American Hospital Association
Advancing Health in America
Cybersecurity Advisory

May 21, 2021

FBI Issues ‘Conti’ Ransomware Alert as High-impact Global Attacks Persist against Health Care and Critical Infrastructure

AHA, U.S. law enforcement warn of regular, regionally disruptive threats that could impact the delivery of patient care

The Federal Bureau of Investigation May 20 issued an alert regarding “Conti,” a highly disruptive ransomware variant. Attacks associated with Conti and the previously published Darkside ransomware variant are believed to be emanating from criminal networks operating from a non-cooperative foreign jurisdiction.

The FBI says it identified at least 16 Conti ransomware attacks targeting U.S. health care and first responder networks, including law enforcement agencies, emergency medical services, 911 dispatch centers and municipalities within the last year.

Ransomware attacks associated with these variants have resulted in regionally disruptive impacts to critical infrastructure, including hospitals and health systems in the United States and Ireland. Most recently, hospitals in New Zealand have been hit by disruptive ransomware attacks.

These ransomware attacks have delayed or disrupted the delivery of patient care and pose significant potential risks to patient safety and the communities that rely on hospitals’ availability.

AHA TAKE

The AHA remains concerned about cyberattacks with the potential to disrupt patient care and jeopardize patient safety. As stated in our testimony before the Senate Homeland Security Committee in December 2020, AHA believes that a ransomware attack on a hospital or health system crosses the line from an economic crime to a threat-to-life crime.

The AHA acknowledges and commends the U.S. government’s efforts to share timely and actionable cyber-threat intelligence. However, relying on victimized organizations to individually defend themselves against these attacks is not the solution to this national strategic threat. The vast majority of these attacks originate from outside the United States, often beyond the reach of U.S. law enforcement, where ransomware gangs are provided safe harbor and allowed to operate with impunity, sometimes with the active assistance of adversarial nations.

In response, the AHA has urged the government to embark upon a coordinated campaign that will use all diplomatic, financial, law enforcement, intelligence and military cyber capabilities to disrupt these criminal organizations and seize their illegal proceeds, as was done so effectively during the global fight against terrorism.

What You Can Do

Please review and share with your leadership and cyber security teams the following compilation of the latest federal government ransomware bulletins. Along with AHA and partner resources, below contains details on ransomware technical signatures and best practices for preventing and responding to ransomware attacks. These include the need for highly secure, network segmented network and data backups; the use of multi-factor authentication for all remote access to networks and privilege escalation; and the importance of a current, frequently tested cross function cyber incident response plan.

- FBI Liaison Alert System (FLASH) CP-000147-MW TLP: WHITE, Conti
- Ransomware Attacks Impact Healthcare and First Responder Networks Cybersecurity and Information Security Agency's (CISA) Ransomware Activity Targeting the Healthcare and Public Health Sector Alert (AA20-302A)
- CISA's Ransomware Alerts and Tips page
- AHA's page on cybersecurity and risk advisory services
- Health and Public Health Sector Coordinating Council's crisis response guide to help health care providers respond to critical incidents
- Department of Health and Human Services Office of the Assistant Secretary for Preparedness and Response's comprehensive resource to help hospitals and health systems effectively care for patients and maintain business practices and readiness should a cybersecurity incident affect the health care operational environment
- National Institute of Standards and Technology's Tips and Tactics for Dealing with Ransomware
- Department of Health and Human Services' Health Sector Cybersecurity Coordination Center
- Institute for Security and Technology Ransomware Task Force's Combatting Ransomware Report

Further Questions

For more information on these or other related issues, contact John Riggi, AHA's senior advisor for cybersecurity and risk advisory services, at jriggi@aha.org.