Security Rabbits

Your Security Rabbits report for March 07, 2022

Source: Ransom Watch

Ransomware attacks

everest	Target: Backus, Meyer & Branch, LLP(2022-03-07)
lockbit2	Target: brownsville-pub . . . (2022-03-07)
everest	Target: Centro Hospitalar de SetÃƒÂºbal(2022-03-07)
everest	Target: Greenberg & Stein New York City Personal Injury Lawyers(2022-03-07)
lockbit2	Target: luzeirosfortale . (2022-03-07)
alphv	Target: BAUCENTER | ujhazbudapest . hu(2022-03-07)
everest	Target: Campbell Sales and Service, Inc(2022-03-07)
everest	Target: Federal land inc . (2022-03-07)
everest	Target: Law Offices of Brandon Sua & Associates(2022-03-07)

Hot topics

Nothing today

News

The Hacker News

2 New Mozilla Firefox 0-Day Bugs Under Active Attack -- Patch Your Browser ASAP!
Mozilla has pushed out-of-band software updates to its Firefox web browser to contain two high-impact security vulnerabilities, both of which it says are being actively exploited in the wild. Tracked as CVE-2022-26485 and CVE-2022-26486, the zero-day flaws have been described as use-after-free issues impacting the Extensible Stylesheet Language Transformations (XSLT) parameter processing and the

Cyware News - Latest Cyber News

Adafruit Discloses Customer Data Leak from Ex-employee's GitHub Repository
The data set did not contain any user passwords or financial information such as credit cards. However, the exposure of real user data, including order details, could be abused by phishing actors.

Security Affairs

Anonymous offers $52,000 worth of Bitcoin to Russian troops for surrendered tank. Is it fake news?
The popular hacker collective Anonymous is offering to Russian troops $52,000 in BTC for each surrendered tank. The popular hacker collective Anonymous will reportedly pay $52,000 in BTC for a tank surrendered by Russian troops. Ukrainian media reported that the hacker group claims to have collected over RUB 1 billion (worth PS7.8 million at the [...] The post Anonymous offers $52,000 worth of Bitcoin to Russian troops for surrendered tank. Is it fake news? appeared first on Security Affairs.

Security Affairs

Feb 27- Mar 05 Ukraine - Russia the silent cyber conflict
This post provides a timeline of the events related to the Russia invasion of Ukraine from the cyber security perspective. March 5 - Anonymous #OpRussia Thousands of sites hacked, data leaks and more Anonymous and its affiliates continue to target Russia and Belarus, it is also targeting the Russian disinformation machine. March 5 - Thousands [...] The post Feb 27- Mar 05 Ukraine - Russia the silent cyber conflict appeared first on Security Affairs.

Security Affairs

Mozilla addresses two actively exploited zero-day flaws in Firefox
Mozilla fixed two critical actively exploited zero-day bugs in Firefox with the release of 97.0.2, ESR 91.6.1, Firefox for Android 97.3.0, and Focus 97.3.0. Mozilla has released Firefox 97.0.2, Firefox ESR 91.6.1, Firefox for Android 97.3.0, and Focus 97.3.0 to address a couple of critical zero-day vulnerabilities, tracked as CVE-2022-26485 and CVE-2022-26485, actively exploited in [...] The post Mozilla addresses two actively exploited zero-day flaws in Firefox appeared first on Security Affairs.

The Hacker News

SharkBot Banking Malware Spreading via Fake Android Antivirus App on Google Play Store
The threat actor behind a nascent Android banking trojan named SharkBot has managed to evade Google Play Store security barriers by masquerading as an antivirus app. SharkBot, like its malware counterparts TeaBot, FluBot, and Oscorp (UBEL), belongs to a category of financial trojans capable of siphoning credentials to initiate money transfers from compromised devices by circumventing

Cyware News - Latest Cyber News

A new flaw in Linux Kernel cgroups feature allows container escape
The issue is a privilege escalation flaw affecting the Linux kernel feature called control groups (groups), that limits, accounts for, and isolates the resource usage of a collection of processes.

Security Affairs

Anonymous hacked Russian streaming services to broadcast war footage
Anonymous hacked into the most popular Russian streaming services to broadcast war footage from Ukraine. The popular hacker collective Anonymous continues to target Russian entities, a few hours ago the group hacked into the most popular Russian streaming services to broadcast war footage from Ukraine and demonstrate to Russians the atrocity of the invasion ordered [...] The post Anonymous hacked Russian streaming services to broadcast war footage appeared first on Security Affairs.

Security Affairs

CVE-2022-0492 flaw in Linux Kernel cgroups feature allows container escape
A Linux kernel flaw, tracked as CVE-2022-0492, can allow an attacker to escape a container to execute arbitrary commands on the container host. A now-patched high-severity Linux kernel vulnerability, tracked as CVE-2022-0492 (CVSS score: 7.0), can be exploited by an attacker to escape a container to execute arbitrary commands on the container host. The issue is [...] The post CVE-2022-0492 flaw in Linux Kernel cgroups feature allows container escape appeared first on Security Affairs.

Naked Security

Firefox patches two actively exploited zero-day holes: update now!
Firefox just published a double-zero-day patch - "remote code execution" combined with "sandbox escape". Update now!

Cyware News - Latest Cyber News

Recent Ransom DDoS Extortion Attack Peaked at 2.5 Million RPS
Imperva on Friday said it recently mitigated a ransom distributed denial-of-service (DDoS) attack targeting an unnamed website that peaked at 2.5 million requests per second (RPS).

Twitter

Rob Portman

Im proud the Senate moved quickly this week to pass the bipartisan Strengthening American Cybersecurity Act I introduced to give the National Cyber Director, CISA & others broad visibility into the cyberattacks taking place across our nation.

PressReader

To our readers and partners, PressReader thanks you immensely for your support and understanding as we navigated through this cyber security incident. Updates in thread (1/6)

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-2021-46703

** UNSUPPORTED WHEN ASSIGNED ** In the IsolatedRazorEngine component of Antaris RazorEngine through 4.5.1-alpha001, an attacker can execute arbitrary **.NET** code in a sandboxed environment (if users can externally control template contents). NOTE: This vulnerability only affects products that are no longer supported by the maintainer.

UNRATED Vector: unkown Created: 2022-03-06 Updated: 2022-03-07

CVE-2021-44749

A vulnerability affecting **F-Secure SAFE browser protection** was discovered improper URL handling can be triggered to cause universal cross-site scripting through browsing protection in a SAFE web browser. User interaction is required prior to exploitation. A successful exploitation may lead to arbitrary code execution.

UNRATED Vector: unkown Created: 2022-03-06 Updated: 2022-03-07

CVE-2022-0845

Code Injection in **GitHub** repository pytorchlightning/pytorch-lightning prior to 1.6.0.

UNRATED Vector: unkown Created: 2022-03-05 Updated: 2022-03-07

CVE-2022-25044

Espruino 2v11.251 was discovered to contain a stack buffer overflow via src/jsvar.c in jsvNewFromString.

UNRATED Vector: unkown Created: 2022-03-05 Updated: 2022-03-07

CVE-2022-26496

In nbd-server in nbd before 3.24, there is a stack-based buffer overflow. An attacker can cause a buffer overflow in the parsing of the name field by sending a crafted NBD_OPT_INFO or NBD_OPT_GO message with an large value as the length of the name.

UNRATED Vector: unkown Created: 2022-03-06 Updated: 2022-03-07

CVE-2022-26487

Mitel MiCollab before 9.4 SP1 FP1 and **MiVoice** Business **Express** through 8.1 allow remote attackers to obtain sensitive information and cause a denial of service (performance degradation and excessive outbound traffic).

UNRATED Vector: unkown Created: 2022-03-06 Updated: 2022-03-07

CVE-2022-0697

Open Redirect in **GitHub** repository archivy/archivy prior to 1.7.0.

UNRATED Vector: unkown Created: 2022-03-06 Updated: 2022-03-07

CVE-2022-24921

regexp.Compile in Go before 1.16.15 and 1.17.x before 1.17.8 allows stack exhaustion via a **deeply** nested expression.

UNRATED Vector: unkown Created: 2022-03-05 Updated: 2022-03-07

CVE-2022-0766

Server-Side Request Forgery (SSRF) in **GitHub** repository janeczku/calibre-web prior to 0.6.17.

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2021-24824

The [field] shortcode included with the Custom Content Shortcode **WordPress** plugin before 4.0.1, allows authenticated users with a role as low as contributor, to access arbitrary post metadata. This could lead to sensitive data disclosure, for example when used in combination with

CVE-2022-26505

A DNS rebinding issue in **ReadyMedia** (formerly MiniDLNA) before 1.3.1 allows a remote web server to exfiltrate media files.

UNRATED Vector: unkown Created: 2022-03-06 Updated: 2022-03-07

CVE-2021-44748

A vulnerability affecting **F-Secure SAFE** browser was discovered whereby browsers loads images automatically this vulnerability can be exploited remotely by an attacker to execute the JavaScript can be used to trigger universal cross-site scripting through the browser. User interaction is required prior to exploitation, such as entering a malicious website to trigger the vulnerability.

UNRATED Vector: unkown Created: 2022-03-06 Updated: 2022-03-07

CVE-2022-25465

Espruino 2v11 release was discovered to contain a stack buffer overflow via src/jsvar.c in jsvGetNextSibling.

UNRATED Vector: unkown Created: 2022-03-05 Updated: 2022-03-07

CVE-2021-46704

In GenieACS 1.2.x before 1.2.8, the UI interface API is vulnerable to unauthenticated OS command injection via the ping host argument (lib/ui/api.ts and lib/ping.ts). The vulnerability arises from insufficient input validation combined with a missing authorization check.

UNRATED Vector: unkown Created: 2022-03-06 Updated: 2022-03-07

CVE-2022-26495

In nbd-server in nbd before 3.24, there is an integer overflow with a resultant heap-based buffer overflow. A value of 0xffffffff in the name length field will cause a zero-sized buffer to be allocated for the name, resulting in a write to a dangling pointer. This issue exists for the NBD_OPT_INFO, NBD_OPT_GO, and NBD_OPT_EXPORT_NAME messages.

UNRATED Vector: unkown Created: 2022-03-06 Updated: 2022-03-07

CVE-2022-0869

Multiple Open Redirect in **GitHub** repository nitely/spirit prior to 0.12.3.

UNRATED Vector: unkown Created: 2022-03-06 Updated: 2022-03-07

CVE-2022-0868

Open Redirect in **GitHub** repository medialize/uri.js prior to 1.19.10.

UNRATED Vector: unkown Created: 2022-03-06 Updated: 2022-03-07

CVE-2022-0767

Server-Side Request Forgery (SSRF) in **GitHub** repository janeczku/calibre-web prior to 0.6.17.

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2022-26490

st21nfca_connectivity_event_received in drivers/nfc/st21nfca/se.c in the **Linux** kernel through 5.16.12 has EVT_TRANSACTION buffer overflows because of untrusted length parameters.

UNRATED Vector: unkown Created: 2022-03-06 Updated: 2022-03-07

CVE-2022-0267

The **AdRotate WordPress** plugin before 5.8.22 does not sanitise and escape the adrotate_action before using it in a SQL statement via the adrotate_request_action function available to admins, leading to a SQL injection

WooCommerce, the email address of orders can be retrieved

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2021-24953

The Advanced **iFrame WordPress** plugin before 2022 does not sanitise and escape the ai_config_id parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting issue

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2022-0440

The Catch Themes Demo Import **WordPress** plugin before 2.1.1 does not validate one of the file to be imported, which could allow high privivilege admin to upload an arbitrary PHP file and gain RCE even in the case of an hardened **blog** (ie DISALLOW_UNFILTERED_HTML, DISALLOW_FILE_EDIT and DISALLOW_FILE_MODS constants set to true)

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2021-25009

The CorreosExpress **WordPress** plugin through 2.6.0 generates log files which are publicly accessible, and contain sensitive information such as sender/receiver names, **phone** numbers, physical and email addresses

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2021-24820

The Cost Calculator **WordPress** plugin through 1.6 allows authenticated users (Contributor+ in versions < 1.5, and Admin+ in versions <= 1.6) to perform path traversal and local PHP file inclusion on **Windows** Web Servers via the Cost Calculator post's Layout

UNRATED Vector: unkown Created: 2022-02-28 Updated: 2022-03-07

CVE-2021-24826

The Custom Content Shortcode **WordPress** plugin before 4.0.2 does not escape custom fields before outputting them, which could allow Contributor+ (v < 4.0.1) or Admin+ (v < 4.0.2) users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed. Please note that such attack is still possible by admin+ in single site blogs by default (but won't be when the unfiltered_html is disallowed)

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2022-0533

The Ditty (formerly Ditty **News** Ticker) **WordPress** plugin before 3.0.15 is affected by a Reflected Cross-Site Scripting (XSS) vulnerability.

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2022-0535

The E2Pdf **WordPress** plugin before 1.16.45 does not sanitise and escape some of its settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2022-0347

The **LoginPress** | Custom Login Page Customizer **WordPress** plugin before 1.5.12 does not escape the redirect-page parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2022-0349

The NotificationX **WordPress** plugin before 2.3.9 does not sanitise and escape the nx_id parameter before using it in a SQL statement, leading to an Unauthenticated Blind SQL Injection

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2021-25098

The Pricing Tables **WordPress** Plugin WordPress plugin before 3.1.3 does not verify the CSRF nonce when removing posts, allowing attackers to make a logged in admin remove arbitrary posts from the **blog** via a CSRF attack, which will be put in the trash

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2022-0420

The **RegistrationMagic WordPress** plugin before 5.0.2.2 does not sanitise and escape the rm_form_id parameter before using it in a SQL statement in the Automation admin dashboard, allowing high privilege users to perform SQL injection attacks

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2021-24778

The test parameter of the xmlfeed in the Tradetracker-Store **WordPress** plugin before 4.6.60 is not sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection.

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2022-0384

The Video Conferencing with **Zoom WordPress** plugin before 3.8.17 does not have authorisation in its vczapi_get_wp_users AJAX action, allowing any authenticated users, such as subscriber to download the list of email addresses registered on the blog

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2021-24216

The **All-in-One** WP Migration **WordPress** plugin before 7.41 does not validate uploaded files' extension, which allows administrators to upload PHP files on their site, even on multisite installations.

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2021-24952

The Conversios.io **WordPress** plugin before 4.6.2 does not sanitise, validate and escape the sync_progressive_data parameter for the tvcajax_product_sync_bantch_wise AJAX **action** before using it in a SQL statement, allowing any authenticated user to perform SQL injection attacks.

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2021-24821

The Cost Calculator **WordPress** plugin before 1.6 allows users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks via the Description fields of a Cost Calculator > Price Settings (which gets injected on the edit page as well as any page that embeds the calculator using the shortcode), as well as the Text Preview field of a Project (injected on the edit project page)

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2022-0448

The CP Blocks **WordPress** plugin before 1.0.15 does not sanitise and escape its "License ID" settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed.

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2021-24825

The Custom Content Shortcode **WordPress** plugin before 4.0.2 does not validate the data passed to its load shortcode, which could allow Contributor+ (v < 4.0.1) or Admin+ (v < 4.0.2) users to display arbitrary files from the filesystem (such as logs, .htaccess etc), as well as perform Local File Inclusion attacks as PHP files will be executed. Please note that such attack is still possible by admin+ in single site blogs by default (but won't be when either the unfiltered_html or file_edit is disallowed)

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2021-25087

The **Download Manager WordPress** plugin before 3.2.35 does not have any authorisation checks in some of the REST API endpoints, allowing unauthenticated attackers to call them, which could lead to sensitive information disclosure, such as posts passwords (fixed in 3.2.24) and files Master Keys (fixed in 3.2.25).

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2022-0439

The Email Subscribers & **Newsletters WordPress** plugin before 5.3.2 does not correctly escape the `order` and `orderby` parameters to the `ajax_fetch_report_list` action, making it vulnerable to blind SQL injection attacks by users with roles as low as Subscriber. Further, it does not have any CSRF protection in place for the action, allowing an attacker to trick any logged in user to perform the action by clicking a link.

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2022-0441

The MasterStudy LMS **WordPress** plugin before 2.7.6 does to validate some parameters given when registering a new account, allowing unauthenticated users to register as an admin

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2022-0434

The Page View Count **WordPress** plugin before 2.4.15 does not sanitise and escape the post_ids parameter before using it in a SQL statement via a REST endpoint, available to both unauthenticated and authenticated users. As a result, unauthenticated attackers could perform SQL injection attacks

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2022-0426

The Product Feed PRO for **WooCommerce WordPress** plugin before 11.2.3 does not escape the rowCount parameter before outputting it back in an attribute via the woosea_categories_dropdown AJAX **action** (available to any authenticated user), leading to a Reflected Cross-Site Scripting

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2022-0163

The Smart **Forms WordPress** plugin before 2.6.71 does not have authorisation in its rednao_smart_forms_entries_list AJAX action, allowing any authenticated users, such as subscriber, to download arbitrary form's data, which could include sensitive information such as PII depending on the form.

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2022-0442

The UsersWP **WordPress** plugin before 1.2.3.1 is missing access controls when updating a user avatar, and does not make sure file names for user avatars are unique, allowing a logged in user to overwrite another users avatar.

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2021-24777

The view submission functionality in the Hotscot Contact Form **WordPress** plugin before 1.3 makes a get request with the sub_id parameter which not sanitised, escaped or validated before inserting to a SQL statement, leading to an SQL injection.

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2022-0422

The White Label CMS **WordPress** plugin before 2.2.9 does not sanitise and validate the wlcms[_login_custom_js] parameter before outputting it back in the response while previewing, leading to a Reflected Cross-Site Scripting issue

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2021-24961

The **WordPress** File Upload WordPress plugin before 4.16.3, wordpress-file-upload-pro WordPress plugin before 4.16.3 does not escape some of its shortcode argument, which could allow users with a role as low as Contributor to perform Cross-Site Scripting attacks

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2021-25038

The **WordPress** Multisite User Sync/Unsync WordPress plugin before 2.1.2 does not sanitise and escape the wmus_source_blog and wmus_record_per_page parameters before outputting them back in attributes, leading to Reflected Cross-Site Scripting issues

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2022-0429

The WP Cerber Security, **Anti-spam** & Malware **Scan WordPress** plugin before 8.9.6 does not sanitise the $url variable before using it in an attribute in the Activity tab in the **plugins** dashboard, leading to an unauthenticated stored Cross-Site Scripting vulnerability.

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2022-0389

The WP Time Slots Booking Form **WordPress** plugin before 1.1.63 does not sanitise and escape Calendar names, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2022-0205

The **YOP Poll WordPress** plugin before 6.3.5 does not sanitise and escape some of the settings (available to users with a role as low as author) before outputting them, leading to a Stored Cross-Site Scripting issue

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2021-24960

The **WordPress** File Upload WordPress plugin before 4.16.3, wordpress-file-upload-pro WordPress plugin before 4.16.3 allows users with a role as low as Contributor to configure the upload form in a way that allows uploading of SVG files, which could be then be used for Cross-Site Scripting attacks

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2021-25039

The **WordPress** Multisite Content Copier/Updater WordPress plugin before 2.1.0 does not sanitise and escape the wmcc_content_type, wmcc_source_blog and wmcc_record_per_page parameters before outputting them back in attributes, leading to Reflected Cross-Site Scripting issues

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2022-0445

The **WordPress** Real **Cookie** Banner: GDPR (DSGVO) & ePrivacy Cookie Consent WordPress plugin before 2.14.2 does not have CSRF checks in place when resetting its settings, allowing attackers to make a logged in admin reset them via a CSRF attack

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2021-24810

The WP **Event Manager WordPress** plugin before 3.1.23 does not escape some of its Field Editor settings when outputting them, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2022-0410

The WP Visitor **Statistics** (Real Time Traffic) **WordPress** plugin before 5.6 does not sanitise and escape the id parameter before using it in a SQL statement via the refUrlDetails AJAX action, available to any authenticated user, leading to a SQL injection

UNRATED Vector: unkown Created: 2022-03-07 Updated: 2022-03-07

CVE-2022-0849

Use After Free in r_reg_get_name_idx in **GitHub** repository radareorg/radare2 prior to 5.6.6.

UNRATED Vector: unkown Created: 2022-03-05 Updated: 2022-03-07

Source: Hybrid Analysis

Top malicious files

100% Threat score	notepad2 (.) exe
100% Threat score	DGSetup_Home_BZ (.) exe
100% Threat score	Actp2Exe (.) exe
100% Threat score	0d95f767c5f828695761e199b6e0b9fe62ace2902221540a33d331859648e761
92% Threat score	HappyMod-Download-2-7-5 (.) apk
85% Threat score	NMM-0 (.) 83 (.) 4 (.) exe
81% Threat score	c7a2ea098ffb5949f98ffee5c169fb9331aba20eb488e38c8ce3dbaa8b60767a (.) xlsx
76% Threat score	c7a2ea098ffb5949f98ffee5c169fb9331aba20eb488e38c8ce3dbaa8b60767a (.) xlsx
73% Threat score	auserverapi (.) dll
72% Threat score	Intunewin Create and Extract (.) exe
71% Threat score	FmWhatsApp-v9 (.) 21_YTricks (.) net (.) apk

100% Threat score	pptv5 (.) 1 (.) 1 (.) 0002 (.) exe
100% Threat score	Actp1Exe (.) exe
100% Threat score	2022-02-25_1337 (.) xlsm
100% Threat score	Hack (.) exe
85% Threat score	VC_redist (.) x86 (.) exe
85% Threat score	rightscansetup2204 (.) exe
80% Threat score	SubtitleEdit-3 (.) 6 (.) 4-Setup (.) exe
75% Threat score	WINCMD32 (.) EXE
72% Threat score	SAC-x64 (.) msi
71% Threat score	CSHFware (.) dll

Source: Hybrid Analysis

Top malicious URL

100% Threat score	http://27 (.) 194 (.) 236 (.) 44:55674/bin (.) sh
100% Threat score	https://magyarposta (.) psl-security (.) com/magyarposta

100% Threat score	http://69 (.) 113 (.) 228 (.) 249:39892/i
97% Threat score	http://115 (.) 59 (.) 255 (.) 212:43359/bin (.) sh

96%
Threat score
http://112 (.) 30 (.) 1 (.) 155:49409/i

93%
Threat score
http://3 (.) 112 (.) 243 (.) 28/webber/60220124731 (.) png

93%
Threat score
http://124 (.) 165 (.) 26 (.) 21:42313/i

93%
Threat score
http://117 (.) 215 (.) 215 (.) 140:45481/bin (.) sh

86%
Threat score
http://13 (.) 58 (.) 89 (.) 178/vaafrw/OIUYTREWFGNLJFD (.) gif

82%
Threat score
http://ambingenieria (.) com/

81%
Threat score
http://52 (.) 186 (.) 122 (.) 65/putt/putty (.) exe

77%
Threat score
http://rabobank-nl (.) com/

77%
Threat score
http://familytech-dev (.) byu (.) edu/

75%
Threat score
http://clinicordismedica (.) com (.) br/wp-content/plugins/wp-whatsapp-chat/assets/frontend/js/

74%
Threat score
http://www (.) mourlanne (.) com/

72%
Threat score
http://zguoe (.) smtpgaze (.)
com/tracking/qaR9ZGLkZGx0BQZjZGN4BGt0BGZ0APM5qzS4qaR9ZQbjJN

72%
Threat score
http://dweut (.) smtpgaze (.)
com/tracking/qaR9ZGLkZGx0ZGx3ZGD0AQpkZGDlAPM5qzS4qaR9ZQbjIt

93%
Threat score
http://39 (.) 73 (.) 122 (.) 38:54552/i

93%
Threat score
http://219 (.) 156 (.) 76 (.) 128:46337/i

93%
Threat score
http://39 (.) 73 (.) 122 (.) 38:54552/bin (.) sh

88%
Threat score
http://52 (.) 186 (.) 122 (.) 65/z/zone (.) exe

84%
Threat score
http://ec2-54-163-171-189 (.) compute-1 (.) amazonaws (.) com/XPU (.) exe

82%
Threat score
http://xtm9j (.) mjt (.)
lu/lnk/AMoAAMEjXwMAAAAAAAAAAC2Mi1AAAAAAfisAAAAAABKiqwBiJK2Jy53R4

77%
Threat score
http://lnkiy (.) in/ljpyl

77%
Threat score
http://www (.) mikehoustonfootballcampsllc (.) com/

77%
Threat score
http://naijahug (.) net/

75%
Threat score
http://acwpvc (.) ambingenieria (.) com/# (.)
dDR0bG9yM3Uub2xkanVuaW9yc3Rlbm5pcy5vcmcvKiZeJSRXJDU2Ny83NDM5MTgyMzAtM

74%
Threat score
http://raw (.) githubusercontent (.) com/hoshsadiq/adblock-nocoin-list/master/noco
0&application=chrome&applicationVersion=99 (.) 0 (.) 4844 (.) 51&platform=chr
51&lastVersion=204&downloadCount=4%2B&disabled=false&_sm_byp=iVVS32W

72%
Threat score
http://getlowestratestoday (.) com/

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

#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 Thailand
- #5 Indonesia
- #6 Algeria
- #7 Viet Nam
- #8 Brazil
- #9 Iran (Islamic Republic of)
- #10 Pakistan

Source: SpamHaus

Top phishing countries

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

Source: Have I been pwned?

Have I been pwnd

Nothing today

Source: Imperva DDOS Map

Top DDOS attackers

Source: Imperva DDOS Map

Top DDOS country targets

Source: Imperva DDOS Map

Top DDOS techniques

Source: Imperva DDOS Map

Top DDOS industry targets