Your Security Rabbits report for April 10, 2022

Source: Ransom Watch

Ransomware attacks

clop	ALEXIM.COM	clop	BOLTONUSA.COM
clop	EDAN.COM	lockbit2	https://groupem...
lockbit2	l	clop	MCH-GROUP.COM
lockbit2	sadeco.fr	lockbit2	spirit-ord.com
lockbit2	www.farmaciasta...	lockbit2	anasia.co
lockbit2	clinique.cob-os...	clop	ENPRECIS.COM
clop	SWIRESPO.COM		

Hot topics

Nothing today

News

Security Affairs

A DDoS attack took down Finnish govt sites as Ukraine's President addresses MPs

A massive DDoS attack took down Finnish government websites while Ukrainian President Zelenskyy addressed Finland's members of parliament (MPs). On April 8, a denial-of-service attack took down the websites of the Finnish ministries of Defense and Foreign Affairs. The attack started at about noon, while Ukrainian President Zelenskyy addressed Finland's members of parliament (MPs). "A [...] The post A DDoS attack took down Finnish govt sites as Ukraine's President addresses MPs appeared first on Security Affairs.

Cyware News - Latest Cyber News

Chinese Group Expands its Attack Scope Across the Globe

Cicada or APT10 is targeting organizations across different sectors, including government, legal, religious, and NGOs, in an ongoing espionage campaign that began months ago. Multiple attacks were spotted on Microsoft Exchange Servers, suggesting exploitation of a known or unpatched vulnerability to gain access to victim networks.

Cyware News - Latest Cyber News

FFDroider Slurps Browser Cookie to Get Inside Your Social Media

Security researchers discovered a new information stealer named FFDroider that steals credentials and cookies stored in browsers in order to hijack victims' social media accounts. FFDroider spreads via software cracks, games, free software, and files downloaded from

Security Affairs

China-linked threat actors target Indian Power Grid organizations

China-linked threat actors continue to target Indian power grid organizations, most of the attacks involved the ShadowPad backdoor. Recorded Future's Insikt Group researchers uncovered a campaign conducted by a China-linked threat actor targeting Indian power grid organizations. The security firm is tracking this cluster of malicious activities under the moniker Threat Activity Group 38 aka [...] The post China-linked threat actors target Indian Power Grid organizations appeared first on Security Affairs.

Security Affairs

Facebook blocked Russia and Belarus threat actors' activity against Ukraine

Facebook/Meta said Russia-linked threat actors are attempting to use the social network against Ukraine with hate speech, bullying, and fake news. Facebook/Meta revealed that Russia-linked threat actors are attempting to weaponize the social network to target Ukraine. The company blocked about 200 accounts operated from Russia that were used to falsely report people for various [...] The post Facebook blocked Russia and Belarus threat actors' activity against Ukraine appeared first on Security Affairs.

Security Affairs

NB65 group targets Russia with a modified version of Conti's ransomware

NB65 hacking group created its ransomware based on the leaked source code of the Conti ransomware and targets Russia. According to BleepingComputer, NB65 hacking group is targeting Russian organizations with ransomware that they have developed using the leaked torrent sites. Users are advised to upload their downloads to VirusTotal to check if the download files or software are genuine or malicious.

Security Affairs

SharkBot Banking Trojan spreads through fake AV apps on Google Play

Experts discovered malicious Android apps on the Google Play Store masqueraded as antivirus solutions spreading the SharkBot Trojan. Researchers from the Check Point Research (CPR) team discovered several malicious Android apps on the official Google Play Store masqueraded as antivirus solutions that were used to deliver the SharkBot banking Trojan. Sharkbot is an information stealer steals used [...] The post SharkBot Banking Trojan spreads through fake AV apps on Google Play appeared first on Security Affairs.

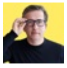
source code of the Conti ransomware. The NB65 hacking group, since the beginning of the invasion, the [...] The post NB65 group targets Russia with a modified version of Conti's ransomware appeared first on Security Affairs.

Cyware News - Latest Cyber News

Ukraine CERT Warns of Increasing Attacks by Armageddon Group

Ukraine CERT warned against a spear-phishing campaign by Russia-linked Armageddon APT. While one campaign targets Ukrainian organizations, the other focuses on government agencies in the EU. Concerned organizations are recommended to follow the guideline at the CERT-UA site for countermeasures.

Twitter



Spiros Margaris

Why your #bank knows exactly how you hold your #phone #fintech #banking #cybersecurity @davidbyers26 @George_Nixon97 @thetimes @Shirastweet @m49D4ch3lly @mclynd @missdkingsbury @ChuckDBrooks @digitalcloudgal @cgledhill @Visible_Banking @natashakyp

Jan Achakzai /

#PTI' social media prowess becoms a cyber security threat: -can malign any institution, job 4 Indian cyber world. -has a team in Singapore. Pak's cyber capability pales in comparison 2 #Indiabut also PTI, (re FIA' cyber unit has 150,0000 complaints tasked 2 few officers)

The Daily Beast

A cybersecurity expert promised one of his clients help in setting up a security system. It ended up costing the client nearly $600,000.

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
EZFNCore_2,0,0,8,exe

100%
Threat score
tmpoj6ftn_5

100%
shipaudit,exe

100%
setup,exe

Threat score		Threat score	
100% Threat score	checksusp,exe	100% Threat score	loaded_03f74ac49d5a8f69054e8265d1d7f0e4550000b9db6a7e65179ac737f41d072f_1
100% Threat score	^57433,exe	100% Threat score	Server,exe
100% Threat score	tmp56ptc4lz	100% Threat score	Viewbot,exe
100% Threat score	ESET MOBILE SECURITY & ANTIVIRUS V7,3,8,0 [PREMIUM],apk	100% Threat score	tmp2yycujcq
100% Threat score	CoinBase Checker,exe	100% Threat score	X0u,exe
100% Threat score	2022-03-01_1100,xlsm	100% Threat score	31AA8EC187E1241A94127336996F9CB38719EB9B
100% Threat score	tmpjdjhlfgh	100% Threat score	tmp6se6nx0h
92% Threat score	tmpez944n_0	87% Threat score	tmpaxmktxjt
85% Threat score	wakan_full_167,exe	85% Threat score	Supremo,exe
85% Threat score	iQIYI Video â€“ Dramas Movies_v6,3,0_apkpure,com,apk	85% Threat score	actiplay-build,exe
80% Threat score	FlexASIO,GUIInstaller_0,32,exe		

Source: Hybrid Analysis

Top malicious URL

100% Threat score	https://znzhou,top/wp-admin/5384_0163087/	86% Threat score	http://111,90,150,43/%206384691420130320,dat
79% Threat score	https://bit,ly/3JpFXp4		

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 Viet Nam

#7 Algeria

#8 Brazil

#9 Pakistan

#10 Venezuela (Bolivarian Republic of)

Source: SpamHaus

Top phishing countries

#1 United States

#2 Netherlands

#3 United Kingdom

#4 Singapore

#5 Australia

#6 Russia

#7 India

#8 Germany

#9 Bulgaria

#10 Belize

Source: Have I been pwned?

Have I been pwnd

Nothing today

Source: Imperva DDOS Map

Top DDOS attackers

United States (31%)

Germany (17%)

Netherlands (8%)

Source: Imperva DDOS Map

Top DDOS country targets

Russia (40%)

United States (20%)

Ukraine (14%)

Source: Imperva DDOS Map

Top DDOS techniques

51%	**DDoS**
36%	**Automated Threat**
13%	**OWASP**

Source: Imperva DDOS Map

Top DDOS industry targets

44%	**Financial Services**
20%	**Business**
9%	**Computing & IT**