From the Division of Critical Infrastructure Protection | Office of Security, Intelligence, and Information Management

ASPR
ASSISTANT SECRETARY FOR
PREPAREDNESS AND RESPONSE

Healthcare and Public Health Sector Notification

Ransomware Activity Targeting the Healthcare and Public Health Sector (Update 2)

This email is from the the Division of Critical Infrastructure Protection (CIP) within the U.S. Department of Health and Human Services, Office of the Assistant Secretary for Preparedness and Response. For more information, e-mail CIP@hhs.gov or to subscribe to our email newsletters, visit our website.

Traffic Light Protocol (TLP) Designation: WHITE

○○○

TLP: WHITE information may be distributed without restriction.

Situation Update

This joint message was coauthored by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS).

CISA, FBI, and HHS continue to assess the threat of ransomware cybercriminal activity targeting the HPH sector. At this time, we consider the threat to be credible, ongoing, and persistent. Of note, some recent healthcare sector victims have experienced very short periods of time between initial compromise and activation – even under a few hours. CISA, FBI, and HHS urge health delivery organizations and other HPH sector entities to work towards enduring and operationally sustainable protections against ransomware threats both now and in the future.

Potential risk mitigation measures for consideration are included in the 28 Oct joint alert, “Ransomware Activity Targeting the Healthcare and Public Health Sector,” describing the use of Trickbot, BazarLoader, and other techniques to eventually deploy ransomware (like Ryuk) for extortion and financial gain. In general, maintaining anti-ransomware best practices like the 3-2-1 backup system or conducting regular vulnerability scanning to identify and address vulnerabilities will help protect your organization against future threats from other ransomware operators. Organizations should balance their operational needs with the current threat level and develop processes and postures for normal operating status and higher threat periods. The threat from ransomware is ongoing and entities should develop effective deterrent procedures while maintaining effective care delivery.

HHS, CISA, and FBI are closely monitoring both the threat and activity. We will provide further guidance as more information becomes available.

Upcoming HPH Sector Coordination Calls

At this time, no HPH Sector Coordination Calls are scheduled.

Reporting Incidents

Contacting FBI:

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field-offices, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at CyWatch@fbi.gov.

Please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

Contacting CISA:

To request incident response resources or technical assistance related to these threats, contact CISA at Central@cisa.dhs.gov.

Contacting the U.S. Food and Drug Administration:

In general, if you think you had a problem with your medical device or a medical device your patient uses, the FDA encourages you to report the problem through the MedWatch Voluntary Reporting Form.

For urgent matters, such as potential medical device impacts related to a cyber attack affecting your hospital system, please contact CyberMed@fda.hhs.gov.

***DISCLAIMER**: This product is provided "as is" for informational purposes only. The Department of Health and Human Services (HHS) does not provide any warranties of any kind regarding any information contained within. The HHS does not endorse any commercial product or service referenced in this product or otherwise. Further* *dissemination of this product is governed by the Traffic Light Protocol (TLP) marking noted above.*

You are receiving this information because you previously signed up for an ASPR CIP mailing list. If you do not want to receive communications from ASPR CIP or the HPH Sector, you can unsubscribe using the link at the bottom of this message.

ASPR
ASSISTANT SECRETARY FOR
PREPAREDNESS AND RESPONSE

U.S. Department of Health & Human Services, Office of the Assistant Secretary for Preparedness & Response
200 C Street, SW
Washington, DC 20024