Your Security Rabbits report for March 28, 2022

Source: Ransom Watch

Ransomware attacks

alphv	DC Solutions FR&Switzerland (dcsolution.ch)	lockbit2	zentrum-dreilin...
conti	UNITEK Contracting Group	clop	THENOC.NET
clop	SSMSJUSTICE.COM	lockbit2	qarch.nl
suncrypt	Oklahoma City Indian Clinic	clop	OAKDELL.COM
clop	MTMRECOGNITION.COM	stormous	MIGROS
vicesociety	Jammal Trust Bank	clop	JDAVIDTAXLAW.COM
lockbit2	https://pirsonh...	blackbyte	h1{
lockbit2	girlguidingl	lockbit2	pirsonholland.c...
clop	FAIR-RITE.COM	clop	DRIVEANDSHINE.COM
clop	DRC-LAW.COM	blackbyte	Diamond Pet Foods
lockbit2	comune.g		

Hot topics

Nothing today

News

The Hacker News

'Purple Fox' Hackers Spotted Using New Variant of FatalRAT in Recent Malware Attacks

The operators of the Purple Fox malware have retooled their malware arsenal with a new variant of a remote access trojan called FatalRAT, while also simultaneously upgrading their evasion mechanisms to bypass security software. "Users' machines are targeted via trojanized software packages masquerading as legitimate application installers," Trend Micro researchers said in a report published on

Cyware News - Latest Cyber News

Clear Skye raises $14 million to close the gap between identity and business processes

Clear Skye announced that the company has completed a $14 million Series A funding round, bringing total funding for the company to nearly $20 million since its initial seed round in 2020.

Cyware News - Latest Cyber News

Cybercriminals launched 9.75 million DDoS attacks in 2021

During the second half of 2021, cybercriminals launched approximately 4.4 million DDoS attacks, bringing the total number of DDoS attacks in 2021 to 9.75 million, a NETSCOUT report reveals.

Cyware News - Latest Cyber News

EU and US agree new data transfer deal

The detail of what has been agreed by the EU and U.S. in principle -- and how exactly the two sides have managed to close the gap between what remain two very differently oriented legal systems -- is not clear.

Security Affairs

GhostWriter APT targets state entities of Ukraine with Cobalt Strike Beacon

Ukraine CERT-UA warns that the Belarus-linked GhostWriter APT group is targeting state entities of Ukraine with Cobalt Strike Beacon. Ukraine CERT-UA uncovered a spear-phishing campaign conducted by Belarus-linked GhostWriter APT group targeting Ukrainian state entities with Cobalt Strike Beacon. The phishing messages use a RAR-archive named "Saboteurs.rar", which contains RAR-archive "Saboteurs 21.03.rar." This second archive [...] The post GhostWriter APT targets state entities of Ukraine with Cobalt Strike Beacon appeared first on Security Affairs.

Cyware News - Latest Cyber News

Hodur: A New Korplug Variant from Chinese Hackers

A new variant of PlugX RAT, named Hodur, is being used by Mustang Panda against East and Southeast Asian entities, with a few in Europe and Africa too. Its phishing lures include a regional aid map for a European country, updated COVID-19 travel restrictions, and the Regulations of the European Parliament and of the Council. The infection ends with the deployment of the Hodur backdoor on the targeted Windows systems.

Security Affairs

Mar 20- Mar 26 Ukraine - Russia the silent cyber conflict

This post provides a timeline of the events related to the Russian invasion of Ukraine from the cyber security perspective. March 25 - Anonymous leaked 28GB of data stolen from the Central Bank of Russia Anonymous announced that the affiliate group Black Rabbit World has leaked 28 GB of data stolen from the Central Bank [...] The post Mar 20- Mar 26 Ukraine - Russia the silent cyber conflict appeared first on Security Affairs.

The Hacker News

Muhstik Botnet Targeting Redis Servers Using Recently Disclosed Vulnerability

Muhstik, a botnet infamous for propagating via web application exploits, has been observed targeting Redis servers using a recently disclosed vulnerability in the database system. The vulnerability relates to CVE-2022-0543, a Lua sandbox escape flaw in the open-source, in-memory, key-value data store that could be abused to achieve remote code execution on the underlying machine. The

Cyware News - Latest Cyber News

North Korean Groups Share Zero-Day Exploit in Chrome

Google's TAG uncovered two attack campaigns by distinct North Korean state actors abusing the same Chrome zero-day. The attacks were aimed at IT organizations, news media, and crypto-banks in the U.S. Organizations are recommended to adopt proactive security measures and implement multiple layers of security to tackle such threats.

IT Security Guru

One tenth of UK staff bypass corporate security

A new study from Cisco has found that a tenth of UK employees actively circumvent their organisation's security measures. The network technology company polled over 1000 UK professionals working for organisations that allow hybrid working, in order to better understand the potential security risks of the modern, flexible workplace. The research has revealed that many [...] The post One tenth of UK staff bypass corporate security appeared first on IT Security Guru.

Operation Dragon Castling Targets Betting Companies

Operation Dragon Castling is yet another campaign by a Chinese-speaking APT

Purple Fox Uses New Arrival Vector and Improves Malware Arsenal

Cyware News - Latest Cyber News

group targeting betting companies in Southeast Asian countries. One of the malicious files used in this campaign is the MulCom backdoor that is believed to be loaded by a malicious file, CorePlugin. The researchers have spotted notable code similarities between the MulCom backdoor and FFRat malware samples.

Cyware News - Latest Cyber News

Trend Micro investigated Purple Fox's new arrival vector and early access loaders. Users' machines seem to be targeted with malicious payloads masquerading as legitimate application installers.

Security Affairs

Shopping trap: The online stores' scam that hits users worldwide

Shopping trap: Criminal gangs from China have been using copies of online stores of popular brands to target users all over the world Malicious schemas linked to online stores are on the rise in 2022. Criminal gangs from China have been using copies of online stores of popular brands to target users all over the [...] The post Shopping trap: The online stores' scam that hits users worldwide appeared first on Security Affairs.

Security Affairs

Sophos Firewall affected by a critical authentication bypass flaw

Sophos has addressed a critical vulnerability, tracked as CVE-2022-1040, in its Sophos Firewall that allows remote code execution (RCE). Sophos has fixed an authentication bypass vulnerability, tracked as CVE-2022-1040, that resides in the User Portal and Webadmin areas of Sophos Firewall. The CVE-2022-1040 flaw received a CVSS score of 9.8 and impacts Sophos Firewall versions 18.5 MR3 (18.5.3) and earlier. [...] The post Sophos Firewall affected by a critical authentication bypass flaw appeared first on Security Affairs.

ZDNet | security RSS

Sophos patches critical remote code execution vulnerability in Firewall

Sophos Firewall is a network protection solution for the enterprise market.

Cyware News - Latest Cyber News

Vidar Spyware Abuses CHM File Formats to Evade Detection

Threat actors are hiding Vidar malware in Microsoft Compiled HTML files to avoid detection in email spam campaigns to target victims and harvest their data. This allows the malware to set up its configuration and start data harvesting, including cryptocurrency account credentials and credit card information. The spyware is capable of downloading and executing further malware payloads as well.

Security Affairs

Western Digital addressed a critical bug in My Cloud OS 5

Western Digital fixed a critical flaw affecting My Cloud OS 5 devices that allowed attackers to gain remote code execution with root privileges. Western Digital has addressed a critical vulnerability, tracked as CVE-2021-44142, that could have allowed attackers to gain remote code execution with root privileges on unpatched My Cloud OS 5 devices. The CVE-2021-44142 [...] The post Western Digital addressed a critical bug in My Cloud OS 5 appeared first on Security Affairs.

Cyware News - Latest Cyber News

Western Digital fixes critical bug giving root on My Cloud NAS devices

This out-of-bounds heap read/write flaw can be exploited by unauthenticated threat actors in low complexity attacks targeting My Cloud devices running vulnerable firmware versions.

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

Dave Rubin

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

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.

Spiros Margaris

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

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-2021-45491

3CX System through 2022-03-17 stores cleartext passwords in a database.

UNRATED Vector: unkown Created: 2022-03-28 Updated: 2022-03-28

CVE-2022-26271

74cmsSE v3.4.1 was discovered to contain an arbitrary file read vulnerability via the $url parameter at \index\controller\Download.php.

UNRATED Vector: unkown Created: 2022-03-28 Updated: 2022-03-28

CVE-2022-26259

A buffer over flow in Xiongmai DVR devices NBD80X16S-KL, NBD80X09S-KL, NBD80X08S-KL, NBD80X09RA-KL, AHB80X04R-MH, AHB80X04R-MH-V2, AHB80X04-R-MH-V3, AHB80N16T-GS, AHB80N32F4-LME, and NBD90S0VT-QW allows attackers to cause a Denial of Service (DoS) via a crafted RSTP request.

UNRATED Vector: unkown Created: 2022-03-28 Updated: 2022-03-28

CVE-2021-44617

A SQL Injection vulnerability exits in the Ramo plugin for **GLPI** 9.4.6 via the idu parameter in plugins/ramo/ramoapirest.php/getOutdated.

UNRATED Vector: unkown Created: 2022-03-28 Updated: 2022-03-28

CVE-2022-26255

Clash for **Windows** v0.19.8 was discovered to allow arbitrary code execution via a crafted payload injected into the Proxies name column.

UNRATED Vector: unkown Created: 2022-03-28 Updated: 2022-03-28

CVE-2022-26258

D-Link DIR-820L 1.05B03 was discovered to contain a remote command execution (RCE) vulnerability via the Device Name parameter in /lan.asp.

UNRATED Vector: unkown Created: 2022-03-28 Updated: 2022-03-28

CVE-2022-26273

EyouCMS v1.5.4 was discovered to lack parameter filtering in \user\controller\shop.php, leading to **payment** logic vulnerabilities.

CVE-2021-26599

ImpressCMS before 1.4.3 allows include/findusers.php groups SQL Injection.

UNRATED Vector: unkown Created: 2022-03-28 Updated: 2022-03-28

CVE-2021-26601 **ImpressCMS** before 1.4.3 allows libraries/image-editor/image-edit.php image_temp Directory Traversal.

UNRATED Vector: unkown Created: 2022-03-28 Updated: 2022-03-28

CVE-2021-26600 **ImpressCMS** before 1.4.3 has plugins/preloads/autologin.php type confusion with resultant Authentication Bypass (!= instead of !==).

UNRATED Vector: unkown Created: 2022-03-28 Updated: 2022-03-28

CVE-2022-27950 In drivers/hid/hid-elo.c in the **Linux** kernel before 5.16.11, a memory leak exists for a certain hid_parse error condition.

UNRATED Vector: unkown Created: 2022-03-28 Updated: 2022-03-28

CVE-2021-44209 OX **App Suite** through 7.10.5 allows XSS via an HTML 5 element such as AUDIO.

UNRATED Vector: unkown Created: 2022-03-28 Updated: 2022-03-28

CVE-2021-44210 OX **App Suite** through 7.10.5 allows XSS via NIFF (Notation **Interchange** File Format) data.

UNRATED Vector: unkown Created: 2022-03-28 Updated: 2022-03-28

CVE-2021-44213 OX **App Suite** through 7.10.5 allows XSS via uuencoding in a multipart/alternative message.

UNRATED Vector: unkown Created: 2022-03-28 Updated: 2022-03-28

CVE-2021-45490 The client applications in 3CX on Windows, the 3CX app for iOS, and the 3CX application for **Android** through 2022-03-17 lack SSL certificate validation.

UNRATED Vector: unkown Created: 2022-03-28 Updated: 2022-03-28

UNRATED Vector: unkown Created: 2022-03-28 Updated: 2022-03-28

CVE-2021-26598 **ImpressCMS** before 1.4.3 has Incorrect Access Control because include/findusers.php allows access by unauthenticated attackers (who are, by design, able to have a security token).

UNRATED Vector: unkown Created: 2022-03-28 Updated: 2022-03-28

CVE-2022-25757 In **Apache APISIX** before 2.13.0, when decoding JSON with duplicate keys, lua-cjson will choose the **last** occurred value as the result. By passing a JSON with a duplicate key, the attacker can bypass the body_schema validation in the request-validation plugin. For example, `{"string_payload":"bad","string_payload":"good"}` can be used to **hide** the "bad" input. Systems satisfy **three** conditions below are affected by this attack: 1. use body_schema validation in the request-validation plugin 2. upstream application uses a special JSON library that chooses the **first** occurred value, like jsoniter or gojay 3. upstream application does not validate the input anymore. The fix in APISIX is to re-encode the validated JSON input back into the request body at the side of APISIX. Improper Input Validation vulnerability in __COMPONENT__ of Apache APISIX allows an attacker to __IMPACT__. This issue affects Apache APISIX Apache APISIX version 2.12.1 and prior versions.

UNRATED Vector: unkown Created: 2022-03-28 Updated: 2022-03-28

CVE-2021-44212 OX **App Suite** through 7.10.5 allows XSS via a trailing control character such as the SCRIPT\t substring.

UNRATED Vector: unkown Created: 2022-03-28 Updated: 2022-03-28

CVE-2021-44208 OX **App Suite** through 7.10.5 allows XSS via an unknown system message in Chat.

UNRATED Vector: unkown Created: 2022-03-28 Updated: 2022-03-28

CVE-2021-44211 OX **App Suite** through 7.10.5 allows XSS via the class attribute of an element in an HTML e-mail signature.

UNRATED Vector: unkown Created: 2022-03-28 Updated: 2022-03-28

CVE-2022-24303 **Pillow** before 9.0.1 allows attackers to delete files because **spaces** in temporary pathnames are mishandled.

UNRATED Vector: unkown Created: 2022-03-28 Updated: 2022-03-28

CVE-2022-26268 Xiaohuanxiong v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /app/controller/Books.php.

UNRATED Vector: unkown Created: 2022-03-28 Updated: 2022-03-28

Source: Hybrid Analysis

Top malicious files

100% Threat score PO.083322.pdf.exe

100% Threat score FLY170322.PDF.bat

85% Threat score Nor850-3.0.220222.exe

100% Threat score ç'•ç–µè™•ç…§ç‰‡å'Œå¤–åŒ…è£…ç-§-å¯†ç¢¼tw220323.exe

99% Threat score ABKHx64.dll

75% Threat score ç,¹â€â€Œå‡»â€â€å®‰â€è£…
â€Œâ€Œâ€çº¸â€Œé£žâ€Œæœº_â€ç®€â€â€â€ä½"â€â€â€Œä¸â€Œâ€æ–‡â€è¯-â€â€Œâ€è¯€â€â€â€åŒ….com

Source: Hybrid Analysis

Top malicious URL

100% Threat score http://veronica-pratt.github.io/

95% Threat score http://61.3.186.14:47659/Mozi.m

94% Threat score https://github.com/tihanyin/PSSW100AVB/blob/main/ReverseShell_2022_03.ps1

87% Threat score http://inx.lv/htxM?jvw

86% Threat score https://amauezom.co.jp.hqksfym.cn/

83% Threat score http://langkahmejunubulanrahmadhan.co.vu/confirmid.php

100% Threat score http://authlogdiscover01.ddns.us/login.php?cmd=login_submit&id=22f86db9e107b5d13e245d1a05a7c2ab22f86db9e107b5d13e24

95% Threat score https://edukacijacik.ba/core/config/login.php

89% Threat score https://cima-afrique.org/question/jetzt-hd-sonic-the-hedgehog-2-online-2022-ga

87% Threat score http://viperswap.one/

84% Threat score https://u25427179.ct.sendgrid.net/ls/click?upn=r-2FpFHvOCvVcknsU51lcZUU
2FrGT8c0mR3uqUkY5ipufXwB8RQRO9JMwYBDM5b7qKJzpUjUlgPGERr9Erig
2BG3XNuOlt9YPDrmulWUeB4-2BRvzS0EbLOB880jTbgLyvMcZrPX55iPBsqeV
2B3P16YDZBc-2FNSCYt3Z8d2BE4-
2BvlAHCjUOw6RnsD00e8xbLgen0nTlHEMgym4DaDdohupc4NVQbH9b8vrJXp
2BJnouUzSLNYnHRltuHAbQ1rFZWDl1N5gH4ButH-
2BxsuS1nxFYQIWII4BfTLPxea6X3NSL8dTwFkFK1pDU56ql61beLhs4qthdPrG
2BHQ5HfieZ2SYU4Ba8kyoFTRGyEjwCydNNtYgr4gwymzWz9nAEPQUJtv9scJS
2BmdnJwW5NCFUx7CwDExZLGJtnGZB6zax1rPvr-2B8kn8U4JsYEe333usiIxR6
2FpsyseCTeFT8wILPHFiIS0BtaclqfrfRX-2F3qnW-2BO0TRv3xz-2FCG0VbK8Gc

79% Threat score https://www.bitchute.com/video/YkJtJpAxnjqc/

77% Threat score	https://amaeuzom.co.jp.mttthmw.cn/
77% Threat score	http://summitmining.io/
72% Threat score	http://www.quizzop.com/
77% Threat score	http://www.nssce.org/
72% Threat score	http://stargate.finance/
71% Threat score	https://kidbucketlist.com.au/

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

Source: SpamHaus

Top phishing countries

#1 United States	#2 Indonesia

#3 Russia	#4 Germany
#5 Singapore	#6 Netherlands
#7 Hong Kong	#8 Spain
#9 India	#10 Japan

Source: Have I been pwned?

Have I been pwnd

Nothing today

Source: Imperva DDOS Map

Top DDOS attackers

- **United States (27%)**
- **Russia (18%)**
- **Germany (11%)**

Source: Imperva DDOS Map

Top DDOS country targets

- **Russia (49%)**
- **Ukraine (18%)**
- **United States (11%)**

Source: Imperva DDOS Map

Top DDOS techniques

73%	**DDoS**
19%	**Automated Threat**
8%	**OWASP**

Source: Imperva DDOS Map

Top DDOS industry targets

57%	**Financial Services**
22%	**Business**
6%	**Computing & IT**