Security Rabbits

Your Security Rabbits report for April 13, 2022

Source: Ransom Watch

Ransomware attacks

lockbit2	northstari	lockbit2	breadtalk,com
lorenz	DeeZee	lockbit2	inglotcosmetics,,,
everest	Supplies Company Data Leak in British Columbia, Canada	conti	TIC International Corporation

Hot topics

Nothing today

News

Cyware News - Latest Cyber News

Attackers Abuse AWS Lambda to Mine Monero

Researchers stumbled across a new malware variant, dubbed Denonia, that targets AWS Lambda, a scalable cloud computing service used by SMBs and enterprise players worldwide. It is a Go-based wrapper designed to deploy a custom XMRig crypto miner for Monero mining. Experts suggest always using reliable anti-malware solutions and keeping software up-to-date for better protection.

The Hacker News

Critical LFI Vulnerability Reported in Hashnode Blogging Platform

Researchers have disclosed a previously undocumented local file inclusion (LFI) vulnerability in Hashnode, a developer-oriented blogging platform, that could be abused to access sensitive data such as SSH keys, server's IP address, and other network information. "The LFI originates in a Bulk Markdown Import feature that can be manipulated to provide attackers with unimpeded ability to download

Cyware News - Latest Cyber News

Double-Your-Crypto Scams Share Crypto Scam Host - Krebs on Security

The ark-x2[.]org site pretended to be a crypto giveaway website run by Cathie Wood, the founder and CEO of ARKinvest, an established Florida company that manages several exchange-traded investment funds.

The Hacker News

E.U. Officials Reportedly Targeted with Israeli Pegasus Spyware

Senior officials in the European Union were allegedly targeted with NSO Group's infamous Pegasus surveillance tool, according to a new report from Reuters. At least five individuals, including European Justice Commissioner Didier Reynders, are said to have been singled out in total, the news agency said, citing documents and two unnamed E.U. officials. However, it's not clear who used the

Cyware News - Latest Cyber News

BlackCat Ransomware Group Claims Attack on Florida International University

The ransomware group, which most recently attacked North Carolina A&T University, claimed it has stolen a range of personal information from students, teachers, and staff.

The Hacker News

Cross-Regional Disaster Recovery with Elasticsearch

Unsurprisingly, here at Rewind, we've got a lot of data to protect (over 2 petabytes worth). One of the databases we use is called Elasticsearch (ES or Opensearch, as it is currently known in AWS). To put it simply, ES is a document database that facilitates lightning-fast search results. Speed is essential when customers are looking for a particular file or item that they need to restore using

Cyware News - Latest Cyber News

DPRK-Nexus Adversary Targets South Korean Individuals in a New Chapter of Kitty Phishing Operation

Cluster25 traced a recent activity that started in the first days of April 2022 from a DPRK-nexus threat actor using spear-phishing emails containing Korean-based malicious documents with different lures to compromise its victims.

Security Affairs

EU officials were targeted with Israeli surveillance software

According to a report published by Reuters, an Israeli surveillance software was used to spy on senior officials in the European Commission. One of the officials targeted with the infamous spyware there is Didier Reynders, a senior Belgian statesman who has served as the European Justice Commissioner since 2019. The report did not attribute the [...] The post EU officials were targeted with Israeli surveillance software appeared first on Security Affairs.

The Hacker News

FBI, Europol Seize RaidForums Hacker Forum and Arrest Admin

An international law enforcement operation raided and took down RaidForums, one of the world's largest hacking forums notorious for selling access to hacked personal information belonging to users. Dubbed Tourniquet, the seizure of the cybercrime website involved authorities from the U.S., U.K., Sweden, Portugal, and Romania, with the criminal investigation resulting in the arrest of the forum's

Naked Security

Five critical bugs fixed in hospital robot control system

Fortunately, we're not talking about a robot revolution, or about hospital AI run amuck. But these bugs could lead to ransomware, or worse...

WeLiveSecurity

Industroyer2: Industroyer reloaded

This ICS-capable malware targets a Ukrainian energy company The post Industroyer2: Industroyer reloaded appeared first on WeLiveSecurity

Cyware News - Latest Cyber News

Lawmakers Want to Improve Cybersecurity Info Sharing Between DHS, Congress

The Intragovernmental Cybersecurity Information Sharing Act was introduced by US senators Rob Portman (R-OH), Amy Klobuchar (D-MN), Roy Blunt (R-MO), and Gary Peters (D-MI).

Threatpost

Menswear Brand Zegna Reveals Ransomware Attack

Accounting materials from the Italy-based luxury fashion house were leaked online by RansomExx because the company refused to pay.

Security Affairs

Microsoft Partch Tuesday for April 2022 fixed 10 critical vulnerabilities

Microsoft Partch Tuesday security updates for April 2022 fixed 128 vulnerabilities, including an actively exploited zero-day reported by NSA. Microsoft Partch Tuesday security updates for April 2022 fixed 128 vulnerabilities in multiple products, including Microsoft Windows and Windows Components, Microsoft Defender and Defender for Endpoint, Microsoft Dynamics, Microsoft Edge (Chromium-based), Exchange Server, Office and Office [...] The post Microsoft Partch Tuesday for April 2022 fixed 10 critical vulnerabilities appeared first on Security Affairs.

Cyware News - Latest Cyber News

Microsoft's April 2022 Patch Tuesday tackles two zero-day vulnerabilities

Microsoft has fixed problems including numerous remote code execution (RCE) bugs, elevation of privilege (EoP) issues, denial-of-service, information leaks, and spoofing.

New Octo Banking Trojan Abuses Android Accessibility Features

The Hacker News

Finding Attack Paths in Cloud Environments

The mass adoption of cloud infrastructure is fully justified by innumerable advantages. As a result, today, organizations' most sensitive business applications, workloads, and data are in the cloud. Hackers, good and bad, have noticed that trend and effectively evolved their attack techniques to match this new tantalizing target landscape. With threat actors' high reactivity and adaptability, it

CyberScoop

Hospital hallway robots get patches for potentially serious bugs

Five zero-days found in Aethon TUG robots included one that could allow an attacker to control the machines, Cynerio said. The post Hospital hallway robots get patches for potentially serious bugs appeared first on CyberScoop.

CyberScoop

Justice Department seizes major cybercrime spot RaidForums

RaidForums boasted at one point of having close to 10 billion pieces of PII for sale, making it one of the biggest destinations for cybercriminals. The post Justice Department seizes major cybercrime spot RaidForums appeared first on CyberScoop.

Cyware News - Latest Cyber News

LockBit ransomware gang lurked in a U.S. gov network for months

A regional U.S. government agency compromised with LockBit ransomware had the threat actor in its network for at least five months before the payload was deployed, security researchers found.

The Hacker News

Microsoft Issues Patches for 2 Windows Zero-Days and 126 Other Vulnerabilities

Microsoft's Patch Tuesday updates for the month of April have addressed a total of 128 security vulnerabilities spanning across its software product portfolio, including Windows, Defender, Office, Exchange Server, Visual Studio, and Print Spooler, among others. 10 of the 128 bugs fixed are rated Critical, 115 are rated Important, and three are rated Moderate in severity, with one of the flaws

Threatpost

Microsoft Zero-Days, Wormable Bugs Spark Concern

For April Patch Tuesday, the computing giant addressed a zero-day under active attack and several critical security vulnerabilities, including three that allow self-propagating exploits.

Cyware News - Latest Cyber News

New META Stealer is Popular in the Underground Marketplaces

A researcher unearthed a malspam campaign distributing the new META infostealer to steal passwords stored in browsers, including Google Chrome, Edge, and Firefox, as well as cryptocurrency wallets. META tampers with Windows Defender using PowerShell to exclude .exe files from scanning to avoid detection. Users must stay cautious and protect their sensitive info with proper encryption.

NGINX project maintainers fix flaws in LDAP Reference Implementation

The maintainers of the NGINX web server project

Cyware News - Latest Cyber News

ThreatFabric stumbled across Octo, a rental banking trojan capable of gaining remote access to compromised devices. It is said to be a rebrand of a similar Android threat called ExobotCompact. The malicious apps acting as droppers are identified as Pocket Screencaster, Fast Cleaner 2021, Play Store, and others. For protection, experts suggest it's good to have a monitoring system in place to analyze the behavior of installed apps.

ZDNet | security RSS

Only half of organizations reviewed security policies due to the pandemic: Study

Investment is expected to increase but existing cybersecurity strategies are lacking.

Cyware News - Latest Cyber News

Panasonic's Canadian Operations Suffered Ransomware Attack

In a statement provided to TechCrunch, Panasonic said that it was a victim of a "targeted cybersecurity attack" in February that affected some of its systems, processes, and networks.

Krebs on Security

RaidForums Gets Raided, Alleged Admin Arrested

The U.S. Department of Justice (DOJ) said today it seized the website and user database for RaidForums, an extremely popular English-language cybercrime forum that sold access to more than 10 billion consumer records stolen in some of the world's largest data breaches since 2015. The DOJ also charged the alleged administrator of RaidForums -- 21-year-old Diogo Santos Coelho, of Portugal -- with six criminal counts, including conspiracy, access device fraud and aggravated identity theft.

Security Affairs

Russia-linked Sandworm APT targets energy facilities in Ukraine with wipers

Russia-linked Sandworm APT group targeted energy facilities in Ukraine with INDUSTROYER2 and CADDYWIPER wipers. Russia-linked Sandworm threat actors targeted energy facilities in Ukraine with a new strain of the Industroyer ICS malware (INDUSTROYER2) and a new version of the CaddyWiper wiper. According to the CERT-UA, nation-state actors targeted high-voltage electrical substations with INDUSTROYER2, the variant analyzed by [...] The post Russia-linked Sandworm APT targets energy facilities in Ukraine with wipers appeared first on Security Affairs.

The Hacker News

Russian Hackers Tried Attacking Ukraine's Power Grid with Industroyer2 Malware

The Computer Emergency Response Team of Ukraine (CERT-UA) on Tuesday disclosed that it thwarted a cyberattack by Sandworm, a hacking group affiliated with Russia's military intelligence, to sabotage the operations of an unnamed energy provider in the country. "The attackers attempted to take down several infrastructure components of their target, namely: Electrical substations, Windows-operated

Cyware

The Art Exhibition That Fools Facial Recognition Systems

The exhibition has 100 Mona Lisa images. "All look

Security Affairs

addressed a zero-day vulnerability in the Lightweight Directory Access Protocol (LDAP) Reference Implementation. The maintainers of the NGINX web server project have released security updates to address a zero-day vulnerability that resides in its Lightweight Directory Access Protocol (LDAP) Reference Implementation. The NGINX LDAP reference implementation uses [...] The post NGINX project maintainers fix flaws in LDAP Reference Implementation appeared first on Security Affairs.

Security Affairs

Operation TOURNIQUET: Authorities shut down dark web marketplace RaidForums

The dark web marketplace RaidForums has been shut down and its infrastructure seized as a result of Operation TOURNIQUET. The illegal dark web marketplace RaidForums has been shut down and its infrastructure seized as a result of the international law enforcement Operation TOURNIQUET coordinated by Europol's European Cybercrime Centre. Operation TOURNIQUET was conducted by law [...] The post Operation TOURNIQUET: Authorities shut down dark web marketplace RaidForums appeared first on Security Affairs.

Blog â€“ Flashpoint

Raid Forums Is Down. Who's Behind Its Apparent Seizure? [Updated]

Updated April 12: Today, the US Department of Justice (DOJ) issued a press release confirming their seizure of the popular English-language hacking forum, Raid Forums. "Our interagency efforts to dismantle this sophisticated online platform--which facilitated a wide range of criminal activity --should come as a relief to the millions victimized by it, and as a [...] The post Raid Forums Is Down. Who's Behind Its Apparent Seizure? [Updated] appeared first on Flashpoint.

IT Security Guru

RaidForums hacker forum domain seized

RaidForums, one of the world's largest hacking forums, has been raided and taken down by an international law enforcement operation. The forum was notorious for selling access to stolen personal information. The operation, dubbed "Tourniquet", involved authorities from the US, UK, Sweden, Portugal and Romania. The investigation culminated in the arrest of the forum's administrator [...] The post RaidForums hacker forum domain seized appeared first on IT Security Guru.

CyberScoop

Russian hackers thwarted in attempt to take out electrical grid, Ukrainians say

Russian losses near Kyiv and a looming onslaught in eastern Ukraine may be a factor in the attack, a Ukrainian official said. The post Russian hackers thwarted in attempt to take out electrical grid, Ukrainians say appeared first on CyberScoop.

Cyware News - Latest Cyber News

SharkBot Propagates via Fake Antivirus Apps on Google Play

Check Point researchers discovered seven malicious apps on the Google Play Store posing as antivirus solutions to drop the SharkBot banking trojan. These malicious apps were downloaded more than 15,000 times before Google removed them. Researchers advise downloading apps only from trusted/verified publishers and reporting any suspicious apps to the store.

These hackers pretend to poach, recruit rival bank staff in new cyberattacks

News - Latest Cyber News

almost the same as the original one by da Vinci for people, though AI recognizes them as 100 different celebrities," explains Adversa in a blog report.

Cyware News - Latest Cyber News

USPS "Your package could not be delivered" text is a smishing scam

Fake USPS delivery notification spam is a popular tactic for online scammers, and USPS's recent advisory on the topic includes instructions on how to report bogus SMS messages.

ZDNet | security RSS

Employees looking for new career opportunities are the targets.

Twitter

Marcus Hutchins

My intended niche was cybersecurity videos, but the niche I ended up with is people who aren't interested in cybersecurity just listening to me say words because they like my voice. I'll take it though.

FBI

Trained #FBI cyber personnel can arrive on domestic doorsteps within an hour of a #cyber incident, and can travel to meet victims in over 70 other countries within a day. Partner with your local field office to experience our commitment to cybersecurity:

NBC News

Russian military hackers tried and failed to attack Ukraines energy infrastructure last week, the countrys government and a major cybersecurity company say.

Source: NIST

NIST CVE: Critical

Nothing today

Source: NIST

NIST CVE: High

CVE-2021-39114

Affected versions of **Atlassian Confluence** Server and **Data Center** allow users with a valid account on a Confluence Data Center instance to execute arbitrary **Java** code or run arbitrary system commands by injecting an **OGNL** payload. The affected versions are before version 6.13.23, from version 6.14.0 before 7.4.11, from version 7.5.0 before 7.11.6, and from version 7.12.0 before 7.12.5.

HIGH	Vector: network	Created: 2022-04-05	Updated: 2022-04-13

Source: NIST

NIST CVE: Medium

Nothing today

Source: NIST

NIST CVE: Low

Nothing today

Source: NIST

NIST CVE: Unrated

CVE-2022-22279

** UNSUPPORTED WHEN ASSIGNED ** A post-authentication arbitrary file read vulnerability impacting end-of-life Secure **Remote Access** (SRA) products and older firmware versions of **Secure Mobile Access** (SMA) 100 series

CVE-2022-26589

A Cross-Site Request Forgery (CSRF) in **Pluck** products, specifically the SRA appliances running all 8.x, 9.0.0.5-19sv and earlier versions and Secure Mobile Access (SMA) 100 series products running older firmware 9.0.0.9-26sv and earlier versions.

UNRATED Vector: unkown Created: 2022-04-13 Updated: 2022-04-13

CVE-2022-26151

Citrix XenMobile Server 10.12 through RP11, 10.13 through RP6, and 10.14 through RP4 allows Command Injection.

UNRATED Vector: unkown Created: 2022-04-13 Updated: 2022-04-13

CVE-2021-44520

In **Citrix XenMobile Server** through 10.12 RP9, there is an Authenticated Command Injection vulnerability, leading to remote code execution with root privileges.

UNRATED Vector: unkown Created: 2022-04-13 Updated: 2022-04-13

CMS v4.7.15 allows attackers to delete arbitrary pages.

UNRATED Vector: unkown Created: 2022-04-13 Updated: 2022-04-13

CVE-2022-29156

drivers/infiniband/ulp/rtrs/rtrs-clt.c in the **Linux** kernel before 5.16.12 has a double free related to rtrs_clt_dev_release.

UNRATED Vector: unkown Created: 2022-04-13 Updated: 2022-04-13

Source: Hybrid Analysis

Top malicious files

100% Threat score 8216e4c1977597afe01bb3c0a47631bd7608963a38ca6c396790fbf37d0fcffb_pidor,xyz_dedob2,exe

100% Threat score W-1571670251,xlsb

100% Threat score REJ-10525256-Apr-12,xlsb

94% Threat score _10000000,mem

86% Threat score multi-microsoft-teams-1-0-0-5-ks_v3,575,02,080,5,exe

83% Threat score V740 @ PO 0069,xls

100% Threat score GoTo Webinar Opener (1),exe

100% Threat score tmp9i52tryp

95% Threat score Valorant,exe

86% Threat score W-1461729946,xlsb

85% Threat score Content Manager,exe

Source: Hybrid Analysis

Top malicious URL

97% Threat score http://61,177,137,133/x/1sh

86% Threat score http://206,188,197,104/bins/arm7

81% Threat score http://162,33,179,171/bins/realtek,mpsl

91% Threat score http://137,59,195,10:44014/Mozi,m

81% Threat score http://162,33,179,171/linnn

73% Threat score http://uzrut,smtpgaze,com/tracking/

Source: SpamHaus

Top spamming countries

#1 United States of America

#3 Russian Federation

#2 China

#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 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 Iran (Islamic Republic of)

Source: SpamHaus

Top phishing countries

- #1 United States
- #2 Netherlands
- #3 Germany
- #4 Russia
- #5 Singapore
- #6 China
- #7 France
- #8 Hong Kong
- #9 India
- #10 Poland

Source: Have I been pwned?

Have I been pwnd

Nothing today

Source: Imperva DDOS Map

Top DDOS attackers

- **United States (29%)**
- **Germany (15%)**
- **Netherlands (9%)**

Source: Imperva DDOS Map

Top DDOS country targets

- **Russia (36%)**
- **United States (23%)**
- **Ukraine (14%)**

Source: Imperva DDOS Map

Top DDOS techniques

49%	**DDoS**
34%	**Automated Threat**
16%	**OWASP**

Source: Imperva DDOS Map

Top DDOS industry targets

39%	**Financial Services**
23%	**Business**
9%	**Computing & IT**