GORILLA GUIDE® TRAIL MAP

Ransomware for Corporations

Ransomware can happen to anyone, at any time — it is a “when,” not an “if.” Join us to explore the current state of ransomware and the unique threat it poses to corporations of all sizes. Understand what’s behind the recent explosion of ransomware attacks and how corporations can protect themselves.

KEY TERMS

Ransomware:

- A type of malware attack that involves extortion.

Phishing:

- Phishing is a scam wherein a user is duped (as by a deceptive email message) into revealing personal or confidential information.

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.

Breakout time:

- The time it takes an attacker to move beyond their point of initial compromise and compromise another workload or device on the network.

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, ranging from data exfiltration to nation-state espionage or even cyber warfare
- Understanding the motivations of attackers increases the probability of successfully navigating a ransomware incident.

The World of Cybercrime

(LEAP TO CHAPTER 2)

- Attacker specialization is driving a diversified cybercrime economy.
- 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)

- Explore how cyber insurance providers are altering their response to a changing cybercrime ecosystem.
- Supply chain attacks work both ways; defenders take advantage of social splits in attacker groups to learn more about criminal activities.
- 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.

The Ransom Dilemma

(LEAP TO CHAPTER 4)

- To pay or not pay the ransom is an increasingly common legal and ethical dilemma.
- 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.

Defending Yourself Against Ransomware

(LEAP TO CHAPTER 5)

- Learn the basics of modern network defense: prevent, detect, respond and predict.
- The best defense against ransomware remains a “defense in depth” approach: Multiple tools and techniques are needed, including classic defenses such as network segmentation.
- 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

The Gorilla Guide® To... Ransomware for Corporations, Express Edition, will give readers an understanding of the cybercrime economy that supports and launches ransomware attacks, discuss the security challenges faced by corporations and 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

GET YOUR COPY!

the GORILLA GUIDE to...

Ransomware for Corporations

How Best To Defend Your Corporation Against Ransomware

KATHERINE GORHAM

CROWDSTRIKE DLT

POWERED BY ActualTech

DEVELOPED BY ActualTech MEDIA

www.gorilla.guide