Ransomware vs Other Attacks

Similarities and Key Differences

Digital Silence

About Digital Silence

Digital Silence was founded with one goal in mind — to do security consulting *right*. Consistency, commitment to quality, attention to detail, and unsurpassed client care are central to our company's culture and ethos. We strive to be active contributors to the security community and have dedicated training and R&D programs staffed by passionate instructors and researchers.

Our passion and commitment to quality is reflected in both the services we provide and the people we hire.

About

Devin Hill, MS, Digital Forensics & Cyber Investigation

Director of Digital Forensics & Incident Response

Throughout his career, Devin has supported incident teams of various sizes and complexity, including servicing a large inflow of insurance panels and legal work. Devin's focus on finding the threat actor(s) and their motive, techniques, and tactics, along with identifying the steps needed to remediate the issue enables him to support customers in quickly and effectively. In order to make this process even more effective, Devin has written and continues to develop a number of custom tools and procedures that shorten the development of a comprehensive attack narrative, expediting remediation efforts.

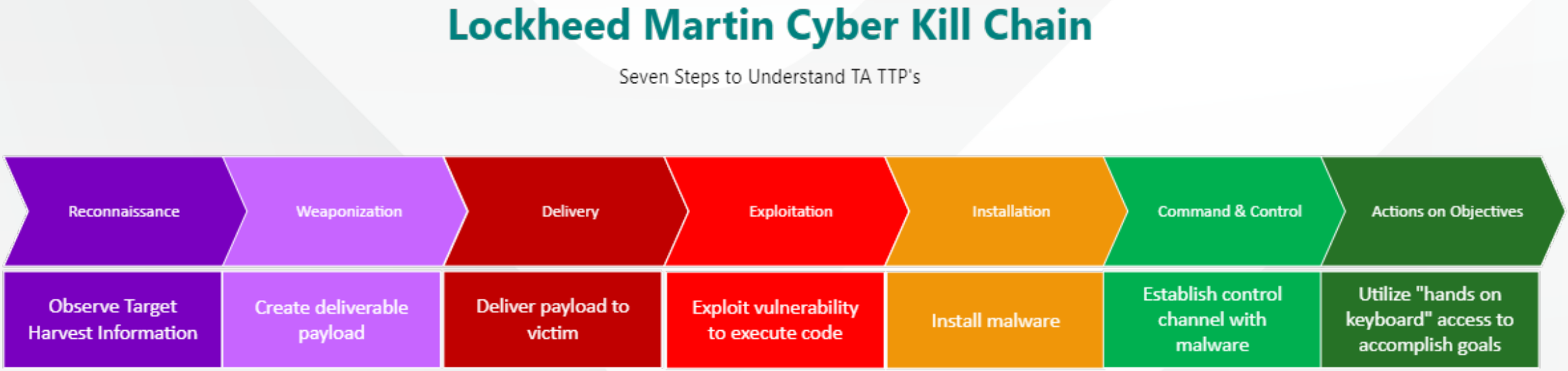
Introduction

Ransomware attacks are on the rise year after year, with no end in sight. As such, it's important to understand the additional challenges presented by ransomware as opposed to other attacks. This talk will:

- Discuss ransomware groups in general terms
- Focus on system intrusion attacks
- Not focus on AWS/Azure or Business Email Compromise attacks that don't specifically target workstations or servers

Kill Chain

Lockheed Martin Cyber Kill Chain

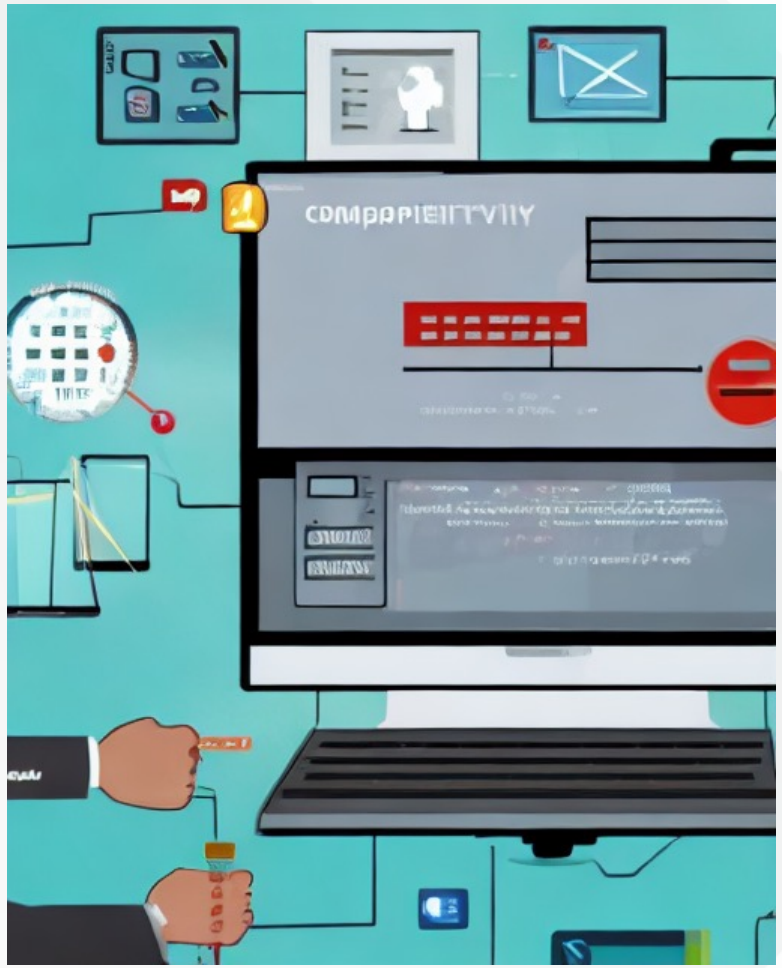


Similarities

Reconnaissance

- Choose a target (might be targeted or random scans)
- Vulnerability scan to outline attack surface
- Intel gathering about employees to target via phishing and other social engineering
- Skip straight to final attack phase by buying access

Weaponization



- Construct phishing messages
- Prepare droppers / configure remote shell
- Infect compromised site/create fake site to distribute malware

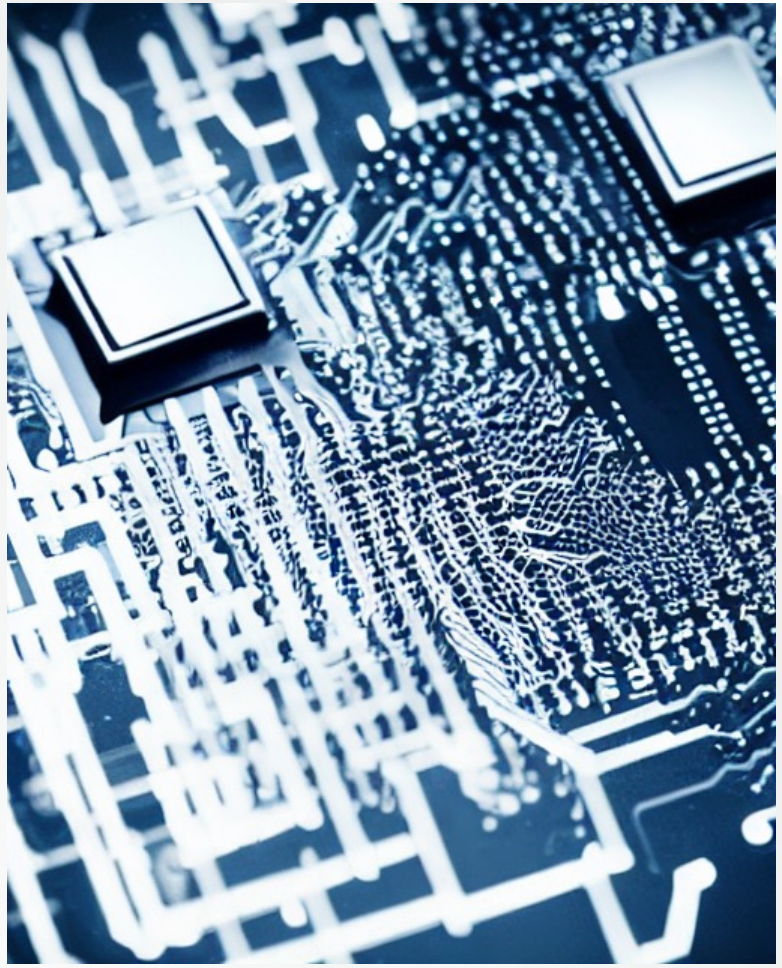
Delivery

Send phishing messages

Drop web shell onto vulnerable web server

User visits compromised web site that downloads dropper

Exploitation

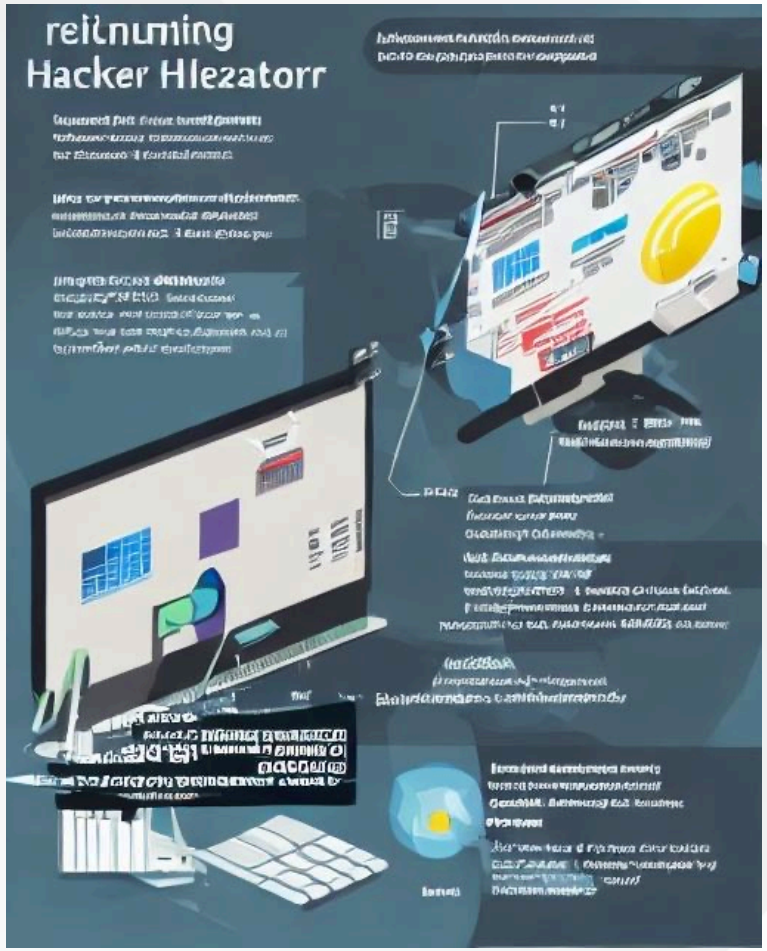


- User clicks phishing message
- TA sends calls to “activate” webshell
- Open RDP/brute force attack
- VPN RCE to dump credential database

Installation

- User opens executable from phishing email
- Web shell utilized to install backdoor
- Downloaded dropper pulls down backdoor
- TA installs backdoor manually via RDP connection

Command & Control (C2)



Dropper establishes comms with C2 to download backdoor

Backdoor establishes comms with C2 to allow TA access

Actions on Objectives

Common Thread: **Extortion**

- Data theft used to extort ransomware victims into paying ransom
- May also be used by state-sponsored actors to intimidate politicians and rich/famous people

Differences

Actions on Objectives

More smash and grab methodology

Use more off-the-shelf tools

Mimikatz

Cobalt Strike

PSEXEC

Adfind.exe

Ransomware groups less likely to use 0-days

Shorter dwell time

Threat Actor Communications

- Need to talk to Threat Actor to:
  - Get decryptor to recover encrypted files
  - Pay ransom to prevent data leakage
- Office of Foreign Assets Control
  - Check to ensure threat actor isn't a sanctioned entity

Reasons for Differences

Ransomware groups

- In it for the money
- All actions taken to make sure ransom is paid
- Not worried about getting caught

- APT Groups
- State-run/sponsored APT group
  - Steal data for government use
  - Disrupt organizations to weaken economy
- Hacktivist APT groups
  - Expose corruption or other misdeeds

Key Takeaways

What defenders need to know

Key takeaways

- EDR Monitoring
  - Shorter dwell time increases need for monitoring
- TA communications
  - Threat actor communications/negotiations add another layer to recovery efforts