Your Security Rabbits report for April 07, 2022

Hot topics

Nothing today

Source: Ransom Watch

Ransomware attacks

hiveleak	FCCH	conti	Barwick Bathroom Distribution LLP
ragnarlocker	International Centre Leaked	lorenz	Keicorp(ICPM)
lockbit2	rnrinc.com	lockbit2	toothbuds.com
everest	United States of America GOV	lockbit2	wania.at

Source: NIST

NIST CVE: Critical

Nothing today

News

Threatpost

Attackers Spoof WhatsApp Voice-Message Alerts to Steal Info
Threat actors target Office 365 and Google Workspace in a new campaign, which uses a legitimate domain associated with a road-safety center in Moscow to send messages.

Cyware News - Latest Cyber News

Australia warns of money recovery phishing luring past victims
According to the Australian Competition & Consumer Commission, the losses reported in Q1 2022 are estimated to be $270,000 (up by 301% compared to 2021), which add up to losses incurred by victims who previously fell for the same type of scam.

IT Security Guru

Cash App notifies 8 million customers of data breach
Cash App, a popular stock trading app, has suffered a data breach impacting up to 8.2 million former and current users. It has been reported that the breach was caused by a former employee illegitimately accessing customer information. Block, Cash App's owner, notified the Security and Exchange Commission (SEC) of the breach on Monday. The filing [...] The post Cash App notifies 8 million customers of data breach appeared first on IT Security Guru.

Cyware News - Latest Cyber News

Digital transformation requires security intelligence
It's no surprise that many organizations are struggling with how to best manage their data and secure it, especially when data and systems reside not only in separate siloes, but within different teams, on-premises, and in the cloud.

Cyware News - Latest Cyber News

Fake Android Shopping Applications Steal Bank Account Logins, 2FA Codes
On Wednesday, ESET's cybersecurity team published new research documenting three separate fake apps targeting customers who belong to eight Malaysian banks to steal their account logins.

WeLiveSecurity

Fake e-shops on the prowl for banking credentials using Android malware
ESET researchers analyzed three malicious applications targeting customers of eight Malaysian banks The post Fake e-shops on the prowl for banking credentials using Android malware appeared first on WeLiveSecurity

IT Security Guru

Germany closes Russian "Hydra" darknet marketplace
The Hydra Market, a Russian-language darknet marketplace formerly specialising in the sale of illicit drugs, forged documents, intercepted data and illegal digital service, has been shut down by German Federal police. Working in conjunction with the United States Justice Department, authorities closed German servers of the marketplace on Tuesday, seizing $25m in Bitcoin of alleged [...] The post Germany closes Russian "Hydra" darknet marketplace

Cyware News - Latest Cyber News

Australia to develop a data security framework
The Australian Department of Home Affairs has commenced work on a new national data security action plan as part of the federal government's wider digital economy strategy.

Security Affairs

Block discloses data breach involving Cash App potentially impacting 8.2 million US customers
Block disclosed a data breach related to the Cash App investing app and is notifying 8.2 million current and former US customers. The data breach involved a former employee that downloaded some unspecified reports of its Cash App Investing app that contained some U.S. customer information. Cash App is an app that allows users to [...] The post Block discloses data breach involving Cash App potentially impacting 8.2 million US customers appeared first on Security Affairs.

Cyware News - Latest Cyber News

Dell ships patch for vulnerable filesystem
The most critical of the vulnerabilities, with a CVSS score of 9.1, is CVE-2022-26851. Affected versions of the PowerScale OneFS software contain "a predictable file name from observable state".

IT Security Guru

Electric vehicle chargers hacked to show pornography
Electric vehicle owners in the Isle of Wight, UK, were surprised yesterday when public charging points displayed pornography. Service screens at the council-owned car parks across Quay Road, Cross Street, Cowes and Moa Place, Freshwater were supposed to display the council website, but hackers changed several of them to show explicit images. The Isle of [...] The post Electric vehicle chargers hacked to show pornography appeared first on IT Security Guru.

ZDNet | security RSS

Fake Android shopping apps steal bank account logins, 2FA codes
Customers of Malaysian banks are being turned into cash cows.

The Hacker News

FBI Shut Down Russia-linked "Cyclops Blink" Botnet That Infected Thousands of Devices
The U.S. Department of Justice (DoJ) announced that it neutralized Cyclops Blink, a modular botnet controlled by a threat actor known as Sandworm, which has been attributed to the Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU). "The operation copied and removed malware from vulnerable internet-connected firewall devices that Sandworm used

The Hacker News

Hackers Distributing Fake Shopping Apps to Steal Banking Data of Malaysian Users
Threat actors have been distributing malicious applications under the guise of seemingly harmless shopping apps to target customers of eight Malaysian banks since at least November 2021. The attacks involved setting up fraudulent but legitimate-looking websites to trick users into downloading the apps, Slovak cybersecurity firm ESET said in a report shared with The Hacker News. The

appeared first on IT Security Guru.

Cyware News - Latest Cyber News

Hackers flood internet with what they say are Russian companies' files
Since Russia's invasion of Ukraine, Distributed Denial of Secrets team has been inundated with files that hacktivists say they've stolen from Russian banks, energy companies, government agencies and media companies.

Cyware News - Latest Cyber News

India: China Cyber Attack On Power Grid Near Ladakh, Minister Says Hack Failed
The attacks took place between August last year and March, sources said. The investigation found the data passing in and out of Indian Load Despatch Centres to the Chinese state-sponsored C2 servers spread across the world, researchers said.

ZDNet | security RSS

Israeli officials are being catfished by AridViper hackers
APT-C-23 is targeting high-ranking individuals in defense, law, and emergency services.

Cyware News - Latest Cyber News

New Denonia Malware Targets AWS Lambda Environments
Lambda is a scalable compute service offered by Amazon Web Services (AWS) for running code, server and OS maintenance, capacity provisioning, logging, and operating numerous backend services.

The Hacker News

Researchers Uncover How Colibri Malware Stays Persistent on Hacked Systems
Cybersecurity researchers have detailed a "simple but efficient" persistence mechanism adopted by a relatively nascent malware loader called Colibri, which has been observed deploying a Windows information stealer known as Vidar as part of a new campaign. "The attack starts with a malicious Word document deploying a Colibri bot that then delivers the Vidar Stealer," Malwarebytes Labs said in an

Cyware News - Latest Cyber News

Texas Department of Insurance Exposed Data of 1.8 Million People
The exposed information includes names, addresses, phone numbers, dates of births, and partial or full social security numbers, as well as information about injuries and worker compensation claims.

ZDNet | security RSS

This new malware targets AWS Lambda environments
Denonia malware is abusing servers to run cryptocurrency miners.

Security Affairs

Ukraine warns of attacks aimed at taking over Telegram accounts
Ukraine's technical security and intelligence service warns of threat actors targeting aimed at gaining access to users' Telegram accounts. State Service of Special Communication and Information Protection (SSSCIP) of Ukraine spotted a new wave of cyber attacks aimed at gaining access to users' Telegram accounts. The Ukrainian CERT attributes the hacking campaign to threat actors [...] The post Ukraine warns of attacks aimed at taking over Telegram accounts appeared first on Security Affairs.

Cyware News - Latest Cyber News

Ukraine Warns of Cyberattack Aiming to Hack Users' Telegram Messenger Accounts
The URL, in reality a phishing domain, prompts the victims to enter their phone numbers as well as the one-time passwords sent via SMS that are then used by the threat actors to take over the accounts.

CyberScoop

US says it disrupted Russian botnet 'before it could be weaponized'
Officials attributed the botnet, called Cyclops Blink, to Russia's GRU, which has a long history of high-profile cyberattacks. The post US says it disrupted Russian botnet 'before it could be weaponized' appeared first on CyberScoop.

The Hacker News

VMware Releases Critical Patches for New Vulnerabilities Affecting Multiple Products
VMware has released security updates to patch eight vulnerabilities spanning its products, some of which could be exploited to launch remote code execution attacks. Tracked from CVE-2022-22954 to CVE-2022-22961 (CVSS scores: 5.3 - 9.8), the issues impact VMware Workspace ONE Access, VMware Identity Manager, VMware vRealize Automation, VMware Cloud Foundation, and vRealize Suite Lifecycle Manager

copycat

Cyware News - Latest Cyber News

How often do developers push vulnerable code?
According to a report by Tromzo, 42% of developers push vulnerable code once per month. Developers fix only 32% of known vulnerabilities. 33% believe that developers and security are siloed.

Blog â€“ Flashpoint

ISIS Attacks, March 2022: Key Trends, Statistics, and Geographic Analysis
The following research is based on information gathered by Flashpoint analysts and data collections. For February's report, click here. Key takeaways: March 2022 ISIS attacks Nigeria has now fully cemented itself as, far and away, the country with the most claimed ISIS attacks in a month-to-month period. ISIS claimed responsibility for two high-profile attacks by [...] The post ISIS Attacks, March 2022: Key Trends, Statistics, and Geographic Analysis appeared first on Flashpoint.

Cyware News - Latest Cyber News

Microsoft detects Spring4Shell attacks across its cloud services
Microsoft said that it's currently tracking a "low volume of exploit attempts" targeting the critical Spring4Shell (aka SpringShell) remote code execution (RCE) vulnerability across its cloud services.

Security Affairs

Palo Alto Networks devices affected by CVE-2022-0778 OpenSSL bug
Palo Alto Networks addressed a high-severity OpenSSL infinite loop vulnerability, tracked as CVE-2022-0778, that affects some of its firewall, VPN, and XDR products. In Mid March, OpenSSL released updates to address a high-severity denial-of-service (DoS) vulnerability, tracked as CVE-2022-0778, that affects the BN_mod_sqrt() function used when certificate parsing. The flaw was discovered by the popular Google Project [...] The post Palo Alto Networks devices affected by CVE-2022-0778 OpenSSL bug appeared first on Security Affairs.

Naked Security

Serious Security: Darkweb drugs market Hydra taken offline by German police
Why are Tor sites hard to locate and therefore difficult to take down? We explain in plain English...

Krebs on Security

The Original APT: Advanced Persistent Teenagers
Many organizations are already struggling to combat cybersecurity threats from ransomware purveyors and state-sponsored hacking groups, both of which tend to take days or weeks to pivot from an opportunistic malware infection to a full blown data breach. But few organizations have a playbook for responding to the kinds of virtual "smash and grab" attacks we've seen recently from LAPSUS$, a juvenile data extortion group whose short-lived, low-tech and remarkably effective tactics are putting some of the world's biggest corporations on edge.

Security Affairs

U.S. Treasury Department sanctions darkweb marketplace Hydra Market
The U.S. Treasury Department sanctioned the Hydra Market, the world's largest and longest-running dark web marketplace. The U.S. Treasury Department sanctioned the darkweb marketplace Hydra Market, the same day Germany's Federal Criminal Police Office, the Bundeskriminalamt (BKA), announced they have shut down the illegal platform. The seizure of the Hydra Market is the result of an international [...] The post U.S. Treasury Department sanctions darkweb marketplace Hydra Market appeared first on Security Affairs.

The Hacker News

Ukraine Warns of Cyber attack Aiming to Hack Users' Telegram Messenger Accounts
Ukraine's technical security and intelligence service is warning of a new wave of cyber attacks that are aimed at gaining access to users' Telegram accounts. "The criminals sent messages with malicious links to the Telegram website in order to gain unauthorized access to the records, including the possibility to transfer a one-time code from SMS," the State Service of Special Communication and

Security Affairs

US dismantled the Russia-linked Cyclops Blink botnet
The U.S. government announced the disruption of the Cyclops Blink botnet operated by the Russia-linked Sandworm APT group. The U.S. government announced that it had dismantled the Cyclops Blink botnet operated by the Russia-linked Sandworm APT group. "The Justice Department today announced a court-authorized operation, conducted in March 2022, to disrupt a two-tiered global botnet [...] The post US dismantled the Russia-linked Cyclops Blink botnet appeared first on Security Affairs.

Security Affairs

VMware addressed several critical vulnerabilities in multiple products
VMware fixed critical vulnerabilities in multiple products that could be exploited by remote attackers to execute arbitrary code. VMware has addressed critical remote code vulnerabilities in multiple products, including VMware's Workspace ONE Access, VMware Identity Manager (vIDM), vRealize Lifecycle Manager, vRealize Automation, and VMware Cloud Foundation products. The virtualization giant urges its customers to address [...] The post VMware addressed several critical vulnerabilities in multiple products appeared first on Security Affairs.

ZDNet | security RSS

VMware warns of critical remote code execution bug in Workspace ONE Access
Other severe vulnerabilities have been resolved.

Zoom paid $1.8 million in bug bounty rewards in 2021
Zoom has awarded researchers $1.8 million in bug bounties over 2021, and $2.4

ZDNet | security RSS

Zoom awarded $1.8 million in bug bounty rewards over 2021
The program has paid out $2.4 million since its launch.

IT Security Guru

million since the programs launch. Bug bounties have emerged as a popular cybersecurity method recently, amidst the industry's skill shortage. Estimates suggest that there will be roughly 3.5 million unfilled job openings by 2025 in the US alone. Zoom has experienced a [...] The post Zoom paid $1.8 million in bug bounty rewards in 2021 appeared first on IT Security Guru.

Twitter

Rinki Sethi

Met with a security vendor and was impressed with their ability to give an overview (no bs and just 2 or 3 slides) and demo all within 30 minutes. This is how all #infosec vendors need to sell. Many vendors waste too much time in the intro. #cybersecurity

Nicole Perlrth

This is what Ive been telling students. Just because you arent technical doesnt mean you cant work in cybersecurity. The technical community has done cybersecurity a disservice by failing to communicate these issues in a way normals understand. We need more translators.

U.S. Secret Service

Today the #SecretService Kansas City Field Office discussed BEC attacks, #crypto and the cybercrime investigative mission of our agency at the SecureWorld 10thAnnual Cybersecurity Conference.

Source: Have I been pwned?

Have I been pwnd

Nothing today

Source: Imperva DDOS Map

Top DDOS attackers

United States (32%)

Germany (13%)

Netherlands (9%)

Source: Imperva DDOS Map

Top DDOS country targets

Russia (40%)

United States (18%)

Ukraine (16%)

Source: Imperva DDOS Map

Top DDOS techniques

56% **DDoS**

30% **Automated Threat**

13% **OWASP**

Source: Imperva DDOS Map

Top DDOS industry targets

46% **Financial Services**

20% **Business**

7% **Computing & IT**

Source: Hybrid Analysis

Top malicious URL

100% Threat score — http://cdn.cloudfronter.com/player/upgrade/ext/20210119/842497c20072fc9b92f2b18e1d690103.exe

91% Threat score — http://42.231.240.169:58267/Mozi.m

91% Threat score — http://182.123.197.247:48902/Mozi.m

78% Threat score — http://fplutility.com/

78% Threat score — https://6ixpr.r.a.d.sendibm1.com/mk/cl/f/vmC59_oUFj1kQ2NzHEQLeURpUFCiAz9zhASgAffmYL6J3N13BxqLVwOJ3pvGHRliI26xyfcHXjDUzRnRm_s4XjUB5mAiGtb7Bnq9okC08gmoJ0v12MOEizlR4hYQTlQtJXtmwSjVALMfQTBBCc1_-8C8y6msS-gwvVCwt-4bmhfDVhorfKaYoY5Rpos_n9e3jgOoAD9KPMWTrZj3YqvNni7XYFX6Ra9pjzpRca2eFro3rNlk0BWuclYMEZtE8YNnI7GTTjk54Lw7TReOyWxdJzzsU

75% Threat score — http://ep6y8ivoul.vitalitaetsapotheke.com.de/

73% Threat score — http://tapestry.tapad.com/tapestry/1?ta_partner_id=950&ta_redirect=http%3A%2F%2Fwww.yojiya.co.jp%2Fls.html

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-2020-27374 — Dr Trust USA iCheck **Connect** BP Monitor BP Testing 118 1.2.1 is vulnerable to a Replay Attack to BP Monitoring.
UNRATED Vector: unkown Created: 2022-04-07 Updated: 2022-04-07

CVE-2020-27373 — Dr Trust USA iCheck **Connect** BP Monitor BP Testing 118 1.2.1 is vulnerable to Plain text command over BLE.
UNRATED Vector: unkown Created: 2022-04-07 Updated: 2022-04-07

CVE-2020-27376 — Dr Trust USA iCheck **Connect** BP Monitor BP Testing 118 version 1.2.1 is vulnerable to Missing Authentication.
UNRATED Vector: unkown Created: 2022-04-07 Updated: 2022-04-07

CVE-2020-27375 — Dr Trust USA iCheck **Connect** BP Monitor BP Testing 118 version 1.2.1 is vulnerable to Transmitting Write Requests and Chars.
UNRATED Vector: unkown Created: 2022-04-07 Updated: 2022-04-07

CVE-2022-27819 — SWHKD 1.1.5 allows unsafe parsing via the -c option. An information leak might occur but there is a simple denial of service (memory exhaustion) upon an attempt to parse a large or infinite file (such as a block or character device).
UNRATED Vector: unkown Created: 2022-04-07 Updated: 2022-04-07

CVE-2022-27818 — SWHKD 1.1.5 unsafely uses the /tmp/swhkd.sock pathname. There can be an information leak or denial of service.
UNRATED Vector: unkown Created: 2022-04-07 Updated: 2022-04-07

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 Japan	#4 Germany
#5 Canada	#6 Netherlands
#7 France	#8 Singapore
#9 India	#10 Australia

Source: Hybrid Analysis

Top malicious files

100% Threat score	MonitorFPKPVer.exe	100% Threat score	MonitorFPKPVer.exe
100% Threat score	S-564948034.xlsb	100% Threat score	JDownloaderSetup.exe
100% Threat score	tmp_r529mod	100% Threat score	PAYMENT COPY.exe
100% Threat score	mpnp-win-ts8130-1_02-ea34_2.exe	100% Threat score	12_06_13.exe
97% Threat score	Invoice 18274764.xlsx	95% Threat score	SAIKsetup35-r20211206.exe
85% Threat score	SX1261Calculator_setup.exe	85% Threat score	Re Payment Confirmation_part_002.xlsx
80% Threat score	KutoolsforExcelSetup.exe	77% Threat score	S-1093600994.xlsb
77% Threat score	task.exe	72% Threat score	image maker.exe