



Your Security Rabbits report for March 06, 2022

Source: *Ransom Watch*

Ransomware attacks

conti Target: Cummins-Wagner(2022-03-06) lockbit2 Target: abcp . or(2022-03-05)

Hot topics

Nothing today

News



Security
Affairs

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. Anonymous announced to have hacked more than 2,500 websites linked to the Russian and Belarusian governments, state-owned media outlets spreading disinformation, Russian private organizations, banks, hospitals, airports. The attacks were conducted as part of the #OpRussia launched [...] The post Anonymous #OpRussia Thousands of sites hacked, data leaks and more appeared first on Security Affairs.



Cyware
News -
Latest Cyber
News

Conti's Source Code Now Publicly Available

The Russia-Ukraine cyberwar continues to evolve, with a researcher leaking a big chunk of internal messages and source code associated with the Conti ransomware group. The leak includes how the threat actors are organized like a business, how they avoid law enforcement, and much more. Meanwhile, some experts fear that this code may now be leveraged by other attackers to develop new malware variants.



Naked
Security

Firefox patches two in-the-wild exploits - update now!

Firefox just published a double-zero-day patch - "remote code execution" combined with "sandbox escape". Update now!



Cyware
News -
Latest Cyber
News

New Side-Channel Attack on Homomorphic Encryption

A group of researchers has demonstrated the first side-channel attack on homomorphic encryption that can let anyone read the data in encrypted mode. The attack exploiting the flaw is named RevEAL and exploits the Gaussian sampling that exists in Microsoft SEAL's encryption phase. This manifests that even next-generation encryption technologies are susceptible to cyberattacks.



Security
Affairs

Charities and NGOs providing support in Ukraine hit by malware

Malware based attacks are targeting charities and non-governmental organizations (NGOs) providing support in Ukraine Charities and non-governmental organizations (NGOs) that in these weeks are providing support in Ukraine are targeted by malware attacks aiming to disrupt their operations. The news was reported by Amazon that associates the attacks with state-sponsored hackers and confirmed that it [...] The post Charities and NGOs providing support in Ukraine hit by malware appeared first on Security Affairs.



Cyware
News -
Latest Cyber
News

European Officials Aiding the Ukrainian Refugee Movement are Under Attack

Security researchers found a campaign, dubbed Asylum Ambuscade, targeting European government personnel helping Ukrainian refugees with attachments containing the SunSeed malware. The attachment uses the Emergency Meeting of the NATO Security Council as a lure. To stay protected, victims are urged to follow recommendations provided by security agencies and organizations that are actively tracking these cyber attacks.



Security
Affairs

Lapsus\$ gang leaks data allegedly stolen from Samsung Electronics

The Lapsus\$ ransomware group claimed to have hacked Samsung Electronics and leaked alleged stolen confidential data. The Lapsus\$ ransomware gang claims to have stolen a huge trove of sensitive data from Samsung Electronics and leaked 190GB of alleged Samsung data as proof of the hack. The gang announced the availability of the sample data on [...] The post Lapsus\$ gang leaks data allegedly stolen from Samsung Electronics appeared first on Security Affairs.



Cyware
News -
Latest Cyber
News

RuRAT Campaign Uses Innovative Lure to Target Potential Victims

BleepingComputer spotted a spear-phishing campaign venture capital firm to infect victims with RuRAT malware and gain initial access to the targeted systems. The phishing email originates from an IP address belonging to a U.K virtual server company. Experts recommend always staying alert whenever an email appears suspicious.

Twitter

WSJ

The Wall
Street
Journal

Hundreds of thousands of Ukrainian technology workers have taken part in cyberattacks against Russias government, media and financial institutions in recent days, a top Ukrainian cybersecurity official said Friday



Patricia
Arquette

Reminder- Trump's 'cyber security unit' plan with Putin | CNN Politics



NSA
Cyber

Thousands of cybersecurity students and network defenders have used #Ghidra to build and research current technologies since its release head over to to check it out.



Senator
Dick
Durbin

This is exactly why the Senate is working on bipartisan bills to strengthen our cybersecurity infrastructure. We must make sure we are prepared for increased Russian aggression, wherever it may appear.

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	<p>** 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.</p> <div>UNRATEDVector: unknownCreated: 2022-03-06Updated: 2022-03-06</div>	CVE-2022-26505	<p>A DNS rebinding issue in ReadyMedia (formerly MiniDLNA) before 1.3.1 allows a remote web server to exfiltrate media files.</p> <div>UNRATEDVector: unknownCreated: 2022-03-06Updated: 2022-03-06</div>
CVE-2021-46704	<p>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.</p> <div>UNRATEDVector: unknownCreated: 2022-03-06Updated: 2022-03-06</div>	CVE-2022-26496	<p>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.</p> <div>UNRATEDVector: unknownCreated: 2022-03-06Updated: 2022-03-06</div>
CVE-2022-26495	<p>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.</p> <div>UNRATEDVector: unknownCreated: 2022-03-06Updated: 2022-03-06</div>	CVE-2022-26487	<p>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).</p> <div>UNRATEDVector: unknownCreated: 2022-03-06Updated: 2022-03-06</div>
CVE-2022-0869	<p>Multiple Open Redirect in GitHub repository nitely/spirit prior to 0.12.3.</p> <div>UNRATEDVector: unknownCreated: 2022-03-06Updated: 2022-03-06</div>	CVE-2022-26490	<p>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.</p> <div>UNRATEDVector: unknownCreated: 2022-03-06Updated: 2022-03-06</div>

Source: Hybrid Analysis

Top malicious files

100% Threat score	invoice-02-01-2022 (.) xls	100% Threat score	eset_smart_security_premium_live_installer (.) exe
100% Threat score	WeMod-Setup (.) exe	100% Threat score	\$RVGFH60 (.) exe
100% Threat score	DeskGo_3_2_1445_127_lite (.) exe	100% Threat score	WinRAR-x64-Portable (.) exe
100% Threat score	36bd5616fec9430c14a3b7c80af13d7ed24cf506e4e0a20cd6fd3e7d99221f16 (.) msi	100% Threat score	c1a6a22617039f7b0c23f16261d1b0f3af0ff4c36a9855c2f29d14c12407282a (.) exe
100% Threat score	Setup Cracked (.) exe	100% Threat score	2570_1645889198_7539 (.) exe
100% Threat score	DDOS PANEL TROPICAL (.) exe	100% Threat score	2ben_mal_5e (.) exe
100% Threat score	FoxHack (.) exe	100% Threat score	2ben_mal_4 (.) exe
100% Threat score	Beast V2 (.) exe	100% Threat score	eset_internet_security_live_installer (2) (.) exe
100% Threat score	torbrowser-install-win64-11 (.) 5a4_en-US (.) exe	100% Threat score	nebula (.) exe
100% Threat score	AnyDesk (.) exe	96% Threat score	Master PDF Editor 5 (.) 8 (.) 03 x64 portable (TA-5 (.) 2 (.) 10) (.) exe

95% Threat score	anti-vm (.) exe
---------------------	-----------------

Source: Hybrid Analysis

Top malicious URL

100% Threat score	https://monzo-secure-cancel (.) com/	97% Threat score	http://115 (.) 59 (.) 201 (.) 63:54277/Mozi (.) m
97% Threat score	http://27 (.) 215 (.) 27 (.) 62:46412/i	97% Threat score	http://77 (.) 45 (.) 135 (.) 89:33538/Mozi (.) m
97% Threat score	http://222 (.) 137 (.) 149 (.) 225:44120/i	97% Threat score	http://115 (.) 55 (.) 168 (.) 85:37092/Mozi (.) m
96% Threat score	http://171 (.) 35 (.) 161 (.) 21:41166/i	96% Threat score	http://171 (.) 35 (.) 161 (.) 21:41166/bin (.) sh
95% Threat score	http://41 (.) 86 (.) 18 (.) 149:43226/Mozi (.) a	94% Threat score	http://116 (.) 212 (.) 132 (.) 188:48422/Mozi (.) m
93% Threat score	http://115 (.) 50 (.) 98 (.) 108:38022/i	93% Threat score	http://115 (.) 50 (.) 70 (.) 89:44235/Mozi (.) m
93% Threat score	http://113 (.) 116 (.) 194 (.) 88:58434/Mozi (.) m	93% Threat score	http://112 (.) 95 (.) 45 (.) 141:33533/Mozi (.) m
93% Threat score	http://113 (.) 87 (.) 97 (.) 68:57796/mozi (.) a	93% Threat score	http://182 (.) 119 (.) 248 (.) 231:43066/i
93% Threat score	http://222 (.) 93 (.) 244 (.) 179:40651/Mozi (.) m	93% Threat score	http://222 (.) 141 (.) 90 (.) 31:57541/Mozi (.) m
93% Threat score	http://114 (.) 226 (.) 220 (.) 97:56922/Mozi (.) m	93% Threat score	http://61 (.) 54 (.) 235 (.) 162:35615/mozi (.) m
93% Threat score	http://84 (.) 213 (.) 147 (.) 95:45979/Mozi (.) m	93% Threat score	http://115 (.) 58 (.) 130 (.) 51:42154/Mozi (.) m
93% Threat score	http://189 (.) 85 (.) 35 (.) 145:50088/Mozi (.) m	93% Threat score	http://189 (.) 85 (.) 35 (.) 55:51138/Mozi (.) a
93% Threat score	http://119 (.) 123 (.) 226 (.) 81:56713/Mozi (.) m	93% Threat score	http://115 (.) 56 (.) 141 (.) 82:33222/i
93% Threat score	http://59 (.) 94 (.) 135 (.) 31:36850/Mozi (.) m	93% Threat score	http://117 (.) 196 (.) 54 (.) 33:50435/bin (.) sh
93% Threat score	http://117 (.) 222 (.) 175 (.) 230:60697/Mozi (.) m	93% Threat score	http://27 (.) 41 (.) 90 (.) 220:41619/Mozi (.) m
93% Threat score	http://42 (.) 234 (.) 148 (.) 74:49698/bin (.) sh	93% Threat score	http://115 (.) 63 (.) 230 (.) 202:42460/i
93% Threat score	http://119 (.) 191 (.) 121 (.) 124:53498/Mozi (.) a	93% Threat score	http://59 (.) 94 (.) 129 (.) 177:47817/i
93% Threat score	http://115 (.) 55 (.) 146 (.) 117:48501/Mozi (.) m	88% Threat score	http://117 (.) 208 (.) 138 (.) 56:41916/i
88% Threat score	http://117 (.) 241 (.) 184 (.) 9:44303/i	88% Threat score	http://59 (.) 178 (.) 74 (.) 208:51127/Mozi (.) m
88% Threat score	http://27 (.) 45 (.) 11 (.) 180:60812/Mozi (.) a	88% Threat score	http://115 (.) 49 (.) 210 (.) 208:48447/Mozi (.) m
88% Threat score	http://59 (.) 99 (.) 134 (.) 223:35223/Mozi (.) m	88% Threat score	http://123 (.) 13 (.) 4 (.) 209:53688/i
88% Threat score	http://182 (.) 121 (.) 45 (.) 210:59416/Mozi (.) m	88% Threat score	http://59 (.) 99 (.) 206 (.) 79:45887/bin (.) sh
88% Threat score	http://59 (.) 99 (.) 202 (.) 192:58222/Mozi (.) m	88% Threat score	http://42 (.) 224 (.) 156 (.) 62:33712/Mozi (.) m
88% Threat score	http://42 (.) 235 (.) 181 (.) 196:45286/i	88% Threat score	http://117 (.) 241 (.) 185 (.) 136:45334/i
88% Threat score	http://117 (.) 193 (.) 122 (.) 185:42424/Mozi (.) m	88% Threat score	http://188 (.) 16 (.) 150 (.) 131:41752/Mozi (.) a
82% Threat score	http://inx (.) lvjFW0	77% Threat score	http://b-butter (.) com/
77% Threat score	http://twenty20 (.) com/	77% Threat score	http://ipower (.) sa/










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 hosts
 #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 Pakistan	 #10 Iran (Islamic Republic of)

Source: SpamHaus

Top phishing countries

 #1 United States	 #2 Brazil



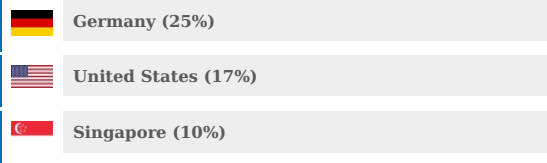
Source: [Have I been pwnd?](#)

Have I been pwnd

Nothing today

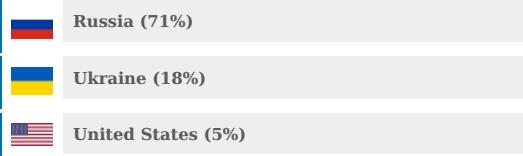
Source: [Imperva DDOS Map](#)

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

