Your Security Rabbits report for April 08, 2022

Source: Ransom Watch

Ransomware attacks

lockbit2	feuerschutzbock...	lockbit2	get-entkernung....
midas	Jiangsu Kaili Carpet Co., Ltd.	midas	SUPREME SERVICES
lockbit2	tnt	lockbit2	unholz.ch

Hot topics

Nothing today

News

IT Security Guru

50% of security leaders consider quitting due to stress

A new study from Vectra AI has revealed that half of UK cybersecurity leaders consider leaving their jobs due to the pressure they face at work. The security vendor polled 200 security chiefs in the UK in order to better understand the emerging industry health crisis. The study revealed that two out of five security […] The post 50% of security leaders consider quitting due to stress appeared first on IT Security Guru.

Cyware News - Latest Cyber News

A Bad Luck BlackCat

Kaspersky claims that at least some members of the new BlackCat group have links to the BlackMatter group, because they modified and reused a custom exfiltration tool we call Fendr and which has only been observed in BlackMatter activity.

Krebs on Security

Actions Target Russian Govt. Botnet, Hydra Dark Market

The U.S. Federal Bureau of Investigation (FBI) says it has disrupted a giant botnet built and operated by a Russian government intelligence unit known for launching destructive cyberattacks against energy infrastructure in the United States and Ukraine. Separately, law enforcement agencies in the U.S. and Germany moved to decapitate "Hydra," a billion-dollar Russian darknet drug bazaar that also helped to launder the profits of multiple Russian ransomware groups.

Cyware News - Latest Cyber News

Bank of Ireland Fined EUR463,000 Over Data Breaches

Bank of Ireland has been fined EUR463,000 (~$503,000) by the Data Protection Commission (DPC) for a number of data breaches from November 2018 to June 2019 affecting customer personal information.

Cyware News - Latest Cyber News

Beastmode Powered With Newly Added Exploits

A Mirai variant called Beastmode was found exploiting disclosed vulnerabilities in TOTOLINK routers. Attackers abused five new exploits within a month. Beastmode has also added some older bugs for a variety of routers from different vendors, all rated 9.8 on the CVSS scale. TOTOLINK device users are suggested to visit the vendor's download center to apply updates.

Security Affairs

Colibri Loader employs clever persistence mechanism

Recently discovered malware loader Colibri leverages a trivial and efficient persistence mechanism to deploy Windows Vidar data stealer. Malwarebytes researchers observed a new loader, dubbed Colibri, which has been used to deploy a Windows information stealer tracked as Vidar in a recent campaign. The Colibri Loader first appeared in the threat landscape in August 2021 […] The post Colibri Loader employs clever persistence mechanism appeared first on Security Affairs.

CyberScoop

CrowdStrike, Mandiant announce 'strategic partnership'

CrowdStrike's Falcon platform will be integrated into Mandiant's services for existing customers. More crossover is planned later this year. The post CrowdStrike, Mandiant announce 'strategic partnership' appeared first on CyberScoop.

Security Affairs

CVE-2022-0778 OpenSSL flaw affects multiple Palo Alto devices

Palo Alto Networks plans to fix CVE-2022-0778 OpenSSL flaw in some of its firewall, VPN, and XDR, products during April 2022. In Mid March, OpenSSL released updates to address a high-severity denial-of-service (DoS) vulnerability, tracked as CVE-2022-0778, that affects the BN_mod_sqrt() function used when certificate parsing. The flaw was discovered by the popular Google Project Zero […] The post CVE-2022-0778 OpenSSL flaw affects multiple Palo Alto devices appeared first on Security Affairs.

Security Affairs

CVE-2022-22292 flaw could allow hacking of Samsung Android devices

Experts discovered a vulnerability, tracked as CVE-2022-22292, which can be exploited to compromise Android 9, 10, 11, and 12 devices. Researchers from mobile cybersecurity firm Kryptowire discovered a vulnerability, tracked as CVE-2022-22292, in Android 9, 10, 11, and 12 devices. The vulnerability resides in the pre-installed Phone app that executes with system privileges on Samsung […] The post CVE-2022-22292 flaw could allow hacking of Samsung Android devices appeared first on Security Affairs.

Cyware News - Latest Cyber News

Deep Panda Uses Fire Chili Windows Rootkit

Deep Panda was found exploiting Log4Shell to deploy the new Fire Chili rootkit in compromised networks of organizations in the travel, finance, and cosmetic industries. Fire Chili helps keep file operations, registry key additions, processes, and malicious network connections concealed from the user and security software running on the targeted machine.

Cyware News - Latest Cyber News

Employee Info Among 13 Million Records Leaked by Fox News

A security configuration error exposed millions of internal records traced back to Fox News, including personally identifiable information on employees, researchers have claimed.

CyberScoop

FIN7 hacker sentenced to five years

Denys Iarmak, a Ukrainian national, was involved with the Russia-linked hacking group between November 2016 and November 2018. The post FIN7 hacker sentenced to five years appeared first on CyberScoop.

The Hacker News

First Malware Targeting AWS Lambda Serverless Platform Discovered

A first-of-its-kind malware targeting Amazon Web Services' (AWS) Lambda serverless computing platform has been discovered in the wild. Dubbed "Denonia" after the name of the domain it communicates with, "the malware uses newer address resolution techniques for command and control traffic to evade typical detection measures and virtual network access controls," Cado Labs researcher Matt Muir said

IT Security Guru

Fox News leaks 13 million internal records

Researchers have claimed that a misconfiguration has exposed millions of internal records, including employees' personally identifiable information, belonging to Fox News. The exposure was discovered by a team at Website Planet led by Jeremiah Fowler, who claimed that theoretically, anyone with an internet connection could have found the 58GB of internal records, which was left […] The post Fox News leaks 13 million internal records appeared first on IT Security Guru.

Cyware News -

Google boosts Android security with new set of dev policy changes

Starting from November 1, 2022, all newly released/published apps must target an Android API level released within one year from the latest major Android version release.

Cyware News -

Hacking group claim it has leaked more than 900,000 emails from Russian state media

The NB65 or Network Battalion 65 group, which is allied with the notorious hacker collective Anonymous, allegedly leaked more than 900,000 emails from

Latest Cyber News

The Hacker News

Hamas-linked Hackers Targeting High-Ranking Israelis Using 'Catfish' Lures

A threat actor with affiliations to the cyber warfare division of Hamas has been linked to an "elaborate campaign" targeting high-profile Israeli individuals employed in sensitive defense, law enforcement, and emergency services organizations. "The campaign operators use sophisticated social engineering techniques, ultimately aimed to deliver previously undocumented backdoors for Windows and

Cyware News - Latest Cyber News

How many steps does it take for attackers to compromise critical assets?

The XM Cyber research team analyzed the methods, attack paths and impacts of attack techniques that imperil critical assets across on-prem, multi-cloud and hybrid environments.

The Hacker News

Into the Breach: Breaking Down 3 SaaS App Cyber Attacks in 2022

During the last week of March, three major tech companies - Microsoft, Okta, and HubSpot - reported significant data breaches. DEV-0537, also known as LAPSUS$, performed the first two. This highly sophisticated group utilizes state-of-the-art attack vectors to great success. Meanwhile, the group behind the HubSpot breach was not disclosed. This blog will review the three breaches based on

Threatpost

MacOS Malware: Myth vs. Truth - Podcast

Huntress Labs R&D Director Jamie Levy busts the old "Macs don't get viruses" myth and offers tips on how MacOS malware differs and how to protect against it.

The Hacker News

Microsoft Obtains Court Order to Take Down Domains Used to Target Ukraine

Microsoft on Thursday disclosed that it obtained a court order to take control of seven domains used by APT28, a state-sponsored group operated by Russia's military intelligence service, with the goal of neutralizing its attacks on Ukraine. "We have since re-directed these domains to a sinkhole controlled by Microsoft, enabling us to mitigate Strontium's current use of these domains and enable

The Hacker News

New Octo Banking Trojan Spreading via Fake Apps on Google Play Store

A number of rogue Android apps that have been cumulatively installed from the official Google Play Store more than 50,000 times are being used to target banks and other financial entities. The rental banking trojan, dubbed Octo, is said to be a rebrand of another Android malware called ExobotCompact, which, in turn, is a "lite" replacement for its Exobot predecessor, Dutch mobile security firm

CyberScoop

Obama says he underestimated the threats posed by disinformation

The former president said the U.S. and other democracies helped disinformation flourish by growing complacent. The post Obama says he underestimated the threats posed by disinformation appeared first on CyberScoop.

The Hacker News

SharkBot Banking Trojan Resurfaces On Google Play Store Hidden Behind 7 New Apps

As many as seven malicious Android apps discovered on the Google Play Store masqueraded as antivirus solutions to deploy a banking trojan called SharkBot. "SharkBot steals credentials and banking information," Check Point researchers Alex Shamshur and Raman Ladutska said in a report shared with The Hacker News. "This malware implements a geofencing feature and evasion techniques, which makes it

CyberScoop

Suspected Chinese hackers are targeting India's power grid

Chinese hackers have been targeting India's power supply for years. The post Suspected Chinese hackers are targeting India's power grid appeared first on CyberScoop.

Cyware News - Latest Cyber News

The Original APT: Advanced Persistent Teenagers - Krebs on Security

Since surfacing in late 2021, LAPSUS$ has gained access to the networks or contractors for some of the world's largest technology companies, including Microsoft, NVIDIA, Okta and Samsung.

IT Security Guru

Website of Russian oil giant allegedly hacked

Gazprom Neft, the oil arm of Russian state gas company Gazprom, has allegedly suffered a hack on Wednesday bringing down its website. A statement allegedly from Gazprom CEO Alexie Miller was displayed on the website, appearing to criticise Russia's invasion of Ukraine. Miller is a close friend of President Vladimir Putin. The website went down [...] The post Website of Russian oil giant allegedly hacked appeared first on IT Security Guru.

Cyware News - Latest Cyber News

Zero-Day Bugs Bug the Biggies

In the past few days, several attackers have been observed exploiting new zero-day vulnerabilities in commonly used software products by Google, Apple, and others. Apple has released emergency fixes for two zero-day flaws. Trend Micro fixed a high-severity vulnerability in its Apex Central. Meanwhile, Google recently fixed a high-severity zero-day bug in the Google Chrome.

Latest Cyber News

the All-Russia State Television and Radio Broadcasting Company (VGTRK).

Security Affairs

Hamas-linked threat actors target high-profile Israeli individuals

Hamas-linked threat actors conducted an elaborate campaign aimed at high-profile Israeli individuals employed in sensitive sectors. Researchers from Cybereason observed a sophisticated cyberespionage campaign conducted by APT-C-23 group campaigns targeting Israeli high-profile targets working for sensitive defense, law enforcement, and emergency services organization. The threat actors use sophisticated social engineering techniques to infect Windows and Android [...] The post Hamas-linked threat actors target high-profile Israeli individuals appeared first on Security Affairs.

WeLiveSecurity

How secure is your cloud storage? Mitigating data security risks in the cloud

As cloud systems are increasingly the bedrock on which digital transformation is built, keeping a close eye on how they are secured is an essential cybersecurity best practice The post How secure is your cloud storage? Mitigating data security risks in the cloud appeared first on WeLiveSecurity

ZDNet | security RSS

Israeli officials are being catfished by APT-C-23 hackers

APT-C-23 is targeting high-ranking individuals in defense, law, and emergency services.

Security Affairs

Microsoft disrupted APT28 attacks on Ukraine through a court order

Microsoft obtained a court order to take over seven domains used by the Russia-linked APT28 group to target Ukraine. Microsoft on Thursday announced it has obtained a court order to take over seven domains used by Russia-linked cyberespionage group APT28 in attacks against Ukraine. The APT28 group (aka Fancy Bear, Pawn Storm, Sofacy Group, Sednit, and STRONTIUM) has been active since at least 2007 [...] The post Microsoft disrupted APT28 attacks on Ukraine through a court order appeared first on Security Affairs.

IT Security Guru

Mobile banking overwhelmingly safer for UK consumers

Mobile banking is the safest way to bank for UK consumers, RiskOps platform for financial risk management Feedzai revealed in their Q2 2022 Financial Crime Report, based on the analysis of over 18 billion global banking transactions throughout 2021. According to the report, banking represented 88% of all banking transactions in the U.K. during this [...] The post Mobile banking overwhelmingly safer for UK consumers appeared first on IT Security Guru.

Cyware News - Latest Cyber News

New Spyware Actively Targets Android Users

An Android spyware impersonates a process manager app to target users and steal their data. While analyzing the spyware, the research team discovered that it downloads additional payloads to compromised devices. Organizations and users are suggested to always monitor and review the app permissions in their phones.

Naked Security

S3 Ep77: Bugs, busts and old-school PDP-11 hacking [Podcast]

Latest episode - listen now! Cybersecurity news and advice in plain English.

Threatpost

SSRF Flaw in Fintech Platform Allowed for Compromise of Bank Accounts

Researchers discovered the vulnerability in an API already integrated into many bank systems, which could have defrauded millions of users by giving attackers access to their funds.

Cyware News - Latest Cyber News

The Mysterious Borat RAT is an All-In-One Threat

Cyble discovered a new RAT, dubbed Borat. With a builder, feature modules, and a server certificate, it offers ransomware and DDOS attack services. It is not known whether Borat is being sold or freely shared among cybercriminals. While analyzing the campaign and digging into its origin, a researchers group discovered the payload executable to be AsyncRAT, depicting a connection between the two.

The Hacker News

Ukrainian FIN7 Hacker Gets 5-Year Sentence in the United States

A 32-year-old Ukrainian national has been sentenced to five years in prison in the U.S. for the individual's criminal work as a "high-level hacker" in the financially motivated group FIN7. Denys Iarmak, who worked as a penetration tester for the cartel from November 2016 through November 2018, had been previously arrested in Bangkok, Thailand in November 2019, before being extradited to the U.S.

Cyware News - Latest Cyber News

Website of Russian Oil Giant Gazprom Neft Down After Alleged Hack

The website of Gazprom Neft, the oil arm of Russian state gas company Gazprom, was offline on Wednesday after an alleged hack, in what appears to be the latest hack on a government-associated site following Russia's invasion of Ukraine.

Twitter

CVE

CVE-2022-24136 Hospital Management System v1.0 is affected by an unrestricted upload of dangerous file type vulnerability in treatmentrecord.php. To exploit, an attacker can upload any PHP file, and then execute it.

Robo Shadow Alerts

Potentially Critical CVE Detected! CVE-2021-43722 D-Link DIR-645 1.03 A1 is vulnerable to Buffer Overflow. The hnap_main function in the cgibin handler uses sprintf to fo... CVSS: 9.11 #D-link #CVE #CyberSecurity

Threat Intel Center

NEW: CVE-2022-24136 Hospital Management System v1.0 is affected by an unrestricted upload of dangerous file type vulnerability in treatmentrecord.php. To exploit, an attacker can upload any PHP file, and then ex... (click for more) Severity: CRITICAL

Threat Intel Center

NEW: CVE-2022-24136 Hospital Management System v1.0 is affected by an unrestricted upload of dangerous file type vulnerability in treatmentrecord.php. To exploit, an attacker can upload any PHP file, and then ex... (click for more)

V

vulnonym

One night, CVE-2022-24136 wished upon a star, and today that wish has been granted. It now has a name, like a real, live vulnerability: Trembly Dragonfish

phpadvisories

CVE-2022-24136 | Hospital Management System 1.0 treatmentrecord.php erweiterte Rechte #phpsec

MFA Russia

#Zakharova: We strongly advise the mass media & analysts to be more demanding in asking the #US administration for explanations about the reasons & sources of increased cybersecurity threats for economic activities.

Threat Intel Center

NEW: CVE-2022-24136 Hospital Management System v1.0 is affected by an unrestricted upload of dangerous file type vulnerability in treatmentrecord.php. To exploit, an attacker can upload any PHP file, and then ex... (click for more)

CVE

CVE-2021-43722 D-Link DIR-645 1.03 A1 is vulnerable to Buffer Overflow. The hnap_main function in the cgibin handler uses sprintf to format the soapaction header onto the stack and has no limit on the size.

CVE.report

CVE-2022-24136 : Hospital Management System v1.0 is affected by an unrestricted upload of dangerous file type vulnerability in treatmentrecord.php. To exploit, an attacker can upload any PHP file, and then execute it....

Robo Shadow Alerts

Potentially Critical CVE Detected! CVE-2022-24136 Hospital Management System v1.0 is affected by an unrestricted upload of dangerous file type vulnerability in treatmentre... CVSS: 9.50 #HospitalManagement #CVE #CyberSecurity

Threat Intel Center

NEW: CVE-2022-24136 Hospital Management System v1.0 is affected by an unrestricted upload of dangerous file type vulnerability in treatmentrecord.php. To exploit, an attacker can upload any PHP file, and then ex... (click for more)

ThreatMeter

CVE-2022-24136 Hospital Management System v1.0 is affected by an unrestricted upload of dangerous file type vulnerability in treatmentrecord.php. To exploit, an attacker can upload any PHP file, and then execute it. (CVSS:0.0) (Last Update:2022-03-31)

Source: NIST

NIST CVE: Critical

CVE-2021-43722

D-Link DIR-645 1.03 A1 is vulnerable to Buffer Overflow. The hnap_main function in the cgibin handler uses sprintf to format the soapaction header onto the stack and has no limit on the size.

CRITICAL Vector: network Created: 2022-03-31 Updated: 2022-04-08

CVE-2022-24136

Hospital Management System v1.0 is affected by an unrestricted upload of dangerous file type vulnerability in treatmentrecord.php. To exploit, an attacker can upload any PHP file, and then execute it.

CRITICAL Vector: network Created: 2022-03-31 Updated: 2022-04-08

Source: NIST

NIST CVE: High

CVE-2022-25915

Improper access control vulnerability in **ELECOM** LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, **WRC-2533GST2** firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to bypass access restriction and to access the management **screen** of the product via unspecified vectors.

HIGH Vector: adjacent_network Created: 2022-03-31 Updated: 2022-04-08

CVE-2021-34257

Multiple Remote Code Execution (RCE) vulnerabilities **exist** in WPanel 4 4.3.1 and below via a malicious PHP file upload to (1) Dashboard's **Avatar** image, (2) Posts Folder image, (3) Pages Folder image and (4) **Gallery** Folder image.

HIGH Vector: network Created: 2022-03-31 Updated: 2022-04-08

CVE-2022-1176

Loose comparison causes IDOR on multiple endpoints in **GitHub** repository livehelperchat/livehelperchat prior to 3.96.

HIGH Vector: network Created: 2022-03-31 Updated: 2022-04-08

CVE-2022-1191

SSRF on index.php/cobrowse/proxycss/ in **GitHub** repository livehelperchat/livehelperchat prior to 3.96.

HIGH Vector: network Created: 2022-03-31 Updated: 2022-04-08

Source: NIST

NIST CVE: Medium

CVE-2021-20729

Cross-site scripting vulnerability in **pfSense** CE and pfSense **Plus** (pfSense CE software versions 2.5.2 and earlier, and pfSense Plus software versions 21.05 and earlier) allows a remote attacker to inject an arbitrary script via a malicious URL.

MEDIUM Vector: network Created: 2022-03-31 Updated: 2022-04-08

Source: NIST

NIST CVE: Low

Nothing today

Source: NIST

NIST CVE: Unrated

CVE-2021-43453

A Heap-based Buffer Overflow vulnerability exists in **JerryScript** 2.4.0 and prior versions via an out-of-bounds read in parser_parse_for_statement_start in the js-parser-statm.c file. This issue is similar to CVE-2020-29657.

UNRATED Vector: unkown Created: 2022-04-07 Updated: 2022-04-08

CVE-2022-27063

AeroCMS v0.0.1 was discovered to contain a stored cross-site scripting (XSS) vulnerability via view_all_comments.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Comments text field.

UNRATED Vector: unkown Created: 2022-04-08 Updated: 2022-04-08

CVE-2021-43474

An Access Control vulnerability exists in **D-Link DIR-823G** REVA1 1.02B05 (Lastest) via any parameter in the HNAP1 function

UNRATED Vector: unkown Created: 2022-04-07 Updated: 2022-04-08

CVE-2022-28000

Car Rental System v1.0 was discovered to contain a SQL injection vulnerability at /Car_Rental/booking.php via the id parameter.

UNRATED Vector: unkown Created: 2022-04-08 Updated: 2022-04-08

CVE-2022-27357

Ecommerce-Website v1 was discovered to contain an arbitrary file upload vulnerability via /customer_register.php. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file.

UNRATED Vector: unkown Created: 2022-04-08 Updated: 2022-04-08

CVE-2022-28001

Movie Seat Reservation v1 was discovered to contain a SQL injection vulnerability at /index.php?page=reserve via the id parameter.

UNRATED Vector: unkown Created: 2022-04-08 Updated: 2022-04-08

CVE-2022-27064

Musical World v1 was discovered to contain an arbitrary file upload vulnerability via uploaded_songs.php. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file.

UNRATED Vector: unkown Created: 2022-04-08 Updated: 2022-04-08

CVE-2021-36202

Server-Side Request Forgery (SSRF) vulnerability in Johnson Controls **Metasys** could allow an authenticated attacker to inject malicious code into the MUI PDF export feature. This issue affects: Johnson Controls Metasys All 10 versions versions prior to 10.1.5; All 11 versions versions prior to 11.0.2.

UNRATED Vector: unkown Created: 2022-04-07 Updated: 2022-04-08

CVE-2022-28805

singlevar in lparser.c in Lua through 5.4.4 lacks a certain luaK_exp2anyregup call, leading to a heap-based buffer over-read that might affect a system that compiles untrusted Lua code.

UNRATED Vector: unkown Created: 2022-04-08 Updated: 2022-04-08

CVE-2022-27349

Social Codia SMS v1 was discovered to contain an arbitrary file upload vulnerability via addteacher.php. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file.

UNRATED Vector: unkown Created: 2022-04-08 Updated: 2022-04-08

CVE-2022-24681

Zoho ManageEngine ADSelfService **Plus** before 6121 allows XSS via the welcome name attribute to the Reset Password, Unlock Account, or User Must Change Password **screen**.

UNRATED Vector: unkown Created: 2022-04-07 Updated: 2022-04-08

CVE-2022-27351

Zoo Management System v1.0 was discovered to contain an arbitrary file upload vulnerability via /public_html/apply_vacancy. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file.

UNRATED Vector: unkown Created: 2022-04-08 Updated: 2022-04-08

CVE-2022-27062

AeroCMS v0.0.1 was discovered to contain a stored cross-site scripting (XSS) vulnerability via add_post.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Post Title text field.

UNRATED Vector: unkown Created: 2022-04-08 Updated: 2022-04-08

CVE-2022-27061

AeroCMS v0.0.1 was discovered to contain an arbitrary file upload vulnerability via the Post Image function under the Admin panel. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file.

UNRATED Vector: unkown Created: 2022-04-08 Updated: 2022-04-08

CVE-2022-26624

Bootstrap v3.1.11 and v3.3.7 was discovered to contain a cross-site scripting (XSS) vulnerability via the Title parameter in /vendor/views/add_product.php.

UNRATED Vector: unkown Created: 2022-04-08 Updated: 2022-04-08

CVE-2022-27346

Ecommece-Website v1.1.0 was discovered to contain an arbitrary file upload vulnerability via /admin/index.php?slides. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file.

UNRATED Vector: unkown Created: 2022-04-08 Updated: 2022-04-08

CVE-2022-28796

jbd2_journal_wait_updates in fs/jbd2/transaction.c in the **Linux** kernel before 5.17.1 has a use-after-free caused by a transaction_t race condition.

UNRATED Vector: unkown Created: 2022-04-08 Updated: 2022-04-08

CVE-2022-28002

Movie Seat Reservation v1 was discovered to contain an unauthenticated file disclosure vulnerability via /index.php?page=home.

UNRATED Vector: unkown Created: 2022-04-08 Updated: 2022-04-08

CVE-2022-27991

Online Banking System in PHP v1 was discovered to contain multiple SQL injection vulnerabilities at /staff_login.php via the Staff ID and Staff Password parameters.

UNRATED Vector: unkown Created: 2022-04-08 Updated: 2022-04-08

CVE-2022-27352

Simple **House Rental** System v1 was discovered to contain an arbitrary file upload vulnerability via /app/register.php. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file.

UNRATED Vector: unkown Created: 2022-04-08 Updated: 2022-04-08

CVE-2022-27348

Social Codia SMS v1 was discovered to contain a stored cross-site scripting (XSS) vulnerability via add_post.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Post Title text field.

UNRATED Vector: unkown Created: 2022-04-08 Updated: 2022-04-08

CVE-2022-1219

SQL injection in RecyclebinController.php in **GitHub** repository pimcore/pimcore prior to 10.3.5. This vulnerability is capable of steal the data

UNRATED Vector: unkown Created: 2022-04-08 Updated: 2022-04-08

CVE-2022-27992

Zoo Management System v1.0 was discovered to contain a SQL injection vulnerability at /public_html/animals via the class_id parameter.

UNRATED Vector: unkown Created: 2022-04-08 Updated: 2022-04-08

Source: Hybrid Analysis

Top malicious files

100% Threat score	Malicious.apk	100% Threat score	sicurezza-posteitaliane.apk
100% Threat score	Valak Client - Evolut.exe	100% Threat score	dmvhQEY5P8.dll
100% Threat score	tmpeniutjr_	100% Threat score	tmpvjthuxlm
100% Threat score	dod-upload.dodortar.ru	100% Threat score	message-9.xls

100% Threat score	dmvhQEY5P8.dll
85% Threat score	helium_15.exe
76% Threat score	hartman.exe
75% Threat score	Imploded-keygen.exe
71% Threat score	BoosterX_v1.15.exe

Source: Hybrid Analysis

Top malicious URL

100% Threat score	http://tvoetokafe.eu/
100% Threat score	https://towsrus.net/007/
93% Threat score	http://171.42.127.215:49506/i
91% Threat score	http://182.126.126.129:44578/bin.sh
89% Threat score	http://coplaltd.eu/images/
86% Threat score	http://107.172.75.154/700/vbc.exe
85% Threat score	https://vvvvvv-roblox.com/users/9898816836/profile
80% Threat score	http://billa-ag.at/
80% Threat score	https://0fficlal-exchan9e.com/bitFlyer-0fficial/flyer/?shiny
75% Threat score	https://linkprotect.cudasvc.com/url?a=http%3A%2F%2Fsecure.redstarkitchens.com%2F&c=E%2C1%2CXDPXisbaxb7CpVe2xt_ZyirTmtvshzQI2_F
75% Threat score	http://101-bg.com/
75% Threat score	http://www.ntbg.bg/
73% Threat score	https://fromamazon.enteramazonyour.top/signim/? openid.pape.max_auth_age=0&openid.return_to=https%3A%2F%2Fwww.amazon.co.jp%2F%3Fref_%3Dnav_em_hd_re_signin&openid.identity=http%3A%2F%2Fspecs.openid.net%2Fa
73% Threat score	http://elaspany.ddns.net/
73% Threat score	https://santomikhael.ac.id/.proceedings#elaineapp%40hollard.co.za

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 Uruguay
- #9 Brazil
- #10 Japan

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 **Michael Persaud**
Long time snowshoe type spammer, raided by FBI then indicted in 2017 on federal wire fraud charges tied to his spamming operations.

#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 **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.

#7 **RR Media**
A high volume spam operation based in or run from Huntington Beach, CA, USA. The operation uses a variety of different names.

#8 **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.

#9 **Richpro Trade Inc. / Richvestor GmbH**
Uses botnets or hires botnet spammers to send spam linking back to suspect investment, "quack-health-cures" and other sites that he owns or is an affiliate of. Botnet spamming and hosting sites on hacked servers is fully criminal in much of the world. Managed or owned by a Timo Richert.

Source: SpamHaus

Top countries with botnet

- #1 China
- #2 India
- #3 United States of America
- #4 Indonesia
- #5 Thailand
- #6 Viet Nam
- #7 Algeria
- #8 Brazil
- #9 Pakistan
- #10 Venezuela (Bolivarian Republic of)

Source: SpamHaus

Top phishing countries

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

Source: Have I been pwned?

Have I been pwnd

Travelio (travelio.com)
In November 2021, the Indonesian real estate website Travelio suffered a data breach that exposed over 470k customer accounts. The data included email addresses, names, password hashes, phone numbers and for some accounts, dates of birth, physical address and Facebook auth tokens. The data was provided to HIBP by a source who requested it be attributed to "white_peacock@riseup.net".

Count: 471376 Created: 2021-11-23 Updated: 2022-04-08

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