Your Security Rabbits report for February 13, 2022

Hot topics

Nothing today

News

Security Affairs

Analyzing Phishing attacks that use malicious PDFs

Cybersecurity researchers Zoziel Pinto Freire analyzed the use of weaponized PDFs in phishing attacks Every day everybody receives many phishing attacks with malicious docs or PDFs. I decided to take a look at one of these files. I did a static analysis and I went straight to the point to make this reading simple and […] The post Analyzing Phishing attacks that use malicious PDFs appeared first on Security Affairs.

Security Affairs

Croatian phone carrier A1 Hrvatska discloses data breach

Croatian phone carrier A1 Hrvatska has disclosed a data breach that has impacted roughly 200,000 customers. Croatian phone carrier A1 Hrvatska has disclosed a data breach that has impacted 10% of its customers, roughly 200,000 people. Threat actors had access to sensitive personal information of the customers, including names, personal identification numbers, physical addresses, and […] The post Croatian phone carrier A1 Hrvatska discloses data breach appeared first on Security Affairs.

Security Affairs

CISA, FBI, NSA warn of the increased globalized threat of ransomware

CISA, FBI and NSA published a joint advisory warning of ransomware attacks targeting critical infrastructure organizations. 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. Almost any sector was hit by sophisticated, high-impact ransomware attacks, including the Defense Industrial […] The post CISA, FBI, NSA warn of the increased globalized threat of ransomware appeared first on Security Affairs.

Security Affairs

Organizations are addressing zero-day vulnerabilities more quickly, says Google

Organizations are addressing zero-day vulnerabilities more quickly, compared to last year, Google's Project Zero reported. According to Google's Project Zero researchers, organizations are addressing zero-day vulnerabilities more quickly, compared to last year. Software vendors took an average of 52 days to address vulnerabilities reported from Project Zero while 3 years ago the average was of […] The post Organizations are addressing zero-day vulnerabilities more quickly, says Google appeared first on Security Affairs.

Source: NIST

NIST CVE: Critical

Nothing today

Source: NIST

NIST CVE: High

Nothing today

Source: Hybrid Analysis

Top malicious files

100%
Threat score

tmpow00g31z

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

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

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.

#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 Singapore

#8 Australia

#9 India

#10 Japan