Kentucky Hospital Research & Education Foundation
Emergency Preparedness Update
for May 21, 2021

Kentucky COVID Update for Friday

(WKYT) Governor Beshear reported 544 new COVID-19 cases on Friday, bringing the state total to 455,150 cases. The governor says the state is seeing a 2.62% positivity rate. Of Friday's new cases, 112 are in kids 18 or younger. There were five reported COVID-19 related deaths on Friday. That brings the state total to 6,698.

As of Friday, 365 people are hospitalized for COVID-19 related reasons, 108 are in the ICU, and 51 are on ventilators.

Story source: https://www.wkyt.com/app/2021/05/21/gov-beshear-reports-544-new-covid-19-cases-262-positivity-rate/

ASPR Focus on Healthcare Supply Chain
Extracts from the May 20th Edition

- ✓ FDA Authorizes Longer Time for Refrigeration Storage of Thawed Pfizer-BioNTech COVID-19 Vaccine Prior to Dilution, Making Vaccine More Widely Available
- ✓ Pfizer-BioNTech Will Start to Ship Smaller Packs of Its COVID-19 Vaccine, in a Effort to Reach More People
- ✓ Johnson & Johnson Vaccine Shipments to States Dwindle to Zero as Production Freeze Continues
- ✓ New Senate Legislation Would Enhance Pandemic Preparedness, Strengthen Medical Supply Chain

Read full ASPR Healthcare Supply Chain Edition <Click here for Web version>

Supporting Heroes Class for Public Safety on
HONOR and BENEFITS

This FREE six-hour class focuses on two important aspects of line-of-duty death, *HONOR and BENEFITS,* and examines how they are connected. June 8, 9 AM to 3:30 PM (ET). Location is in Prospect, KY (Louisville). Class size is limited. << Flyer >>

>>>> CLICK HERE TO REGISTER

"Conti Ransomware Attacks Impact Healthcare and First Responder Networks"

Summary: The FBI has posted an advisory on the InfraGard site which discusses that they have identified at least 16 Conti ransomware attacks targeting US healthcare and first responder networks, including law enforcement agencies, emergency medical services, 9-1-1 dispatch centers, and municipalities within the last year. These healthcare and first responder networks are among the more than 400 organizations worldwide victimized by Conti, over 290 of which are located in the U.S. Like most ransomware variants, Conti typically steals victims' files and encrypts the servers and workstations in an effort to force a ransom payment from the victim. The ransom letter instructs victims to contact the actors through an online portal to complete the transaction. If the ransom is not paid, the stolen data is sold or published to a public site controlled by the Conti actors. Ransom amounts vary widely and we assess are tailored to the victim. Recent ransom demands have been as high as $25 million.

Cyber attacks targeting networks used by emergency services personnel can delay access to real-time digital information, increasing safety risks to first responders and could endanger the public who rely on calls for service to not be delayed. Loss of access to law enforcement networks may impede investigative capabilities and create prosecution challenges. Targeting healthcare networks can delay access to vital information, potentially affecting care and treatment of patients including cancellation of procedures, rerouting to unaffected facilities, and compromise of Protected Health Information.

Conti actors gain unauthorized access to victim networks through weaponized malicious email links, attachments, or stolen Remote Desktop Protocol (RDP) credentials. Conti weaponizes Word documents with embedded Powershell scripts, initially staging code via the Word documents and then dropping other code onto the network, giving the actor access to deploy ransomware. Once Conti actors deploy the ransomware, they may stay in the network and beacon out using Anchor DNS.

Recommended Mitigations

- ➢ Regularly back up data, air gap, and password protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.
- ➢ Implement network segmentation.
- ➢ Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (i.e., hard drive, storage device, the cloud).
- ➢ Install updates/patch operating systems, software, and firmware as soon as they are released.

- Use multifactor authentication where possible.
- Use strong passwords and regularly change passwords to network systems and accounts, implementing the shortest acceptable timeframe for password changes. Avoid reusing passwords for multiple accounts.
- Disable unused remote access/RDP ports and monitor remote access/RDP logs.
- Require administrator credentials to install software.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
- Install and regularly update anti-virus and anti-malware software on all hosts.
- Only use secure networks and avoid using public Wi-Fi networks. Consider installing and using a VPN.
- Consider adding an email banner to messages coming from outside your organizations.
- Disable hyperlinks in received emails.
- Focus on cyber security awareness and training. Regularly provide users with training on information security principles and techniques as well as overall emerging cybersecurity risks and vulnerabilities (i.e., ransomware and phishing scams).

To review the full FLASH document you must login to the InfraGard system. This document is located on the secure site: Publications > Documents > Flash & Pins.

Not an InfraGard member? Learn more: https://www.infragard.org/Files/InfraGard_Brochure_10-11-2018.pdf

[Note as of May 21st: The InfraGard program is not currently accepting new applications. They will re-open the application process in the near term as they transition to a new application form. They apologize for any inconvenience. Please check back: https://www.infragard.org/Application/General/NewApplication]]
