Your Security Rabbits report for February 21, 2022

Hot topics

Nothing today

News

Cyware News - Latest Cyber News

83% of employees continue accessing old employer's accounts
The security threat this poses is coupled with the fact that 56% of these employees said they had used this continued access with the specific intent of harming their former employer, as per a report.

Security Affairs

BEC scammers impersonate CEOs on virtual meeting platforms
The FBI warned US organizations and individuals are being increasingly targeted in BECattacks on virtual meeting platforms The Federal Bureau of Investigation (FBI) warned this week that US organizations and individuals are being increasingly targeted in BEC (business email compromise) attacks on virtual meeting platforms. Business Email Compromise/Email Account Compromise (BEC/EAC) is a sophisticated scam that [...] The post BEC scammers impersonate CEOs on virtual meeting platforms appeared first on Security Affairs.

The Hacker News

Hackers Exploiting Infected Android Devices to Register Disposable Accounts
An analysis of SMS phone-verified account (PVA) services has led to the discovery of a rogue platform built atop a botnet involving thousands of infected Android phones, once again underscoring the flaws with relying on SMS for account validation. SMS PVA services, since gain prevalence in 2018, provide users with alternative mobile numbers that can be used to register for other online services

Cyware News - Latest Cyber News

New phishing campaign targets Monzo online-banking customers
Users of Monzo, one of the UK's most popular digital-only banking platforms, are being targeted by phishing messages supported by a growing network of malicious websites.

Cyware News - Latest Cyber News

ShadowPad Linked to Chinese MSS and PLA
Hackers affiliated with the Chinese Ministry of State Security and the People's Liberation Army are increasingly deploying the ShadowPad advanced modular RAT against its targets. It can steal sensitive system information, interact with the file system and registry, and deploy new modules to propagate. Organizations should monitor for TTPs associated with the ShadowPad backdoor to stay protected.

Security Affairs

Threat actors stole at least $1.7M worth of NFTs from tens of OpenSea users
Threat actors have stolen and flipped high-valued NFTs from the users of the world's largest NFT exchange, OpenSea. The world's largest NFT exchange, OpenSea on Sunday confirmed that tens of some of its users have been hit by a phishing attack and had lost valuable NFTs worth $1.7 million. The phishing attack was confirmed by [...] The post Threat actors stole at least $1.7M worth of NFTs from tens of OpenSea users appeared first on Security Affairs.

Cyware News - Latest Cyber News

Update: White House pins Ukraine DDoS attacks on Russian GRU hackers
The White House has linked the recent DDoS attacks that knocked down the sites of Ukrainian banks and defense agencies to Russia's Main Directorate of the General Staff of the Armed Forces.

Security Affairs

A flaw in the encryption algorithm of Hive Ransomware allows retrieving encrypted files
Researchers discovered a flaw in the encryption algorithm used by Hive ransomware that allowed them to decrypt data. Researchers discovered a flaw in the encryption algorithm used by Hive ransomware that allowed them to decrypt data without knowing the private key used by the gang to encrypt files. The Hive ransomware operation has been active [...] The post A flaw in the encryption algorithm of Hive Ransomware allows retrieving encrypted files appeared first on Security Affairs.

Cyware News - Latest Cyber News

CISA warns of hybrid operations threat to US critical infrastructure
CISA urged U.S. critical infrastructure organizations to increase their resilience against risks posed by foreign influence operations using misinformation, disinformation, and malformation tactics.

Cyware News - Latest Cyber News

Hackers Target Microsoft Teams Users in Chats
Cybercriminals are planting maldocs in chat threads on Microsoft Teams. Users accessing it might end up giving control of their systems to hackers. Organizations are suggested to deploy email gateway security that secures communication applications, and employees should contact IT whenever a suspicious file is observed.

Cyware News - Latest Cyber News

Poisoned Pipeline Execution Attacks - A New Wave of Threats
A security researcher demonstrated the possibility of poisoned pipeline attacks that can be triggered by abusing permissions in source code management (SCM) repositories. The pipelines that execute unreviewed code are more exposed to PPE attacks. Applications not developed with a security-first approach are deemed to face challenges related to PPE.

Cyware News - Latest Cyber News

Social media attacks surged in 2021, financial institutions targeted the most
According to the findings from PhishLabs, the number of social media attacks per target increased 103% from January 2021, when enterprises were experiencing an average of just over one threat per day.

Security Affairs

Threat Report Portugal: Q4 2021
The Threat Report Portugal: Q4 2021 compiles data collected on the malicious campaigns that occurred from July to September, Q4, of 2021. The Portuguese Abuse Open Feed 0xSI_f33d is an open sharing database with the ability to collect indicators from multiple sources, developed and maintained by Seguranca-Informatica. This feed is based on automatic searches and is also supported [...] The post Threat Report Portugal: Q4 2021 appeared first on Security Affairs.

Twitter

Kotaku

'Hacker' steals NFTs 'worth' millions from Opensea marketplace:

Ran NeuNer

GM (except to the following; @JustinTrudeau , @GaryGensler , the Opensea hacker , anyone who isnt buying this dip)

An international watchdog that monitors cyber security and the Governance of the internet @netblocks will be monitoring Zimbabwes internet today after fears that it might be deliberately slowed down to black out #YellowSunday rally. Share you

KreekCraft

That was the craziest stream ever.. We teamed up with the owner of HD Admin and caught the hackers behind all the recent game hacks like MeepCity & Find The Markers. Not only that, we talked to the entire Tubers93 hacking group on Discord. Thanks to the entire 40k who tuned in!

Ran NeuNer

I understand why hackers would target normal (fungible) tokens, they are easy to liquidate them and can't really be traced. NFT'S are not fungible though. Anyone buying an NFT that was stolen is clearly buying stolen property. Is there really a market for marked stolen Jpegs?

With current geopolitical uncertainty, I convened my team to discuss ongoing cybersecurity efforts. Our state is an attractive target for cyber criminals & foreign adversaries, but New Yorkers should be confident that we are hard at

Hopewell Chinono

intern experiences tagging them too

The Lincoln Project

Before the United States has to penalize someone in response to cybersecurity threats and attacks, the first question it needs to answer is WWPD - What would Putin do? @nicoleperlroth explains on this encore of the podcast:

Cheap Ass Gamer

Soul Hackers Collection?

Newsmax

A former top U.S. cybersecurity official said on Sunday the financial services industry is probably the No.1 target for Russian retaliation if there are U.S.-imposed sanctions over Ukraine.

Kathy Hochul

work watching & preparing for any threats.

g1

Americanas e Submarino voltam a tirar sites do ar aps suspeita de ataque hacker #g1

Hustler

We established it was a phishing email that caused the hack on Open Sea yesterday, but I see no one bringing up this point: Open Sea sent out an email and the format of it people didnt like. Whatever, but HOW did the hackers get everyones emails to send a phishing email?

Robert M. Lee

As I try to continue to distract cybersecurity professionals from thinking about work in non-work hours[...] Angels Envy rye Barr Hill gin Imprint Brewery beer Thank me later

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-2022-0691

Authorization Bypass Through User-Controlled Key in NPM **url-parse** prior to 1.5.9.

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-21

CVE-2022-0589

Cross-site Scripting (XSS) - Stored in Packagist librenms/librenms prior to 22.1.0.

UNRATED Vector: unkown Created: 2022-02-15 Updated: 2022-02-21

CVE-2022-0588

Exposure of Sensitive Information to an Unauthorized Actor in Packagist librenms/librenms prior to 22.2.0.

UNRATED Vector: unkown Created: 2022-02-15 Updated: 2022-02-21

CVE-2022-0587

Improper Authorization in Packagist librenms/librenms prior to 22.2.0.

UNRATED Vector: unkown Created: 2022-02-15 Updated: 2022-02-21

CVE-2022-0576

Cross-site Scripting (XSS) - Generic in Packagist librenms/librenms prior to 22.1.0.

UNRATED Vector: unkown Created: 2022-02-14 Updated: 2022-02-21

CVE-2022-0575

Cross-site Scripting (XSS) - Stored in Packagist librenms/librenms prior to 22.2.0.

UNRATED Vector: unkown Created: 2022-02-14 Updated: 2022-02-21

CVE-2022-0580

Improper Access Control in Packagist librenms/librenms prior to 22.2.0.

UNRATED Vector: unkown Created: 2022-02-14 Updated: 2022-02-21

CVE-2022-25297

This affects the package drogonframework/drogon before 1.7.5. The unsafe handling of file names during upload using HttpFile::save() method may enable attackers to write files to arbitrary locations outside the designated target folder.

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-21

Source: Hybrid Analysis

Top malicious files

100% Threat score	vPWNp4Iy5miJo99 (.) exe
100% Threat score	gs-pechat-blankov-pl_383981107 (.) exe
100% Threat score	EGRECONTA634980001 EGRECONTA634980006 (.) bin
100% Threat score	mine (.) exe
100% Threat score	tmpj1xmt6_b
100% Threat score	MJ-2011818454 (.) xlsb
80% Threat score	setup (.) exe

100% Threat score	Evolution (.) exe
100% Threat score	gatherNetworkInfo (.) vbs
100% Threat score	crack (.) exe
100% Threat score	glock-cracked (.) exe
100% Threat score	aded4e686227c932c77fe158ec18251aad4d7097 (.) malware
84% Threat score	ACTT_WINDOWS_Scripta (.) ps1
80% Threat score	setup (.) exe

78%
Threat score
ENOC GROUP companies Inquiry (.) exe

75%
Threat score
SetupDcDesk (.) exe

74%
Threat score
LuniteLauncher (.) jar

74%
Threat score
FIFA_Players_Status _Department (.) pdf (.) htm

Source: Hybrid Analysis

Top malicious URL

100%
Threat score
http://aquatecns (.) com/Webmail/mail (.) php?email=molise%40inail (.) it&%3Bdata=04%7C01%7Cmolise%40inail (.) it%7C05c8415bb7984808c74708d9f527455f%7C418322d35401446f99969e2e03ee3a5e%7C0%7C0%7C637810371288210348%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAw

86%
Threat score
https://proximis (.) net/fquagiu/rdmaemstapcoeietimgsursmuel-ul-ouvtenn

78%
Threat score
http://minecraft-java-edition (.) org/get/latest-version

77%
Threat score
http://vicki (.) vinci (.) redutec-es (.) com (.) br/horse?vicki (.) vinci%40kireygroup (.) com

73%
Threat score
http://email (.) marcusevansonline (.) 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 Korea, Republic of

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 Indonesia

#5 Thailand

#6 Algeria

#7 Viet Nam

#8 Brazil

#9 Pakistan

#10 Iran (Islamic Republic of)

Source: SpamHaus

Top phishing countries

#1 United States

#2 Germany

#3 Russia

#4 India

#5 Finland

#6 Netherlands

#7 Japan

#8 France

#9 Hong Kong

#10 Canada