



Your Security Rabbits report for April 17, 2022

Source: [Ransom Watch](#)


Ransomware attacks

conti	Ministerio de Hacienda - Rep�blica de Costa Rica	clop	SA1SOLUTIONS.COM
clop	SLIMSTOCK.COM	clop	SSMSJUSTICE.COM
conti	Tucker Door & Trim	clop	ZISSERFAMILYLAW.COM
clop	ALTERNATIVETECHS.COM	clop	DRC-LAW.COM
clop	DRIVEANDSHINE.COM	clop	FAIR-RITE.COM
clop	JBINSTANTLAWN.NET	clop	JDAVIDTAXLAW.COM
clop	OAKDELL.COM	clop	ORBITELECTRIC.COM
everest	Standard Building Supplies Ltd,		



Hot topics

Nothing today

News

 The Hacker News	Get Lifetime Access to This 60-Hour Java Programming Training Bundle @ 97% Discount Java is a very versatile programming language. From Android apps to Oracle databases, it can be used to power a wide range of software and systems. As with most technical skills, the best way to learn Java is through building your own projects. But you can definitely speed things up with high-quality training. The Complete 2022 Java Coder Bundle provides plenty of that -- nine full-length video	 Security Affairs	The unceasing action of Anonymous against Russia This week the Anonymous collective and its affiliates have targeted multiple Russian organizations stealing gigabytes of data. This week Anonymous and other hacker groups affiliated with the collective have launched multiple attacks against Russian government agencies and organizations. The week started with the announcement of the hack of Russia's Ministry of Culture, Anonymous leaked 446 [...] The post The unceasing action of Anonymous against Russia appeared first on Security Affairs.
 Security Affairs	Threat actors target the Ukrainian gov with IcedID malware Threat actors are targeting Ukrainian government agencies with phishing attacks delivering the IcedID malware. The Ukrainian Computer Emergency Response Team (CERT-UA) uncovered new phishing campaigns aimed at infecting systems of Ukrainian government agencies with the IcedID malware. IcedID banking trojan first appeared in the threat landscape in 2017, it has capabilities similar to other financial threats [...] The post Threat actors target the Ukrainian gov with IcedID malware appeared first on Security Affairs.	 Security Affairs	U.S. Gov believes North Korea-linked Lazarus APT is behind Ronin Validator cyber heist The U.S. government blames North Korea-linked APT Lazarus for the recent \$600 million Ronin Validator cyber heist. The U.S. government attributes the recent \$600 million Ronin Validator cryptocurrency heist to the North Korea-linked APT Lazarus. The U.S. Treasury announced in a notice the sanctions against the Ethereum address used by the APT to receive the [...] The post U.S. Gov believes North Korea-linked Lazarus APT is behind Ronin Validator cyber heist appeared first on Security Affairs.

Twitter

 Government of Rajasthan	Ecosystem #_ 2022-23 Center for Cyber Security #_	 Spiros Margaritis	The #BusinessCase For Simplifying #Cybersecurity #fintech #insurtech #insurance @ForcepointSec @Shirastweet @m49D4ch3lly @mclynd @missdkingsbury @ChuckDBrooks @digitalcloudgal @ScottBVS
---	---	--	---

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	faw.apk	100% Threat score	8e24803de9d71899f4e146569462b15f42c0c2d19529482c9e67a2e9d39db374.apk
100% Threat score	PurgeStealer.exe	96% Threat score	mernis.exe
92% Threat score	NP Manager v3.0.37.apk	86% Threat score	auto driver installation(1).exe
78% Threat score	Samsung Pass ìžē™ ì™„ì„± (com.samsung.android.samsungpassautofill)-3.0.03.1(300301000)-SamsungPassAutofill_v1.apk	75% Threat score	Kiwi-20191007091034-arm64.apk







Source: *Hybrid Analysis*

Top malicious URL

93% Threat score	http://42.224.90.239:38774/Mozi.a	93% Threat score	http://115.53.224.245:47166/bin.sh
93% Threat score	http://117.196.51.9:39036/Mozi.m	91% Threat score	http://171.38.220.77:55631/Mozi.a
91% Threat score	http://123.14.81.77:56939/i	91% Threat score	http://115.58.89.28:47141/Mozi.m
88% Threat score	http://117.194.171.61:44248/Mozi.m	86% Threat score	http://192.72.17.236:54374/Mozi.m
75% Threat score	http://www.chalbo.in/	73% Threat score	https://taylorhicks.ning.com/photo/watch-hdstream

Source: *SpamHaus*








Top spamming countries

 #1 United States of America	 #2 China
 #3 Russian Federation	 #4 Mexico
 #5 Dominican Republic	 #6 Saudi Arabia
 #7 Uruguay	 #8 India
 #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	 #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
---	--

	bulletproof Chinese & Russian web hosting.		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 United States of America
	#3 India		#4 Indonesia
	#5 Thailand		#6 Viet Nam
	#7 Algeria		#8 Brazil
	#9 Pakistan		#10 Japan

Source: [SpamHaus](#)

Top phishing countries

	#1 United States		#2 Germany
	#3 Japan		#4 Sweden
	#5 Hong Kong		#6 Russia
	#7 Canada		#8 France
	#9 Australia		#10 Netherlands

Source: [Have I been pwnd?](#)

Have I been pwnd

Nothing today

Source: [Imperva DDOS Map](#)

Top DDOS attackers

Source: [Imperva DDOS Map](#)

Top DDOS country targets

Source: [Imperva DDOS Map](#)

Top DDOS techniques

Source: [Imperva DDOS Map](#)

Top DDOS industry targets