Emergency Management and Response - Information Sharing and Analysis Center (EMR-ISAC)

The InfoGram

Volume 20 — Issue 44 | October 29, 2020

Critical drug shortages further complicate pandemic response

Cases of COVID-19 are trending upward across the United States as cooler weather sets in and medical facilities are already feeling the squeeze for supplies. A new study suggests we can add COVID-19-related drug shortages to the list of things to be concerned about.

The report from the Center for Infectious Disease Research and Policy (CIDRAP) at the University of Minnesota found that 29 out of 40, or approximately 73 percent, of drug treatments for COVID-19 are experiencing shortages. On top of spikes in treatment in hotspots, multiple factors contribute to shortages such as manufacturing halts, supply chain disruptions and international export restrictions.

As these drugs have multiple uses, the shortages may affect people who don't have COVID-19. For example, albuterol is used in asthma inhalers, something many people rely on every day.

CIDRAP discusses the overarching consequences of drug shortages, the need for better transparency, reliance on foreign sources and how a series of events (intentional or natural) could put us at even higher risk.

This is part six in a series on COVID-19. See the CIDRAP website for the other reports in the series.

(Source: CIDRAP)

Increased and imminent cyber threat to healthcare and public health

A recently published joint cybersecurity advisory coauthored by the Cybersecurity and Infrastructure Security Agency (CISA), the FBI and the Department of Health and Human Services (HHS) discusses credible information detailing an increased and imminent cybercrime threat to hospitals and healthcare providers in the United States. Key Findings:

- CISA, FBI and HHS assess malicious cyber actors are targeting the Healthcare and Public Health (HPH) Sector with Trickbot malware, often leading to ransomware attacks, data theft and the disruption of healthcare services.
- These issues will be particularly challenging for organizations within the COVID-19 pandemic; therefore, administrators will need to balance this risk when determining their cybersecurity investments.

This advisory describes the tactics, techniques and procedures (TTPs) used by cybercriminals against targets in the HPH Sector to infect systems with Ryuk ransomware for financial gain.

The advisory lists technical aspects of these kinds of attacks, which may be of use to those responsible for security networks and other computer systems. In addition, it lists best practices used to avoid having systems locked such as:

- Patching operating systems, software and firmware as soon as manufacturers release updates.

Highlights

Critical drug shortages further complicate pandemic response

Increased and imminent cyber threat to healthcare and public health

2020 Wildfire Risk Report

FEMA hosting integrated preparedness planning workshop series

Cyber Threats

U.S. Fire Administration

The U.S. Fire Administration operates the Emergency Management and Response – Information Sharing and Analysis Center (EMR-ISAC).

For information regarding the EMR-ISAC visit www.usfa.dhs.gov/emr-isac or contact the EMR-ISAC office at:
(301) 447-1325 and/or
emr-isac@fema.dhs.gov.

Subscribe here

- Regularly backing up systems to a location NOT stored on the network.
- Ensuring you are able to use the backup files to restore all systems and data.

This information is intended to provide warning to healthcare providers to ensure that they take timely and reasonable precautions to protect their networks from these threats.

(Source: CISA)

2020 Wildfire Risk Report

CoreLogic released the 2020 Wildfire Risk report, which takes a look at some of the new wildfire challenges faced, new ways to examine risk, losses from the year to date and methods of reducing those losses.

According to the report, up to the end of September this year over 7 million acres have burned in the United States. Responding to wildfires in 2020 has been extremely challenging not only due to new challenges from COVID-19 but also because of the number and size of fire. Recovering from them may also be more challenging.

The report also shares the 10 cities Core Logic found as having the highest rate of potential risk of loss from wildfire. These including Denver; Austin and San Antonio, Texas; Los Angeles, San Diego, Thousand Oaks, Truckee, Riverside, and Sacramento, Calif. The 2020 report also identifies areas where multiple family housing units may be at greater risk of loss.

According to the report, “No one can predict what the future may bring, but with the knowledge of risk, tools to combat challenges ahead and grit to work together, communities can pave a path towards a safer tomorrow.”

(Source: CoreLogic)

FEMA hosting integrated preparedness planning workshop series

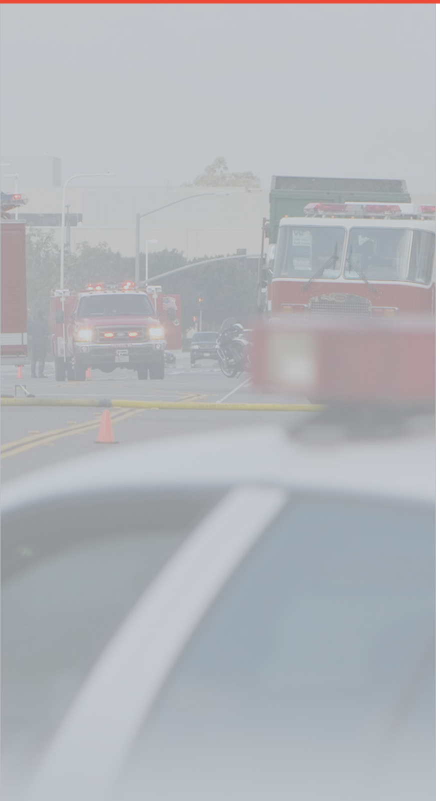
The Federal Emergency Management Agency (FEMA) is hosting a series of 10 webinars starting Oct. 29, 2020, and running through Nov. 30, 2020, to assist with the implementation of the Integrated Preparedness Plan (IPP) and Integrated Preparedness Planning Workshop (IPPW) model.

FEMA developed the IPP/IPPW model to support the coordination, planning and scheduling of activities across the preparedness cycle, a component of the revised 2020 Homeland Security Exercise and Evaluation Program (HSEEP) Doctrine.

The IPP/IPPW model has been piloted and refined. Currently there are nine webinars scheduled throughout November. Please visit the HSEEP Webinar webpage to see the dates available and register.

In addition, the HSEEP Course (K/L 0146) is currently being updated and will be released soon. Continue to monitor the HSEEP webpage at the Emergency Management Institute for release date information.

(Source: FEMA)

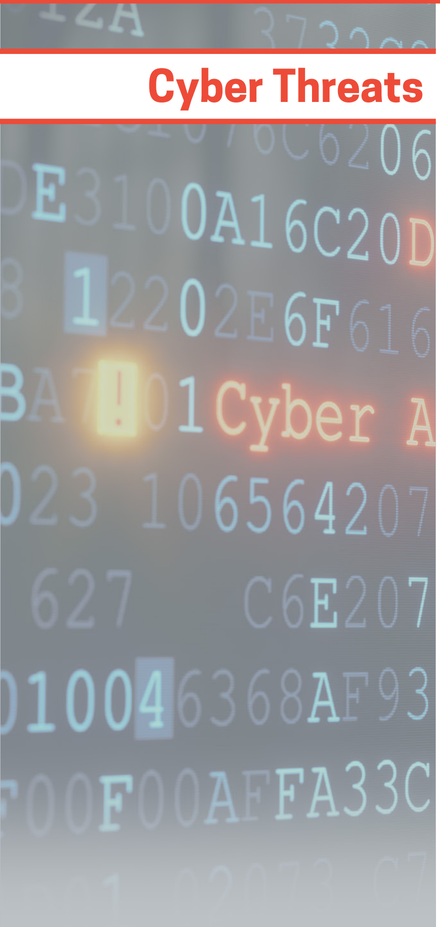


Fair Use Notice:
This InfoGram may contain copyrighted material that was not specifically authorized by the copyright owner.

The EMR-ISAC believes this constitutes “fair use” of copyrighted material as provided for in section 107 of the U.S. Copyright Law.

If you wish to use copyrighted material contained within this document for your own purposes that go beyond “fair use,” you must obtain permission from the copyright owner.

Disclaimer of Endorsement:
The appearance of external hyperlinks does not constitute endorsement of the linked websites or the information, products or services contained therein. Reference to any specific commercial products, process or service by trade name, trademark, manufacturer or otherwise, does not necessarily constitute or imply its endorsement, recommendation or favoring by the EMR-ISAC or the U.S. government.



Cyber Threats

Old school security tips that are more relevant than ever

Cybersecurity hygiene has never been as crucial as it is today. We are working remotely, putting in more hours and dealing with new situations.

For many, this change is not only stressful, but also distracting. These changes have upended the traditional workday and, in many cases, our concentration, which introduces risk. Even the most security-conscious engineers and employees might miss something important or overlook a task that would previously be a routine security activity.

During the period of January to April 2020, more than 48,000 malicious URLs were created, which would have been used for phishing attacks and malware delivery. With this acceleration level, now seems like a good time to step back, take a breath, and re-consider the basics of cybersecurity.

(Source: SecurityWeek)

Google's Waze can allow hackers to identify and track users

A security researcher discovered an API flaw in the Waze navigation app that allowed hackers to track the specific movements of nearby drivers in real time and even identify exactly who they are.

Waze uses crowd-sourced info aimed at warning drivers about obstacles that may be in their way of an easy commute and then suggests alternative and faster routes around these obstacles. The apps also displays the location of other drivers in close proximity as well as their GPS locations.

(Source: ThreatPost)

How to pinpoint rogue Internet of Things devices on your network

A random device floating on your network may not be cause for concern – at first. But when did it join the network? What is it doing? Is it the only one? These questions can help discern a benign connected device from a malicious product trying to infiltrate an organization.

"The amount of unmanaged devices has pretty much exploded in the last five years," said the head of threat research at Awake Security in a talk last week. More people are connecting to corporate networks with devices that aren't managed to the level you might expect corporate infrastructure and devices to be managed.

This is a growing problem, in large part because most Internet of Things (IoT) device traffic is unencrypted.

(Source: DarkReading)

Phishing fears cause workers to reject real business communications

Employees are trying to avoid suspicious emails and phone calls, and rightly so, as they can result in malware infections and business email compromise attacks. But hyper-vigilance also has its drawbacks. The problem is that real communications and fake ones are getting harder to distinguish from each other.

(Source: SCMagazine)

Cyber Information and Incident Assistance Links

MS-ISAC
SOC@cisecurity.org
1-866-787-4722

IdentityTheft.gov

IC3

Cybercrime Support Network

General Information Links

FTC scam list

CISA alerts

Law Enforcement Cyber Center

TLP Information