



Your Security Rabbits report for March 08, 2022

Source: [Ransom Watch](#)

Ransomware attacks

alphv	Target: Carpenter & Zuckerman cz . law(2022-03-08)	snatch	Target: Warren Resources(2022-03-08)
snatch	Target: Xtera(2022-03-08)	everest	Target: BEAUTYWEST, INC . (2022-03-07)
conti	Target: EUROPA GROUP(2022-03-07)	conti	Target: Fuchs North America(2022-03-07)
conti	Target: Fujioka Eletro Imagem SA(2022-03-07)	everest	Target: Gershon Biegeleisen & Co(2022-03-07)
everest	Target: IDFC FIRST Bank(2022-03-07)	blackbyte	Target: INVIMA(2022-03-07)
lockbit2	Target: jrlichard-paysag . . . (2022-03-07)	everest	Target: Ledcor(2022-03-07)
conti	Target: Loepthien Maeder Treuhand AG(2022-03-07)	lockbit2	Target: stanthonys . slou . . . (2022-03-07)
everest	Target: Turner Construction Company(2022-03-07)		

Hot topics

Nothing today

News



25,000 Russian-linked accounts blocked by Coinbase

Coinbase has announced its full support of Russian sanctions, revealing the extent to which it has worked with governments. The organisation has also revealed that they have blocked 25,000 accounts linked to Russians suspected of illicit activity. "Many of which we have identified through our own proactive investigations," the company said. "Once we identified these [...]" The post 25,000 Russian-linked accounts blocked by Coinbase appeared first on IT Security Guru.



8X Increase in Russian-Based Phishing

Avanan analyzed more than two million customer email inboxes since February 16. On the 27th, the attacks increased by eight times as compared to the baseline volume.



Adafruit suffers GitHub data breach - don't let this happen to you

Training data stashed in GitHub by mistake... unfortunately, it was *real* data



Anonymous hacked Russian TV and streaming services with Ukraine footage

According to Anonymous, three Russian-state TV channels, Russia 24, Moscow 24, and Channel One and two Netflix-like Russian streaming services, Ivi and Wink, were targeted in the attack.



Cloudflare not fully backing out of Russia, company says, as tech firms are forced to weigh in

Cloudflare, a major web infrastructure firm that keeps websites online by protecting them from distributed denial-of-service attacks, said Monday that it will continue to provide some services within Russia despite several calls to pull out, stating that "Russia needs more Internet access, not less." The statement is just the latest example of internet infrastructure firms having to explain how they are approaching business in Russia as that country's government continues its brutal assault on Ukraine, and the government of Ukraine seeks to isolate Russia from the internet by publicly calling out major tech and web firms with business interests there. In a statement, Cloudflare CEO Matthew [...]



Coinbase blocked 25,000 crypto addresses linked to Russian individuals and entities

Coinbase announced that it's blocking access to more than 25,000 blockchain addresses linked to Russian individuals and entities. The popular cryptocurrency exchange Coinbase announced today that it's blocking access to more than 25,000 blockchain addresses linked to Russian people and entities. Coinbase chief legal officer Paul Grewal explained that its company is complying with sanctions [...] The post Coinbase blocked 25,000 crypto addresses linked to Russian individuals and entities appeared first on Security Affairs.



Conti Ransomware Group Diaries, Part IV: Cryptocrime

Three stories here last week pored over several years' worth of internal chat records stolen from the Conti ransomware group, the most profitable ransomware gang in operation today. The candid messages revealed how Conti evaded law enforcement and intelligence agencies, what it was like on a typical day at the Conti office, and how Conti secured the digital weaponry used in their attacks. This final post on the Conti conversations explores different schemes that Conti pursued to invest in and steal cryptocurrencies.



Critical "Access:7" Supply Chain Vulnerabilities Impact ATMs, Medical and IoT Devices

As many as seven security vulnerabilities have been disclosed in PTC's Axeda software that could be weaponized to gain unauthorized access to medical and IoT devices. Collectively called "Access:7," the weaknesses - three of which are rated Critical in severity - potentially affect more than 150 device models spanning over 100 different manufacturers, posing a significant supply chain risk.



Critical Bugs in TerraMaster TOS Could Open NAS Devices to Remote Hacking

Researchers have disclosed details of critical security vulnerabilities in TerraMaster network-attached storage (TNAS) devices that could be chained to attain unauthenticated remote code execution with the highest privileges. The issues reside in TOS, an abbreviation for TerraMaster Operating System, and "can grant unauthenticated attackers access to the victim's box simply by knowing the IP



Critical Firefox Zero-Day Bugs Allow RCE, Sandbox Escape

Both vulnerabilities are use-after-free issues in Mozilla's popular web browser.



Cyber-readiness in the face of an escalated gray zone conflict

Organizations worldwide should remain on high alert for cyberattacks as the




Cyberattack hits PressReader

The worlds largest digital newspaper and magazine distributor has been hit with a cyberattack, leaving users without access to more than 7000 publications. PressReader is headquartered in Vancouver, Canada, but has


[WeLiveSecurity](#) risk of major cyber-spillover from the crisis in Ukraine continues to loom large The post Cyber-readiness in the face of an escalated gray zone conflict appeared first on WeLiveSecurity


offices in both Dublin, Ireland and Manila, Philippines. The organisation began experiencing network outages on Thursday, affecting its Branded Editions website and apps, alongside [...] The post Cyberattack hits PressReader appeared first on IT Security Guru.

 **Dirty Pipe Linux flaw allows gaining root privileges on major distros**
Dirty Pipe is a Linux vulnerability, tracked as CVE-2022-0847, that can allow local users to gain root privileges on all major distros. Security expert Max Kellermann discovered a Linux flaw, dubbed Dirty Pipe and tracked as CVE-2022-0847, that can allow local users to gain root privileges on all major distros. The vulnerability affects Linux Kernel [...] The post Dirty Pipe Linux flaw allows gaining root privileges on major distros appeared first on Security Affairs.

CYWARE
SOCIAL
Cyware
News -
Latest Cyber
News

Fake Purchase Order Used to Deliver Agent Tesla
FortiGuard Labs recently came across an interesting phishing e-mail masquerading as a purchase order addressed to a Ukrainian manufacturing organization that deals with raw materials and chemicals.

 **FBI** Warns of the Impersonation of Law Enforcement and Government Officials
IC3.gov
News

 **Sophos**
Naked
Security

Firefox patches two actively exploited 0-day holes: update now!
Firefox just published a double-zero-day patch - "remote code execution" combined with "sandbox escape". Update now!

cyberscoop Global news app PressReader says it's back up after cyberattack

Digital media company PressReader was hit with a cyberattack late last week, the company confirmed Monday on Twitter, but its operations are now fully up and running -- though some content published during the delay in operations is still being uploaded. The company said it did not see any evidence that customer data was compromised in the Thursday attack. The attack came just days after the site pulled Russian publications. There is no evidence the two events are related. PressReader is a subscription app that works with hotels, airlines and public institutions like libraries to automatically grant guests access to a library of more than 7,000 publications as soon as they connect to the com[...]

CYWARE SOCIAL

Cyware
News -
Latest Cyber
News


How the tech community has rallied to Ukraine's cyber-defense

Responding to cyberattacks and building national cyber resilience has never been - and will never be - the sole responsibility of governments. It requires a whole-of-society approach grounded in international cooperation efforts.

CYWARE
SOCIAL
Cyware
News -
Latest Cyber
News

Japanese beauty retailer Acro blames third-party hack for breach of 100k payment cards

In a data breach notice, Acro revealed that customers of two of its beauty product websites were impacted as the result of the exploitation of a vulnerability in a third-party payment processing vendor.

 **KnowBe4 tackles Security Culture with new Maturity Model**

With 85% of data breaches caused by social engineering or human error, creating a company-wide security culture has risen up the agenda for many organisations. However, the phrase can be problematic in itself - as definitions vary, with some even equating it to security awareness training. KnowBe4 says it wants to change this and recognise [...] The post KnowBe4 tackles Security Culture with new Maturity Model appeared first on IT Security Guru.

Log4Shell Exploit Channelized to Launch DDoS and Cryptomining Attacks
According to a report by Barracuda, the volume of attacks attempting to exploit the Log4Shell vulnerability remained relatively constant over the past two months. Mirai and its other versions appeared in most of the attacks that made use of the Log4Shell exploit.


The Hacker News

Microsoft Azure 'AutoWarp' Bug Could Have Let Attackers Access Customers' Accounts

Details have been disclosed about a now-addressed critical vulnerability in Microsoft's Azure Automation service that could have permitted unauthorized access to other Azure customer accounts and take over control. "This attack could mean full control over resources and data belonging to the targeted account, depending on the permissions assigned by the customer," Orca Security researcher Yanir

CYWARE SOCIAL
Cyware
News -
Latest Cyber
News

Microsoft fixes critical Azure bug that exposed customer data
Microsoft has addressed a vulnerability in the Azure Automation service that could have allowed attackers to take complete control over the data of other Azure customers.



CYWARE

SOCIAL

Cyware

News -

Latest Cyber

News

MS Office Files Involved Again in Recent Emotet Trojan Campaign - Part I

Fortinet captured over 500 Excel files that were involved in a campaign to deliver the Emotet Trojan. The malicious macro downloads Emotet via two extracted files, "uidpjewl.bat" and "tjspowj.vbs".

Threatpost [Novel Attack Turns Amazon Devices Against Themselves](#)
Researchers have discovered how to remotely manipulate the Amazon Echo through its own speakers.

NVIDIA's Stolen Code-Signing Certs Used to Sign Malware
NVIDIA certificates are being used to sign malware, enabling malicious programs to pose as legitimate and slide past security safeguards on Windows machines.

cyberscoop
CyberScoop

Ransomware gang Conti has already bounced back from damage caused by chat leaks, experts say

A Twitter account known as ContiLeaks debuted to much fanfare in late February, with people around the globe watching as tens of thousands of leaked chats between members of the Russia-based ransomware gang Conti hit the web. In the days after the leaks, many celebrated what they thought would be a devastating blow to Conti, which a Ukrainian security researcher had apparently punished by leaking the internal chats because the gang threatened to "strike back" at any entities that organized "any war activities against Russia." But ten days after the leaks began, Conti appears to be thriving. Experts say the notorious ransomware gang has pivoted all too easily, replacing much of the infrastruc[...]

CYWARE
SOCIAL
Cyware
News -
Latest Cyber
News

[Researchers find new way to neutralize side-channel memory attacks](#)
The new solution is to shape memory requests by running them through a request shaper, called DAGuise, that uses a graph structure to process requests and send them to the memory controller on a fixed schedule.

Researchers Warn of Linux Kernel 'Dirty Pipe' Arbitrary File Overwrite Vulnerability

Linux distributions are in the process of issuing patches to address a newly disclosed security vulnerability in the kernel that could allow an attacker to overwrite arbitrary data into any read-only files and allow for a complete takeover of affected systems. Dubbed "Dirty Pipe" (CVE-2022-0847, CVSS score: 7.8) by IONOS software developer Max Kellermann, the flaw "leads to privilege escalation"

Samsung Confirms Lapsus\$ Ransomware Hit, Source Code Leak
The move comes just a week after GPU-maker NVIDIA was hit by Lapsus\$ and every employee credential was leaked.







Samsung Source Codes Stolen

Threat actors have breached the South Korean tech giant Samsung Electronics and stolen several source codes. The source codes in question are instrumental in the operation of the organisation's Galaxy devices. In a statement to SamMobile on Monday, the company revealed that it had strengthened its security measures after identifying a breach "relating to certain [...] The post Samsung Source Codes Stolen appeared first on IT Security Guru.



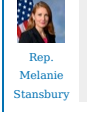





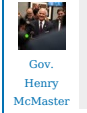

SharkBot, the new generation banking Trojan distributed via Play Store
SharkBot banking malware was able to evade Google Play Store security checks masqueraded as an antivirus app. SharkBot is a banking trojan that has been active since October 2021, it allows to steal banking account credentials and bypass multi-factor authentication mechanisms. The malware was spotted at the end of October by researchers from cyber security firms [...] The post SharkBot, the new generation banking Trojan distributed via Play Store appeared first on Security Affairs.

The Continuing Threat of Unpatched Security Vulnerabilities
Unpatched software is a computer code containing known security weaknesses. Unpatched vulnerabilities refer to weaknesses that allow attackers to leverage a known security bug that has not been patched by running malicious code. Software vendors write additions to the codes, known as "patches," when they come to know about these application vulnerabilities.

Ukraine will join NATO cyber hub
Ukraine is set to join the NATO cyber-defence centre following a vote confirming its admission. The move is expected to anger Russia and bring Ukraine closer to NATO. The Cooperative Cyber Defence Centre of Excellence (CCDCOE) announced that Ukraine and several other non-NATO countries will become a "contributing participant". "Capability and knowledge comes from experience. [...] The first Ukraine will join NATO cyber hub appeared

	to secure these weaknesses. Adversaries		first on IT Security Guru.
	Ukrainian CERT Warns Citizens of Phishing Attacks Using Compromised Accounts Ukraine's Computer Emergency Response Team (CERT-UA) warned of new phishing attacks aimed at its citizens by leveraging compromised email accounts belonging to three different Indian entities with the goal of compromising their inboxes and stealing sensitive information. The agency cautioned that the emails arrive with the subject line "Uvaga" (meaning "Attention") and claim to be from a		Ukrainian WordPress Sites Witness Massive Attack Volumes Wordfence recorded a whopping 144,000 attacks on February 25, 2022, and a total of 209,624 attacks between February 25 and 27. Most of the attacks were focused on a subset of 376 academic websites.
	Understanding How Hackers Recon Cyber-attacks keep increasing and evolving but, regardless of the degree of complexity used by hackers to gain access, get a foothold, cloak their malware, execute their payload or exfiltrate data, their attack will begin with reconnaissance. They will do their utmost to uncover exposed assets and probe their target's attack surface for gaps that can be used as entry points. So, the first line		War in Ukraine highlights vulnerability of critical energy infrastructure DW 07.03.2022 As the Russian army pushes deeper into Ukraine and hackers take down government websites in waves of cyber attacks, the security of Ukraine's power sector has been thrown into question.
	What Russia's Ongoing Cyberattacks in Ukraine Suggest About the Future of Cyber Warfare While some attacks, such as those against infrastructure, are nearly impossible for companies to prepare for, there are steps that they should take as a matter of course.		Why the World Needs a Global Collective Cyber Defense As cyberattacks grow in scale and sophistication, private and public sector entities are recognizing the need for a system to proactively share threat intelligence information: a global collective defense.

Twitter

	While a growing number of U.S. companies are breaking business ties with Russia, three major cybersecurity companies are volunteering to protect U.S. utilities and hospitals free amid concerns about retaliatory hacks.		The investment to expand @DakotaState's cyberresearch program passed the House and is on its way to my desk! This project will help bring the next big industry to our state. Now more than ever, South Dakota needs to lead the way in advancing our nation's cybersecurity.
	After a whirlwind weekend back in New Mexicoheaded back to DC to get the federal budget across the finish line, address aid to Ukraine, and a number of homeland and cyber security bills. Ready to get this budget done!		Russia poses a serious threat to not only Ukraine but to the U.S. and our partners. Im continuing to lead the charge as @hsgac Chair to strengthen our cyber defenses. This past week the Senate passed my historic bipartisan cybersecurity bill.
	The SECs Investor Advisory Committee is going to have a meeting on March 10 to discuss artificial intelligence and cybersecurity. The meeting will be webcast. For more:		Samsung Electronics suffers a cybersecurity breach that exposed internal company data, including source code for the operation of its Galaxy smartphones
	Google in talks to buy cybersecurity firm Mandiant - The Information		Cybersecurity isnt just about protecting our data its also about protecting our democracy.
	Joined the South Coast Cyber Summit today in Beaufort to discuss the latest cyber initiatives in South Carolina. To stay ahead we must commit to investing in our cybersecurity workforce and bringing cyber-focused companies to South Carolina.		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-2021-36809	A local attacker can overwrite arbitrary files on the system with VPN client logs using administrator privileges, potentially resulting in a	CVE-2021-43944	This issue exists to document that a security improvement in the way that Jira Server and Data Center use templates has been implemented. Affected versions of Atlassian Jira Server and Data Center allowed remote attackers with system administrator
-----------------------	---	-----------------------	--

denial of service and data loss, in all versions of **Sophos SSL VPN** client.

UNRATED

Vector: unown Created: 2022-03-08 Updated: 2022-03-08

permissions to execute arbitrary code via Template Injection leading to Remote Code Execution (RCE) in the Email Templates feature. The affected versions are before version 8.13.15, and from version 8.14.0 before 8.20.3.

UNRATED

Vector: unown Created: 2022-03-08 Updated: 2022-03-08

Source: Hybrid Analysis

Top malicious files

100% Threat score	PowerBISmartPivot-x86x64-2 (.) 5 (.) 2106 (.) 164 (.) exe	100% Threat score	Server (.) exe
100% Threat score	7a400376da1e40241ae2d8c9a9e42403b7c080b3719aaf72230f9fa96ca67fd3	100% Threat score	65675039 (.) exe
100% Threat score	Notify for Amazfit Zepp_v14 (.) 3 (.) 4_apkpure (.) com (.) apk	100% Threat score	mypersonnel (.) xls
100% Threat score	55937445 (.) exe	100% Threat score	Server (.) exe
100% Threat score	server (.) exe	100% Threat score	33492462 (.) exe
100% Threat score	the-unliving-v-d-nlAua5LQrr (.) exe	100% Threat score	48677247 (.) exe
100% Threat score	51196179 (.) exe	100% Threat score	64162804 (.) exe
100% Threat score	Firefox Installer (.) exe	100% Threat score	64097802 (.) exe
100% Threat score	5e_mal5mts_baseben (.) exe	100% Threat score	41_mal5mts_baseben (.) exe
100% Threat score	55d97cc5ecb0d0d679a1bd4610f76dc105955a0a3c5a10835d4c882e5453d8c1	100% Threat score	5e_malbenbase_nosleep (.) exe
100% Threat score	41_malbenbase_nosleep (.) exe	100% Threat score	5e_def_nosleep_system (.) exe
100% Threat score	defense_nosleep_system (.) exe	100% Threat score	67603114 (.) exe
100% Threat score	Server (.) exe	85% Threat score	KeePassXC-2 (.) 6 (.) 6-Win32 (.) msi
80% Threat score	623-diw_tgh_221 (.) exe		

Source: Hybrid Analysis






Top malicious URL

94% Threat score	http://45 (.) 23 (.) 22 (.) 186:55370/bin (.) sh	94% Threat score	http://123 (.) 129 (.) 135 (.) 85:53634/bin (.) sh
93% Threat score	http://125 (.) 46 (.) 183 (.) 186:56787/bin (.) sh	93% Threat score	http://123 (.) 10 (.) 22 (.) 111:51907/i
93% Threat score	http://171 (.) 38 (.) 150 (.) 232:54007/Mozi (.) m	82% Threat score	http://rebrand (.) ly/ac-antizapret-pac
77% Threat score	http://www (.) dupont (.) es/cookie	74% Threat score	http://www (.) panambicollection (.) com:443/
72% Threat score	http://www (.) dupont (.) ru/	72% Threat score	http://www (.) dupont (.) es/privacy (.) html?elqTrackId=edd1d5343aaa4918aba907457ce72c78&elq=3ac1a8d86351406bae2c5daf86d4366f&elqaid=802&elqat=1&elqCampaignId=647
72% Threat score	http://airwaterice (.) 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 Russia		#4 Netherlands
	#5 Vietnam		#6 Japan
	#7 Singapore		#8 Iran
	#9 India		#10 Hong Kong

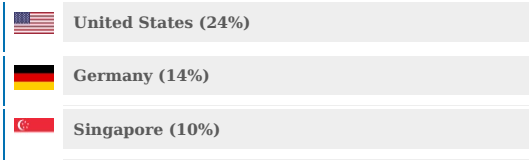
Source: [Have I been pwned?](#)

Have I been pwnd

Nothing today

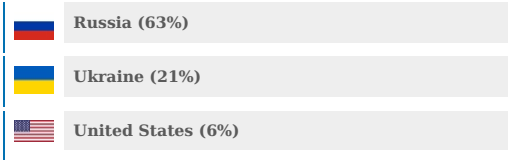
Source: [Imperva DDOS Map](#)

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

