Your Security Rabbits report for April 03, 2022

Source: Ransom Watch

Ransomware attacks

lockbit2	bazzisrl.it	clop	BOLTONUSA.COM
clop	DUTTONFIRM.COM	lockbit2	eksltd.com
lockbit2	fec-corp.com	midas	New Company 04.2022
clop	SWIRESPO.COM	conti	Ackerman Plumbing
clop	ENPRECIS.COM		

Hot topics

Nothing today

News

Security Affairs

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 data. Anonymous continues to target Russian government entities and private businesses, this week the group claimed to have hacked the private firms Thozis Corp and Marathon Group owned by oligarchs. Now the collective announced the hack of the [...] The post Anonymous leaked 15 GB of data allegedly stolen from the Russian Orthodox Church appeared first on Security Affairs.

Security Affairs

Beastmode Mirai botnet now includes exploits for Totolink routers
Operators behind the Mirai-based distributed denial-of-service (DDoS) botnet Beastmode (aka B3astmode) added exploits for Totolink routers. The Mirai-based distributed denial-of-service (DDoS) botnet Beastmode (aka B3astmode) now includes exploits for Totolink routers. Like most DDOS botnets, Beastmode attempt to infect other devices by launching brute-forcing attacks or exploiting multiple vulnerabilities. Between February and March 2022, researchers from the FortiGuard Labs [...] The post Beastmode Mirai botnet now includes exploits for Totolink routers appeared first on Security Affairs.

Cyware News - Latest Cyber News

Hive Ransomware Evolves to Add Many New Features
Hive is a relatively new ransomware outfit that made its appearance in late June 2021. It gained notoriety through over 350 attacks on organizations across several sectors.

Cyware News - Latest Cyber News

Supply Chain Attacks Against Open-Source Software Soar
Towards the beginning of March, researchers from Sonatype identified hundreds of counterfeit packages in npm and PyPI repositories that were used to execute Remote Access Trojans (RATs).

Security Affairs

UK Police charges two teenagers for their alleged role in the Lapsus$ extortion group
The City of London Police charged two of the seven teenagers who were arrested for their alleged role in the LAPSUS$ data extortion gang. The duo has been released on bail after appearing in the Highbury Corner Magistrates Court court on Friday. The City of London Police charged two of the seven teenagers recently arrested [...] The post UK Police charges two teenagers for their alleged role in the Lapsus$ extortion group appeared first on Security Affairs.

Security Affairs

Ukraine intelligence leaks names of 620 alleged Russian FSB agents
The Ukrainian Defense Ministry's Directorate of Intelligence leaked personal data belonging to 620 alleged Russian FSB agents. The Ukrainian Defense Ministry's Directorate of Intelligence has leaked the alleged personal data of 620 Russian FSB officers. Personal details leaked by the Ukrainian body include names, phone numbers, addresses, vehicle license plates, SIM cards, date and location [...] The post Ukraine intelligence leaks names of 620 alleged Russian FSB agents appeared first on Security Affairs.

Twitter

Dr. Dp Awjd

5 reasons to become a Cyber Security Analyst or Consultant in 2022: Very decent salary Tackle different challenges Great career with diverse prospects Opportunity to do impactful work Excellent demand on the market What did I miss?

KY Secretary of State Michael Adams

The self-described cybersecurity expert conducting an election misinformation tour says the tour's site has - wait for it - been hacked. Can't make this stuff up, folks.

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

LouisColumbus

Nvidia is bringing zero trust security into data centers #cybersecurity #DataCenters #ZeroTrust #ZeroTrustSecurity #ZTNA $NVDA

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

CVE-2022-1210

A vulnerability **classified** as problematic was found in **LibTIFF** 4.3.0. Affected by this vulnerability is the TIFF File Handler of tiff2ps. Opening a malicious file leads to a denial of service. The attack can be launched remotely but requires user interaction. The exploit has been disclosed to the public and may be used.

UNRATED Vector: unkown Created: 2022-04-03 Updated: 2022-04-03

CVE-2022-0088

Cross-Site Request Forgery (CSRF) in **GitHub** repository yourls/yourls prior to 1.8.3.

UNRATED Vector: unkown Created: 2022-04-03 Updated: 2022-04-03

CVE-2022-28368

Dompdf 1.2.1 allows remote code execution via a .php file in the src:url field of an @font-face Cascading Style Sheets (CSS) statement (within an HTML input file).

UNRATED Vector: unkown Created: 2022-04-03 Updated: 2022-04-03

CVE-2022-28376

Verizon LVSKIHP 5G outside devices through 2022-02-15 allow anyone (knowing the device's serial number) to access a CPE admin website, e.g., at the 10.0.0.1 IP address. The password (for the verizon username) is calculated by concatenating the serial number and the **model** (i.e., the LVSKIHP string), running the sha256sum program, and extracting the **first** seven characters concatenated with the **last** seven characters of that SHA-256 value.

UNRATED Vector: unkown Created: 2022-04-03 Updated: 2022-04-03

Source: Hybrid Analysis

Top malicious files

100% Threat score	DevID_agent_installer_1883080084.exe	100% Threat score	tmplric7rlg
100% Threat score	tmp0lzyv5j2	100% Threat score	system.apk
100% Threat score	Client.exe	100% Threat score	å¦‚æœˆçœŸç¾ã®è²¨æ‰.exe
100% Threat score	tmpo_njvwux	100% Threat score	launcher-disbalancer-go-client-windows-amd64.exe
100% Threat score	roblox-script--new-full-2022.exe	100% Threat score	Amir Antivirus.exe
100% Threat score	keygen.exe	100% Threat score	6fe99e1ad9f91735ffecf032c4bc4f57a16a21f104a34442381b23b259fd9c9c.exe
100% Threat score	tmpo36ajl1d	100% Threat score	tmphtooarsc
100% Threat score	tmpr3nkgfcb	100% Threat score	rockstar.gen.22.exe
99% Threat score	aef610b66b9efd1fa916a38f8ffea8b988c20c5deebf4db83b6be63f7ada2cc0.exe	97% Threat score	xmogum.x86
94% Threat score	_HeartSender_.exe	92% Threat score	Busuu_v22.9.1.703(348728).apk
85% Threat score	setup-cyowcopy-1.9.0.822-x64.exe	85% Threat score	GoodSync.exe
81% Threat score	swishMax4.exe	78% Threat score	tmpceigbirt
77% Threat score	GoodSync.exe	76% Threat score	gsync.exe
75% Threat score	Office365 - Activation.html		

Source: Hybrid Analysis

Top malicious URL

100% Threat score	https://mlcrosoft.site/msdn.cpp	100% Threat score	http://osrq.xyz/fre
100% Threat score	http://www.suncitycamp.com/	100% Threat score	http://osrq.xyz/dtf/b
100% Threat score	http://ape.run/dtf/b	95% Threat score	http://117.221.185.219:48385/Mozi.m
95% Threat score	http://117.217.150.249:38948/bin.sh	91% Threat score	http://182.121.51.177:36338/Mozi.m

82% Threat score	http://medjrnlscholarexplore.biz/submit-manuscript.php?journal=17	77% Threat score	http://makemoney4.elementfx.com/gxdvtg/
77% Threat score	http://khassidaenpdf.free.fr/	77% Threat score	http://mqcfr.smtpgaze.com/tracking/qaR9ZGLlZQ
77% Threat score	http://ngkz.luzodnmedia.com/nrfdr.html#YS5hcmlvbmVAaW5haWwuaXQ%3D%26amp%3Brecovery%3DstopRecovery	77% Threat score	http://rvymu.smtpgaze.com/tracking/qaR9ZGLlZG
77% Threat score	http://kreb.xyz/fre	74% Threat score	http://ape.run/fre
74% Threat score	http://hansol1.zzz.com.ua/index.php	74% Threat score	https://u26027317.ct.sendgrid.net/wf/unsubscribe 2B0zU7Gj6e4dViObYCBYQA7HKS6j8cXRjtIPv6rr 2BduvNUUrel12HXNySVoV4bTLvju0yqPeqZKbh 2BAKVHd6CGVqyl5cSHKFhUqfyvAlqMyo5eQ9I1
72% Threat score	http://rdlqx.smtpgaze.com/tracking/qaR9ZGLlZGDmAQt1ZGDmZGZ1BQD2APM5qzS4qaR9ZQbjIt	72% Threat score	http://bqcld.smtpgaze.com/tracking/qaR9ZGLlZQ
72% Threat score	http://jvwws.smtpgaze.com/tracking/qaR9ZGLlZGN0ZGDjBGHjBGZ2AmtjBPM5qzS4qaR9ZQbjDD	72% Threat score	http://madqb.smtpgaze.com/tracking/qaR9ZGLlZ
72% Threat score	http://eofbq.smtpgaze.com/tracking/qaR9ZGLlZGtlAQt3AmR0AmV3AGV2APM5qzS4qaR9ZQbjJD	72% Threat score	http://tmksa.smtpgaze.com/tracking/qaR9ZGLlZG
72% Threat score	http://ggcey.smtpgaze.com/tracking/qaR9ZGLlZGH3AwD5AGt3AGNmBGVmZvM5qzS4qaR9ZQbjIN		

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 Russia
- #3 Netherlands
- #4 Germany
- #5 Singapore
- #6 Japan
- #7 South Korea
- #8 Portugal
- #9 Australia
- #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 (19%)**
- **Singapore (10%)**

Source: Imperva DDOS Map

Top DDOS country targets

- **Russia (39%)**
- **United States (18%)**
- **Ukraine (17%)**

Source: Imperva DDOS Map

Top DDOS techniques

55%	**DDoS**
33%	**Automated Threat**
12%	**OWASP**

Source: Imperva DDOS Map

Top DDOS industry targets

50%	**Financial Services**
22%	**Business**
8%	**Computing & IT**