36TH ANNUAL AHA RURAL HEALTH CARE | LEADERSHIP CONFERENCE

FEBRUARY 19-22, 2023 | SAN ANTONIO, TX

JW MARRIOTT SAN ANTONIO HILL COUNTRY

American Hospital Association™

Advancing Health in America

AHA Events

Defending Against Cyberthreats on a Rural Hospital Budget

Please note that the views expressed by the conference speakers do not necessarily reflect the views of the American Hospital Association.

Speakers

<u>John Riggi</u>

National Advisor for Cybersecurity and Risk

American Hospital Association

<u>Michael Hamilton</u>

Co-Founder and CISO

Critical Insight

Please note that the views expressed by the conference speakers do not necessarily reflect the views of the American Hospital Association.

Critical Insight

The preferred choice for hospitals

American Hospital Association Preferred Cybersecurity Provider for The Critical Insight Healthcare Security Program

American Hospital Association™
Preferred Cybersecurity Service

Managed Detection and Response

Catch intruders in minutes, not months.

HIPAA Security Risk Assessments

Compliance and custom action plans

Continuous Vulnerability Identification

Scan your network, with expert assistance included

Unwanted Outcomes, Actors

- Unauthorized disclosure of protected records
- Theft through business email compromise (BEC)
- Extortion through ransomware or denial-of-service
- Intentional disruption

- Organized crime
- Nation-states
- Mercenaries
- Activists
  - **All using…**
- Gullible Insiders
- Unaddressed technical issues
- Overly permissive user access

The Criminal Ecosystem

January 10, 2023

Sophisticated Cybercrime Group Targeting Health Care Providers

John Schieszer, MA

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and Department of Health and Human Services (HHS) are warning health care providers about the Daixin Team. It is a ransomware and data extortion group that is actively targeting US businesses, predominantly in the Healthcare and Public Health (HPH) Sector, with ransomware and data extortion operations.

Daixin Team actors gain initial access to health care targets through virtual private network servers. *Credit: Getty Images.*

The new advisory was issued because the FBI Internet Crime Complaint Center (IC3) reported victims were being targeted by the Daixin Team with malware across all 16 critical infrastructure sectors. However, the HPH Sector accounted for 25% of ransomware attacks. According to an IC3 annual report in 2021, 649 ransomware reports were made across 14 critical infrastructure sectors and the HPH Sector accounted for the most reports at 148.

The Daixin Team has been targeting the HPH Sector with ransomware and data extortion operations since at least June 2022. Since then, the Daixin Team cybercrime actors have caused ransomware incidents at multiple HPH sector organizations where they deployed ransomware to encrypt servers responsible for health care services, including electronic health records, diagnostics, imaging, and intranet services, personal identifiable information (PII), and protected health information (PHI). The group also threatened to release the information if a ransom was not paid.

- Operates as a corporation
- Hack-for-hire mercenaries
- State-connected actors
- Optimizing efficiency and risk management
- Distributed tasking: initial access, lateral movement, privilege escalation, payload deployment
- Affiliate programs and ransomware-as-a-service
- Targeting based on criticality and cost of downtime
- Coding competitions, conferences, bonuses

Add To That…

- Russia: FBI warns that Sandworm state-affiliated group is deploying ransomware
- China: Accused of $20M in financial fraud perpetrated by APT41, a state-sponsored group
- North Korea: large-scale theft of cryptocurrency and financial sector funds, used to fund weapons programs

Russian Sandworm Hackers Linked to New Ransomware Blitz

An infamous Russian state-backed APT group could be behind a new wave of ransomware attacks against Ukrainian targets, according to researchers at ESET.

The security vendor claimed in a series of tweets that it alerted the Ukrainian Computer Emergency Response Team (CERT-UA) about the RansomBoggs variant it discovered targeting several local organizations.

The .NET malware is new, but deployed in a similar manner to previous campaigns linked to the Russian military intelligence (GRU) Sandworm group, it said.

There are apparently several references to Pixar movie Monsters Inc. in the malware.

"The ransom note (SullivanDecryptsYourFiles.txt) shows the authors impersonate James P. Sullivan, the main character of the movie, whose job is to scare kids. The executable file is also named Sullivan.exe and references are present in the code as well," ESET explained.

"There are similarities with previous attacks conducted by Sandworm: a PowerShell script used to distribute the .NET ransomware from the domain controller is almost identical to the one seen last April during the Industroyer2 attacks against the energy sector."

That script has been dubbed "PowerGap" by CERT-UA and was also used to deploy the destructive CaddyWiper malware alongside Industroyer 2 at the time, using the ArguePatch loader.

"RansomBoggs generates a random key and encrypts files using AES-256 in CBC mode (not AES-128 like mentioned in the ransom note), and appends the .chsch file extension. The key is then RSA encrypted and written to aes.bin," ESET continued.

Rural Health Targeted

Why Hackers are Going 'Down Market' In their Attacks

HHS alert warns KillNet hacktivist group targeted US healthcare entity

"While KillNet's DDoS attacks usually do not cause major damage, they can cause service outages lasting several hours or even days," according to the alert. "The group should be considered a threat to government and critical infrastructure organizations, including healthcare."

https://www.scmagazine.com/analysis/threat-intelligence/hhs-alert-warns-killnet-hacktivist-group-targeted-us-healthcare-entity

At small and rural hospitals, ransomware attacks are causing unprecedented crises

Hackers shifting focus to small hospitals, clinics and tech companies to siphon off patient data, report finds

Cybersecurity investments could go by the wayside at cash-strapped hospitals, Fitch warns

National Rural Health Resource Center

[Cybersecurity Toolkit for Rural Hospitals and Clinics | National Rural Health Resource Center (ruralcenter.org)]

Cybersecurity Toolkit for Rural Hospitals and Clinics

Downloads & Links

Cybersecurity Toolkit for Rural Hospitals and Clinics (PDF Document - 16 pages)

April 2020
Author: National Rural Health Resource Center (The Center)

Ransomware and cybercrime are growing threats to all health care facilities – big or small. Protecting a facility for cyber threats can be a daunting task. However, failure to protect a facility from cyber attacks can result in fees, fines, litigation, media stories, mistrust, and decreased market capture.

The toolkit is organized into four steps to guide rural hospitals and clinics in developing and fostering a well-rounded cybersecurity program, including awareness, assessment, implementation & remediation, and education. This toolkit includes a survey of available resources from various governmental and non-profit organizations. It includes checklists and tools that are appropriate for all audiences, including hospitals and clinics in rural settings.

"Bang-for-the-Buck" Focus Areas

- Limiting user access to the Internet
- Training and testing users
- Preparing for and practicing incident response
- Using multi-factor authentication
- Identifying Medical IoT and using strong access-control
- Use of managed and professional services
- Interns!
- Hospital Districts – use the SLCGP funding