

Week of July 22, 2024

# **Cybersecurity Headlines**

# **Official Security Bulletins**

Headlines from CISA, MS-ISAC, and other official sources

# Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution

www.cisecurity.org

Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could allow for arbitrary code execution. Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution in the ...

Guidance for CrowdStrike Windows Outage

www.cisecurity.org

Information and actions to take regarding the CrowdStrike Windows Outage.

NCSWIC Planning Training, and Exercise Committee releases the Human Factors Resource Guide

www.cisa.gov

NCSWIC's Planning, Training, and Exercise Committee releases "Set Your PACE Plan" Flyer

www.cisa.gov

What's on the State and Local IT Radar for the **Next Six Months?** 

# AI Ethics and Why It Matters www.isaca.org

Artificial intelligence ethics considerations must be top-of-mind for organizations when leveraging AI as trust, bias, security, privacy and other important elements should not be overlooked.

# What's on the State and Local IT Radar for the Next Six Months? - NASCIO

The audience is in the driver's seat for this webinar as we take your questions on the latest trends impacting state and local government CIOs: What are the areas of focus of IT executives for the rest of 2024? What's the latest on budgeting, operati...

Statement from CISA Director Easterly on Leadership Changes at CISA

www.cisa.gov

# **Cybercrimes, Scams & Incidents**

Headlines related to cybercrimes and scams including international cybersecurity news and high-profile incidents like ransomware and malware attacks

# **Industry News**

Headlines collected from across the cybersecurity industry related to legislation, business, and big tech



www.nascio.org

Rim Jong Hyok (림종혁) is a North Korean hacker associated with the malicious cyber group Andariel, which is controlled by North Korea's military intelligence agency.

Rim and others conspired to hack into the computer system of U.S. nospitals and other healthcare providers, install Maui ransomware and extort a ransom. Using the ransom payments, they funded malicious cyber operations targeting U.S. government entities and U.S. and foreign defense contractors, among others.

If you have information leading to the identification or location of Rim, associated individuals, entities, and/or activities, contact us ia our Tor-based tip line below.





### US indicts alleged North Korean state hacker for ransomware attacks on hospitals

therecord.media

Rim Jong Hyok was allegedly involved in ransomware attacks conducted in 2021 and 2022, including one on a hospital in Kansas.



#### Inside Minnesota's Dollar-Driven Cyber Defense Tool

www.govtech.com

Minnesota's new cybersecurity tool translates cyber risk into dollars and cents, empowering agencies to make data-driven decisions that protect critical assets and optimize security spending.



Columbus reports cyber incident as multiple cities recover from ransomware attacks therecord.media

The city of Columbus, Ohio said it is working to restore its systems after a cybersecurity incident forced the government to sever internet connectivity.



IR Trends: Ransomware on the rise, while technology becomes most targeted sector blog.talosintelligence.com

Although there was a decrease in BEC engagements from last quarter, it was still a major threat for the second quarter in a row.



How a North Korean Fake IT Worker Tried to Infiltrate Us blog.knowbe4.com How a North Korean Fake IT Worker Tried to Infiltrate Us



5 critical IT policies every organization should have in place

www.csoonline.com

From acceptable use policies to remote work guidelines, identifying the rules and procedures for all individuals accessing your organization's IT resources is an IT security fundamental.



ServiceNow embroiled in DOJ probe of government contract award

# www.cio.com

The probe also involves what ServiceNow said was the improper hiring of the Army CIO to serve as ServiceNow's global head of public sector. That executive, Raj Iyer, told CIO "I resigned because I didn't want to be associated with this fiasco in any ...



# CrowdStrike's unforced error puts its reputation on the line

www.cybersecuritydive.com

The widespread release of defective code suggests CrowdStrike didn't properly test its update before it was released or that process failed to catch the mistake, experts said.



PINEAPPLE and FLUXROOT Hacker Groups Abuse Google Cloud for Credential Phishing thehackernews.com



CrowdStrike disruption direct losses to reach \$5.4B for Fortune 500, study finds www.cybersecuritydive.com



Cybercriminals Exploit CrowdStrike Update Mishap to Distribute Remcos RAT Malware thehackernews.com

CrowdStrike warns of Remcos RAT malware targeting Latin America amid flawed update crisis causing IT disruptions.



Federal judge greenlights securities fraud charges against SolarWinds and its CISO www.csoonline.com

Although the court dismissed most of the SEC's charges in its lawsuit against SolarWinds, the by far most serious charge – securities fraud by both the company and its CISO – survived. CISOs have little reason to celebrate.



#### New Play ransomware Linux version targets VMware ESXi VMs

www.bleepingcomputer.com

Play ransomware is the latest ransomware gang to start deploying a dedicated Linux locker for encrypting VMware ESXi virtual machines.



## Banking, oil and IT industry reps call on Congress to harmonize cyber regulations ... again

cyberscoop.com

Industry representatives in a House hearing pointed to the Biden administration's cyber reporting mandate as an example of overlapping regulations.

#### **Phish-Friendly Domain Registry**

#### krebsonsecurity.com

The Chinese company in charge of handing out domain names ending in ".top" has been given until mid-August 2024 to show that it has put in place systems for managing phishing reports and suspending abusive domains, or else forfeit its license to sell domains. The warning comes amid the release of new findings that .top was the most common suffix in phishing websites over the past year...

Please be advised that the following resources and materials are for informational purposes only. The opinions and views expressed in these materials are the opinions of the designated authors and do not reflect the opinions or views of the Commonwealth of Massachusetts, the Executive Office of Technology Services and Security, and/or the Enterprise Risk Management Office, (the Commonwealth). The information posted on this website includes hypertext links or pointers to information created and maintained by other public and/or private organizations. These links and pointers are provided solely for the information and convenience of the user. By selecting a link to an outside website, the user is subject to the privacy, copyright, security, and information quality policies of that website. The Commonwealth is not responsible for transmissions users receive from linked websites.

AlScoop

BleepingComputer

🕀 CISA

Cisco Talos Intelligence Group

GyberScoop

🕀 cis

Gybersecurity Dive

Cyware	CyberWire	FedScoop	Government Executive
Government Technology	isaca	Herebs on Security	₩ MITRE ATT&CK®
	⊕ NIST	Genetic Schneier on Security	StateScoop
The Hacker News	The Record		