. Threat actors are actively exploiting the two vulnerabilities that are reported in the following table: CVE ID Vulnerability Name Due [...] The post CISA adds two Zabbix flaws to its Known Exploited Vulnerabilities Catalog appeared first on Security Affairs.



The Hacker
News

CISA Alerts on Actively Exploited Flaws in Zabbix Network Monitoring Platform

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has warned of active exploitation of two security flaws impacting Zabbix open-source enterprise monitoring platform, adding them to its Known Exploited Vulnerabilities Catalog. On top of that, CISA is also recommending that Federal Civilian Executive Branch (FCEB) agencies patch all systems against the vulnerabilities by March 8,



Cyware
News -
Latest Cyber
News

Citibank phishing baits customers with fake suspension alerts

An ongoing large-scale phishing campaign is targeting customers of Citibank, requesting recipients to disclose sensitive personal details to lift alleged bank account holds.



Cyware
News -
Latest Cyber
News

Cuba Ransomware Operations Exploits Microsoft Exchange Servers to Gain Access to Corporate Networks

The Cuba ransomware operation is exploiting Exchange vulnerabilities to gain access to corporate networks and encrypt devices. Cuba is a ransomware operation that launched at the end of 2019.



Threatpost

Cyberattackers Leverage DocuSign to Steal Microsoft Outlook Logins

A targeted phishing attack takes aim at a major U.S. payments company.



ZDNet |
security RSS

Darktrace acquires attack surface analytics firm Cybersprint

Darktrace says the deal will bolster the firm's artificial intelligence (AI) capabilities.



Security
Affairs

Data wiper attacks on Ukraine were planned at least in November and used ransomware as decoy

Experts reported that the wiper attacks that yesterday hit hundreds of systems in Ukraine used a GoLang-based ransomware decoy. Yesterday, researchers from cybersecurity firms ESET and Broadcom's Symantec discovered a new data wiper malware that was employed in a recent wave of attacks that hit hundreds of machines in Ukraine. A tweet from ESET revealed that the company's telemetry shows [...] The post Data wiper attacks on Ukraine were planned at least in November and used ransomware as decoy appeared first on Security Affairs.



Security
Affairs

Deadbolt Ransomware targets Asustor and QNAP NAS Devices

Deadbolt ransomware operators are targeting Asustor NAS (network-attached storage) appliances. Storage solutions provider Asustor is warning its customers of a wave of Deadbolt ransomware attacks targeting its NAS devices. Since January, Deadbolt ransomware operators are targeting QNAP NAS devices worldwide, its operators claim the availability of a zero-day exploit that allows them to encrypt the [...] The post Deadbolt Ransomware targets Asustor and QNAP NAS Devices appeared first on Security Affairs.



Cyware
News -
Latest Cyber
News

eSentire Raises US\$325M in Funding

The MDR provider eSentire raised US\$325M in private equity funding. The round was led by Georgian, with participation from Caisse de depot et placement du Quebec (CDPQ) and Warburg Pincus.



CyberScoop

FBI, CISA, Cyber Command take aim at cyber-espionage by Iran's MuddyWater group

U.S. and U.K. government agencies called out Iranian government-affiliated hackers Thursday, accusing them of being behind cyber-espionage targeting the defense, local government, oil and natural gas and telecommunications sectors across the globe. The joint alert points a finger at MuddyWater, which the U.S. government for the first time last month attributed directly to Tehran. In the latest warning, the government agencies said that they have observed MuddyWater on the move in Africa, Asia, Europe and North America since 2018. "MuddyWater actors are positioned both to provide stolen data and accesses to the Iranian government and to share these with other malicious cyber actors," reads th[...]



IT Security
Guru

Free Cyber Skills Training Launched for UK Pupils

The UK government has announced plans to provide free cyber skills training secondary school pupils. The program, dubbed Cyber Explorers, intends to educate 30,000 11 to 14-year-olds on many cybersecurity concepts, including open-source intelligence, digital forensics and social engineering. Students will use a new online learning platform to explore a range of scenarios, collecting virtual [...] The post Free Cyber Skills Training Launched for UK Pupils appeared first on IT Security Guru.



The Hacker
News

From Pet Systems to Cattle Farm -- What Happened to the Data Center?

























There's something about craftsmanship. It's personal, its artistry, and it can be incredibly effective in achieving its goals. On the other hand, mass-market production can be effective in other ways, through speed, efficiency, and cost savings. The story of data centers is one of going from craftsmanship - where every individual machine is a pet project, maintained with great care - to mass


















WeLiveSecurity

HermeticWiper: New data-wiping malware hits Ukraine

Hundreds of computers in Ukraine compromised just hours after a wave of DDoS attacks brings down a number of Ukrainian websites The post HermeticWiper: New data-wiping malware hits Ukraine appeared first on WeLiveSecurity

 Threatpost	Microsoft App Store Sizzling with New 'Electron Bot' Malware The SEO poisoning bot, capable of full system takeover, is actively taking over social media accounts, masquerading as popular games like Temple Run.	 Cyware News - Latest Cyber News	Network Hackers Focus on Selling Access to High-Value Targets in the U.S. A CrowdStrike report looking into access brokers' advertisements since 2019 has identified a preference in academic, government, and technology entities based in the United States.
 The Hacker News	New Flaws Discovered in Cisco's Network Operating System for Switches Cisco has released software updates to address four security vulnerabilities in its software that could be weaponized by malicious actors to take control of affected systems. The most critical of the flaws is CVE-2022-20650 (CVSS score: 8.8), which relates to a command injection flaw in the NX-API feature of Cisco NX-OS Software that stems from a lack of sufficient input validation of	 Security Affairs	New Wiper Malware HermeticWiper targets Ukrainian systems Cybersecurity experts discovered a new data wiper malware that was used in attacks against hundreds of machines in Ukraine. The threat of hybrid warfare is reality, Russia-linked APT group have supported the operations of the Russian army while preparing for the invasion. Researchers from cybersecurity firms ESET and Broadcom's Symantec discovered a new data wiper malware that was employed in [...] The post New Wiper Malware HermeticWiper targets Ukrainian systems appeared first on Security Affairs.
 Cyware News - Latest Cyber News	New York to Get Statewide Cybersecurity Center The center was announced by state governor Kathy Hochul on Tuesday at a joint conference held with the mayors of New York City, Albany, Buffalo, Rochester, Syracuse, and Yonkers.	 The Hacker News	Notorious TrickBot Malware Gang Shuts Down its Botnet Infrastructure The modular Windows crimeware platform known as TrickBot formally shuttered its infrastructure on Thursday after reports emerged of its imminent retirement amid a lull in its activity for almost two months, marking an end to one of the most persistent malware campaigns in recent years. "TrickBot is gone... It is official now as of Thursday, February 24, 2022. See you soon... or not," AdvIntel's
 The Hacker News	Putin Warns Russian Critical Infrastructure to Brace for Potential Cyber Attacks The Russian government on Thursday warned of cyber attacks aimed at domestic critical infrastructure operators, as the country's full-blown invasion of Ukraine enters the second day. In addition to cautioning of the "threat of an increase in the intensity of computer attacks," Russia's National Computer Incident Response and Coordination Center said that the "attacks can be aimed at disrupting	 CyberScoop	Putin's government warns Russian critical infrastructure of potential cyberattacks The Russian government warned its domestic critical infrastructure operators Thursday of the "threat of an increase in the intensity of computer attacks," and said that any failure in the operation of critical infrastructure that doesn't have a "reliably established" cause should be considered "the result of a computer attack." The warning, issued through Russia's National Computer Incident Response & Coordination Center, comes as the Russian military carries out a widespread attack on Ukraine, and after the Ukrainian government accused the Russians of launching a series of distributed denial-of-service attacks and the deployment of wiper malware on Ukrainian government systems ahead of [...]
 IT Security Guru	Ransomware extortion doesn't end after paying up A study carried out by cyber security specialist Venafi has confirmed existing fears that in most cases of paying the ransom, extortion simply continues. Key findings include: 18% of victims who paid the ransom still had their data exposed on the dark web. 8% refused to pay the ransom, and the attackers tried to extort [...] The post Ransomware extortion doesn't end after paying up appeared first on IT Security Guru.	 Cyware News - Latest Cyber News	Ransomware used as decoy in data-wiping attacks on Ukraine The ransomware decoy also dropped a ransom note on compromised systems, with a political message saying that "The only thing that we learn from new elections is we learned nothing from the old!"
 Cyware News - Latest Cyber News	Ransomware wreaked havoc last year, manufacturing was most targeted While phishing was the most common cause of cyberattacks in general in the past year, there was a 33% increase in attacks caused by vulnerability exploitation of unpatched software.	 Sophos Naked Security	S3 Ep71: VMware escapes, PHP holes, WP plugin woes, and scary scams [Podcast + Transcript] Latest episode - listen now!
 Threatpost	The Art of Non-boring Cybersec Training-Podcast With human error being the common factor in most cyberattacks, employee training has got to get better. To that end, Trustwave cybersec training expert Darren Van Booven explains the importance of fish stress balls and management buy-in.	 Threatpost	The Harsh Truths of Cybersecurity in 2022, Part II Sonya Duffin, ransomware and data-protection expert at Veritas Technologies, shares three steps organizations can take today to reduce cyberattack fallout.
 The Hacker News	TrickBot Gang Likely Shifting Operations to Switch to New Malware TrickBot, the infamous Windows crimeware-as-a-service (CaaS) solution that's used by a variety of threat actors to deliver next-stage payloads like ransomware, appears to be undergoing a transition of sorts, with no new activity recorded since the start of the year. The lull in the malware campaigns is "partially due to a big shift from Trickbot's operators, including working with the operators	 The Hacker News	U.S., U.K. Agencies Warn of New Russian Botnet Built from Hacked Firewall Devices Intelligence agencies in the U.K. and the U.S. disclosed details of a new botnet malware called Cyclops Blink that's been attributed to the Russian-backed Sandworm hacking group and deployed in attacks dating back to 2019. "Cyclops Blink appears to be a replacement framework for the VPNFilter malware exposed in 2018, which exploited network devices, primarily small office/home office (SOHO)
 Cyware News - Latest Cyber News	UK Launches Free Cyber Skills Training for Secondary School Pupils The Cyber Explorers program aims to educate 30,000 11 to 14-year-olds on a range of cybersecurity concepts, such as open-source intelligence, digital forensics and social engineering.	 IT Security Guru	Ukraine calls for volunteer hackers to aid in cyber-war Ukraine's government has reportedly called for volunteers with hacking skills to aid in the protection of the country's critical infrastructure. Reuters reported on February 24 that government-backed notices have appeared in online forums. Co-founder of Cyber Unit Technologies and major Ukrainian promotor of ethical hacking Yegor Aushev told the news agency that he wrote the [...] The post Ukraine calls for volunteer hackers to aid in cyber-war appeared first on IT Security Guru.
 ZDNet security RSS	Ukraine calls for volunteer hackers to protect critical infrastructure: report The country is reportedly asking volunteers to join digital defensive and surveillance missions.	 Security Affairs	US and UK details a new Python backdoor used by MuddyWater APT group US and UK cybersecurity agencies provided details of a new malware used by Iran-linked MuddyWater APT. CISA, the FBI, the US Cyber Command's Cyber National Mission Force (CNMF), UK's National Cyber Security Centre (NCSC-UK), and the NSA, and law enforcement agencies have published a joint advisory on new malware used by Iran-linked MuddyWater APT group [...] The post US and UK details a new Python backdoor used by MuddyWater APT group appeared first on Security Affairs.
 Cyware News - Latest Cyber News	US braces for Russian cyberattacks as Ukraine conflict escalates. Here's how that might play out The US government is on high alert for the possibility of the conflict spilling over into cyberspace, where Russia has shown an ability to cause significant disruption and damage in the past.	 Cyware News - Latest Cyber News	Vishing Makes Phishing Campaigns Three Times More Successful Phishing emerged as the number one threat vector in 2021, but cases of vulnerability exploitation surged 33% year-on-year thanks to the impact of Log4Shell, according to IBM.
 The Hacker News	Warning -- Deadbolt Ransomware Targeting ASUSTOR NAS Devices ASUSTOR network-attached storage (NAS) devices have become the latest victim of Deadbolt ransomware, less than a month after similar attacks singled out QNAP NAS appliances. In response to the infections, the company has released firmware updates (ADM 4.0.4.RQO2) to "fix related security issues." The company is also urging users to take the following actions to keep data secure -	 Threatpost	Web Filtering and Compliances for Wi-Fi Providers Demand for public Wi-Fi is on the rise. Usually free of charge, but there is a risk of expensive losses. Learn ways to protect yourself from cyber-threats.
	White House Denies Mulling Massive Cyberattacks Against Russia		Zenly Social-Media App Bugs Allow Account Takeover

 Threatpost	The options reportedly included tampering with trains, electric service and internet connectivity, hampering Russia's military operations in Ukraine.	 Threatpost	A pair of bugs in the Snap-owned tracking app reveal phone numbers and allow account hijacking.
Twitter			
 CVE	CVE-2022-22912 Prototype pollution vulnerability via .parse() in Plist before v3.0.4 allows attackers to cause a Denial of Service (DoS) and may lead to remote code execution.	 CVE	CVE-2021-44868 A problem was found in ming-soft MCMS v5.1. There is a sql injection vulnerability in /ms/cms/content/list.do
 Threat Intel Center	NEW: CVE-2021-44868 A problem was found in ming-soft MCMS v5.1. There is a sql injection vulnerability in /ms/cms/content/list.do	 Remotely Alerts	Severity: A problem was found in ming-soft MCMS v5... CVE-2021-44868 Link for more:
 Threat Intel Center	NEW: CVE-2021-44868 A problem was found in ming-soft MCMS v5.1. There is a sql injection vulnerability in /ms/cms/content/list.do Severity: CRITICAL	 ThreatMeter	CVE-2021-44868 A problem was found in ming-soft MCMS v5.1. There is a sql injection vulnerability in /ms/cms/content/list.do (CVSS:0.0) (Last Update:2022-02-17)
 Tribe Security Inc.	CVE-2021-44868 #TribeSecure #CyberAwareness	 Vulmon Vulnerability Feed	CVE-2021-44868 A problem was found in ming-soft MCMS v5.1. There is a sql injection vulnerability in /ms/cms/content/list.do
 Remotely Alerts	Severity: Prototype pollution vulnerability via .p... CVE-2022-22912 Link for more:	 Threat Intel Center	NEW: CVE-2022-22912 Prototype pollution vulnerability via .parse() in Plist before v3.0.4 allows attackers to cause a Denial of Service (DoS) and may lead to remote code execution. Severity: CRITICAL
 Threat Intel Center	NEW: CVE-2022-22912 Prototype pollution vulnerability via .parse() in Plist before v3.0.4 allows attackers to cause a Denial of Service (DoS) and may lead to remote code execution.	 Vulmon Vulnerability Feed	CVE-2022-22912 Prototype pollution vulnerability via .parse() in Plist before v3.0.4 allows attackers to cause a Denial of Service (DoS) and may lead to remote code execution.
 Jane Lytvynenko	NEWSROOMS: Make sure your reporters, eds, photographers, admin staff, and anyone else involved in covering this war has strong cybersecurity hygiene. Vet sources. Check documents. Be aware of phishing attack potential. 2fa everywhere via an app. Password variation. Everything.		

Source: [NIST](#)

NIST CVE: Critical

CVE-2021-44868	A problem was found in ming-soft MCMS v5.1. There is a sql injection vulnerability in /ms/cms/content/list.do CRITICAL Vector: network Created: 2022-02-17 Updated: 2022-02-25	CVE-2022-22912	Prototype pollution vulnerability via .parse() in Plist before v3.0.4 allows attackers to cause a Denial of Service (DoS) and may lead to remote code execution. CRITICAL Vector: network Created: 2022-02-17 Updated: 2022-02-25
----------------	--	----------------	--

Source: [NIST](#)

NIST CVE: High

CVE-2022-23318	A heap-buffer-overflow in pcf2bdf, versions >= 1.05 allows an attacker to trigger unsafe memory access via a specially crafted PCF font file. This out-of-bound read may lead to an application crash, information disclosure via program memory or other context-dependent impact. HIGH Vector: local Created: 2022-02-17 Updated: 2022-02-25	CVE-2022-24683	HashiCorp Nomad and Nomad Enterprise 0.9.2 through 1.0.17, 1.1.11, and 1.2.5 allow operators with read-fs and alloc-exec (or job-submit) capabilities to read arbitrary files on the host filesystem as root. HIGH Vector: network Created: 2022-02-17 Updated: 2022-02-25
CVE-2021-46368	TRIGONE Remote System Monitor 3.61 is vulnerable to an unquoted path service allowing local users to launch processes with elevated privileges. HIGH Vector: local Created: 2022-02-17 Updated: 2022-02-25		

Source: [NIST](#)

NIST CVE: Medium

CVE-2022-23319	A segmentation fault during PCF file parsing in pcf2bdf versions >=1.05 allows an attacker to trigger a program crash via a specially crafted PCF font file. This crash affects the availability of the software and dependent downstream components. MEDIUM Vector: local Created: 2022-02-17 Updated: 2022-02-25	CVE-2022-0638	Cross-Site Request Forgery (CSRF) in Packagist microweber/microweber prior to 1.2.11. MEDIUM Vector: network Created: 2022-02-17 Updated: 2022-02-25
CVE-2022-0585	Large loops in multiple protocol dissectors in Wireshark 3.6.0 to 3.6.1 and 3.4.0 to 3.4.11 allow denial of service via packet injection or crafted capture file MEDIUM Vector: network Created: 2022-02-18 Updated: 2022-02-25		

Source: [NIST](#)

NIST CVE: Low

Source: NIST

NIST CVE: Unrated			
CVE-2022-23835	<p>** DISPUTED ** The Visual Voice Mail (VVM) application through 2022-02-24 for Android allows persistent access if an attacker temporarily controls an application that has the READ_SMS permission, and reads an IMAP credentialing message that is (by design) not displayed to the victim within the AOSP SMS/MMS messaging application. (Often, the IMAP credentials are usable to listen to voice mail messages sent before the vulnerability was exploited, in addition to new ones.) NOTE: some vendors characterize this as not a "concrete and exploitable risk."</p> <p>UNRATED Vector: unknown Created: 2022-02-25 Updated: 2022-02-25</p>	CVE-2022-24948	<p>A carefully crafted user preferences for submission could trigger an XSS vulnerability on Apache JSPWiki, related to the user preferences screen, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim. Apache JSPWiki users should upgrade to 2.11.2 or later.</p> <p>UNRATED Vector: unknown Created: 2022-02-25 Updated: 2022-02-25</p>
CVE-2021-34359	<p>A cross-site scripting (XSS) vulnerability has been reported to affect QNAP device running Proxy Server. If exploited, this vulnerability allows remote attackers to inject malicious code. We have already fixed this vulnerability in the following versions of Proxy Server: QTS 4.5.x: Proxy Server 1.4.2 (2021/12/30) and later</p> <p>UNRATED Vector: unknown Created: 2022-02-25 Updated: 2022-02-25</p>	CVE-2021-34361	<p>A cross-site scripting (XSS) vulnerability has been reported to affect QNAP device running Proxy Server. If exploited, this vulnerability allows remote attackers to inject malicious code. We have already fixed this vulnerability in the following versions of Proxy Server: QTS 4.5.x: Proxy Server 1.4.2 (2021/12/30) and later</p> <p>UNRATED Vector: unknown Created: 2022-02-25 Updated: 2022-02-25</p>
CVE-2021-3930	<p>An off-by-one error was found in the SCSI device emulation in QEMU. It could occur while processing MODE_SELECT commands in mode_sense_page() if the 'page' argument was set to MODE_PAGE_ALLS (0x3f). A malicious guest could use this flaw to potentially crash QEMU, resulting in a denial of service condition.</p> <p>UNRATED Vector: unknown Created: 2022-02-18 Updated: 2022-02-25</p>	CVE-2022-24947	<p>Apache JSPWiki user preferences form is vulnerable to CSRF attacks, which can lead to account takeover. Apache JSPWiki users should upgrade to 2.11.2 or later.</p> <p>UNRATED Vector: unknown Created: 2022-02-25 Updated: 2022-02-25</p>
CVE-2022-0746	<p>Business Logic Errors in GitHub repository dolibarr/dolibarr prior to 16.0.</p> <p>UNRATED Vector: unknown Created: 2022-02-25 Updated: 2022-02-25</p>	CVE-2022-24288	<p>In Apache Airflow, prior to version 2.2.4, some example DAGs did not properly sanitize user-provided params, making them susceptible to OS Command Injection from the web UI.</p> <p>UNRATED Vector: unknown Created: 2022-02-25 Updated: 2022-02-25</p>
CVE-2021-45229	<p>It was discovered that the "Trigger DAG with config" screen was susceptible to XSS attacks via the 'origin' query argument. This issue affects Apache Airflow versions 2.2.3 and below.</p> <p>UNRATED Vector: unknown Created: 2022-02-25 Updated: 2022-02-25</p>		

Source: Hybrid Analysis

Top malicious files			
100% Threat score	d957239ba4d314e47de9748e77a229f4f969f55b3fcf54a096e7971c7f1bab7d	100% Threat score	Ãñilek v1 (.) 4 (.) exe
100% Threat score	BFFA331C60CF3BF37158B1A75F8B2369B9045A6020404BA110A80696702486A9	100% Threat score	FBF2C76ACB5612320A23945892ED8246D9063ED9E06556399584C454417702C
100% Threat score	59e4510b7b15011d67eb2f80484589f7211e67756906a87ce466a7bb68f2095b	100% Threat score	93bb93d87cedb0a99976c18a37d65f816dc904942a0fb39cc177d49372ed54e5
100% Threat score	833070159999aa255420441ba2f2f188ab949b170d766b840a5be0885f745457	100% Threat score	59d212b7a8455a10162064b153fa9b0968ef6e29ab6bda4b5d6c5fc1f99cd8f7
100% Threat score	78b16177d8c5b2e06622688a9196ce7452ca1b25a350daae8c4f12c2e415065c	100% Threat score	c42865e79497dbba80cfd806e0d3dc58769212fca2f9e82620029503b6ef7d8a
100% Threat score	rapport-25022022 (.) xism	100% Threat score	tmpd93e2_z0
100% Threat score	avast_one_essential_setup_online (.) exe	100% Threat score	top566543 (.) exe
100% Threat score	VAB362106274YL (.) xls	100% Threat score	Setup (.) exe
100% Threat score	1ade7bd06099af280d58303c74ecf505282e5682c39f9eb0cd1d56e96228c59b	96% Threat score	nv (.) i586
95% Threat score	birth certificate (.) pdf	85% Threat score	2022-02-25_1538 (.) xism
80% Threat score	e4069c98fa80dec6b89388c437a81cb451bc6b2ee55194155b8c5b7422d4ff1e	80% Threat score	e4069c98fa80dec6b89388c437a81cb451bc6b2ee55194155b8c5b7422d4ff1e
79% Threat score	hfekfbse (.) txt	75% Threat score	setup (.) exe
75% Threat score	zarplataup_2_9661 (.) exe	71% Threat score	c556922f-0037-4e18-a12e-2e75d90248b2 (.) exe











Source: Hybrid Analysis

Top malicious URL			
100% Threat score	http://surname192 (.) temp (.) swtest (.) ru/prapor/su/flags (.) gif	100% Threat score	https://www (.) cuisine-house (.) com/readme (.) php

88% Threat score	http://117(.)222(.)169(.)30:60888/i	88% Threat score	http://117(.)205(.)85(.)56:46333/Mozi(.)a
87% Threat score	http://leaniconetechnology(.)com/	86% Threat score	https://hoverspec(.)com/123(.)exe
85% Threat score	https://secure(.)seoserviceexpert(.)com/~rickrichardsinc/wp-admin/maint/chip/webapp/english(.)php?email=luis(.)leiva%40curiumpharma(.)com	85% Threat score	https://hoverspec(.)com/3(.)exe
82% Threat score	http://links(.)155hotel(.)com(.)br/accounts/132446/messages/20/clicks/42946/57?envelope_id=9	82% Threat score	http://nujg(.)ptic(.)ir/(.)xOEwG2lkuR(.)aHR0cHM6Ly9sb2dpci5ob21lLn9za2p1cy54eXovVktlQmtWV0g/ZW09cm9sYW5kdG9oQGZ1bGxlcuRvbi5jb20uc2c=
81% Threat score	http://coin-coin-data-6(.)com/files/341_1639757201_8653(.)exe	77% Threat score	https://gacs(.)com(.)pk/
77% Threat score	http://gridservicemarket(.)com/	77% Threat score	http://www(.)lendersubmitsecuritycontrolling2022(.)com/
77% Threat score	http://www(.)belizehighcommission(.)co(.)uk/	74% Threat score	https://u9313450(.)ct(.)sendgrid(.)net/ls/click?upn=XOagnSYYPGQ8cGAZqa-2FUeAPhpU0hMT2yri3GKZkDs8pHdlUiePD-2BGDEe9MQLFnnvcv4Hj_9qMgOv4s0KC3P8zeNZhIg-2Bzf-2F7QQafxt0yXtLeZtvX83AZFAErS0SYbIUo-2BUaQ83hXreUkCGKulb4MmKTdHv9p85gcQdVzI3yAtQBmOvlbrZOKYQNLWKmDB09o2LWluhj-2FNXvY-2BUTPWs0Baja4DoB3FXUL71-2FIdK0FKN9lR-2BrxuNIqt08u42V6djx9p-2FldRt0FgnNGC3VDUrLBYGUqOAd8JdCL-2BVCMlJd-2F5Wllb8OZ2n-2F9EiD6v4mzc2MxAEtHnHL6Xtw19XdDdiUBKKB7Jpeoy4lVEdlBDpU2fm0nGBRi92hPtjYbIp0pe9jhnedIv2%3E










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 Brazil
 #9 Japan	 #10 Korea, Republic of

Source: SpamHaus









Top spammers

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

Source: SpamHaus

Top countries with botnet

 #1 China	 #2 India
--	--

	#3 United States of America		#4 Indonesia
	#5 Thailand		#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 Japan		#4 Russia
	#5 Netherlands		#6 Hong Kong
	#7 France		#8 India
	#9 United Kingdom		#10 Australia