



Your Security Rabbits report for February 19, 2022

Hot topics

Nothing today

News



Attackers Abuse Poorly Regulated Top-Level Domains in Ongoing Redirect Campaign
One of the more common infections that seen is the site-wide redirects to spam and scam sites, achieved by attackers exploiting newly found vulnerabilities in popular WordPress plugins.



Critical Flaw Uncovered in WordPress Backup Plugin Used by Over 3 Million Sites
Patches have been issued to contain a "severe" security vulnerability in UpdraftPlus, a WordPress plugin with over three million installations, that can be weaponized to download the site's private data using an account on the vulnerable sites. "All versions of UpdraftPlus from March 2019 onwards have contained a vulnerability caused by a missing permissions-level check, allowing untrusted users



Documents shed light on ID.me's marketing to states about powerful facial recognition tech
Identity verification technology company ID.me quietly deployed a powerful form of facial recognition on unemployment benefits applicants while encouraging state partners to dispel the idea that the company used the technology, according to Oregon state records the American Civil Liberties Union shared with CyberScoop. The documents show that in the months following the introduction of facial recognition software that matched a photo across a wider database -- known as "1:many" -- into its fraud detection service, ID.me disseminated talking points to the Oregon Employment Department (OED) and other state partners to combat media reports that it used the more powerful form of facial recognit[...]



Google Privacy Sandbox promises to protect user privacy online
Google introduces Privacy Sandbox on Android aimed at leading to more private advertising solutions for mobile users. Google announced Privacy Sandbox on Android to limit user data sharing and prevent the use of cross-app identifiers. The company states that the Privacy Sandbox technologies are still in development. "Privacy Sandbox on Android will strengthen privacy, while [...] The post Google Privacy Sandbox promises to protect user privacy online appeared first on Security Affairs.



Iran-linked TunnelVision APT is actively exploiting the Log4j vulnerability
Iran-linked TunnelVision APT group is actively exploiting the Log4j vulnerability to deploy ransomware on unpatched VMware Horizon servers. Researchers from SentinelOne have observed the potentially destructive Iran-linked APT group TunnelVision is actively exploiting the Log4j vulnerability to deploy ransomware on unpatched VMware Horizon servers. TunnelVision's TTPs overlap with the ones associated with Iran-linked nation-state actors Phosphorus, Charming Kitten [...] The post Iran-linked TunnelVision APT is actively exploiting the Log4j vulnerability appeared first on Security Affairs.



Irony alert! PHP fixes security flaw in input validation code
What's wrong with this sequence? 1. Step into the road 2. Check if it's safe 3. Keep on walki...



Microsoft Warns of 'Ice Phishing' Threat on Web3 and Decentralized Networks
Microsoft has warned of emerging threats in the Web3 landscape, including "ice phishing" campaigns, as a surge in adoption of blockchain and DeFi technologies emphasizes the need to build security into the decentralized web while it's still in its early stages. The company's Microsoft 365 Defender Research Team called out various new avenues through which malicious actors may attempt to trick



New Critical RCE Bug Found in Adobe Commerce, Magento
Adobe updated its recent out-of-band security advisory to add another critical bug, while researchers put out a PoC for the one it emergency-fixed last weekend.



New WordPress Plugin Leaks Millions of Personal Information; Immediate Update is Suggested
A new WordPress plugin vulnerability is now putting millions of WordPress users at risk. This security issue is specifically found on UpdraftPlus, a cloning plugin for WordPress.



Conti ransomware gang takes over TrickBot malware operation
Researchers at cybercrime and adversarial disruption company Advanced Intelligence noticed that in 2021 Conti had become the only beneficiary of TrickBot's supply of high-quality network accesses.



Critical vulnerabilities in Zabbix Web Frontend allow authentication bypass, code execution on servers
SonarSource researchers, who discovered the bugs, noted that Zabbix is a high-profile target for threat actors due to its popularity, features, and its privileged position in most company's networks.



DSbD's Four Nations Roadshow Begins
Next week, UK Research and Innovation's Digital Security by Design (DSbD) challenge's Four Nations Roadshow begins. The roadshow will journey across England, Scotland, Wales, and Ireland and will feature talks from multiple speakers highlighting the developments in computing across the decades, the state of computing in the present day, and how we can move towards [...] The post DSbD's Four Nations Roadshow Begins appeared first on IT Security Guru.



How Russian and Ukrainian Militias Are Using Social Media and Chat Platforms to Recruit Volunteers in the Donbas and Fund Their Causes
As of this publishing, Russia has amassed 190,000 troops along the Ukrainian border, according to U.S. intelligence, in the Donbas region of Ukraine. Despite varying accounts from the frontlines, and constant posturing in the media from both Russian President Vladimir Putin and U.S. President Biden, the prospect of war remains an imminent possibility and not [...] The post How Russian and Ukrainian Militias Are Using Social Media and Chat Platforms to Recruit Volunteers in the Donbas and Fund Their Causes appeared first on Flashpoint.



Iranian State Broadcaster Clobbered by 'Clumsy, Buggy' Code
Researchers said a Jan. 27 attack that aired footage of opposition leaders calling for assassination of Iran's Supreme Leader was a clumsy and unsophisticated wiper attack.



Master Decryption Keys Released for Multiple Ransomware
The master decryption keys for Maze, Eggegor, and Sekhmet ransomware victims were released, as claimed, by one of the developers of the three ransomware. The poster on the forum said that this was a planned leak and did not have any relation to law enforcement operations. Though, experts suspect that the release of keys could be an attempt to trick law enforcement agencies.















Multiple Vulnerabilities in Adobe Commerce and Magento Could Allow for Remote Code Execution
Depending on the privileges associated with the user an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights in Adobe Commerce and Magento Open Source.















New Golang botnet empties Windows users' cryptocurrency wallets
A new Golang-based botnet under active development has been ensnaring hundreds of Microsoft Windows devices each time its operators deploy a new command and control (C2) server.



NSA Provides Guidance on Cisco Device Passwords
Cisco devices are used throughout the DoD, the defense industrial base, and national security systems, and any unsecured credentials on these devices could lead to entire networks getting compromised.

 <div>Cyware News - Latest Cyber News</div>	Phishing Emails and Excel Macros: Emotet Cooks New Infection Recipe Palo Alto Networks unearthed an ongoing email campaign by Emotet operators, which now propagates through malicious Excel files while also implementing other obfuscation techniques. For this, attackers have used email thread hijacking and some other attack tactics. Experts revealed they have been delivering an Excel file with an obfuscated Excel 4.0 macro via socially engineered emails since December 2021.	 <div>Cyware News - Latest Cyber News</div>	PseudoManuscript Malware Borrows Delivery Tactics from CryptBot to Attack Windows Systems Windows machines located in South Korea have been targeted by a botnet tracked as PseudoManuscript since at least May 2021 by employing the same delivery tactics of another malware called CryptBot.
 <div>The Hacker News</div>	PseudoManuscript Malware Spreading the Same Way as CryptBot Targets Koreans Numerous Windows machines located in South Korea have been targeted by a botnet tracked as PseudoManuscript since at least May 2021 by employing the same delivery tactics of another malware called CryptBot. "PseudoManuscript is disguised as an installer that is similar to a form of CryptBot, and is being distributed," South Korean cybersecurity company AhnLab Security Emergency Response Center ( <div>Threatpost</div>	Severe WordPress Plug-In UpdraftPlus Bug Threatens Backups An oversight in a WordPress plug-in exposes PII and authentication data to malicious insiders.
 <div>The Hacker News</div>	U.S. Cybersecurity Agency Publishes List of Free Security Tools and Services The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Friday published a repository of free tools and services to enable organizations to mitigate, detect, and respond effectively to malicious attacks and further improve their security posture. The "Free Cybersecurity Services and Tools" resource hub comprises a mix of services provided by CISA, open-source utilities, and other	 <div>Cyware News - Latest Cyber News</div>	Updated Trickbot Now Targets Technology and Financial Firms Check Point disclosed that an updated version of the TrickBot malware is targeting customers of 60 financial and technology firms primarily located in the U.S. Researchers believe that the actual victims are not the brands themselves but their customers. The malware stands as a priority threat, requiring continuous monitoring and tracking by the security community around the globe.
 <div>Security Affairs</div>	UpdraftPlus WordPress plugin update forced for million sites WordPress forces the update of the UpdraftPlus plugin patch on 3 million sites to fix a high-severity vulnerability. WordPress has forced the update of the UpdraftPlus plugin around three million sites to address a high-severity vulnerability, tracked as CVE-2022-0633 (CVSS v3.1 score of 8.5) that can allow website subscribers to download the latest database backups, which could potentially [...] The post UpdraftPlus WordPress plugin update forced for million sites appeared first on Security Affairs.	 <div>Cyware News - Latest Cyber News</div>	US, Britain Accuse Russia of Cyberattacks Targeting Ukraine The White House blamed Russia for this week's cyberattacks targeting Ukraine's defense ministry and major banks and warned of the potential for more significant disruptions in the days ahead.
 <div>Cyware News - Latest Cyber News</div>	VMware NSX Data Center Flaw Can Expose Virtual Systems to Attacks The vulnerability is tracked as CVE-2022-22945 and it has a CVSS score of 8.8. VMware described it as a CLI shell injection vulnerability affecting the product's NSX Edge appliance component.	 <div>Cyware News - Latest Cyber News</div>	Web Skimming Attackers Infect Element Vape E-cigarette Store to Steal Credit Cards Element Vape's website was found loading a malicious JavaScript file from a third-party website that appears to contain a credit card stealer, as reported by BleepingComputer.
 <div>Security Affairs</div>	White House and UK Gov attribute DDoS attacks on Ukraine to Russia's GRU The White House has linked the recent DDoS attacks against Ukraine 's banks and defense agencies to Russia's GRU. The White House has linked the recent DDoS attacks that took offline the sites of banks and defense agencies of Ukraine to Russia's Main Directorate of the General Staff of the Armed Forces (aka GRU). This [...] The post White House and UK Gov attribute DDoS attacks on Ukraine to Russia's GRU appeared first on Security Affairs.	 <div>CyberScoop</div>	White House attributes Ukraine DDoS incidents to Russia's GRU Russia was behind recent disruptions of Ukrainian government and banking websites, a top White House official said Friday. "We have assessed that Russia was responsible for the distributed denial-of-service [DDoS] attacks that occurred earlier this week," said Anne Neuberger, deputy national security adviser for cyber and emerging technology. Neuberger said the U.S. has "technical information" that shows digital infrastructure belonging Russia's main intelligence directorate, the GRU, "transmitting high volumes of communication to Ukraine-based IP addresses and domains." The British government also attributed the attacks to the GRU on Friday. DDoS incidents involve flooding websites with bog[...]

Twitter

 <div>RedPacket Security</div>	HUAWEI EMUI/Magic UI code execution CVE-2021-39994 -	 <div>RedPacket Security</div>	HUAWEI EMUI/Magic UI code execution CVE-2021-39997 -
 <div>CVE</div>	CVE-2021-39994 There is an arbitrary address access vulnerability with the product line test code.Successful exploitation of this vulnerability may affect service confidentiality, integrity, and availability.	 <div>CVE</div>	CVE-2021-39997 There is a vulnerability of unstrict input parameter verification in the audio assembly.Successful exploitation of this vulnerability may cause out-of-bounds access.
 <div>Wolfgang Sesin</div>	New post from (CVE-2021-39997) has been published on	 <div>www.sesin.at</div>	New post from (CVE-2021-39997) has been published on
 <div>www.sesin.at</div>	New post from (Huawei EMUI Audio out-of-bounds read [CVE-2021-39997]) has been published on	 <div>Wolfgang Sesin</div>	New post from (Huawei EMUI Audio out-of-bounds read [CVE-2021-39997]) has been published on
 <div>Threat Intel Center</div>	NEW: CVE-2021-39997 There is a vulnerability of unstrict input parameter verification in the audio assembly.Successful exploitation of this vulnerability may cause out-of-bounds access. Severity: CRITICAL	 <div>Threat Intel Center</div>	NEW: CVE-2021-39997 There is a vulnerability of unstrict input parameter verification in the audio assembly.Successful exploitation of this vulnerability may cause out-of-bounds access. Severity: CRITICAL
 <div>Remotely Alerts</div>	Severity: There is a vulnerability of unstrict inp... CVE-2021-39997 Link for more:	 <div>Threat Intel Center</div>	NEW: CVE-2021-39997 There is a vulnerability of unstrict input parameter verification in the audio assembly.Successful exploitation of this vulnerability may cause out-of-bounds access. Severity: CRITICAL

Source: [NIST](#)

NIST CVE: Critical

CVE-2020-14523	Multiple Mitsubishi Electric Factory Automation products have a vulnerability that allows an attacker to execute arbitrary code. <div>CRITICAL Vector: network Created: 2022-02-11 Updated: 2022-02-19</div>	CVE-2022-24704	The rad_packet_recv function in opt/src/accel-pppd/radius/packet.c suffers from a buffer overflow vulnerability, whereby user input len is copied into a fixed buffer &attr->val.integer without any bound checks. If the client connects to the server and sends a large radius packet, a buffer overflow vulnerability will be triggered. <div>CRITICAL Vector: network</div>
-----------------------	--	-----------------------	---

			Created: 2022-02-14 Updated: 2022-02-19
CVE-2022-24705	The rad_packet_recv function in radius/packet.c suffers from a memcpy buffer overflow, resulting in an overly-large recvfrom into a fixed buffer that causes a buffer overflow and overwrites arbitrary memory. If the server connects with a malicious client, crafted client requests can remotely trigger this vulnerability.	CVE-2022-24206	Tongda2000 v11.10 was discovered to contain a SQL injection vulnerability in /mobile_seal/get_seal.php via the DEVICE_LIST parameter.
	CRITICAL Vector: network Created: 2022-02-14 Updated: 2022-02-19		CRITICAL Vector: network Created: 2022-02-14 Updated: 2022-02-19
CVE-2022-23902	Tongda2000 v11.10 was discovered to contain a SQL injection vulnerability in export_data.php via the d_name parameter.	CVE-2022-0559	Use After Free in GitHub repository radareorg/radare2 prior to 5.6.2.
	CRITICAL Vector: network Created: 2022-02-14 Updated: 2022-02-19		CRITICAL Vector: network Created: 2022-02-16 Updated: 2022-02-19
CVE-2022-0290	Use after free in Site isolation in Google Chrome prior to 97.0.4692.99 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.	CVE-2022-23992	XCOM Data Transport for Windows, Linux, and UNIX 11.6 releases contain a vulnerability due to insufficient input validation that could potentially allow remote attackers to execute arbitrary commands with elevated privileges.
	CRITICAL Vector: network Created: 2022-02-12 Updated: 2022-02-19		CRITICAL Vector: network Created: 2022-02-14 Updated: 2022-02-19

NIST CVE: High

Source: *NIST*

CVE-2022-0201	The Permalink Manager Lite WordPress plugin before 2.2.15 and Permalink Manager Pro WordPress plugin before 2.2.15 do not sanitise and escape query parameters before outputting them back in the debug page, leading to a Reflected Cross-Site Scripting issue	CVE-2022-0176	The PowerPack Lite for Beaver Builder WordPress plugin before 1.2.9.3 does not sanitise and escape the tab parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting
	MEDIUM Vector: network Created: 2022-02-14 Updated: 2022-02-19		MEDIUM Vector: network Created: 2022-02-14 Updated: 2022-02-19
CVE-2021-25018	The PPOM for WooCommerce WordPress plugin before 24.0 does not have authorisation and CSRF checks in the ppom_settings_panel action AJAX action, allowing any authenticated to call it and set arbitrary settings. Furthermore, due to the lack of sanitisation and escaping, it could lead to Stored XSS issues	CVE-2021-25050	The Remove Footer Credit WordPress plugin before 1.0.11 does properly sanitise its settings, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed.
	MEDIUM Vector: network Created: 2022-02-14 Updated: 2022-02-19		MEDIUM Vector: network Created: 2022-02-14 Updated: 2022-02-19
CVE-2021-24446	The Remove Footer Credit WordPress plugin before 1.0.6 does not have CSRF check in place when saving its settings, which could allow attacker to make logged in admins change them and lead to Stored XSS issue as well due to the lack of sanitisation	CVE-2022-0212	The SpiderCalendar WordPress plugin through 1.5.65 does not sanitise and escape the callback parameter before outputting it back in the page via the window AJAX action (available to both unauthenticated and authenticated users), leading to a Reflected Cross-Site Scripting issue.
	MEDIUM Vector: network Created: 2022-02-14 Updated: 2022-02-19		MEDIUM Vector: network Created: 2022-02-14 Updated: 2022-02-19
CVE-2021-25115	The WP Photo Album Plus WordPress plugin before 8.0.10 was vulnerable to Stored Cross-Site Scripting (XSS). Error log content was handled improperly, therefore any user, even unauthenticated, could cause arbitrary javascript to be executed in the admin panel.	CVE-2022-0200	Themify Portfolio Post WordPress plugin before 1.1.7 does not sanitise and escape the num_of_pages parameter before outputting it back the response of the themify_create_popup_page_pagination AJAX action (available to any authenticated user), leading to a Reflected Cross-Site Scripting
	MEDIUM Vector: network Created: 2022-02-14 Updated: 2022-02-19		

		MEDIUM Vector: network Created: 2022-02-14 Updated: 2022-02-19
CVE-2021-46557	Vicidial 2.14-783a was discovered to contain a cross-site scripting (XSS) vulnerability via the input tabs.	MEDIUM Vector: network Created: 2022-02-15 Updated: 2022-02-19

Source: [NIST](#)

NIST CVE: Low

Nothing today

Source: [NIST](#)

NIST CVE: Unrated

CVE-2022-25133	A command injection vulnerability in the function isAssocPriDevice of TOTOLINK Technology router T6 V3 Firmware T6_V3_V4.1.5cu.748_B20211015 allows attackers to execute arbitrary commands via a crafted MQTT packet.	CVE-2022-25132	A command injection vulnerability in the function meshSlaveDlfw of TOTOLINK Technology router T6 V3 Firmware T6_V3_V4.1.5cu.748_B20211015 allows attackers to execute arbitrary commands via a crafted MQTT packet.
	UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-19		UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-19
CVE-2022-25136	A command injection vulnerability in the function meshSlaveUpdate of TOTOLINK Technology routers T6 V3 Firmware T6_V3_V4.1.5cu.748_B20211015 and T10 V2 Firmware V4.1.8cu.5207_B20210320 allows attackers to execute arbitrary commands via a crafted MQTT packet.	CVE-2022-25135	A command injection vulnerability in the function recv_mesh_info_sync of TOTOLINK Technology router T6 V3 Firmware T6_V3_V4.1.5cu.748_B20211015 allows attackers to execute arbitrary commands via a crafted MQTT packet.
	UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-19		UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-19
CVE-2022-25131	A command injection vulnerability in the function recvSlaveCloudCheckStatus of TOTOLINK Technology routers T6 V3 Firmware T6_V3_V4.1.5cu.748_B20211015 and T10 V2 Firmware V4.1.8cu.5207_B20210320 allows attackers to execute arbitrary commands via a crafted MQTT packet.	CVE-2022-25137	A command injection vulnerability in the function recvSlaveUpgstatus of TOTOLINK Technology routers T6 V3 Firmware T6_V3_V4.1.5cu.748_B20211015 and T10 V2 Firmware V4.1.8cu.5207_B20210320 allows attackers to execute arbitrary commands via a crafted MQTT packet.
	UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-19		UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-19
CVE-2022-25134	A command injection vulnerability in the function setUpgradeFW of TOTOLINK Technology router T6 V3 Firmware T6_V3_V4.1.5cu.748_B20211015 allows attackers to execute arbitrary commands via a crafted MQTT packet.	CVE-2022-25130	A command injection vulnerability in the function updateWifiInfo of TOTOLINK Technology routers T6 V3 Firmware T6_V3_V4.1.5cu.748_B20211015 and T10 V2 Firmware V4.1.8cu.5207_B20210320 allows attackers to execute arbitrary commands via a crafted MQTT packet.
	UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-19		UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-19
CVE-2021-46361	An issue in the Freemark Filter of Magnolia CMS v6.2.11 and below allows attackers to bypass security restrictions and execute arbitrary code via a crafted FreeMarker payload.	CVE-2021-45082	An issue was discovered in Cobbler through 3.3.0. In the templar.py file, the function check_for_invalid_imports can allow Cheetah code to import Python modules via the "#from MODULE import" substring. (Only lines beginning with #import are blocked.)
	UNRATED Vector: unkown Created: 2022-02-11 Updated: 2022-02-19		UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-19
CVE-2022-24980	An issue was discovered in the Kitodo .Presentation (aka dif) extension before 2.3.2, 3.x before 3.2.3, and 3.3.x before 3.3.4 for TYPO3 . A missing access check in an eID script allows an unauthenticated user to submit arbitrary URLs to this component. This results in SSRF, allowing attackers to view the content of any file or webpage the webserver has access to.	CVE-2022-24979	An issue was discovered in the Varnishcache extension before 2.0.1 for TYPO3 . The Edge Site Includes (ESI) content element renderer component does not include an access check. This allows an unauthenticated user to render various content elements, resulting in insecure direct object reference (IDOR), with the potential of exposing internal content elements.
	UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-19		UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-19
CVE-2021-44302	BaiCloud-cms v2.5.7 was discovered to contain multiple SQL injection vulnerabilities via the tongji and baidu_map parameters in /user/ztconfig.php.	CVE-2022-25366	Cryptomator through 1.6.5 allows DYLIB injection because, although it has the flag 0x1000 for Hardened Runtime, it has the com.apple.security.cs.disable-library-validation and com.apple.security.cs.allow-dyld-environment-variables entitlements. An attacker can exploit this by creating a malicious .dylib file that can be executed via the DYLD_INSERT_LIBRARIES environment variable.
	UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-19		UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-19
CVE-2022-25365	Docker Desktop before 4.5.1 on Windows allows attackers to move arbitrary files. NOTE: this issue exists because of an incomplete fix for CVE-2022-23774.	CVE-2022-25256	SAS Web Report Studio 4.4 allows XSS. /SASWebReportStudio/logonAndRender.do has two parameters: sasdfs_request_backlabel list and sasdfs_request_backurl list. The first one affects the content of the button placed in the top left. The second affects the page to which the user is directed after pressing the button, e.g., a malicious web page. In addition, the second parameter executes JavaScript, which means XSS is possible by adding a javascript: URL.
	UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-19		UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-19
CVE-2016-20013	sha256crypt and sha512crypt through 0.6 allow attackers to cause a denial of service (CPU consumption) because the algorithm's runtime is proportional to the square of the length of the password.	CVE-2022-0409	Unrestricted Upload of File with Dangerous Type in Packagist showdoc/showdoc prior to 2.10.2.
	UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-19		UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-19

Source: [Hybrid Analysis](#)

Top malicious files

100% Threat score	Toyota Launcher (.) exe	100% Threat score	SRG000484QUO (.) bin
100% Threat score	PB DeCompiler 2013 (.) 06 (.) 30 (.) exe	100% Threat score	Setup (.) exe

100% Threat score	Black Worm (.) exe	100% Threat score	stub (.) exe
100% Threat score	f3b0fed4b1ba6da067663fed061d1ba03c883ab4 (.) malware	100% Threat score	Kings Bounty II v1 (.) 2 Plus 23 Trainer (.) exe
100% Threat score	ddmsetup2090 (.) exe	100% Threat score	tmpydzic_0a
100% Threat score	tmp7wn1esmn	100% Threat score	setup (.) bat
100% Threat score	6111eed9a58057a6948c4b6c031b9699fcae5bb2 (.) malware	100% Threat score	Systeminfo
85% Threat score	Hgwsgo (.) exe	85% Threat score	winrar-x64-602ru (.) exe
80% Threat score	SDIO_R742 (.) exe	75% Threat score	ADD2412B6DE02A101D98C4542299E63507CF7F5F8C643740138CF341B2ED99F
75% Threat score	9A92B3B15D0862A57AEFD08071334534087F6778651665E33F3A984E74CC4220		











Source: Hybrid Analysis

Top malicious URL

100% Threat score	https://tryedmate (.) com/redrect (.) php	96% Threat score	http://lavanyadentalcare (.) com/
93% Threat score	http://loginwebmailnic (.) dynssl (.) com/	92% Threat score	http://getadobeflashdownloader (.) proxydns (.) com/
89% Threat score	https://thetinytask (.) com/	72% Threat score	http://www (.) mediafire (.) com/file/dbfod9u5q9ii9nd/macOS_Big_Sur_11 (.) 0 (.) 1_%25










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 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.	

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 Iran (Islamic Republic of)		#10 Pakistan

Top phishing countries

	#1 United States		#2 Russia
	#3 Germany		#4 Netherlands
	#5 Hong Kong		#6 Poland
	#7 Singapore		#8 France
	#9 United Kingdom		#10 Japan