Your Security Rabbits report for February 14, 2022

Hot topics

Nothing today

News

Blog â€“ Flashpoint

2021 Sets Record for Most Vulnerabilities Disclosed

Today, the 2021 Year End Vulnerability QuickView Report, from Brian Martin, Vice President of Vulnerability Intelligence at Risk Based Security, was released. Powered by VulnDB, this report details trends in vulnerabilities for the year, and features a viewpoint from Flashpoint's Global Threat Intelligence Team on the year's most significant vulnerability: Log4Shell. Vulnerability disclosures recover from [...] The post 2021 Sets Record for Most Vulnerabilities Disclosed appeared first on Flashpoint.

Security Affairs

Alleged ransomware attack disrupted operations at Slovenia's Pop TV station

Last week, a cyberattack hit Pop TV, Slovenia's most popular TV channel, disrupting the operations. Last week, a cyber-attack has disrupted the operations of Pop TV, the Slovenian most popular TV channel. The attack, which likely was a ransomware attack, impacted the computer network of the TV channel and caused the cancellation of the evening [...] The post Alleged ransomware attack disrupted operations at Slovenia's Pop TV station appeared first on Security Affairs.

Cyware News - Latest Cyber News

CISA orders federal agencies to update iPhones, Macs until Feb 25th

The CISA has added a new entry to its catalog of vulnerabilities exploited in the wild, which is an Apple WebKit remote code execution bug used to target iPhones, iPads, and Macs.

The Hacker News

Critical Magento 0-Day Vulnerability Under Active Exploitation -- Patch Released

Adobe on Sunday rolled out patches to contain a critical security vulnerability impacting its Commerce and Magento Open Source products that it said is being actively exploited in the wild. Tracked as CVE-2022-24086, the shortcoming has a CVSS score of 9.8 out of 10 on the vulnerability scoring system and has been characterized as an "improper input validation" issue that could be weaponized to

Security Affairs

Critical Magento zero-day flaw CVE-2022-24086 actively exploited

Adobe addressed a critical vulnerability (CVE-2022-24086) impacting Magento Open Source products that is being actively exploited in the wild. Adobe rolled out security updates to address a critical security vulnerability, tracked as CVE-2022-24086, affecting its Commerce and Magento Open Source products that is being actively exploited in the wild. "Adobe is aware that CVE-2022-24086 has [...] The

The Hacker News

Critical Security Flaws Reported in Moxa MXview Network Management Software

Technical details have been disclosed regarding a number of security vulnerabilities affecting Moxa's MXview web-based network management system, some of which could be chained by an unauthenticated adversary to achieve remote code execution on unpatched servers. The five security weaknesses "could allow a remote, unauthenticated

post Critical Magento zero-day flaw CVE-2022-24086 actively exploited appeared first on Security Affairs.

attacker to execute code on the hosting machine with the highest

Security Affairs

Organizations paid at least $602 million to ransomware gangs in 2021

Organizations have paid more than $600 million in cryptocurrency during 2021, nearly one-third to the Conti ransomware gang. Last week, cybersecurity agencies from the U.K., the U.S. and Australia have published a joint advisory warning of an increased globalised threat of ransomware worldwide in 2021. According to a report published by the blockchain analysis firm [...] The post Organizations paid at least $602 million to ransomware gangs in 2021 appeared first on Security Affairs.

ZDNet | security RSS

Patch now: Adobe releases emergency fix for exploited Commerce, Magento zero-day

Adobe says the vulnerability is being used in attacks targeting Adobe Commerce users.

IT Security Guru

San Francisco 49ers hit with ransomware attack

Mere hours before the Super Bowl kick off, the San Francisco 49ers confirmed they were the most recent victims of the BlackByte ransomware group. In a statement to ZDNet, the team said it "recently became aware of a network security incident" causing disruption to their corporate IT network. "Upon learning of the incident, we immediately initiated [...] The post San Francisco 49ers hit with ransomware attack appeared first on IT Security Guru.

Security Affairs

San Francisco 49ers NFL team discloses BlackByte ransomware attack

A ransomware attack hit the corporate IT network of the San Francisco 49ers NFL team, The Record reported. The San Francisco 49ers NFL team has fallen victim to a ransomware attack, the news was reported by The Record. The team disclosed the attack after that the BlackByte ransomware added the team to the list of [...] The post San Francisco 49ers NFL team discloses BlackByte ransomware attack appeared first on Security Affairs.

The Hacker News

Spanish Police Arrest SIM Swappers Who Stole Money from Victims Bank Accounts

Spain's National Police Agency, the Policia Nacional, said last week it dismantled an unnamed cybercriminal organization and arrested eight individuals in connection with a series of SIM swapping attacks that were carried out with the goal of financial fraud. The suspects of the crime ring masqueraded as trustworthy representatives of banks and other organizations and used traditional phishing

Cyware News - Latest Cyber News

The importance of implementing security scanning in the software development lifecycle

Continuous security testing using multiple scanning types is fast becoming the norm as organizations recognize the need to analyze the software they build across multiple dimensions.

Cyware News - Latest Cyber News

Using mobile networks for cyber attacks as part of a warfare strategy

AdaptiveMobile Security published a research study that highlights how vulnerabilities in mobile network infrastructure could be weaponized in offensive military operations.

Source: NIST

NIST CVE: Critical

Nothing today

Source: NIST

NIST CVE: High

Nothing today

Source: Hybrid Analysis

Top malicious files

Nothing today

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 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 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 Netherlands

#4 Russia

#5 Hong Kong

#6 France

 #7 Canada

 #8 Brazil

 #9 Japan

 #10 Australia