Agenda

- Ransomware Threat Comprehension
- Ransomware Response Playbooks
- Industry-wide Collaborative Efforts
RANSOMWARE THREAT COMPREHENSION
Redefining Ransomware

A type of malware that attempts financial extortion by gaining leverage over the victim's computing resources

- Crypto Ransomware
- Data Exfiltration Ransomware
- Purely Destructive “Ransomware”

Financially motivated

Politically / ideologically motivated
Overall Threat Landscape - Public Sector

- Public sectors systems under increased threat
- **Diversity** and refinement in attack vectors
- General responsiveness of ransomware actors
- **Targeted** and **manual** ransomware attacks gaining traction
- Increasing ransom demands indicate successful business model

Example scenario
- Organization hit with a ransomware
  - Attack vector: Compromised credentials
  - Impact: Multiple systems
  - Demand: $100,000 - $(MILLIONS)
Ransomware-as-a-Service (RaaS) versus The Victim
RANSOMWARE RESPONSE PLAYBOOKS
Ransomware Incident Response (FAQs)

- When does ransomware response begin?
  - Planning versus execution
- How regularly should the response playbook be updated?
  - Establishing update cadence
- How should the playbook be communicated?
  - Ensuring communication and comprehension
- When should response be escalated?
  - Establishing escalation criteria
- How to resolve ambiguity in the response playbooks?
  - Defining terms, teams, stakeholders, system tiers
- How to ensure proper containment?
  - Establishing timely containment procedures
- How to maintain an updated list of internal and external resources?
  - Enumerating response resources
Effective Ransomware Response Playbooks

1. KNOW YOUR ENVIRONMENTS - Hardware, Software, Applications, Data Flows
2. KNOW YOUR ADVERSARY - Who is attacking and how might they do it?
3. OUTLINE TEAMS AND RESPONSIBILITIES - Who is accountable / responsible for what?
4. OUTLINE INTERNAL AND EXTERNAL STAKEHOLDERS - Who should be involved?
5. UNDERSTAND, TEST, IMPROVE, REPEAT - Well-understood, Well-practiced response activities
6. ORDER OF OPERATIONS - Priorities and timelines
Challenges

- Creating a consistent criteria for assessing the true impact, scope, severity
- Tapping into the relevant threat intelligence feeds to update response strategy
- Comprehending the true cost of a ransomware incident

Strategic

Tactical

- Determining the appropriate internal and external stakeholders to be involved
- Assigning responsibilities while minimizing gaps and overlaps in response efforts
- Working with the affected teams to understand the architecture and technology stack
INDUSTRY-WIDE COLLABORATION
# Standardized Threat Mapping (MITRE ATT&CK)

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Exfiltration</th>
</tr>
</thead>
<tbody>
<tr>
<td>9 techniques</td>
<td>39 techniques</td>
<td>15 techniques</td>
<td>9 techniques</td>
<td>17 techniques</td>
<td>9 techniques</td>
</tr>
<tr>
<td>Drive-by Compromise</td>
<td>Abuse Elevation Control Mechanism</td>
<td>Brute Force</td>
<td>Exploitation of Remote Services</td>
<td>Archive Collected Data (3)</td>
<td>Automated Exfiltration (1)</td>
</tr>
<tr>
<td>Exploit Public-Facing Application</td>
<td>Access Token Manipulation (5)</td>
<td>Credentials from Password Stores (5)</td>
<td>Internal Spear phishing</td>
<td>Audio Capture</td>
<td>Data Transfer Size Limits</td>
</tr>
<tr>
<td>Hardware Additions</td>
<td>Build Image on Host</td>
<td>Forced Authentication</td>
<td>Remote Service Session Hijacking (2)</td>
<td>Clipboard Data</td>
<td>Exfiltration Over C2 Channel</td>
</tr>
<tr>
<td>Phishing (3)</td>
<td>Deobfuscate/Decode Files or Information</td>
<td>Forge Web Credentials (2)</td>
<td>Remote Services (6)</td>
<td>Data from Cloud Storage Object</td>
<td>Exfiltration Over Other Network Medium (1)</td>
</tr>
<tr>
<td>Replication Through Removable Media</td>
<td>Deploy Container</td>
<td>Input Capture (4)</td>
<td>Replication Through Removable Media</td>
<td>Data from Configuration Repository (2)</td>
<td></td>
</tr>
<tr>
<td>Supply Chain Compromise (3)</td>
<td>Direct Volume Access</td>
<td>Man-in-the-Middle (2)</td>
<td></td>
<td>Data from Information Repositories (2)</td>
<td></td>
</tr>
</tbody>
</table>
Rapid Standardized Communication

**Pre-incident analysis**
- Identify your specific security technology stack
- **Identify gaps in security coverage**
- Address gaps and reassess periodically

**Post-incident assessment**
- Identify gaps that led to the ransomware incident
- Identify additional security controls required to address these gaps
- Share lessons learned with the community

https://cyberdefensematrix.com/
Conclusion

- Post-breach assumption: strategize next steps
  - Zero-trust architectures
  - Response strategies
  - Business continuity and disaster recovery (beyond just backups)
- Know thy enemy:
  - RaaS, tactics, techniques, and procedures (TTPs), motives
  - Develop internal and/or external threat intelligence channels
- Know thyself:
  - Technology stacks, mission-critical environments
  - Gaps in security controls, visibility, detection methodologies
- Industry-wide collaboration:
  - Timely information-sharing via trusted partners
THANK YOU