Your Security Rabbits report for February 12, 2022

Hot topics

Nothing today

News

Cyware News - Latest Cyber News

50% of malicious office documents were downloaded via Google Drive in 2021

According to a recently released Netskope report, Google Drive overtook the top spot from Microsoft OneDrive, which led malicious office document download apps in 2020 with 34%.

Cyware News - Latest Cyber News

Apple fixes actively exploited iOS, macOS zero-day (CVE-2022-22620)

CVE-2022-22620 is a use after free issue in WebKit, the browser engine used in Safari and all iOS web browsers. Apple fixed it in iOS 15.3.1 and iPadOS 15.3.1, macOS Monterey 12.2.1, and Safari 15.3.

Naked Security

Apple zero-day drama for Macs, iPhones and iPads - patch now!

Sudden update! Zero-day browser hole! Drive-by malware danger! Patch Apple laptops and phones now...

Security Affairs

Apple addressed a third zero-day in 2022, which is actively exploited

Apple addressed a new WebKit zero-day affecting iOS, iPadOS, macOS, and Safari that may have been actively exploited in the wild. Apple has addressed a zero-day vulnerability, tracked as CVE-2022-22620, in the WebKit affecting iOS, iPadOS, macOS, and Safari that may have been actively exploited in the wild. This is the third zero-day vulnerability fixed by the IT giant [...] The post Apple addressed a third zero-day in 2022, which is actively exploited appeared first on Security Affairs.

Threatpost

Apple Patches Actively Exploited WebKit Zero Day

A memory issue affects myriad iPhone, iPad and MacOS devices and allows attackers to execute arbitrary code after processing malicious web content.

CyberScoop

CIA 'secret bulk collection program' picked up some Americans' data, senators reveal

Some data belonging to Americans was swept up in a secret CIA mass surveillance program that operated under atypical legal authority for such an operation, according to a letter released Thursday night by two Democratic members of the Senate Intelligence Committee. The unnamed program operates "entirely outside the statutory framework that Congress and the public believe govern this collection, and without any of the judicial, congressional or even executive branch oversight" that otherwise would apply, according to the letter from Sens. Ron Wyden, D-Ore., and Martin Heinrich, D-N.M. The senators said the "secret bulk collection program" was authorized under presidential Executive

Order 1233[...]

Security Affairs

CISA adds 15 new vulnerabilities to its Known Exploited Vulnerabilities Catalog

The U.S. CISA has added to the catalog of vulnerabilities another 15 security vulnerabilities actively exploited in the wild. The US Cybersecurity & Infrastructure Security Agency (CISA) has added fifteen more flaws to the Known Exploited Vulnerabilities Catalog. The 'Known Exploited Vulnerabilities Catalog' is a list of known vulnerabilities that threat actors have abused in attacks [...] The post CISA adds 15 new vulnerabilities to its Known Exploited Vulnerabilities Catalog appeared first on Security Affairs.

Cyware News - Latest Cyber News

CISA Urges Organizations to Patch Actively Exploited Windows SeriousSAM Vulnerability

The U.S. Cybersecurity & Infrastructure Security Agency (CISA) has added to its catalog of actively exploited vulnerabilities another 15 security issues actively used in cyberattacks.

Cyware News - Latest Cyber News

Cloudflare Buys Cloud Access Security Broker Startup Vectrix

Cloudflare has purchased Vectrix to detect and mitigate issues like inappropriate filing sharing and user permission misconfigurations in tools like AWS, Google Workspace and GitHub.

Threatpost

Critical MQTT-Related Bugs Open Industrial Networks to RCE Via Moxa

A collection of five security vulnerabilities with a collective CVSS score of 10 out of 10 threaten critical infrastructure environments that use Moxa MXview.

Cyware News - Latest Cyber News

Cyberattack Disrupts Slovenia's Top TV Station, Impacts Streaming Platform and News Broadcast

The attack, which took place on Tuesday, impacted Pop TV's computer network and prevented the company from showing any computer graphics for the evening edition of 24UR, the station's daily news show.

Threatpost

Cybercrooks Frame Targets by Planting Fabricated Digital Evidence

The 'ModifiedElephant' threat actors are technically unimpressive, but they've evaded detection for a decade, hacking human rights advocates' systems with dusty old keyloggers and off-the-shelf RATs.

IT Security Guru

DomainTools Announces Availability of Iris Detect

DomainTools has announced the availability of DomainTools Iris Detect, an innovative new product designed to discover and monitor domain names spoofing brands, trademarks, or other domains with unprecedented speed, accuracy, and comprehensiveness. Building on the world's largest databases of domain registration and Domain Name System (DNS) data developed by DomainTools and Farsight Security, the discovery engine underpinning Iris Detect [...] The post DomainTools Announces Availability of Iris Detect appeared first on IT Security Guru.

Cyware News - Latest Cyber News

Facebook exposes 'god mode' token miscreants could use

According to a security researcher, a malicious developer could harvest Facebook data using the same access method, because Facebook is exposing a plain-text token described as "god mode."

Security Affairs

FritzFrog P2P Botnet is back and targets Healthcare, Education and Government Sectors

FritzFrog P2P botnet is back and is targeting servers belonging to entities in the healthcare, education, and government sectors. FritzFrog is a sophisticated botnet that was involved in attacks against SSH servers worldwide since January 2020. The bot is written in Golang and implements wormable capabilities, experts reported attacks against entities in the government, education, and finance sectors. [...] The post FritzFrog P2P Botnet is back and

The Hacker News

Hackers Planted Fake Digital Evidence on Devices of Indian Activists and Lawyers

A previously unknown hacking group has been linked to targeted attacks against human rights activists, human rights defenders, academics, and lawyers across India in an attempt to plant "incriminating digital evidence." Cybersecurity firm SentinelOne attributed the intrusions to a group it tracks as "ModifiedElephant," an elusive threat actor that's been operational

targets Healthcare, Education and Government Sectors appeared first on Security Affairs.

since at least 2012, whose

IT Security Guru

Health data of thousands of Dorset patients leaked by mistake

A new study reports that Dorset Healthcare University NHS Foundation Trust (DHC) experienced the fourth highest number of data breaches in the UK. The trust argues this does not tell the whole story. Security website VPNoverview.com sent out Freedom of Information requests to 229 NHS foundations across the UK regarding data breaches. Of those, 152 [...] The post Health data of thousands of Dorset patients leaked by mistake appeared first on IT Security Guru.

IT Security Guru

Microsoft fixes Defender flaw

Microsoft has addressed in the Microsoft Defender Antivirus that allowed attackers to plant and execute malicious payloads while avoiding Defender's malware detection engine. The flaw affected even the latest Windows 10 versions and threat attackers have been able to exploit it since at least 2014. As BleepingComputer previously reported, the flaw resulted from lax security settings [...] The post Microsoft fixes Defender flaw appeared first on IT Security Guru.

Cyware News - Latest Cyber News

Molerats APT Strikes Again with New NimbleMamba Malware

Researchers from Proofpoint spotted a new phishing campaign that targeted multiple Middle Eastern governments, foreign-policy think tanks, and a state-affiliated airline, with the new NimbleMamba trojan. NimbleMamba is believed to share some similarities with Molerats' previous executable LastConn that was first reported in June 2021.

Cyware News - Latest Cyber News

Nearly $700 million spent on ransomware payments in 2020 alone: Report

The report by Chainalysis also listed the most prolific ransomware groups by total payments received, finding that Conti led the way with at least $180 million made from ransoms.

Cyware News - Latest Cyber News

SANS Institute Launches Nationwide Scholarship Program

Cybersecurity training and certification provider SANS Institute is partnering with Historically Black Colleges and Universities to launch a new nationwide cybersecurity education scholarship program.

Cyware News - Latest Cyber News

Series of Magecart Attacks Against Outdated Magento Sites

Another massive wave of Magecart attacks was detected by Sansec last week. This attack, once again, highlights the vulnerability of e-commerce sites running outdated software.

Cyware News - Latest Cyber News

So-called 'red lines' increasingly crossed by ransomware groups in critical infrastructure attacks

We are likely to see ransomware actors increasingly target entities in critical infrastructure and cause disruption in the flow of goods and services that are vital to keeping modern society running.

Cyware News - Latest Cyber News

The Pirate Bay Clones Target Millions of Users Every Month

CyberNews discovered five malicious domains parading around as The Pirate Bay. These domains served malicious ads to more than seven million users every month by using free content to lure targets.

ZDNet | security RSS

These cybercriminals plant criminal evidence on human rights defender, lawyer devices

There's more than one way to silence civil rights activists, it seems.

Cyware News - Latest Cyber News

Vice Society Ransomware Gang Leaks Stolen Customer Files from Optionis Group

What appears to be stolen data belonging to customers of accounting conglomerate Optionis Group has surfaced on the dark web weeks after the firm confirmed intruders had broken into its systems.

WeLiveSecurity

When love hurts: Watch out for romance scams this Valentine's Day

Don't be the next victim - spot the signs of a faux romance in time and send that scammer 'packing' The post When love hurts: Watch out for romance scams this Valentine's Day appeared first on

WeLiveSecurity

Source: NIST

NIST CVE: Critical

Nothing today

Source: NIST

NIST CVE: High

Nothing today

Source: Hybrid Analysis

Top malicious files

75%
Threat score

tmphnwnuxub

Source: Hybrid Analysis

Top malicious URL

Nothing today

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


#2 **PredictLabs / Sphere Digital**
This operation uses dozens of "hosting"

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 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.

#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.

#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.

#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.

companies as fronts to lease IP addresses which are then used to send spam. Based in Chicago, Illinois and Tangier, Morocco.

#4 **Mint Global Marketing / Adgenics / Cabo Networks**
Florida affiliate spammers and bulletproof spam hosters

#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.

#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.

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 Singapore
#5 Netherlands	#6 Hong Kong
#7 France	#8 Australia
#9 Japan	#10 Canada