**Incident Response Report**

Name: Damon Torres

Course: NWIT 247 – Incident Response

# Executive Summary

This report outlines the investigation of a cybersecurity incident involving potential ransomware activity. Through the six phases of the NIST incident response lifecycle—Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned—we examine the breach of Artemis Gas Inc., discuss attacker TTPs observed via MITRE ATT&CK framework, and make recommendations to strengthen incident handling.

# Timeline of the Breach Events

- 12:00 PM: Suspicious BitTorrent activity detected in network capture.  
- 12:15 PM: Analysts began reviewing PCAP with Wireshark.  
- 12:30 PM: Indicators of Compromise (IOCs) identified, including suspicious filenames and IP addresses.  
- 01:00 PM: Registry modification activity flagged.  
- 01:30 PM: Potential ransomware behavior matched against MITRE ATT&CK.  
- 02:00 PM: Containment recommendations submitted to management.

# NIST Incident Response Phases

1. \*\*Preparation:\*\* Team had tools ready (Wireshark, Sysinternals, MITRE ATT&CK Navigator).

2. \*\*Identification:\*\* Suspicious traffic and file transfer over BitTorrent protocol were found.

3. \*\*Containment:\*\* Host was isolated from network to prevent further spread.

4. \*\*Eradication:\*\* Malicious processes and registry entries identified for removal.

5. \*\*Recovery:\*\* System backups initiated, user accounts re-secured.

6. \*\*Lessons Learned:\*\* Emphasis on network segmentation, early threat detection, and endpoint monitoring.

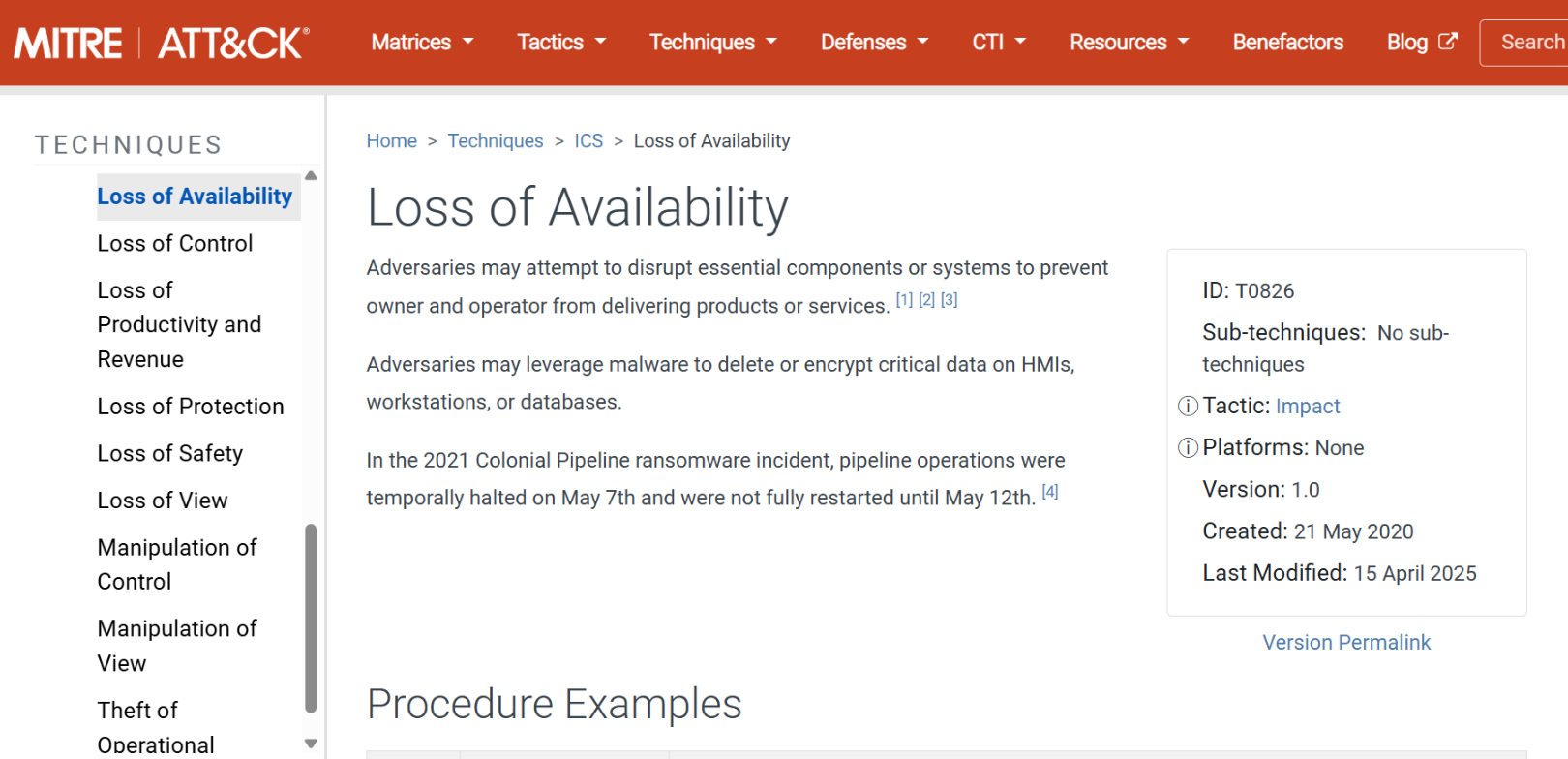
# Indicators of Compromise (IOCs)

|  |  |
| --- | --- |
| Indicator Type | Details |
| Filename | BitTorrent.avi |
| Protocol | BitTorrent |
| Registry Key | HKCU\Software\Microsoft\Windows\CurrentVersion\Run |
| Process | bittorrent.exe |
| MITRE Technique | T1112 - Modify Registry |

# Recommendations

• Deploy IDS/IPS across the network.  
• Regularly audit Windows Registry for unauthorized changes.  
• Educate employees on safe download practices.  
• Monitor outbound traffic for file-sharing patterns.  
• Apply principle of least privilege for user accounts.

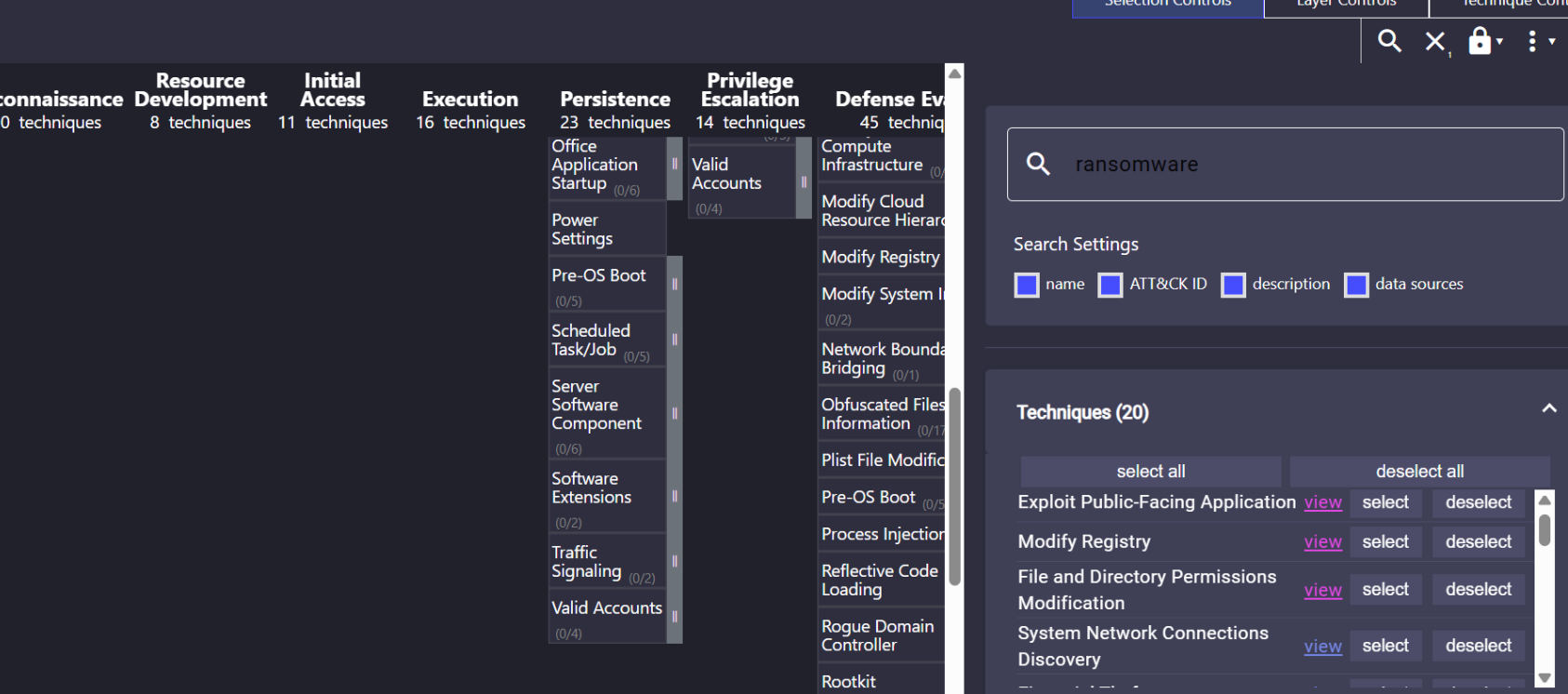
# Appendix: Screenshots



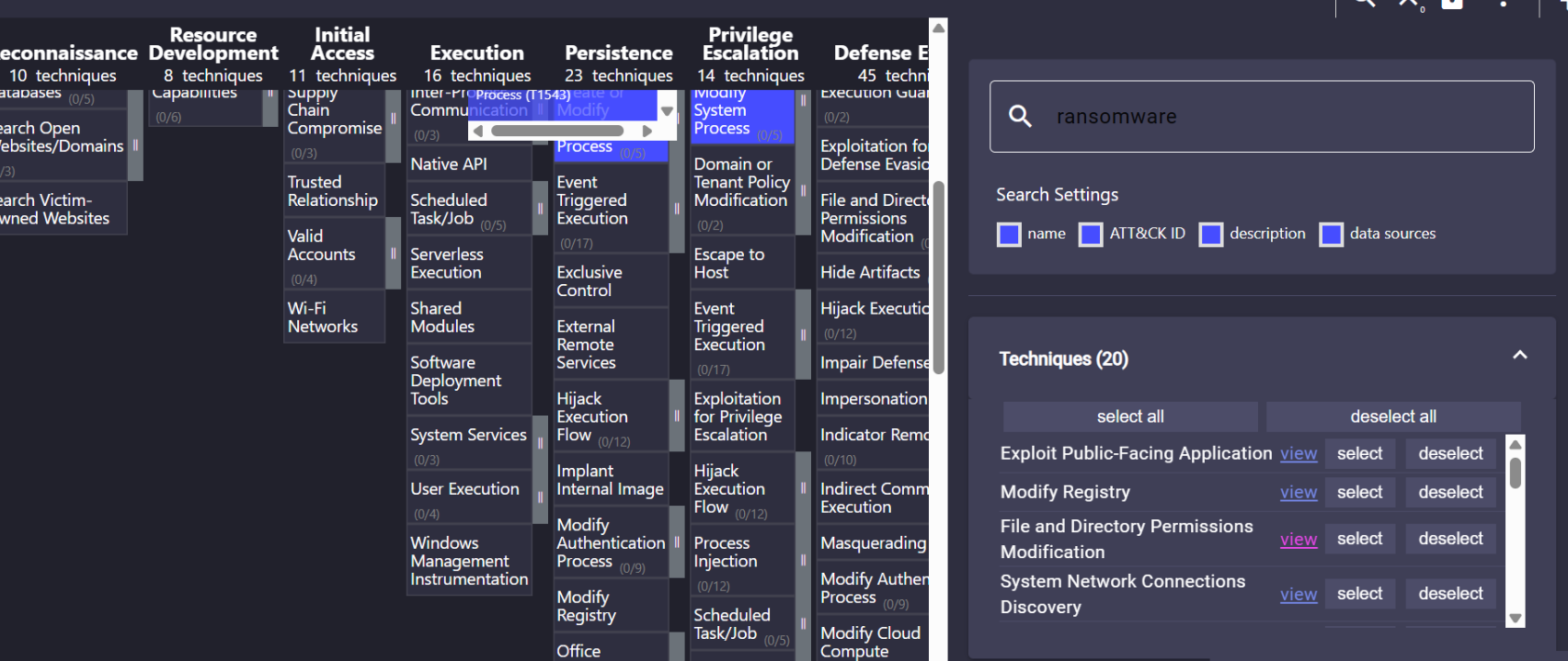
MITRE ATT&CK - Loss of Availability Technique



MITRE ATT&CK - Modify Registry Technique



MITRE ATT&CK - Techniques filtered for 'ransomware'



MITRE ATT&CK - Additional ransomware-related techniques