Security Rabbits

Your Security Rabbits report for March 15, 2022

Source: Ransom Watch

Ransomware attacks

lockbit2	Target: f(2022-03-15)
alphv	Target: Monteleone & McCrory LLP(2022-03-14)
lockbit2	Target: snteseccion30sa . . (2022-03-14)
ransomexx	Target: Viva Air(2022-03-14)
alphv	Target: inibsa . net(2022-03-14)
ragnarlocker	Target: Smith Transport Full Leak(2022-03-14)
everest	Target: UK GOV(2022-03-14)

Hot topics

Nothing today

News

The Hacker News

'Dirty Pipe' Linux Flaw Affects a Wide Range of QNAP NAS Devices
Network-attached storage (NAS) appliance maker QNAP on Monday warned of a recently disclosed Linux vulnerability affecting its devices that could be abused to elevate privileges and gain control of affected systems. "A local privilege escalation vulnerability, also known as 'Dirty Pipe,' has been reported to affect the Linux kernel on QNAP NAS running QTS 5.0.x and QuTS hero h5.0.x," the company

Security Affairs

A massive DDoS attack hit Israel, government sites went offline
Many Israel government websites were offline after a cyberattack, defense sources claim that this is the largest-ever attack that hit the country. Israeli media reported that a massive DDoS attack has taken down many Israel government websites. The Jerusalem Post attributed the attack to an allegedly Iran-linked threat actor that claimed responsibility for the attack. Multiple […] The post A massive DDoS attack hit Israel, government sites went offline appeared first on Security Affairs.

Cyware News - Latest Cyber News

Android Malware 'Escobar' Steals Users' Google Authenticator MFA codes
The main goal of the trojan is to steal enough information to allow the threat actors to take over victims' bank accounts, siphon available balances, and perform unauthorized transactions.

ZDNet | security RSS

Automotive giant Denso confirms hack, Pandora ransomware group takes credit
Denso supplies Toyota, General Motors, and Honda, to name but a few.

WeLiveSecurity

CaddyWiper: New wiper malware discovered in Ukraine
This is the third time in as many weeks that ESET researchers have spotted previously unknown data wiping malware taking aim at Ukrainian organizations The post CaddyWiper: New

WeLiveSecurity

A first look at threat intelligence and threat hunting tools
An overview of some of the most popular open-source tools for threat intelligence and threat hunting The post A first look at threat intelligence and threat hunting tools appeared first on WeLiveSecurity

Cyware News - Latest Cyber News

AMD Updates Spectre Mitigations Following Intel Research
AMD last week informed customers that it has updated mitigations for a variant of the Spectre side-channel attack. The update comes in response to research conducted by Intel.

Security Affairs

Anonymous claims to have hacked German subsidiary of Russian energy giant Rosneft
Anonymous claims to have hacked the systems of the German subsidiary of Russian energy giant Rosneft and stole 20TB of data. The Anonymous hacker collective claimed to have hacked the German branch of the Russian energy giant Rosneft. In hacktivists announced to have stolen 20 terabytes of data from the company. According to the German […] The post Anonymous claims to have hacked German subsidiary of Russian energy giant Rosneft appeared first on Security Affairs.

Security Affairs

CaddyWiper, a new data wiper hits Ukraine
Experts discovered a new wiper, tracked as CaddyWiper, that was employed in attacks targeting Ukrainian organizations. Experts at ESET Research Labs discovered a new data wiper, dubbed CaddyWiper, that was employed in attacks targeting Ukrainian organizations. The security firm has announced the discovery of the malware with a series of tweets: "This new malware erases […] The post CaddyWiper, a new data wiper hits Ukraine appeared first on Security Affairs.

The Hacker News

CaddyWiper: Yet Another Data Wiping Malware Targeting Ukrainian Networks
Two weeks after details emerged about a second data wiper strain delivered in attacks against Ukraine, yet another destructive malware has been detected amid Russia's continuing military invasion of the country. Slovak cybersecurity company

wiper malware discovered in Ukraine appeared first on WeLiveSecurity

Cyware News - Latest Cyber News

China-based TA416 Ramp-Up Espionage Against European Governments

A Chinese-backed threat group has been observed targeting European diplomatic entities indulging in refugee and migrant services. The group takes advantage of web bugs to profile its targets. An analysis revealed that the threat group is using an updated version of PlugX malware. To stay protected, organizations should stay alert and check their security solutions against such crimes.

Naked Security

Cryptocoin ATMs ruled illegal - "Shut down at once", says regulator

If you live in the UK and hadn't yet heard of cryptocoin ATMs... it's too late now!

IT Security Guru

Cybersecurity tops agenda in Asean boardrooms

Businesses in Asean have placed cybersecurity squarely on the agenda, with business leaders discussing plans to plug existing gaps and adopt next-generation capabilities. This focus has been prompted by 94% of organisations in the region reporting a climb in cyberattacks last year, with 24% seeing at least 50% increase in disruptive attacks. 92% of Asean [...] The post Cybersecurity tops agenda in Asean boardrooms appeared first on IT Security Guru.

The Hacker News

Gaming Company Ubisoft Confirms It was Hacked, Resets Staff Passwords

French video game company Ubisoft on Friday confirmed it was a victim of a "cyber security incident," causing temporary disruptions to its games, systems, and services. The Montreuil-headquartered firm said that an investigation into the breach was underway and that it has initiated a company-wide password reset as a precautionary measure. "Also, we can confirm that all our games and services

Cyware News - Latest Cyber News

Hackers Target German Branch of Russian Oil Giant Rosneft

The German subsidiary of Russian energy giant Rosneft has been hit by a cyberattack, the Federal Office for Information Security (BSI) said on Monday, with hacker group Anonymous claiming responsibility.

Cyware News - Latest Cyber News

Hit by ransomware or paid a ransom? Now some companies will have to tell the government

Owners and operators of US critical infrastructure will now in some cases be legally required to report cyberattacks and ransomware payments to the Cybersecurity and Infrastructure Security Agency (CISA).

The Hacker News

Massive DDoS Attack Knocked Israeli Government Websites Offline

A number of websites belonging to the Israeli government were felled in a distributed denial-of-service (DDoS) attack on Monday, rendering the portals inaccessible for a short period of time. "In the past few hours, a DDoS attack against a communications provider was identified," the Israel National Cyber Directorate (INCD) said in a tweet. "As a result, access to several websites, among them

Cyware News - Latest Cyber News

Pre-war spike in phishing attacks targeting infrastructure in Ukraine

It is evident that Ukrainian companies have not been spared when it comes to phishing attacks, and attackers are targeting local communication infrastructures, network providers, and other services.

IT Security Guru

Ransomware groups target "enemies of Russia"

A new report Accenture suggests that cyber-criminals have split into pro-Ukraine and pro-Russia factions, with the latter focusing on western critical national infrastructure (CNI). The consulting giant's Accenture Cyber Threat Intelligence (ACTI) arm has warned that the recent ideological split could mean increased risk for Western organizations, as pro-Kremlin groups morph into quasi-activists. Government, media, [...] The post Ransomware groups target "enemies of Russia" appeared first

ESET dubbed the third wiper "CaddyWiper," which it said it first observed on March 14 around 9:38 a.m. UTC. Metadata associated with the executable ("

Cyware News - Latest Cyber News

Critical Vulnerabilities Patched in Veeam Data Backup Solution

The flaws were identified in the Veeam Distribution Service, which by default listens to TCP port 9380 and allows even unauthenticated users to access internal API functions.

Threatpost

Cybercrooks' Political In-Fighting Threatens the West

They're choosing sides in the Russia-Ukraine war, beckoning previously shunned ransomware groups and thereby reinvigorating those groups' once-diminished power.

CyberScoop

Denial-of-service attack knocked Israeli government sites offline

Sites were restored Monday afternoon, the Israeli government said. The post Denial-of-service attack knocked Israeli government sites offline appeared first on CyberScoop.

Cyware News - Latest Cyber News

Hacker Planned Terabytes of DDoS Traffic Using a Single Packet

Researchers from a number of organizations confirmed that attackers have been exploiting Mitel enterprise collaboration products to amplify DDoS attacks by 4 billion times from a single packet. The exploitation of the flaw began on February 18 and mainly reflected onto ports 80 and 443. Those on the receiving end of the attack are recommended to use DDoS defenses as well.

Naked Security

Happy #PiDay - even if you aren't in North America!

There is a cybersecurity angle here - but you will need to read right to the end to find it :-)

IT Security Guru

Malware hidden in fake Valorant aim-bot

Security analysts from Korea have detected a malware distribution campaign using Valorant cheat lures on YouTube in order to trick players into downloading RedLine, a powerful information stealer. This kind of lure is relatively common as threat actors can easily avoid YouTube's new content submission reviews, or simply create new accounts when old ones are [...] The post Malware hidden in fake Valorant aim-bot appeared first on IT Security Guru.

The Hacker News

New Linux Bug in Netfilter Firewall Module Lets Attackers Gain Root Access

A newly disclosed security flaw in the Linux kernel could be leveraged by a local adversary to gain elevated privileges on vulnerable systems to execute arbitrary code, escape containers, or induce a kernel panic. Tracked as CVE-2022-25636 (CVSS score: 7.8), the vulnerability impacts Linux kernel versions 5.4 through 5.6.10 and is a result of a heap out-of-bounds write in the netfilter

Cyware News - Latest Cyber News

Prophet Spider Exploits Citrix Flaw to Deliver Webshell

Crowdstrike reported a threat group named Prophet Spider that is abusing an RCE vulnerability in Citrix ShareFile to compromise Microsoft's Internet Information Services webserver. The relative path-traversal vulnerability (CVE-2021-22941) was disclosed in ShareFile Zones Storage Controller. Organizations are advised to always follow a proper patch management program.

IT Security Guru

RiskOps platform Feedzai grows +40% year-over-year

Today, RiskOps platform Feedzai announced that it ended its fiscal year with +40% year-over-year growth in exit annual recurring revenue (ARR). With a total of 24 tier one new logos across the globe, the company also recorded no churn on core customers. Additionally, extended contracts were signed with key clients like Citi Bank in North America, Lloyds [...] The post RiskOps platform Feedzai grows +40% year-over-year appeared first on IT Security Guru.

on IT Security Guru.

The Hacker News

[Russian Ransomware Gang Retool Custom Hacking Tools of Other APT Groups]

A Russian-speaking ransomware outfit likely targeted an unnamed entity in the gambling and gaming sector in Europe and Central America by repurposing custom tools developed by other APT groups like Iran's MuddyWater, new research has found. The unusual attack chain involved the abuse of stolen credentials to gain unauthorized access to the victim network, ultimately leading to the deployment of

CyberScoop

[Spy agencies' leaks of Russian plans point to the future of information warfare, Sen. Warner says]

Sen. Mark Warner discussed American intelligence successes and information warfare at a Washington think tank Monday. The post Spy agencies' leaks of Russian plans point to the future of information warfare, Sen. Warner says appeared first on CyberScoop.

Cyware News - Latest Cyber News

[The importance of building in security during software development]

Checkmarx released the UK findings of its report which found that 45% of organizations have suffered at least two security breaches as a direct result of a vulnerable application.

Security Affairs

[Ukraine is using Clearview AI's facial recognition during the conflict]

Ukraine's defense ministry began using Clearview AI's facial recognition technology to uncover Russian assailants, combat misinformation and identify the dead. Ukraine's defense ministry announced it will use the AI's facial recognition technology offered by Clearview. Clearview's chief executive Hoan Ton-That confirmed the news to Reuters, the technology will allow the Ukrainian military to uncover Russian [...] The post Ukraine is using Clearview AI's facial recognition during the conflict appeared first on Security Affairs.

IT Security Guru

[Ukrainian machines hit with another Malware variant]

Security researchers have discovered the fourth destructive malware variant targeting Ukrainian machines so far this year. ESET claimed to have made the find yesterday, noting that the "CaddyWiper" malware was seen on a few dozen systems in a "limited number" of organizations. The malware erases user data and partitions information from attached drives. It also [...] The post Ukrainian machines hit with another Malware variant appeared first on IT Security Guru.

Cyware News - Latest Cyber News

[South Denver Cardiology Associates Discloses Unauthorized Access to its Databases]

SDCA admitted that an unnamed attacker broke into its systems and had access to confidential databases for three days between January 2, 2022, and January 5, 2022, before the breach was detected and thwarted.

Threatpost

[Staff Think Conti Group Is a Legit Employer - Podcast]

The ransomware group's benefits - bonuses, employee of the month, performance reviews & top-notch training - might be better than yours, says BreachQuest's Marco Figueroa.

ZDNet | security RSS

[Ubisoft reveals 'security incident' forcing company-wide password refresh]

The gaming giant remains tight-lipped on the particulars of the assumed hack.

ZDNet | security RSS

[Ukraine reportedly adopts Clearview AI to track Russian invaders]

The facial recognition technology has not been made available to Russia.

The Hacker News

[Why Enterprise Threat Mitigation Requires Automated, Single-Purpose Tools]

As much as threat mitigation is to a degree a specialist task involving cybersecurity experts, the day to day of threat mitigation often still comes down to systems administrators. For these sysadmins it's not an easy task, however. In enterprise IT, sysadmins teams have a wide remit but limited resources. For systems administrators finding the time and resources to mitigate against a growing

Twitter

Rep. Val Demings

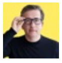
Last night we passed the federal budget to keep us SAFE. I voted to strengthen Americas military and provide strong resources for: - Securing our border - Homeland security grants that protect communities & houses of worship - Cybersecurity - Coast Guard and port security

Gary Gensler

Join us in now at our Investor Advisory Committee Meeting. Todays agenda includes a panel on artificial intelligence and robo-advising and a discussion on cybersecurity disclosures.

Dave Rubin

This man slept with a Chinese spy and is now giving cybersecurity tips. Please fact check me, @twitter[...]



Spiros Margaris

The best #Indian #conferences for #womenintech in 2022 #fintech #cybersecurity @Analyticsindiam

Source: NIST

NIST CVE: Critical

CVE-2021-33293

Panorama Tools **libpano13** v2.9.20 was discovered to contain an out-of-bounds read in the function panoParserFindOLine() in parser.c.

CRITICAL	Vector: network	Created: 2022-03-10	Updated: 2022-03-15

Source: NIST

NIST CVE: High

Nothing today

Source: NIST

NIST CVE: Medium

CVE-2021-3660

Cockpit (and its plugins) do not seem to **protect** itself against clickjacking. It is possible to render a page from a cockpit server via another website, inside an HTML entry. This may be used by a malicious website in clickjacking or similar attacks.

MEDIUM Vector: network Created: 2022-03-10 Updated: 2022-03-15

CVE-2021-34122

The function bitstr_tell at bitstr.c in **ffjpeg** commit 4ab404e has a NULL pointer dereference.

MEDIUM Vector: local Created: 2022-03-10 Updated: 2022-03-15

CVE-2021-35251

Sensitive information could be displayed when a detailed technical error message is posted. This information could disclose environmental details about the **Web Help Desk** installation.

MEDIUM Vector: network Created: 2022-03-10 Updated: 2022-03-15

Source: NIST

NIST CVE: Low

Nothing today

Source: NIST

NIST CVE: Unrated

CVE-2022-27193

CVRF-CSAF-Converter before 1.0.0-rc2 resolves XML External Entities (XXE). This leads to the inclusion of arbitrary (local) file content into the generated output document. An attacker can exploit this to disclose information from the system running the converter.

UNRATED Vector: unkown Created: 2022-03-15 Updated: 2022-03-15

CVE-2022-0945

Stored XSS viva axd and cshtml file upload in star7th/showdoc in **GitHub** repository star7th/showdoc prior to v2.10.4.

UNRATED Vector: unkown Created: 2022-03-15 Updated: 2022-03-15

CVE-2022-0950

Unrestricted Upload of File with Dangerous Type in **GitHub** repository star7th/showdoc prior to 2.10.4.

UNRATED Vector: unkown Created: 2022-03-15 Updated: 2022-03-15

CVE-2022-0951

File Upload Restriction Bypass leading to Stored XSS Vulnerability in **GitHub** repository star7th/showdoc prior to 2.10.4.

UNRATED Vector: unkown Created: 2022-03-15 Updated: 2022-03-15

CVE-2022-0944

Template injection in connection test endpoint leads to RCE in **GitHub** repository sqlpad/sqlpad prior to 6.10.1.

UNRATED Vector: unkown Created: 2022-03-15 Updated: 2022-03-15

Source: Hybrid Analysis

Top malicious files

100% Threat score	naver (.) apk
100% Threat score	attachments-9548 (.) xlsm
100% Threat score	m3bitlockerloader (.) exe
100% Threat score	DOC_1503 (.) xlsm
100% Threat score	CallApp Caller ID & Recording v1 (.) 932 Premium Mod Apk {CracksHash} (.) apk
92% Threat score	ytd (.) exe
86% Threat score	diamag2_setup (.) exe
75% Threat score	purchase Order (.) exe
100% Threat score	BOQ AND SPECIFICATIONS (.) exe
100% Threat score	Electronic form (.) xlsm
100% Threat score	H4CK3D (.) exe
100% Threat score	XEKM_171 (.) xlsm
99% Threat score	433 (.) xlsx
87% Threat score	Telegram (.) exe
77% Threat score	ACWeigh Install (.) msi
75% Threat score	M332x_382x_402x_Series_WIN_SPL_PCL_V3 (.) 12 (.) 29 (.) 00 (.) 21 (.) exe

75%
Threat score
ML-371x_Series_WIN_PCL_V3 (.) 12 (.) 29 (.) 00 (.) 38_CDV1 (.) 33 (.) exe

75%
Threat score
kavremvr (.) exe

Source: Hybrid Analysis

Top malicious URL

100%
Threat score
http://vfxtownhost3092 (.) eu-gb (.) cf (.) appdomain (.) cloud/

100%
Threat score
http://offroadbeasts (.) com/

92%
Threat score
http://apprendrelaudit (.) com/audit-comptable-10-notions-cles-a-maitriser-part-1-3/

90%
Threat score
http://si309222 (.) us-south (.) cf (.) appdomain (.) cloud/

87%
Threat score
http://sourceforge (.) net/projects/kdiff3/files/kdiff3/

76%
Threat score
http://278302p (.) us-south (.) cf (.) appdomain (.) cloud/

75%
Threat score
http://r0g (.) us-south (.) cf (.) appdomain (.) cloud/

74%
Threat score
https://bold-leaf-6294 (.) on (.) fleek (.) co/?clientID=whistleblower%40hkelectric (.) com

72%
Threat score
http://www (.) aahung (.) org/

100%
Threat score
http://www (.) digiovannisrl (.) it/

92%
Threat score
http://3094g3 (.) us-south (.) cf (.) appdomain (.) cloud/

90%
Threat score
https://showpiece (.) trillennium (.) biz/payment/firebase1 (.) php

88%
Threat score
http://lunaribera (.) tk/vvv

85%
Threat score
https://ded4950 (.) inmotionhosting (.) com/

75%
Threat score
http://w30 (.) us-south (.) cf (.) appdomain (.) cloud/

75%
Threat score
http://papersforindustry (.) com/volleyj (.) php?utm_source=7c6&utm_content=b0__%3B%21%21La4veWw%21gQ57eR0HAPwMvegHHSopI-9-N_cA2Gyuaeoa58mhQgIt7TdcptQAEuPTm7oq3b77zhBvWeyhINM%24

72%
Threat score
http://takween-me (.) 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 Brazil

#9 Japan

#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.

#3 **Hosting Response / Michael Boehm**
Snowshoe spam organization that uses large numbers of

#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.

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 Thailand

#5 Indonesia

#6 Algeria

#7 Viet Nam

#8 Iran (Islamic Republic of)

#9 Brazil

#10 Japan

Source: SpamHaus

Top phishing countries

#1 United States

#2 Russia

#3 Singapore

#4 Germany

#5 Netherlands

#6 Bulgaria

#7 Japan

#8 France

#9 Iran

#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