Ransomware in the Healthcare Industry

Dan Costa

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM21-0951

Overview

What is Ransomware?

Who's Behind This Activity?

Why Does This Matter To Us?

What Should We Do About It?

Background / Context

- Critical business process are increasingly reliant on technology
  - … and attackers know this
- Cybercriminals are opportunistic – they seek to take advantage of periods of organizational stress
  - … for example, unprecedented levels of need for healthcare services
- Supply chains continue to increase in complexity
  - … vulnerabilities in the systems of your service providers are your vulnerabilities too
- Cybercriminals continue to increase in their technical sophistication
  - … and have found a market for the tools they use to carry out their attacks

What is Ransomware?

Malware designed to encrypt and exfiltrate data

- Dozens of distinct malware families

Impact of ransomware in the healthcare industry:

- 34% of healthcare organizations were victim to a ransomware attack in the last year
- Average cost to recover from an attack: $1.27M
- In 2020, 92 individual ransomware attacks affected over 600 clinics, hospitals, and other healthcare organizations
  - 18 million patient records affected
  - Estimated cost of $21B

https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-in-healthcare-2021-wp.pdf
https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/

How a Ransomware Attack Works

Attackers g
an organiz
systems

•Primary me
engineering
exploits of

een
kers make
n

ups on user's
eft on file
a email, the
" web page

Who's Doing This?

Cybercriminal Organizations

- Motivated by financial gain
- Willing to invest the time and resources needed to launch sophisticated attacks
- Rapidly-growing technical expertise

Script Kiddies

- Motivated by financial gain
- Consumers of "Ransomware-as-a-service" products
- "Spray and pray" approach

More than 290 enterprises hit by 6 ransomware groups in 2021

A report from eSentire said the six groups have already brought in more than $45 million this year from dozens of local governments, hospitals, universities and multinational conglomerates.

FBI, others crush REvil using ransomware gang's favorite tactic against it

Multi-nation operation succeeds as gang member makes critical mistake.

Notable Incidents in the Healthcare Industry

Universal Health Services reports $67 million in losses after apparent ransomware attack

California Provider to Close After Ransomware Attack Damages System

US healthcare organizations impacted by Blackbaud ransomware attack

‹ Page 5 of 6 ›

Date Reported	Hospital/Organization Name	State	Records Affected
September 14, 2020	Lehigh Valley Health Network	Pennsylvania	81,487
August 26, 2020	Main Line Health	Pennsylvania	60,595
August 17, 2020	Richard J. Caron Foundation	Pennsylvania	22,718
September 8, 2020	The Guthrie Clinic	Pennsylvania	92,064
September 11, 2020	Medical University of South Carolina	South Carolina	54,869
September 8, 2020	Roper st. Francis Healthcare	South Carolina	92,963
September 14, 2020	University of Tennessee Medical Center	Tennessee	234,954

Organizational Defenses Against Ransomware

Phishing Awareness Training

Network Perimeter Defenses and Segmentation

Software Patches

Backup and Recovery Systems

Encryption

Your Role In Defending Against Ransomware

Follow the instructions of your security team

Report suspicious activity

Make sure your data is being backed up

Q&A

For More Information

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=645032

https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-in-healthcare-2021-wp.pdf

https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/

Presenter Contact Information:

Dan Costa, CISSP

Technical Manager, Enterprise Threat and Vulnerability Management

CERT Division, Carnegie Mellon University Software Engineering Institute

dlcosta@sei.cmu.edu