Your Security Rabbits report for April 04, 2022

Source: Ransom Watch

Ransomware attacks

clop	ALTERNATIVETECHS.COM
lockbit2	n
clop	DRIVEANDSHINE.COM
clop	EDAN.COM
lockbit2	greenexperts.co...
clop	MCH-GROUP.COM
lockbit2	nowiny
lockbit2	remar.com.ec
clop	ALEXIM.COM
conti	TRUSTFORD
clop	JBINSTANTLAWN.NET
clop	DRC-LAW.COM
conti	Frey and Winkler GmbH
lockbit2	centralban
clop	CAPCARPET.COM
lockbit2	oldenburgdeurbe...
conti	SLH
lockbit2	wiegaarden.dk

Hot topics

Nothing today

News

The Hacker News

Beastmode DDoS Botnet Exploiting New TOTOLINK Bugs to Enslave More Routers

A variant of the Mirai botnet called Beastmode has been observed adopting newly disclosed vulnerabilities in TOTOLINK routers between February and March 2022 to infect unpatched devices and expand its reach potentially. "The Beastmode (aka B3astmode) Mirai-based DDoS campaign has aggressively updated its arsenal of exploits," Fortinet's FortiGuard Labs Research team said. "Five new exploits were

Security Affairs

China-linked APT Deep Panda employs new Fire Chili Windows rootkit

The China-linked hacking group Deep Panda is targeting VMware Horizon servers with the Log4Shell exploit to install a new Fire Chili rootkit. Researchers from Fortinet have observed the Chinese APT group Deep Panda exploiting a Log4Shell exploit to compromise VMware Horizon servers and deploy previously undetected Fire Chili rootkit. The experts observed opportunistic attacks against organizations [...] The post China-linked APT Deep Panda employs new Fire Chili Windows rootkit appeared first on Security Affairs.

Security Affairs

Experts discovered 15-Year-Old vulnerabilities in the PEAR PHP repository

SonarSource discovered a 15-year-old flaw in the PEAR PHP repository that could have enabled supply chain attacks. Researchers from SonarSource discovered two 15-year-old security flaws in the PEAR (PHP Extension and Application Repository) repository that could have enabled supply chain attacks. PEAR is a framework and distribution system for reusable PHP components. According to the expert, [...] The post Experts discovered 15-Year-Old vulnerabilities in the PEAR PHP repository appeared first on Security Affairs.

Cyware News - Latest Cyber News

Fake Trezor data breach emails used to steal cryptocurrency wallets

Trezor hardware wallet owners recently began receiving data breach notifications prompting recipients to download a fake Trezor Suite software that would steal their recovery seeds.

Security Affairs

Mar 27 - Apr 02 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. Apr 02 - Anonymous leaked 15 GB of data allegedly stolen from the Russian Orthodox Church Anonymous claims to have hacked the Russian Orthodox Church 's charitable wing and leaked 15 GB of alleged stolen [...] The post Mar 27 - Apr 02 Ukraine - Russia the silent cyber conflict appeared first on Security Affairs.

Cyware News - Latest Cyber News

Vulnerabilities and cyberattacks that marked the year 2021

A new report from Rapid7 highlights 50 vulnerabilities from 2021 that posed a considerable risk to businesses of all sizes. Of those 50 vulnerabilities, 43 were exploited in the wild.

Security Affairs

Borat RAT, a new RAT that performs ransomware and DDoS attacks

Cyble researchers discovered a new remote access trojan (RAT) named Borat capable of conducting DDoS and ransomware attacks. Researchers from threat intelligence firm Cyble discovered a new RAT, named Borat, that enables operators to gain full access and remote control of an infected system. Unlike other RATs, the Borat RAT provides Ransomware and DDOS services [...] The post Borat RAT, a new RAT that performs ransomware and DDoS attacks appeared first on Security Affairs.

Cyware News - Latest Cyber News

Documents reveal financial fallout of Salt Lake City IT security breach

That document, obtained by the KSL Investigators through a public records request, states more than 150 databases and all public safety software systems were reviewed for potential compromises but, "none have been found."

The Hacker News

Experts Shed Light on BlackGuard Infostealer Malware Sold on Russian Hacking Forums

A previously undocumented "sophisticated" information-stealing malware named BlackGuard is being advertised for sale on Russian underground forums for a monthly subscription of $200. "BlackGuard has the capability to steal all types of information related to Crypto wallets, VPN, Messengers, FTP credentials, saved browser credentials, and email clients," Zscaler ThreatLabz researchers Mitesh Wani

Cyware News - Latest Cyber News

FBI Warns of Ransomware Attacks Targeting Local Governments

The Federal Bureau of Investigation (FBI) this week warned local government entities of ransomware attacks disrupting operational services, causing public safety risks, and causing financial losses.

Cyware News - Latest Cyber News

The CISO as brand enabler, customer advocate, and product visionary

The CISO role has never been cut-and-dry. Despite its longevity, this role is still in its adolescence - full of promise, mostly headed in the right direction, but not quite fully formed.

Twitter

KatieMoussouris (she/her)

Nothing keeps me up like thinking about how doctoral theses, especially in technology, specifically in cyber security, are the work of students who likely have zero actual hands on work experience in the professional field they are studying. And neither do their thesis advisors.

Spiros Margaris

How #Deepfakes and #AI-generated #faces are corroding #trust in the web #fintech #ArtificialIntelligence #MachineLearning #DeepLearning #cybersecurity @thesundaytimes @Shirastweet @m49D4ch3lly @mclynd @missdkingsbury @ChuckDBrooks @digitalcloudgal

KatieMoussouris (she/her)

In the top 10 ranked undergrad Computer Science programs in the US, none of them require CyberSecurity courses to graduate. (Reply trolls can look up refs in my past Congressional testimony or do their own research) Academics: This isnt a personal insult nor is it aimed at you

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

Nothing today

Source: Hybrid Analysis

Top malicious files

100% Threat score — lcp.exe

100% Threat score — 9350177924ad43cad718e0e15acc4cd955a004a55b5690875b4f2973f0cbdadc.exe

100% Threat score — 96538536.exe

100% Threat score — tmp5ab8krte

100% Threat score — documentaciÃ³n 83.xls

100% Threat score — BetaTest.exe

98% Threat score — IDM_6.4x_Crack_v17.9.exe

95% Threat score — 1.exe

87% Threat score — tmprmwkpgx8

71% Threat score — AcroRead.msi

100% Threat score — ECAP.EXE

100% Threat score — documentaciÃ³n 83.xls

100% Threat score — f98898df74fb2b2fad3a2ea2907086397b36ae496ef3f4454bf6b7125fc103b8.exe

100% Threat score — IMG_1283_Album-So-Yeon-Ha-Lonely-In-Car_Full_5543954399348_1238127589124_348958349054_12381902839012839012

100% Threat score — documentaciÃ³n 83.xls

100% Threat score — BOLTZE ORDER BE99007561 & BOLTZE ORDER DATA SHEET.exe

97% Threat score — KormanSOA_1.xlsx

94% Threat score — nodhide_unpacked.ExE

86% Threat score — e30515d57ee5610a4cc904c94ba3df4e3eca48f6

Source: Hybrid Analysis

Top malicious URL

100% Threat score — http://adamant.finance/

77% Threat score — http://node.minepi.com/

73% — http://ichamber.net/data/elvis/kbpanel/

79% Threat score — http://midstdefine.xyz/

74% Threat score — http://fegcharts-api.fegex.com/

72% Threat score — https://app.getresponse.com/click.html?x=a62b&lc=SZTp9x&mc=rO&s=BtPsp59&u=MGtll&z=EMidwx6

Threat score

72%
Threat score
http://infoscert.net/links/kbpanel/

72%
Threat score
https://greatedu.edu.np/NewestUpdate/?email=patrick.vanlommel%40syncreon.com

72%
Threat score
https://app.getresponse.com/click.html?x=a62b&lc=SZTp9x&mc=rW&s=BtPspsl&u=MGtll&z=EMirS63

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 Uruguay

#9 Brazil

#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 India

#3 United States of America

#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 Germany

#3 Netherlands	#4 Russia
#5 United Kingdom	#6 Singapore
#7 Japan	#8 Australia
#9 France	#10 Hong Kong

Source: Have I been pwned?

Have I been pwnd

Nothing today

Source: Imperva DDOS Map

Top DDOS attackers

- **United States (30%)**
- **Germany (12%)**
- **Singapore (10%)**

Source: Imperva DDOS Map

Top DDOS country targets

- **Russia (30%)**
- **South Korea (18%)**
- **United States (16%)**

Source: Imperva DDOS Map

Top DDOS techniques

57%	**DDoS**
32%	**Automated Threat**
10%	**OWASP**

Source: Imperva DDOS Map

Top DDOS industry targets

41%	**Financial Services**
19%	**Business**
15%	**Law & Government**