



Your Security Rabbits report for April 01, 2022

Source: [Ransom Watch](#)















Ransomware attacks


alphv	Dober	lockbit2	kssente
conti	Lowell	alphv	SSW Consulting
lockbit2	bafokengholding...	alphv	CASTGROUP.COM,BR
lockbit2	keypoint.com	conti	Parker Appliance Company
conti	Prima Sole Components Spa	conti	Rettenmeier Holding AG
lockbit2	studiobrazzale....	lockbit2	yachtcharterfle...

Hot topics

Nothing today

News

 Threatpost	A Blockchain Primer and a Bored Ape Headscratcher - Podcast Mystified? Now's the time to learn about cryptocurrency-associated risks: Listen to KnowBe4's Dr. Lydia Kostopoulos explain blockchain, NFTs and how to stay safe.	 Security Affairs	Anonymous hacked Russian Thozis Corp, but denies attacks on Rosaviatsia The Anonymous collective hacked the Russian investment firm Thozis Corp, but it's a mystery the attack against the Russian Civil Aviation Authority Rosaviatsia. Anonymous continues to target Russian organizations and private foreign businesses the are still operating in the country. The popular collective claims to have hacked the Russian investment firm Thozis Corp, which is [...] The post Anonymous hacked Russian Thozis Corp, but denies attacks on Rosaviatsia appeared first on Security Affairs.
 Security Affairs	Apple issues emergency patches to fix actively exploited zero-days Apple released emergency patches to address two zero-day vulnerabilities actively exploited to compromise iPhones, iPads, and Macs. Apple has released emergency security patches to address two zero-day vulnerabilities actively exploited to hack iPhones, iPads, and Macs. The first zero-day, tracked as CVE-2022-22674, is an out-of-bounds read issue that resides in the Intel Graphics Driver that could [...] The post Apple issues emergency patches to fix actively exploited zero-days appeared first on Security Affairs.	 The Hacker News	Apple Issues Patches for 2 Actively Exploited Zero-Days in iPhone, iPad and Mac Devices Apple on Thursday rolled out emergency patches to address two zero-day flaws in its mobile and desktop operating systems that it said may have been exploited in the wild. The shortcomings have been fixed as part of updates to iOS and iPadOS 15.4.1, macOS Monterey 12.3.1, tvOS 15.4.1, and watchOS 8.5.1. Both the vulnerabilities have been reported to Apple anonymously. Tracked as CVE-2022-22675,
 Sophos Naked Security	Apple pushes out two emergency 0-day updates - get 'em now! More Apple zero-days - mobile devices, laptops and desktops affected. Update now!	 CyberScoop	Attack on Viasat modems possibly came from wiper malware deployed through supply chain Researchers from SentinelOne say there are reasons to disagree with Viasat's most recent statement about the Feb. 24 attack. The post Attack on Viasat modems possibly came from wiper malware deployed through supply chain appeared first on CyberScoop.
 Threatpost	Automaker Cybersecurity Lagging Behind Tech Adoption, Experts Warn A bug in Honda is indicative of the sprawling car-attack surface that could give cyberattackers easy access to victims, as global use of 'smart car tech' and EVs surges.	 Threatpost	Belarusian 'Ghostwriter' Actor Picks Up BitB for Ukraine-Related Attacks Ghostwriter is one of 3 campaigns using war-themed attacks, with cyber-fire coming in from government-backed actors in China, Iran, North Korea & Russia.
 CyberScoop	Biden administration is studying whether to scale back Trump-era cyber authorities at DOD The Biden administration is considering revising the Trump-era policy which gave broad cyber authorities to the Department of Defense and Cyber Command. The post Biden administration is studying whether to scale back Trump-era cyber authorities at DOD appeared first on CyberScoop.	 Cyware News - Latest Cyber News	Biden prolongs national emergency amid increasing cyber threats The extended national emergency declaration comes after the CISA released a warning regarding possible Russian state-sponsored cyberattacks against U.S. organizations following sanctions imposed as a result of the ongoing invasion of Ukraine.
 The Hacker News	Bugs in Wyze Cams Could Let Attackers Takeover Devices and Access Video Feeds Three security vulnerabilities have been disclosed in the popular Wyze Cam devices that grant malicious actors to execute arbitrary code and access camera feeds as well as unauthorizedly read the SD cards, the latter of which remained unresolved for nearly three years after the initial discovery. The security flaws relate to an authentication bypass (CVE-2019-9564), a remote code execution bug	 Security Affairs	CISA adds Sophos firewall bug to Known Exploited Vulnerabilities Catalog The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added a critical Sophos firewall flaw and seven other issues to its Known Exploited Vulnerabilities Catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added the recently disclosed CVE-2022-1040 flaw in the Sophos firewall, along with seven other issues, to its Known Exploited Vulnerabilities Catalog. According to Binding Operational [...] The post CISA adds Sophos firewall bug to Known Exploited Vulnerabilities Catalog appeared first on Security Affairs.
 ZDNet security RSS	Cybersecurity managers with a direct line to executive boards set the tone for investment: Study Moody's examines how incident response and defense have implications for the market.	 KrebsOnSecurity	Fake Emergency Search Warrants Draw Scrutiny from Capitol Hill On Tuesday, KrebsOnSecurity warned that hackers increasingly are using compromised government and police department email accounts to obtain sensitive customer data from mobile providers, ISPs and social media companies. Today, one of the U.S. Senate's most tech-savvy lawmakers said he was troubled by the report and is now asking technology companies and federal agencies for information about the frequency of such schemes.



Security Affairs

[Flaws in Wyze cam devices allow their complete takeover](#)


Wyze Cam devices are affected by three security vulnerabilities that can allow attackers to takeover them and access camera feeds. Bitdefender researchers discovered three security vulnerabilities in the popular Wyze Cam devices that can be exploited by threat actors to execute arbitrary code and access camera feeds. The three flaws reported by the cybersecurity firm [...] The post Flaws in Wyze cam devices allow their complete takeover appeared first on Security Affairs.



Cyware News - Latest Cyber News

[Google warns of multiple hacking groups using the war in Ukraine as a lure in phishing attempts](#)


Hostile hacking groups are exploiting Russia's invasion of Ukraine to carry out cyberattacks designed to steal login credentials, sensitive information, money, and more from victims around the world.



Cyware News - Latest Cyber News

[Lazarus Trojanized DeFi app for delivering malware](#)


The malware operator exclusively used compromised web servers located in South Korea for this attack. The threat actor configured this infrastructure with servers set up as multiple stages.



ZDNet | security RSS

[Meet BlackGuard: a new infostealer peddled on Russian hacker forums](#)


Sophisticated, but potentially cheap.



The Hacker News

[New Python-based Ransomware Targeting JupyterLab Web Notebooks](#)


Researchers have disclosed what they say is the first-ever Python-based ransomware strain specifically designed to target exposed Jupyter notebooks, a web-based interactive computing platform that allows editing and running programs via a browser. "The attackers gained initial access via misconfigured environments, then ran a ransomware script that encrypts every file on a given path on the



Cyware News - Latest Cyber News

[Phishing uses Azure Static Web Pages to impersonate Microsoft](#)


Using the Azure Static Web Apps platform to target Microsoft users is an excellent tactic. Each landing page automatically gets its own secure page padlock in the address bar due to the *.1.azurestaticapps.net wildcard TLS certificate.



Cyware News - Latest Cyber News

[Ransomware Payments Hit New Records](#)


According to a report by Unit 42, the average ransom demand rose 144% to \$2.2 million in 2021. The average ransom payment rose 78% to \$541,010. Thirty-five new ransomware gangs popped up in 2021.



Cyware News - Latest Cyber News

[Russia Prepares Destructive Cyberattacks](#)


Russia is preparing disruptive cyberattacks that could target U.S. energy and financial industries to cause further pain to the Biden administration, in retaliation for heavy sanctions, several people familiar with the matter told Foreign Policy.



Naked Security

[S3 Ep76: Deadbolt, LAPSUS\\$, Zlib, and a Chrome 0-day \[Podcast\]](#)

Latest episode - listen now!



Cyware News - Latest Cyber News

[SunCrypt Ransomware Now Comes With Upgraded Features](#)


SunCrypt--a RaaS that came to prominence in mid-2020--was one of the first threat actors to implement triple extortion in its campaigns. It is a small RaaS, operating with a close circle of affiliates.



CyberScoop

[Treasury sanctions Russian research center blamed for Trisis malware](#)


The list also includes Evgeny Viktorovich Gladkikh, the researcher indicted for creating the malware, which targets industrial control systems. The post Treasury sanctions Russian research center blamed for Trisis malware appeared first on CyberScoop.



Cyware News - Latest Cyber News

[UK NCSC Says its Time to Rethink Russian Supply Chain Risks](#)


The U.K. NCSC has urged the public sector, critical infrastructures (CNI) and other organizations to reconsider the potential risks associated with any "Russian-controlled" parts of their supply chain.



Security Affairs

[Zyxel fixes a critical bug in its business firewall and VPN devices](#)


Zyxel issued security updates for a critical vulnerability that affects some of its business firewall and VPN devices. Networking equipment vendor Zyxel has pushed security updates for a critical flaw, tracked as CVE-2022-0342 (CVSS 9.8), that affects some of its business firewall and VPN products. The vulnerability can be exploited to take control of the [...] The post Zyxel fixes a critical bug in its business firewall and VPN devices appeared first on Security Affairs.



Security Affairs

[Google TAG details cyber activity with regard to the invasion of Ukraine](#)


The Google TAG uses uncovered phishing attacks targeting Eastern European and NATO countries, including Ukraine. The Google Threat Analysis Group (TAG) provided an update about nation-state attacks related ongoing Russian invasion of Ukraine, the experts spotted phishing and malware attacks targeting Eastern European and NATO countries, including Ukraine The researchers uncovered a phishing campaign conducted by a [...] The post Google TAG details cyber activity with regard to the invasion of Ukraine appeared first on Security Affairs.



The Hacker News

[Hackers Increasingly Using 'Browser-in-the-Browser' Technique in Ukraine Related Attacks](#)


A Belarusian threat actor known as Ghostwriter (aka UNC1151) has been spotted leveraging the recently disclosed browser-in-the-browser (BitB) technique as part of their credential phishing campaigns exploiting the ongoing Russo-Ukrainian conflict. The method, which masquerades as a legitimate domain by simulating a browser window within the browser, makes it possible to mount convincing social



Cyware News - Latest Cyber News

[LockBit victim estimates cost of ransomware attack to be \\$42 million](#)


The disruption caused by the cyberattack affected Atento's Brazil-based operations, resulting in a revenue loss of \$34.8 million and an additional \$7.3 million in costs related to mitigating the impact of the incident.



Cyware News - Latest Cyber News

[New Milestones for Deep Panda: Log4Shell and Digitally Signed Fire Chili Rootkits](#)


While examining alerts and telemetry, FortiGuard Labs noticed several infiltrations into victim networks that were achieved via Log4Shell exploitation of vulnerable VMware Horizon servers.



Cyware News - Latest Cyber News

[Next Wave of Ukraine Attacks - DDoS, Malicious Tools, and Infrastructure Disruptions](#)


Russia-Ukraine conflict grew grimmer as researchers found three separate attack incidents of DDoS, malicious tools, and infrastructure disruption, that were launched against Ukraine. One of the attacks has hit the fixed-line telecommunications firm, Ukrtelecom. There could be more cyberattacks launched targeting Ukrainian entities. Government agencies and businesses are recommended to follow the CERT-UA advisory to stay protected.



Threatpost

[QNAP Customers Adrift, Waiting on Fix for OpenSSL Bug](#)


QNAP is warning clients that a recently disclosed vulnerability affects most of its NAS devices, with no mitigation available while the vendor readies a patch.



Cyware News - Latest Cyber News

[Remote 'Brokenwire' Hack Prevents Charging of Electric Vehicles at DC Fast Chargers](#)


The attack targets the Combined Charging System (CCS) -- a widely used DC rapid charging technology -- and it interrupts the communication between the charger and the vehicle.



Cyware News - Latest Cyber News

[Russia warns of 'grave consequences' after U.S. reaffirms threat of sanctions over Ukraine](#)


President Biden reaffirmed the U.S. threat of new sanctions against Russia in case of an escalation or invasion, to which Putin responded with a warning of his own that such a U.S. move could lead to a complete rupture of ties.



The Hacker News

[Security Patch Releases for Critical Zero-Day Bug in Java Spring Framework](#)

The maintainers of Spring Framework have released an emergency patch to address a newly disclosed remote code execution flaw that, if successfully exploited, could allow an unauthenticated attacker to take control of a targeted system. Tracked as CVE-2022-22965, the high-severity flaw impacts Spring Framework versions 5.3.0 to 5.3.17, 5.2.0 to 5.2.19, and other older, unsupported versions. Users



ZDNet | security RSS

[The spectre of Stuxnet: CISA issues alert on Rockwell Automation ICS vulnerabilities](#)


The flaws can be exploited to execute code on vulnerable controllers and workstations.



Naked Security

[Two different "VMware Spring" bugs at large - we cut through the confusion](#)


Whoever came up with the name "Spring4Shell" didn't help at all... we cut through the Spring Bug confusion



Blog â€” Flashpoint

[What Is SpringShell? What We Know About the SpringShell Vulnerability \[Updated\]](#)

Updated March 31 Flashpoint and Risk Based Security have analyzed a new remote code execution (RCE) vulnerability looming in the background, dubbed "SpringShell," which could affect a wide variety of software. In some circles, SpringShell is being hyped and rumored to be as impactful as Log4Shell. But we are still collecting facts and will continuously [...] The post What Is SpringShell? What We Know About the SpringShell Vulnerability [Updated] appeared first on Flashpoint.









The Hacker News

[Zyxel Releases Patches for Critical Bug Affecting Business Firewall and VPN Devices](#)

Networking equipment maker Zyxel has pushed security updates for a critical vulnerability affecting some of its business firewall and VPN products that could enable an attacker to take control of the devices. "An authentication bypass vulnerability caused by the lack of a proper access control mechanism has been found in the CGI program of some firewall versions," the company said in an advisory

Twitter

 Jim Sciutto	>> Weve seen Russian soldiers short of weapons and morale - refusing to carry out orders, sabotaging their own equipment and even accidentally shooting down their own aircraft. - Sir Jeremy Fleming, Director of GCHQ, the UK's Intelligence, Cyber & Security Agency.	 CNN	There's no bigger insult ... to a former KGB officer than to tell him that he's misinformed about his own military and his own war. Russia and cybersecurity expert @DAlperovitch discusses the declassified US intelligence reports and their potential effects on Putin.
 Reuters	The U.S. government began privately warning some American companies the day after Russia invaded Ukraine that Moscow could manipulate software designed by Russian cybersecurity company Kaspersky to cause harm	 Christopher Burgess	Today: @TheJusticeDept unsealed a 26-count indictment of a @NSAGov employee for allegedly sharing classified information over email. #insiderthreat ramifications aplenty - I dig in via @ClearanceJobs #natsec #nispom #cybersecurity #counterintelligence
 Kevin Collier	Google, angling for gov contracts, has published a study of federal workers saying the US government's overreliance on Microsoft is a cybersecurity problem. Message comes from former CISA/NPPD director Jeannette Manfra	 Reuters	BlackBerry misses Q4 revenue estimates, cybersecurity unit growth flat

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-2022-21947	A Improper Access Control vulnerability in Rancher Desktop of SUSE allows attackers in the local network to connect to the Dashboard API (steve) to carry out arbitrary actions. This issue affects: SUSE Rancher Desktop versions prior to V. UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-01	CVE-2021-35117	An Out of Bounds read may potentially occur while processing an IBSS beacon, in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-01
CVE-2022-24803	Asciidoctor-include-ext is Asciidoctor's standard include processor reimplemented as an extension. Versions prior to 0.4.0, when used to render user-supplied input in AsciiDoc markup, may allow an attacker to execute arbitrary system commands on the host operating system. This attack is possible even when 'allow-uri-read' is disabled! The problem has been patched in the referenced commits. UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-01	CVE-2022-24802	deepmerge-ts is a typescript library providing functionality to deep merging of javascript objects. deepmerge-ts is vulnerable to Prototype Pollution via file deepmerge.ts, function defaultMergeRecords(). This issue has been patched in version 4.0.2. There are no known workarounds for this issue. UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-01
CVE-2022-25017	Hitron CHITA 7.2.2.0.3b6-CD devices contain a command injection vulnerability via the Device/DDNS ddnsUsername field. UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-01	CVE-2021-1950	Improper cleaning of secure memory between authenticated users can lead to face authentication bypass in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-01
CVE-2021-35115	Improper handling of multiple session supported by PVM backend can lead to use after free in Snapdragon Auto, Snapdragon Mobile UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-01	CVE-2021-1942	Improper handling of permissions of a shared memory region can lead to memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-01
CVE-2021-30333	Improper validation of buffer size input to the EFS file can lead to memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-01	CVE-2021-30328	Possible assertion due to improper validation of invalid NR CSI-IM resource configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-01
CVE-2021-30332	Possible assertion due to improper validation of OTA configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-01	CVE-2021-30329	Possible assertion due to improper validation of TCI configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-01
CVE-2021-30331	Possible buffer overflow due to improper data validation of external commands sent via DIAG interface in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	CVE-2021-35089	Possible buffer overflow due to lack of input IB amount validation while processing the user command in Snapdragon Auto

	<div>UNRATED</div> Vector: unknownCreated: 2022-04-01Updated: 2022-04-01		<div>UNRATED</div> Vector: unknownCreated: 2022-04-01Updated: 2022-04-01
CVE-2021-35110	Possible buffer overflow to improper validation of hash segment of file while allocating memory in Snapdragon Connectivity, Snapdragon Mobile <div>UNRATED</div> Vector: unknownCreated: 2022-04-01Updated: 2022-04-01	CVE-2021-35106	Possible out of bound read due to improper length calculation of WMI message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables <div>UNRATED</div> Vector: unknownCreated: 2022-04-01Updated: 2022-04-01
CVE-2021-35088	Possible out of bound read due to improper validation of IE length during SSID IE parse when channel is DFS in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking <div>UNRATED</div> Vector: unknownCreated: 2022-04-01Updated: 2022-04-01	CVE-2021-35103	Possible out of bound write due to improper validation of number of timer values received from firmware while syncing timers in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking <div>UNRATED</div> Vector: unknownCreated: 2022-04-01Updated: 2022-04-01
CVE-2021-35105	Possible out of bounds access due to improper input validation during graphics profiling in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables <div>UNRATED</div> Vector: unknownCreated: 2022-04-01Updated: 2022-04-01		

Source: Hybrid Analysis

Top malicious files

100% Threat score	activation.doc	100% Threat score	ivacy-windows-setup.exe
100% Threat score	vbc(1).bin	100% Threat score	qry 0206119600.xls
100% Threat score	APInvoice Invoice Submission - Doc-20220330085307.bin	100% Threat score	Document_371872371_03232021_Copy.xlsm
100% Threat score	3.bin	100% Threat score	tmp1xj7x_x0
100% Threat score	2fc6d7df9252b1e2c4eb3ad70d29c188d87548127c44cebc40db9abe8e5aa35.bin	100% Threat score	loader.exe
100% Threat score	gup5setup.exesrc10000id1v5.0.0.26urlrand30922	100% Threat score	jizovudi.pdf
100% Threat score	0567471093200.exe	100% Threat score	_chrome.exe
85% Threat score	Dividas .lnk	85% Threat score	divergencias .lnk
85% Threat score	AnyDesk.msi	80% Threat score	ConfigMgrTools.msi
79% Threat score	Payment Receipt 01.html	75% Threat score	setup.exe
71% Threat score	CSHFware.dll		

Source: Hybrid Analysis











Top malicious URL

100% Threat score	https://packinsider.com/Community/profile/hftz5wwm-zahra-yuliarti/	100% Threat score	https://emd.agency/nmt/s/dhkAJ2J7X.zip
100% Threat score	http://vitsuae.com/nmt/GO6/dph/zBB/v7hh3zu.zip	95% Threat score	http://42.239.224.198:36304/Mozi.m
94% Threat score	http://111.92.107.14:47686/Mozi.a	86% Threat score	https://urldefense.proofpoint.com/v2/url?u=https-3A-252FKwqiTCOQ16Q1JCi3MdelD7PEvAlqbsgzN18ksh5FBUKuj8szOj2jUGGn95SFOnwPgHhF0fFRRM6z-2D11IDRMzrfsjxSWopdUtSD59cAHGz6JR6mIkNmXGs2Dgx4P3yGGIL1hiIDZbjYJZGLUJZPwNTd0owPR2Woq2DZsfdbgyRymWkU00UJaAu0ki5Nac1nDIZ8P7wZLJh5FooINPWPSEX1LdMCiFY3wOKjVQHpnslA9-5FaUCj3D264&d=DwMCaQ&c=euGZstcaTDllvimEN8b7jXrvYhlF8H4EDpE_mRNviZPQEuSl_58Aflit4XedMIzC1s&
82% Threat score	https://global-data-intelligence-limited.psrv.overlead.net/api/monitor/click/jjthhnltd/aHR0cDovL3d3dy5pdGFseS5nbG9iYXxkYXRhYmFzZS5jb20v	79% Threat score	https://urldefense.com/v3/_http://account-nN5JwUAptcn14VrVlhQ2xs4QFZLMyX-TFeT
79% Threat score	https://urldefense.com/v3/_http://www.hpdocument.com/c157070f25a61592?l=34_%3B%21%21J8jBlT3-xA%21ltqUmHevU8Vr_OWwS07aWkKIBqhiW0kGoClFTHHRZSxjqM5MtBeSYrSQSfKHzwna4rQEhlp1niykCf2UC-U%24	74% Threat score	https://ashirvaadgrand.in/git/rh/Vz/9BHw7F
74% Threat score	http://ts.bt-coin.net/	74% Threat score	https://urldefense.com/v3/_http://www.hpdcxA%21LGrzjwoQjx0E9TNaOzGjQzHfdx2M

74% Threat score	https://urldefense.com/v3/_http://www.hpdocument.com/d12a88c48ddcf9c7?l=34_%3B%21%21J8jBl3-xA%21LHMEiUw5tQAKG96hQ4ihUMCmY8JedamWk9EvgLFA3uKQu3N6-JDnQnoiQ1Pr_Z_pXDGEk0wbo78Gdsh1sw%24	74% Threat score	https://www.yourgoodtracker.com/ar/26509
74% Threat score	https://urldefense.com/v3/_http://www.hpdocument.com/e6c7a92800d100fa?l=34_%3B%21%21J8jBl3-xA%21LHMEiUw5tQAKG96hQ4ihUMCmY8JedamWk9EvgLFA3uKQu3N6-JDnQnoiQ1Pr_Z_pXDGEk0wbo78Gdsh1sw%24	72% Threat score	https://urldefense.com/v3/_http://www.heti
72% Threat score	http://gsboverseas.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 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 Algeria
 #7 Viet Nam	 #8 Brazil
 #9 Pakistan	 #10 Japan


Source: [SpamHaus](#)

Top phishing countries

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

Source: [Have I been pwned?](#)

Have I been pwned



Royal Enfield (royalenfield.com)
In January 2020, motorcycle maker **Royal Enfield** left a database publicly exposed that resulted in the inadvertent publication of over 400k customers. The impacted data included email and physical addresses, names, motorcycle information, social media profiles, passwords, and other personal information. The data was provided to HIBP by a source who requested it be attributed to "white_peacock@riseup.net".




Count: 420873

Created: 2019-01-01

Updated: 2022-03-31




Source: [Imperva DDOS Map](#)

Top DDOS attackers

	United States (27%)
	Germany (15%)
	Russia (12%)

Source: [Imperva DDOS Map](#)

Top DDOS country targets

	Russia (46%)
	Ukraine (18%)
	United States (17%)

Source: [Imperva DDOS Map](#)

Top DDOS techniques

65%	DDoS
24%	Automated Threat
11%	OWASP

Source: [Imperva DDOS Map](#)

Top DDOS industry targets

52%	Financial Services
25%	Business
6%	Computing & IT