Security Rabbits

# Your Security Rabbits report for April 16, 2022

*Source: Ransom Watch*

## Ransomware attacks

| | |
|---|---|
| clop | AFJCONSULTING,NET |
| clop | BOLTONUSA,COM FILES *PART32 - 10,0,0,20\|\|c$\|\|BOD_HQ_CIFS\|\|DB_Dept\|\|DB_DEPT\|\|CLIENT\|\|PBGC-DIS |
| suncrypt | DJS associate |
| clop | MCH-GROUP,COM |
| lockbit2 | enclosuresoluti,,, |
| lockbit2 | http://inland-e,,, |
| lockbit2 | inland-engineer,,, |
| clop | ALEXIM,COM |
| clop | CAPCARPET,COM |
| clop | EDAN,COM |
| conti | [IMPORTANT ANNOUNCEMENT!] |
| clop | ENPRECIS,COM |
| lv | Importador Ferretero Trujillo Cia, Ltda |
| clop | SWIRESPO,COM |

## Hot topics

***Nothing today***

## News

Cyware News - Latest Cyber News

### Attack on Panasonic Canada Shows Conti is Still Dangerous

While the details remain sparse, Panasonic suffered another breach just six months after a high-profile attack--this time at Panasonic Canada. The Conti gang said it was behind the February attack that resulted in the theft of more than 2.8GB of data.

Security Affairs

### Auth bypass flaw in Cisco Wireless LAN Controller Software allows device takeover

Cisco fixed a critical flaw in Cisco Wireless LAN Controller (WLC) that could allow an unauthenticated, remote attacker to take control affected devices. Cisco has released security patches to fix a critical vulnerability (CVSS score 10), tracked as CVE-2022-20695, in Cisco Wireless LAN Controller (WLC). A remote, unauthenticated attacker could exploit the flaw to bypass […] The post Auth bypass flaw in Cisco Wireless LAN Controller Software allows device takeover appeared first on Security Affairs.

### Conti Ransomware Gang claims

Cyware News - Latest Cyber News

### CISA orders agencies to fix actively exploited VMware, Chrome bugs

The CISA has added nine more security flaws to its list of actively exploited bugs, including a VMware privilege escalation flaw and a Google Chrome zero-day that could be used for remote code execution.

Cyware News - Latest Cyber News

### Critical Vulnerability in Elementor Plugin Impacts Millions of WordPress Sites

A critical vulnerability addressed in the Elementor WordPress plugin could allow authenticated users to upload arbitrary files to affected websites, potentially leading to code execution.

Cyware News - Latest Cyber News

### GitHub: Attacker breached dozens of orgs using stolen OAuth tokens

Since this campaign was first spotted on April 12, 2022, the threat actor has already accessed and stolen data from dozens of victim organizations using Heroku and Travis-CI-maintained OAuth apps, including npm.

The Hacker News

### Haskers Gang Gives Away ZingoStealer Malware to Other Cybercriminals for Free

A crimeware-related threat actor known as Haskers Gang has released an information-stealing malware called ZingoStealer for free on, allowing other criminal groups to leverage the tool for nefarious purposes. "It features the ability to steal sensitive information from victims and can download additional malware to infected systems," Cisco Talos researchers Edmund Brumaghin and Vanja Svajcer

Threatpost

### Karakurt Ensnares Conti, Diavol Ransomware Groups in Its Web

Connections that show the cybercriminal teams are working together signal shifts in their respective tactics and an expansion of opportunities to target victims.

The Hacker News

### Lazarus Group Behind $540 Million Axie Infinity Crypto Hack and Attacks on Chemical Sector

Security Affairs

### responsibility for the Nordex hack

The Conti ransomware gang has claimed responsibility for the recent attack against Nordex, one of the largest manufacturers of wind turbines. The Conti ransomware gang claimed responsibility for the cyberattack that hit the manufacturer of wind turbines Nordex on March 31, 2022. Nordex Group shut down "IT systems across multiple locations and business units" as […] The post Conti Ransomware Gang claims responsibility for the Nordex hack appeared first on Security Affairs.

The Hacker News

### GitHub Says Hackers Breached Dozens of Organizations Using Stolen OAuth Access Tokens

Cloud-based repository hosting service GitHub on Friday revealed that it discovered evidence of an unnamed adversary capitalizing on stolen OAuth user tokens to unauthorizedly download private data from several organizations. "An attacker abused stolen OAuth user tokens issued to two third-party OAuth integrators, Heroku and Travis-CI, to download data from dozens of organizations, including NPM

Security Affairs

### Google fixed third zero-day in Chrome since the start of 2022

Google Chrome 100.0.4896.127 addresses a new high-severity zero-day vulnerability tracked as CVE-2022-1364, actively exploited by threat actors in the wild. Google has released Chrome 100.0.4896.127 for Windows, Mac, and Linux to address a high-severity zero-day, tracked as CVE-2022-1364, that is actively exploited by threat actors in attacks. The CVE-2022-1364 zero-day is a type confusion issue […] The post Google fixed third zero-day in Chrome since the start of 2022 appeared first on Security Affairs.

The Hacker News

### JekyllBot:5 Flaws Let Attackers Take Control of Aethon TUG Hospital Robots

As many as five security vulnerabilities have been addressed in Aethon Tug hospital robots that could enable remote attackers to seize control of the devices and interfere with the timely distribution of medication and lab samples. "Successful exploitation of these vulnerabilities could cause a denial-of-service condition, allow full control of robot functions, or expose sensitive information,"

Cyware News - Latest Cyber News

### Karakurt revealed as data extortion arm of Conti cybercrime syndicate

After breaching servers managed by the cybercriminals, security researchers found a connection between Conti ransomware and the recently emerged Karakurt data extortion group, showing that the two gangs are part of the same operation.

The Hacker News

The U.S. Treasury Department has implicated the North Korea-backed Lazarus Group (aka Hidden Cobra) in the theft of $540 million from video game Axie Infinity's Ronin Network last month. On Thursday, the Treasury tied the Ethereum wallet address that received the stolen funds to the threat actor and sanctioned the funds by adding the address to the Office of Foreign Assets Control's (OFAC)

Cyware News - Latest Cyber News

### North Korea's Lazarus Group Stole More than $600 Million in a Single Hack Targeting Axie Infinity

The FBI has blamed hackers associated with the North Korean government for stealing more than $600 million in cryptocurrency last month from a video gaming company -- the latest in a string of audacious cyber heists tied to Pyongyang.

Cyware News - Latest Cyber News

### Spanish FA report cyber attack to police after email accounts, private texts stolen

Documents and information from email accounts, private texts, and audio conversations from top executives of the federation, including president Luis Rubiales, have been stolen in recent months.

Security Affairs

### Threat actors use Zimbra exploits to target organizations in Ukraine

Threat actors are targeting Ukrainian government organizations with exploits for XSS vulnerabilities in Zimbra Collaboration Suite (CVE-2018-6882). Ukraine's CERT (CERT-UA) warns of threat actors that are targeting government organizations with exploits for XSS vulnerabilities in Zimbra Collaboration Suite (CVE-2018-6882). "Cross-site scripting (XSS) vulnerability in the ZmMailMsgView.getAttachmentLinkHtml function in Zimbra Collaboration Suite (ZCS) before 8.7 Patch […] The post Threat actors use Zimbra exploits to target organizations in Ukraine appeared first on Security Affairs.

Security Affairs

### ZingoStealer crimeware released for free in the cybercrime ecosystem

A new powerful crimeware called ZingoStealer was released for free by a threat actor known as Haskers Gang. ZingoStealer is a new information-stealer developed by a threat actor known as Haskers Gang who released it for free after they attempted to sell the source code for $500. The threat actors were also offering their own crypter, dubbed […] The post ZingoStealer crimeware released for free in the cybercrime ecosystem appeared first on Security Affairs.

Cyware News - Latest Cyber News

### Newman Regional Health notifies 52,224 patients after long-running breach of employee email accounts

Newman Regional Health (NRH) is notifying more than 52,000 patients after an investigation revealed unauthorized access to a limited number of their employee e-mail accounts.

CyberScoop

### Prolific cyber extortion group Karakurt might be a Conti side hustle

Links in tooling, crypto wallets and even attacking victims simultaneously strongly suggest a link, researchers say. The post Prolific cyber extortion group Karakurt might be a Conti side hustle appeared first on CyberScoop.

Cyware News - Latest Cyber News

### T-Mobile customers warned of unblockable SMS phishing attacks

The New Jersey Cybersecurity & Communications Integration Cell (NJCCIC) issued a warning after multiple customers have filed reports of being targeted by this new SMS phishing (smishing) campaign.

Naked Security

### Yet another Chrome zero-day emergency update - patch now!

The third emergency Chrome 0-day in three months - the first one was exploited by North Korea, so you might as well get this one ASAP.

## Twitter

Brahma Chellaney

US is getting more deeply involved in the war by transferring offensive weapons to Ukraine, besides providing intelligence on Russian forces and positions and deploying technical teams to Ukraine for cybersecurity, reports @WSJ. Will Moscow respond to such escalation? If so, how?

Marcus Hutchins

I can't decide if to convince more cybersecurity people that TikTok is no worse for privacy than other platforms or just enjoy the lack of competition

The Democrats

The Biden-Harris administration is working to help create and expand programs at our country's HBCUs in fields like manufacturing, health care, and cybersecurity. Building a better America means having a workforce that looks like our country.

60 Minutes

With U.S.-Russia relations at a post-Cold War low, the Biden administration has been releasing intelligence and warning the Kremlin may be planning cyberattacks on American soil. Sunday, Bill Whitaker speaks with U.S. cybersecurity officials about the likelihood of a major hack.

*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-2022-29072

7-Zip through 21.07 on **Windows** allows privilege escalation and command execution when a file with the .7z extension is dragged to the Help>Contents area. This is caused by misconfiguration of 7z.dll and a heap overflow. The command runs in a child process under the 7zFM.exe process,

| UNRATED | Vector: unkown | Created: 2022-04-15 | Updated: 2022-04-16 |
|---|---|---|---|

CVE-2022-29287

**Kentico** CMS before 13.0.66 has an Insecure Direct Object Reference vulnerability. It allows an attacker with user management rights (default is Administrator) to export the user options of any user, even ones with higher privileges (like Global

CVE-2022-29020

**ForestBlog** through 2022-02-16 allows admin/profile/save userAvatar XSS during addition of a user avatar.

| UNRATED | Vector: unkown | Created: 2022-04-16 | Updated: 2022-04-16 |
|---|---|---|---|

Administrators) than the current user. The exported XML contains every option of the exported user (even the hashed password).

|  |  |  |  |
|---|---|---|---|
| UNRATED | Vector: unkown | Created: 2022-04-16 | Updated: 2022-04-16 |

*Source: Hybrid Analysis*

## Top malicious files

|  |  |  |  |
|---|---|---|---|
| 100%<br>Threat score | setup[eMo]Web Browser Optimizer,exe | 100%<br>Threat score | tmpl0ub17ud |
| 100%<br>Threat score | tmpry7nx0fg | 100%<br>Threat score | WiGLE WiFi Wardriving_v2,64_apkpure,com,apk |
| 100%<br>Threat score | Firefox Installer,exe | 100%<br>Threat score | bounty-53137113995718702 |
| 100%<br>Threat score | csrss,exe | 95%<br>Threat score | tmpt7id9fll |
| 86%<br>Threat score | MightyFucker,exe | 85%<br>Threat score | Easy_Notes_v1,1,18,0413,01_VIP,apk |
| 85%<br>Threat score | LiquidLauncher-1,1,3 Setup,exe | 85%<br>Threat score | Fancy Security v3,1,6 Premium (MixRoot),apk |
| 80%<br>Threat score | Utorent,exe | 80%<br>Threat score | pdr-free-online,exe |
| 79%<br>Threat score | com,android,managedprovisioning (1),apk | 79%<br>Threat score | Checkra1n,exe |
| 79%<br>Threat score | NetGuard-2,139,apk | 77%<br>Threat score | com,samsung,android,knox,containercore (1),apk |
| 75%<br>Threat score | DisplayDriver,exe | 74%<br>Threat score | activation office365,html |
| 72%<br>Threat score | aostv_v21,0,0_ads,apk | 71%<br>Threat score | Avast One v22,3,1 Modded by Mixroot,apk |

*Source: Hybrid Analysis*

## Top malicious URL

|  |  |
|---|---|
| 91%<br>Threat score | http://117,212,102,69:39161/Mozi,m |

*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 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 United States of America
- #3 India
- #4 Indonesia
- #5 Thailand
- #6 Algeria
- #7 Viet Nam
- #8 Brazil
- #9 Pakistan
- #10 Japan

*Source: SpamHaus*

## Top phishing countries

- #1 United States
- #2 Netherlands
- #3 Russia
- #4 Germany
- #5 Hong Kong
- #6 Ireland
- #7 Japan
- #8 France
- #9 Sweden
- #10 United Arab Emirates

*Source: Have I been pwned?*

## Have I been pwnd

***Nothing today***

*Source: Imperva DDOS Map*

## Top DDOS attackers

- **United States (20%)**
- **Brazil (11%)**
- **Germany (8%)**

*Source: Imperva DDOS Map*

## Top DDOS country targets

- **China (59%)**
- **Russia (12%)**
- **United States (10%)**

*Source: Imperva DDOS Map*

## Top DDOS techniques

| | |
|---|---|
| 76% | **DDoS** |
| 18% | **Automated Threat** |
| 7% | **OWASP** |

*Source: Imperva DDOS Map*

## Top DDOS industry targets

| | |
|---|---|
| 38% | **Financial Services** |
| 22% | **Business** |
| 11% | **Computing & IT** |