GORILLA GUIDE® TRAIL MAP

Ransomware for Healthcare

Understand what's behind the recent explosion of ransomware attacks, what unique risks are faced by healthcare providers and how they can protect themselves.

KEY TERMS

Ransomware:
- A type of malware attack that involves extortion.

Data Exfiltration:
- When data is copied or transferred without authorization.

Big Game Hunting (BGH):
- Big game hunting is a ransomware tactic that involves a highly focused and sophisticated attack on a target capable of paying a large ransom.

Threat Intelligence:
- Data that's collected, processed and analyzed to understand a threat actor's motives, targets and attack behaviors.

Exploit Kit:
- An exploit kit is an automated piece of malware that requires very little technical knowledge to use, making it an integral part of the ransomware-as-a-service ecosystem.

The Crime That Keeps Changing

(LEAP TO CHAPTER 1)

- Despite being around since the 1980s, ransomware became seriously popular among cybercriminals with the advent of cryptocurrencies in 2010.
- Ransomware isn't just about the money — it's often employed as a "cover" to distract from other crimes, such as data exfiltration.
- Understanding the motivations of attackers increases the probability of successfully navigating a ransomware incident.

The World of Cybercrime

(LEAP TO CHAPTER 2)

- Cybercrime has evolved into a full-fledged criminal industry, complete with specializations, as well as continual innovation and upskilling.
- Learn about the patching dilemma, and why this is a particular problem for healthcare providers.
- Exploit kits, fileless malware and Big Game Hunting are among many tools and tactics used by attackers.

Crime as a Service

(LEAP TO CHAPTER 3)

- Cybercrime specialization lowers the barrier to entry — it's easy to purchase access to networks from access specialists, as well as malware (such as ransomware) from cybercrime software vendors.
- An exploit market allows cybercriminals to buy knowledge of vulnerabilities unknown to a product's vendor, and/or the code required to exploit these vulnerabilities.
- Learn about the evolving role of cyber insurance; regular payouts tempt attackers while also causing insurance companies to adapt their policies to minimize risk.

The Ransom Dilemma

(LEAP TO CHAPTER 4)

- The importance of having a plan: Criminals rely on their victims making poor decisions under pressure!
- Proactive planning — and testing! — such as having backups and an incident response plan, makes it easier to choose not to pay the ransom.
- Know who to notify and how to contact them if the worst happens.

Defending Yourself Against Ransomware

(LEAP TO CHAPTER 5)

- Lean the basics of modern network defense: Prevent, detect, respond and predict.
- The best defense against ransomware remains a "defense in depth" approach: Make use of multiple technologies to defend against attack, while also preparing for how to deal with a cybersecurity incident should one occur.
- Threat intelligence is increasingly important for gaining an understanding of where to focus your efforts and how to appropriately deal with incidents, should they occur.

Download the Full Gorilla Guide

This Gorilla Guide will give you an understanding of the cybercrime economy that supports and launches these attacks and will explain the crucial role of threat intelligence in any defense strategy.

Highlights include:
- A short history of ransomware
- The world of cybercrime
- Ransom dilemma: Plan for the worst
- Gain intelligence about the threats

DOWNLOAD TODAY!

DEVELOPED BY ActualTech MEDIA