GORILLA GUIDE TRAIL MAP

Ransomware for Govies

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 government organizations of all sizes.

Key Terms

Ransomware:

- A type of malware attack that involves extortion.

Data Exfiltration:

- When data is copied or transferred without authorization.

Cryptocurrency:

- Cryptographically secured data that serves as a digital currency (for example, Bitcoin).

Threat Intelligence:

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

Phishing:

- A scam that attempts to dupe an internet user into revealing personal or confidential information (such as through a deceptive email message) that the scammer can use illicitly.

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, with different threat actors specializing in different crimes.
- Phishing and failure to patch software and devices are the two most common vulnerabilities that lead to compromise.
- Cybercrime specialization has advanced to the point that many threat actors now specialize in attacking specific verticals, such as government, education or healthcare.

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.
- Crime as a service includes operational knowledge, such as playbooks, designed to make engaging in cybercrime easier.
- 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.
- Proactive planning, such as having backups and an incident response plan, makes it easier to choose not to pay the ransom.
- Vendors in the cybersecurity space can help you deal with your cybersecurity incidents.

Defending Yourself Against Ransomware

(LEAP TO CHAPTER 5)

- 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.
- Just as cybercriminals are specializing, so too are cybersecurity experts: Securing your network requires bringing together knowledge from multiple security domains.
- 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

GET YOUR COPY!

DEVELOPED BY ActualTech MEDIA