Threat Hunting Project Report

Threat Hunting in the Finance Sector using MITRE ATT&CK

Prepared By:
Junaid AbdulRahman A
Cybersecurity Analyst

Date:11 November 2025

Project Overview

This project focuses on proactive threat hunting within the Finance industry, leveraging the MITRE ATT&CK framework to identify and analyze Advanced Persistent Threat (APT) groups targeting the sector.

The objective was to:

- Identify Finance targeted APTs.
- Analyze their Tactics, Techniques, and Procedures (TTPs).
- Visualize the threat landscape using MITRE Navigator.
- Compare APTs to find common attack vectors.

Objectives

1. Understand the MITRE ATT&CK framework and its application to real-world threat hunting.
2. Research APTs targeting the Finance sector using SOCRadar Labs.
3. Map identified APTs to relevant TTPs in MITRE ATT&CK Navigator.
4. Perform a comparative analysis to highlight overlapping attack patterns.

Tools & Resources

- SOCRadar Labs – For retrieving Finance specific APTs.
- MITRE ATT&CK Navigator – For mapping APTs to their TTPs.
- MITRE ATT&CK Framework – For structured adversary behavior taxonomy.
- OSINT Research – To cross-check TTP details from open sources.

Project Steps

1. Understanding the MITRE ATT&CK Framework

- Studied the MITRE ATT&CK framework structure:

. Tactics – The why of an attack (e.g., Initial Access, Persistence, Defense Evasion, Credential Access, Collection, Command&Control, Exfiltration).
. Techniques – The how of an attack (e.g., phishing, credential dumping).
. Procedures – Real-world implementations of techniques

2. Research APTs Peculiar to the Sector

- Used SOCRadar Labs to identify APT groups targeting Financials sector.
- Found the following: .

. **Lazarus Group**- A North Korean state-sponsored cyber threat group that has been active since at least 2009.

. **Carbanak**- This is a cybercriminal group that has used Carbanak malware to target financial institutions since at least 2013.

. **OilRig-** is a suspected Iranian threat group that has targeted Middle Eastern and international victims since at least 2014. The group has targeted a variety of sectors, including financial, government, energy, chemical, and telecommunications.

. **Cobalt Group-** is a financially motivated threat group that has primarily targeted financial institutions since at least 2016. Cobalt Group has mainly targeted Financial sectors in Eastern Europe, Central Asia, and Southeast Asia.

. **Scattered Spider**- is a native English speaking cybercriminal group active since at least 2022. The group initially targeted customer relationship management (CRM) providers, business process outsourcing (BPO) firms, and telecommunications companies before expanding in 2023 to retail, manufacturing, and financial sectors.

3. Highlight of the TTPs

- For each APT, identified their key TTPs from MITRE:

Example (Cobalt Group):

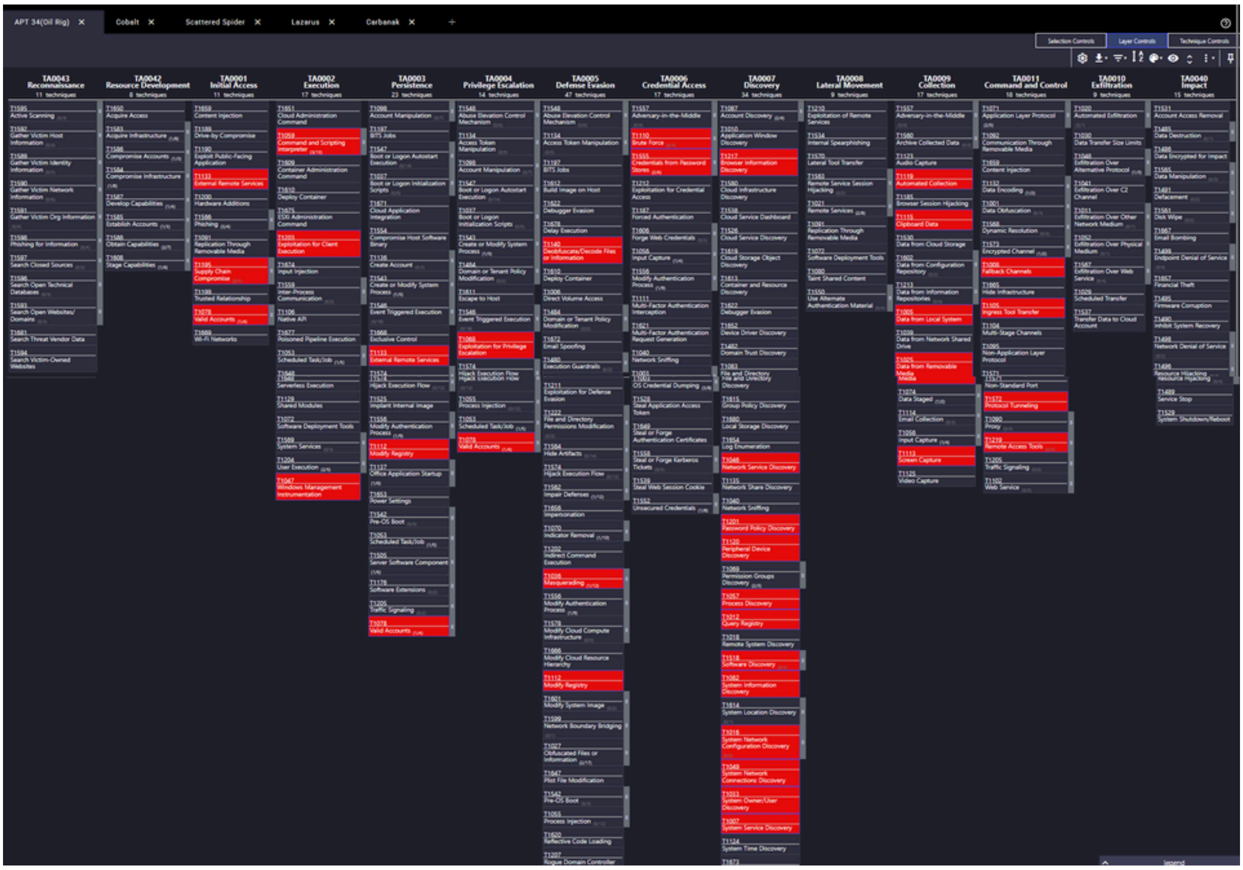
- T1203 – Exploitation for client execution.
- T1055 – Process injection.
- T1572 – Protocol tunneling.
- T1068 – Exploitation for priviledge escalation.
- T1219 – Remote access tool.

4. Map APTs to TTPs using MITRE Navigator

- Created individual layers in MITRE Navigator for each APT.
- Color-coded:

. Red – Techniques confirmed for Oil Rig.
. Orange – Techniques confirmed for Cobalt.
. Yellow – Techniques confirmed for Scattered Spider.
. Green – Techniques confirmed for Lazarus.
. Blue – Techniques confirmed for Carbanak.

TTPs mapped for Oil Rig



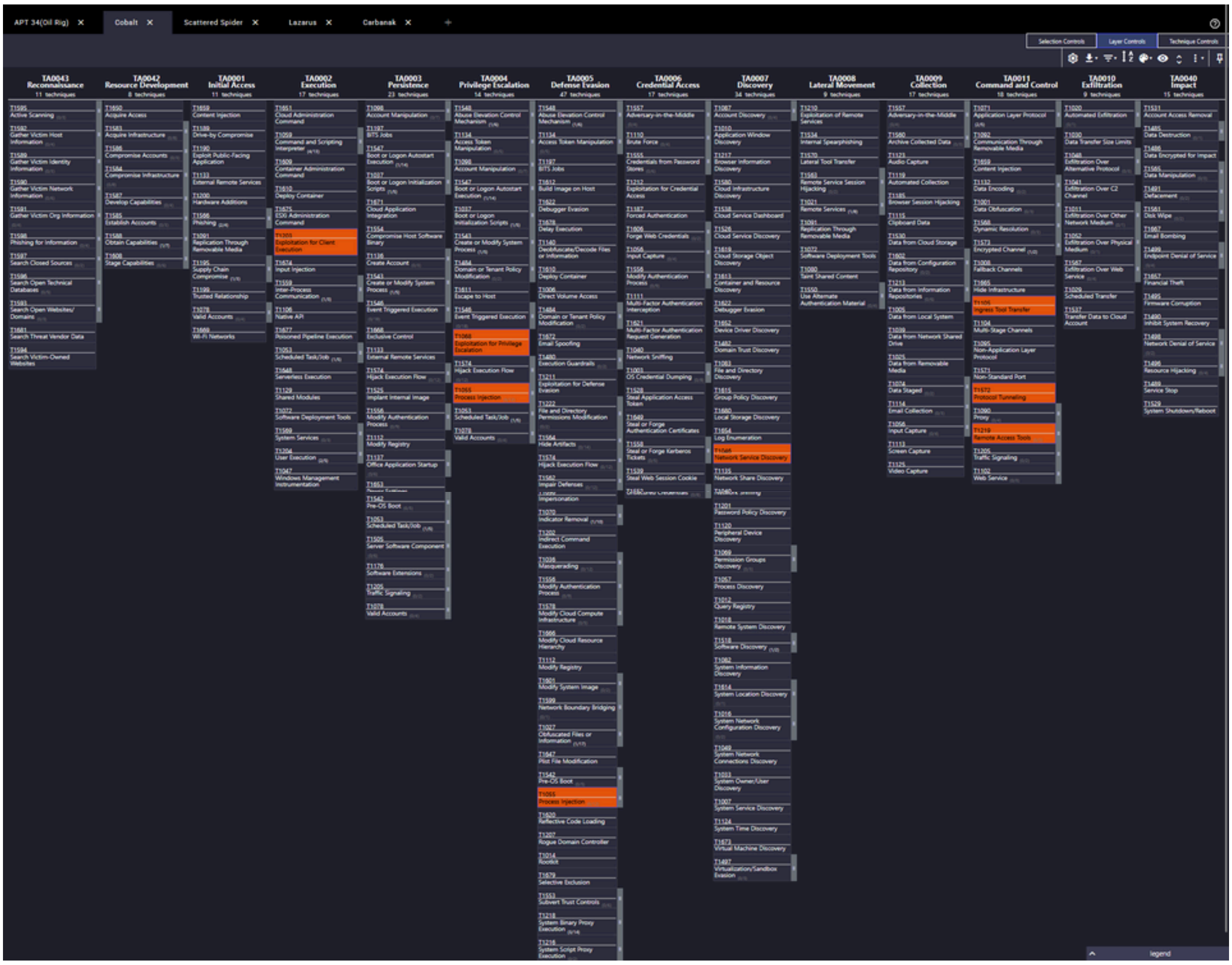
APT 34(Oil Rig) ✕ | Cobalt ✕ | Scattered Spider ✕ | Lazarus ✕ | Carbanak ✕ | +

Selection Controls | Layer Controls | Technique Controls

TA0043 Reconnaissance	TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control	TA0010 Exfiltration	TA0040 Impact
11 techniques	8 techniques	11 techniques	17 techniques	23 techniques	14 techniques	47 techniques	17 techniques	34 techniques	9 techniques	17 techniques	18 techniques	9 techniques	15 techniques

legend

TTPs mapped for Cobalt



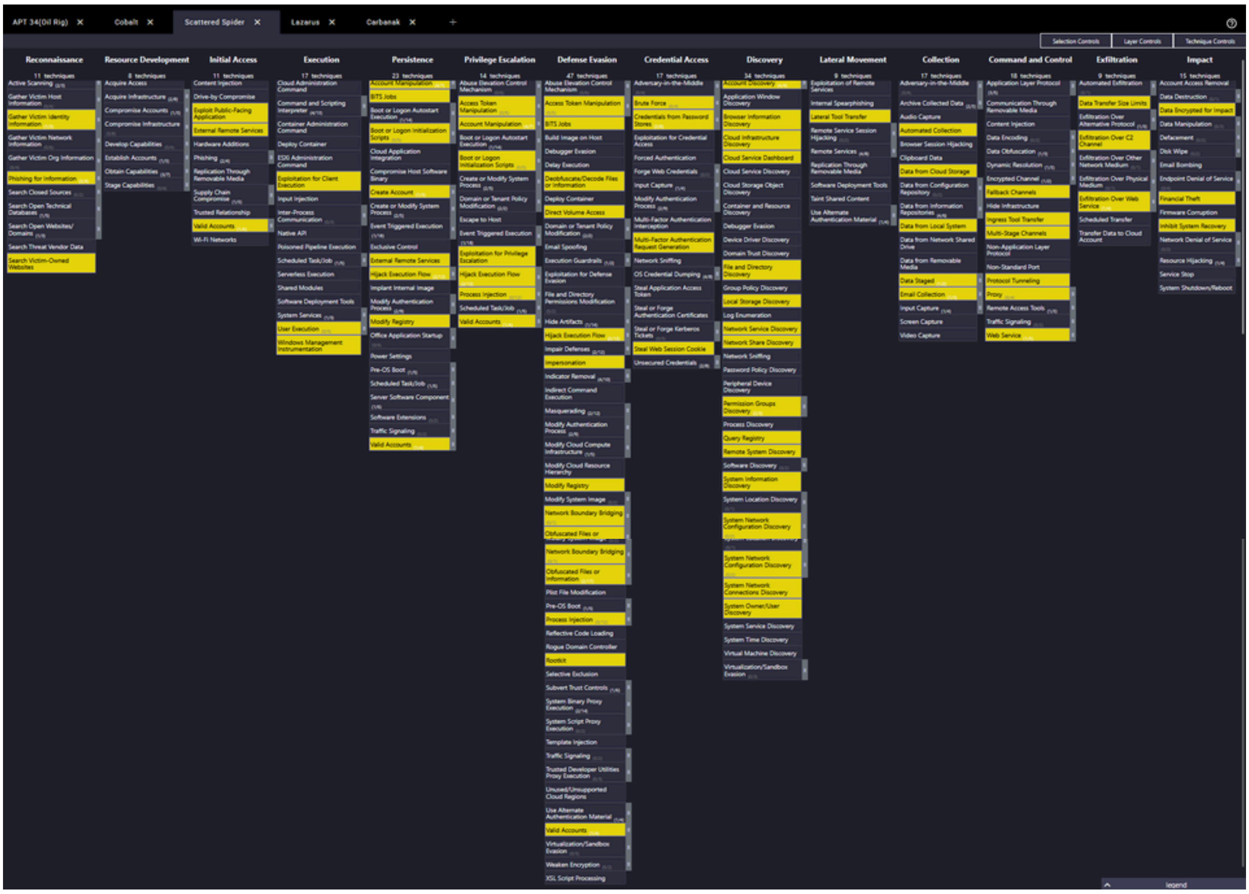
APT 34(Oil Rig) ✕ | Cobalt ✕ | Scattered Spider ✕ | Lazarus ✕ | Carbanak ✕ | +

Selection Controls | Layer Controls | Technique Controls

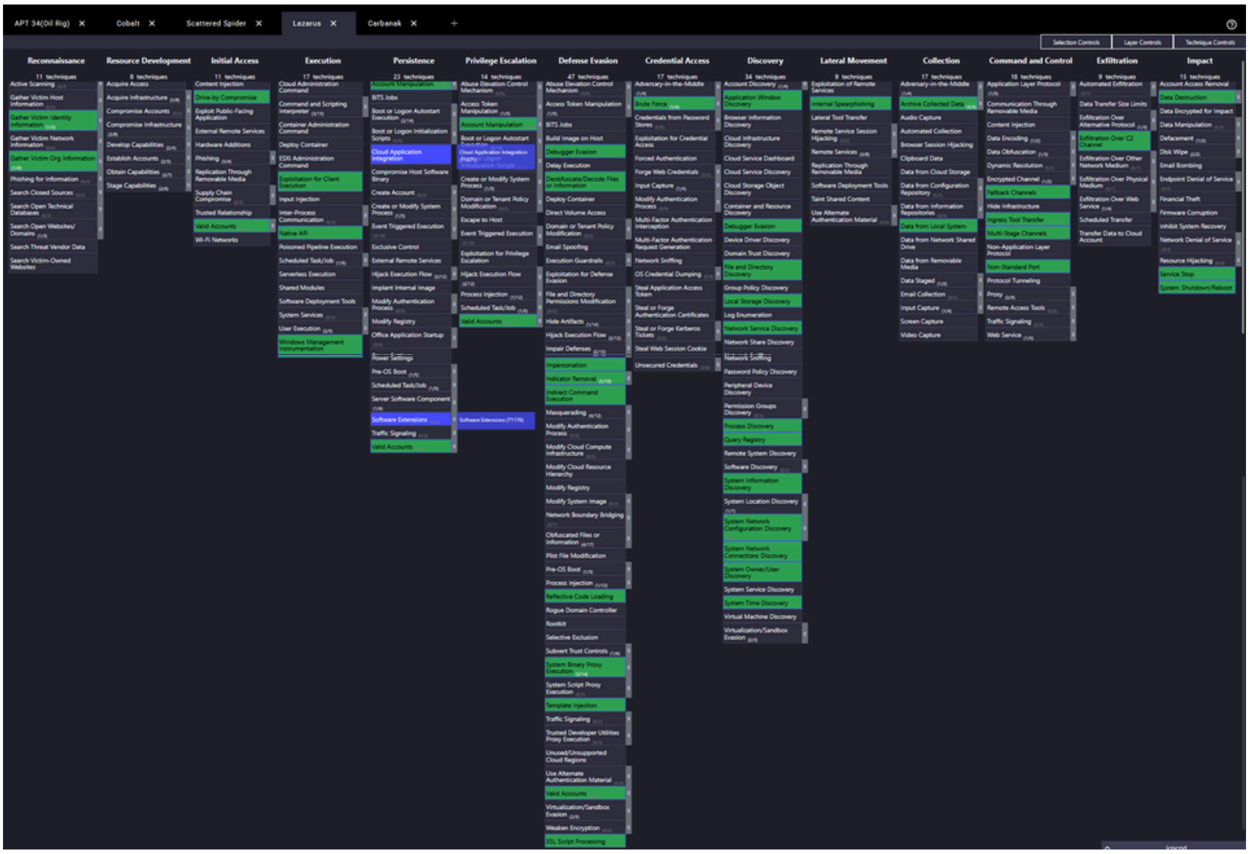
TA0043 Reconnaissance	TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control	TA0010 Exfiltration	TA0040 Impact
11 techniques	8 techniques	11 techniques	17 techniques	23 techniques	14 techniques	47 techniques	17 techniques	34 techniques	9 techniques	17 techniques	18 techniques	9 techniques	15 techniques

legend

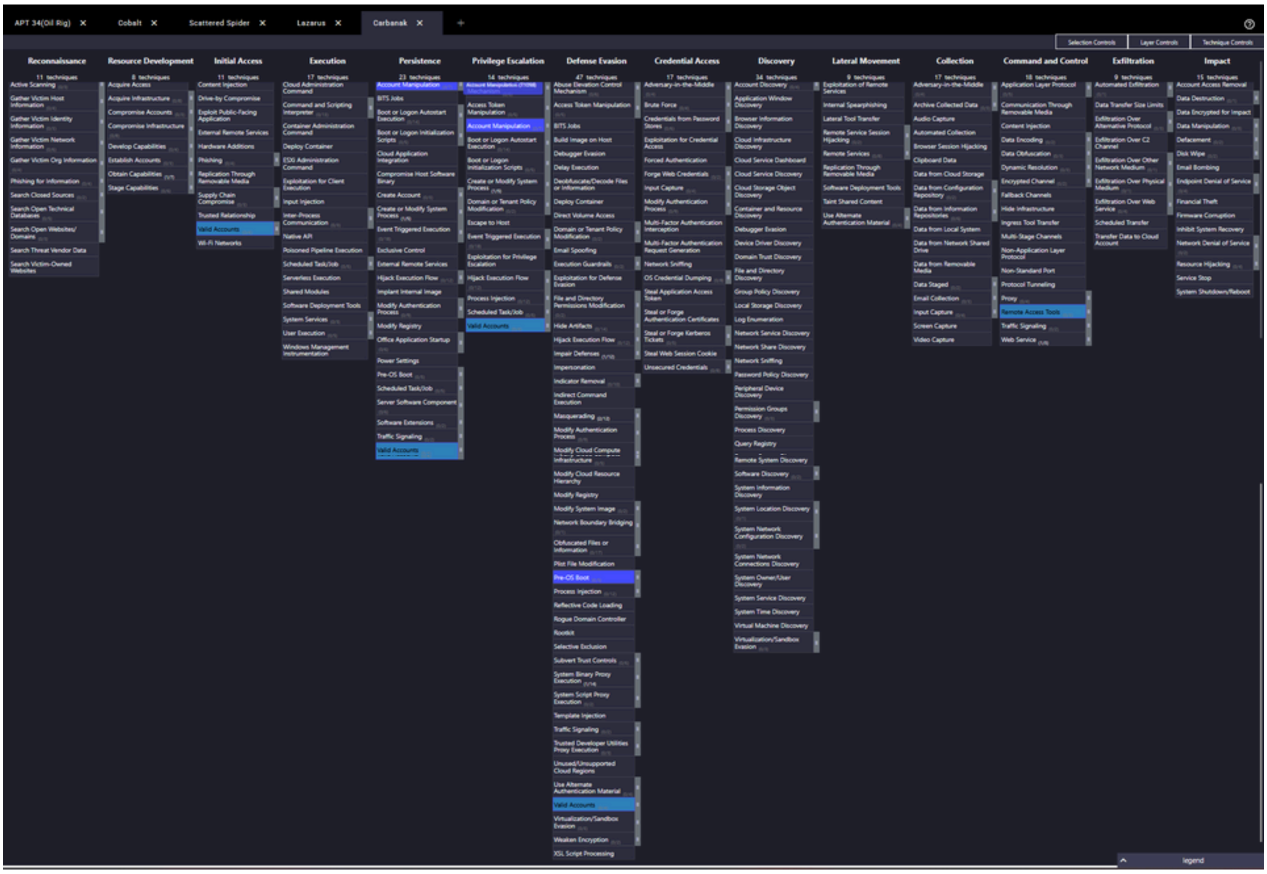
TTPs mapped for Scattered Spider



TTPs mapped for Lazarus



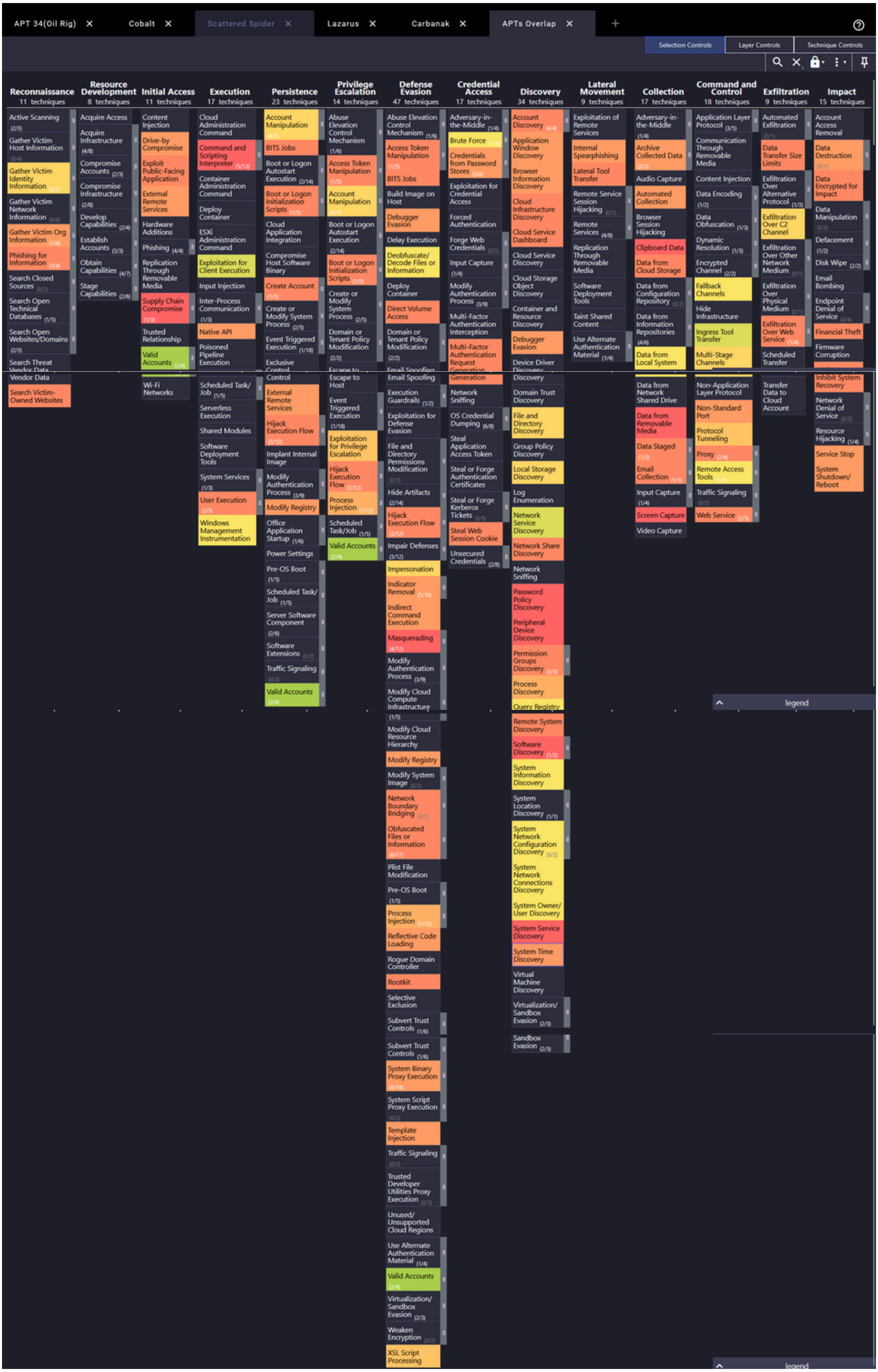
TTPs mapped for Carbanak



5. Compare the APTs

- Imported all five APT layers into a combined Navigator view.
- Noted common techniques across multiple APTs, such as:

o T1589 – Gather victim identity information
o T1078 – Valid Accounts
o T1203 – Exploitation for client execution
o T1098 – Account manipulation
o T1656 – Impersonation
o T1110 – Brute force
o T1012 – Query registry
o T1041 – Exfiltration over C2 channel
o T1657 – Financial theft



Reconnaissance 11 techniques

- Active Scanning (2/3)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (2/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (1/4)
- Phishing for Information (3/4)
- Search Closed Sources (0/2)
- Search Open Technical Databases (1/5)
- Search Open Websites/Domains (2/3)
- Search Threat Vendor Data
- Search Victim-Owned Websites

Resource Development 8 techniques

- Acquire Access
- Acquire Infrastructure (4/8)
- Compromise Accounts (2/3)
- Compromise Infrastructure (2/8)
- Develop Capabilities (2/4)
- Establish Accounts (3/3)
- Obtain Capabilities (4/7)
- Stage Capabilities (2/6)

Initial Access 11 techniques

- Content Injection
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (4/4)
- Replication Through Removable Media
- Supply Chain Compromise (1/3)
- Trusted Relationship
- Valid Accounts (2/4)
- Wi-Fi Networks

Execution 17 techniques

- Cloud Administration Command
- Command and Scripting Interpreter (5/13)
- Container Administration Command
- Deploy Container
- ESXi Administration Command
- Exploitation for Client Execution
- Input Injection
- Inter-Process Communication (1/3)
- Native API
- Poisoned Pipeline Execution
- Scheduled Task/Job (1/5)
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services (1/3)
- User Execution (2/5)
- Windows Management Instrumentation

Persistence 23 techniques

- Account Manipulation (4/7)
- BITS Jobs
- Boot or Logon Autostart Execution (2/14)
- Boot or Logon Initialization Scripts (1/5)
- Cloud Application Integration
- Compromise Host Software Binary
- Create Account (1/3)
- Create or Modify System Process (2/5)
- Event Triggered Execution (1/18)
- Exclusive Control
- External Remote Services
- Hijack Execution Flow (3/12)
- Implant Internal Image
- Modify Authentication Process (3/9)
- Modify Registry
- Office Application Startup (1/6)
- Power Settings
- Pre-OS Boot (1/5)
- Scheduled Task/Job (1/5)
- Server Software Component (2/6)
- Software Extensions (0/2)
- Traffic Signaling (0/2)
- Valid Accounts (2/4)

Privilege Escalation 14 techniques

- Abuse Elevation Control Mechanism (1/6)
- Access Token Manipulation (1/5)
- Account Manipulation (4/7)
- Boot or Logon Autostart Execution (2/14)
- Boot or Logon Initialization Scripts (1/5)
- Create or Modify System Process (2/5)
- Domain or Tenant Policy Modification (2/2)
- Escape to Host
- Event Triggered Execution (1/18)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (3/12)
- Process Injection (1/12)
- Scheduled Task/Job (1/5)
- Valid Accounts (2/4)

Defense Evasion 47 techniques

- Abuse Elevation Control Mechanism (1/6)
- Access Token Manipulation (1/5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Delay Execution
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain or Tenant Policy Modification (2/2)
- Email Spoofing
- Execution Guardrails (1/2)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Hide Artifacts (2/14)
- Hijack Execution Flow (3/12)
- Impair Defenses (3/12)
- Impersonation
- Indicator Removal (5/10)
- Indirect Command Execution
- Masquerading (4/12)
- Modify Authentication Process (3/9)
- Modify Cloud Compute Infrastructure (1/5)
- Modify Cloud Resource Hierarchy
- Modify Registry
- Modify System Image (0/2)
- Network Boundary Bridging (0/1)
- Obfuscated Files or Information (6/17)
- Plist File Modification
- Pre-OS Boot (1/5)
- Process Injection (1/12)
- Reflective Code Loading
- Rogue Domain Controller
- Rootkit
- Selective Exclusion
- Subvert Trust Controls (1/6)
- Subvert Trust Controls (1/6)
- System Binary Proxy Execution (6/14)
- System Script Proxy Execution (0/2)
- Template Injection
- Traffic Signaling (0/2)
- Trusted Developer Utilities Proxy Execution (0/3)
- Unused/Unsupported Cloud Regions
- Use Alternate Authentication Material (1/4)
- Valid Accounts (2/4)
- Virtualization/Sandbox Evasion (2/3)
- Weaken Encryption (0/2)
- XSL Script Processing

Credential Access 17 techniques

- Adversary-in-the-Middle (1/4)
- Brute Force (1/4)
- Credentials from Password Stores (3/6)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (0/2)
- Input Capture (1/4)
- Modify Authentication Process (3/9)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (6/8)
- Steal Application Access Token
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets (0/5)
- Steal Web Session Cookie
- Unsecured Credentials (2/8)

Discovery 34 techniques

- Account Discovery (4/4)
- Application Window Discovery
- Browser Information Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Device Driver Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Local Storage Discovery
- Log Enumeration
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (3/3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (1/2)
- System Information Discovery
- System Location Discovery (1/1)
- System Network Configuration Discovery (0/2)
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtual Machine Discovery
- Virtualization/Sandbox Evasion (2/3)
- Sandbox Evasion (2/3)

Lateral Movement 9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (4/8)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (1/4)

Collection 17 techniques

- Adversary-in-the-Middle (1/4)
- Archive Collected Data (3/3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage
- Data from Configuration Repository (0/2)
- Data from Information Repositories (4/6)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (1/2)
- Email Collection (1/3)
- Input Capture (1/4)
- Screen Capture
- Video Capture

Command and Control 18 techniques

- Application Layer Protocol (3/5)
- Communication Through Removable Media
- Content Injection
- Data Encoding (1/2)
- Data Obfuscation (1/3)
- Dynamic Resolution (1/3)
- Encrypted Channel (2/2)
- Fallback Channels
- Hide Infrastructure
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (2/4)
- Remote Access Tools (1/3)
- Traffic Signaling (0/2)
- Web Service (2/3)

Exfiltration 9 techniques

- Automated Exfiltration (0/1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (1/3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (0/1)
- Exfiltration Over Physical Medium (0/1)
- Exfiltration Over Web Service (1/4)
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact 15 techniques

- Account Access Removal
- Data Destruction (0/1)
- Data Encrypted for Impact
- Data Manipulation (0/3)
- Defacement (1/2)
- Disk Wipe (2/2)
- Email Bombing
- Endpoint Denial of Service (0/4)
- Financial Theft
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (0/2)
- Resource Hijacking (1/4)
- Service Stop
- System Shutdown/Reboot

Findings

This threat hunting exercise focused on identifying APTs targeting the finance sector. Key findings include:

- Identified Tactics, Technique and Procedures associated with APT groups targeting finance institutions
- Detected suspicious command and control (C2) communication and data exfiltration attempts
- Identified potential insider threats

Recommendations

- Implement enhanced threat detection and monitoring for APTs
- Strengthen defenses against C2 communication and data exfiltration
- Enhance incidence response plans and procedures for APT incident
- Conduct regular security assessments and penetration testing
- Implement additional security controls for third party vendors and supply chain partners