Industry-Focused Threat Hunting, APT TTP Mapping & Control Alignment

Target Sector: Government/Public Sector (Austrian Public Administration Focus)

Task 1: Industry Threat Landscape

1.1 Industry Justification

The Government and Public Sector is a prime target for sophisticated cyber adversaries due to its concentration of sensitive data, critical infrastructure, and complex network of contractors. It holds national security secrets, diplomatic communications, and citizen data, making it a high-value target for espionage. As the steward of essential services like energy, transportation, and public health, its compromise could cause significant societal disruption. The sector's reliance on third-party suppliers also creates vulnerabilities for supply chain attacks.

1.2 Selected APT Groups

A. Circles

Primary Motivation**:** Espionage (surveillance via communication interception)

Typical Targets: Telecommunications infrastructure, mobile devices of officials

Known Campaigns**:** Exploits SS7 protocol weaknesses to track locations and intercept calls/SMS

· ***Impact on Government:*** *Compromises confidentiality of official communications and national security*

B. MuddyWater (Seedworm)

· Primary Motivation**:** Espionage

· Typical Targets**:** Government bodies, telecommunications, defense sectors across multiple regions

· Known Campaigns**:** Uses spear-phishing and PowerShell backdoors to target government IT providers

· ***Impact on Government:*** *Persistent threat to sensitive government data and intelligence*

C. Cobalt Group

· Primary Motivation: Financial theft

· Typical Targets: Financial institutions, banks, payment systems

· Known Campaigns: "Carbanak" campaign stealing hundreds of millions; uses supply-chain attacks

· *Impact on Government:* *Risks to government financial authorities through advanced techniques*

D. Turla

· Primary Motivation: Espionage

· Typical Targets: Government agencies, embassies, military across 50+ countries.

· Known Campaigns: Sophisticated operations including "Watering Hole" attacks and custom malware

· ***Impact on Government:*** *Deep, long-term espionage threat to political and military intelligence*

E. GOLD SOUTHFIELD

· Primary Motivation: Financial gain (ransomware)

· Typical Targets: Organizations across sectors via REvil RaaS platform.

· *Known Campaigns*: REvil ransomware with double-extortion tactics

· ***Impact on Government:*** *Threatens operational continuity of public services*

Task 2: TTP Analysis Using MITRE ATT&CK

TTP ANALYSIS FOR MuddyWater;

APT Group	Tactic	Technique ID	Technique Name
MuddyWater	Initial Access	T1566.001	Spearphishing Attachment
MuddyWater	Execution	T1059.001	PowerShell

MuddyWater	Persistence	T1547.001	Registry Run Keys
MuddyWater	Credential Access	T1003.001	OS Credential Dumping: LSASS Memory
MuddyWater	Lateral Movement	T1219	Remote Access Tools
MuddyWater	Command & Control	T1071.001	Web Protocols

TTP ANALYSIS FOR GOLD SOUTHFIELD;

APT Group	**Tactic**	**Technique ID**	**Technique Name**
GOLD SOUTHFIELD	Initial Access	T1195.002	Supply Chain Compromise
GOLD SOUTHFIELD	Execution	T1059.001	PowerShell
GOLD SOUTHFIELD	Defense Evasion	T1027.010	Command Obfuscation
GOLD SOUTHFIELD	Credential Access	T1003	OS Credential Dumping
GOLD SOUTHFIELD	Lateral Movement	T1021.001	Remote Desktop Protocol
GOLD SOUTHFIELD	Command & Control	T1573	Encrypted Channel

TTP ANALYSIS FOR COBALT GROUP;

APT Group	**Tactic**	**Technique ID**	**Technique Name**
Cobalt Group	Initial Access	T1566.001	Spearphishing Attachment
Cobalt Group	Execution	T1059.001	PowerShell
Cobalt Group	Privilege Escalation	T1548.002	Bypass User Account Control
Cobalt Group	Credential Access	T1003	OS Credential Dumping

Cobalt Group	Lateral Movement	T1021.001	Remote Desktop Protocol
Cobalt Group	Command & Control	T1572	Protocol Tunneling

TTP ANALYSIS FOR TURLA;

APT Group	Tactic	Technique ID	Technique Name
Turla	Initial Access	T1566.002	Spearphishing Link
Turla	Execution	T1059.001	PowerShell
Turla	Persistence	T1546.003	WMI Event Subscription
Turla	Credential Access	T1555.004	Credentials from Windows Credential Manager
Turla	Lateral Movement	T1021.002	SMB/Windows Admin Shares
Turla	Command & Control	T1071.001	Web Protocols

TTP ANALYSIS FOR CIRCLE;

APT Group	Tactic	Technique ID	Technique Name
Circles	Collection	T1430.002	Location Tracking: Impersonate SS7 Nodes (Mobile Domain)

Task 3: ATT&CK Navigator Overlap Analysis

Overlap Analysis

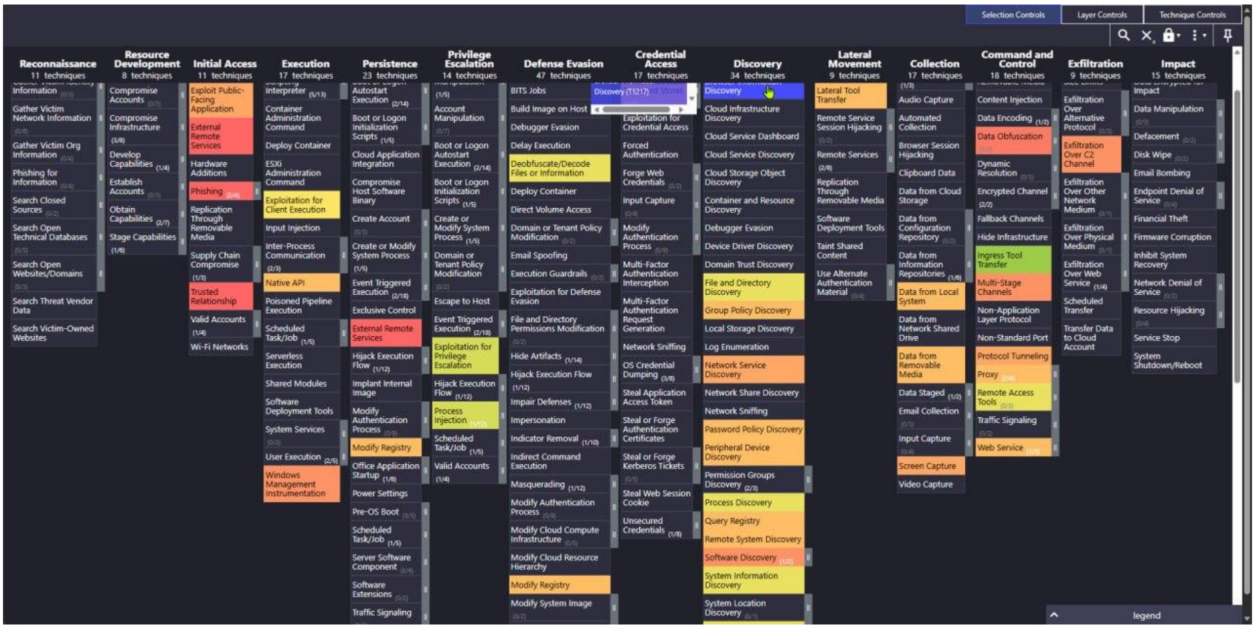
The overlap analysis of techniques shared by two or more APT groups reveals critical patterns that should guide defensive priorities for a government Security Operations Center (SOC). The most prevalent technique is PowerShell (T1059.001), used by all four enterprisefocused groups (MuddyWater, GOLD SOUTHFIELD, Cobalt Group, and Turla). This ubiquity underscores PowerShell's role as a fundamental tool for post-compromise execution, enabling everything from credential theft to lateral movement. For a government SOC, implementing strict PowerShell logging (Module, ScriptBlock, and Transcription) and constraining its use through application control policies would disrupt a wide range of adversaries simultaneously.

Credential access techniques, particularly OS Credential Dumping (T1003), are employed by three groups (MuddyWater, GOLD SOUTHFIELD, and Cobalt Group). This overlap highlights the universal need for attackers to steal credentials to expand their access within a network. Defensive measures like Credential Guard, Restricted Admin Mode for RDP, and monitoring for tools like Mimikatz become high-value controls. Similarly, spearphishing (T1566) remains a common initial access vector, used by MuddyWater and Cobalt Group via attachments and by MuddyWater and Turla via links. This reinforces the need for layered email security, user awareness training, and network filtering.

For lateral movement, both GOLD SOUTHFIELD and Cobalt Group utilize Remote Desktop Protocol (T1021.001), while MuddyWater and Turla use other remote services (T1219, T1021.002). These techniques exploit legitimate administrative channels, suggesting that network segmentation, strict access controls on administrative tools, and monitoring for anomalous RDP or SMB connections are essential.

In command and control, web protocols (T1071.001) are used by MuddyWater and Turla to blend with normal traffic, while encryption (T1573) and tunneling (T1572) are common for evasion. This necessitates network monitoring capable of detecting anomalies in web traffic, potentially using SSL/TLS inspection and analyzing traffic patterns and certificate anomalies.

The significance of these overlapping techniques lies in their role as "choke points" – common dependencies in diverse attack chains. By focusing detection and mitigation efforts on these shared techniques (PowerShell restriction, credential protection, phishing defense, network segmentation, and C2 monitoring), a government SOC can achieve maximum defensive efficiency. This strategic approach allows the SOC to harden the environment against the core methods used by both espionage and financially motivated groups, thereby strengthening the overall security posture against the broad threat landscape facing the public sector.



Reconnaissance 11 techniques
- Information (0/2)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (0/4)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/3)
- Search Threat Vendor Data
- Search Victim-Owned Websites

Resource Development 8 techniques
- Compromise Accounts (0/3)
- Compromise Infrastructure (3/8)
- Develop Capabilities (1/4)
- Establish Accounts (0/3)
- Obtain Capabilities (2/7)
- Stage Capabilities (1/6)

Initial Access 11 techniques
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (2/4)
- Replication Through Removable Media
- Supply Chain Compromise (1/3)
- Trusted Relationship
- Valid Accounts (1/4)
- Wi-Fi Networks

Execution 17 techniques
- Interpreter (5/13)
- Container Administration Command
- Deploy Container
- ESXi Administration Command
- Exploitation for Client Execution
- Input Injection
- Inter-Process Communication (2/3)
- Native API
- Poisoned Pipeline Execution
- Scheduled Task/Job (1/5)
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services (0/3)
- User Execution (2/5)
- Windows Management Instrumentation

Persistence 23 techniques
- Autostart Execution (2/14)
- Boot or Logon Initialization Scripts (1/5)
- Cloud Application Integration
- Compromise Host Software Binary
- Create Account (0/3)
- Create or Modify System Process (1/5)
- Event Triggered Execution (2/18)
- Exclusive Control
- External Remote Services
- Hijack Execution Flow (1/12)
- Implant Internal Image
- Modify Authentication Process (0/9)
- Modify Registry
- Office Application Startup (1/6)
- Power Settings
- Pre-OS Boot (0/5)
- Scheduled Task/Job (1/5)
- Server Software Component (0/5)
- Software Extensions (0/2)
- Traffic Signaling

Privilege Escalation 14 techniques
- (1/5)
- Account Manipulation (0/7)
- Boot or Logon Autostart Execution (2/14)
- Boot or Logon Initialization Scripts (1/5)
- Create or Modify System Process (1/5)
- Domain or Tenant Policy Modification (0/2)
- Escape to Host
- Event Triggered Execution (2/18)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (1/12)
- Process Injection (1/12)
- Scheduled Task/Job (1/5)
- Valid Accounts (1/4)

Defense Evasion 47 techniques
- 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 (0/2)
- Email Spoofing
- Execution Guardrails (0/2)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Hide Artifacts (1/14)
- Hijack Execution Flow (1/12)
- Impair Defenses (1/12)
- Impersonation
- Indicator Removal (1/10)
- Indirect Command Execution
- Masquerading (1/12)
- Modify Authentication Process (0/9)
- Modify Cloud Compute Infrastructure (0/5)
- Modify Cloud Resource Hierarchy
- Modify Registry
- Modify System Image (0/2)

Credential Access 17 techniques
- Discovery (T1217)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (0/2)
- Input Capture (0/4)
- Modify Authentication Process (0/9)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (3/8)
- Steal Application Access Token
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets (0/5)
- Steal Web Session Cookie
- Unsecured Credentials (1/8)

Discovery 34 techniques
- 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 (2/3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (1/2)
- System Information Discovery
- System Location Discovery (0/1)

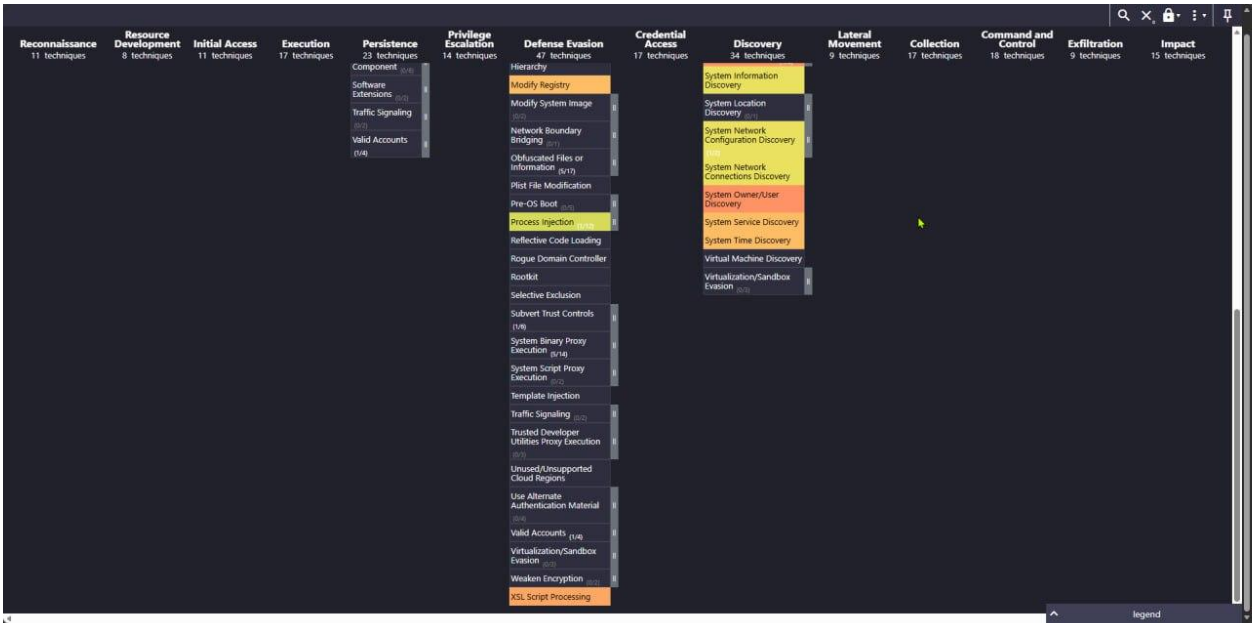
Lateral Movement 9 techniques
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (2/8)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (0/4)

Collection 17 techniques
- (1/3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage
- Data from Configuration Repository (0/2)
- Data from Information Repositories (1/6)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (1/2)
- Email Collection (0/3)
- Input Capture (0/4)
- Screen Capture
- Video Capture

Command and Control 18 techniques
- Content Injection
- Data Encoding (1/2)
- Data Obfuscation
- Dynamic Resolution (0/3)
- Encrypted Channel (2/2)
- Fallback Channels
- Hide Infrastructure
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy
- Remote Access Tools (0/3)
- Traffic Signaling (0/2)
- Web Service

Exfiltration 9 techniques
- Exfiltration Over Alternative Protocol (0/3)
- 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
- Impact
- Data Manipulation (0/3)
- Defacement (0/2)
- Disk Wipe (0/2)
- Email Bombing
- Endpoint Denial of Service (0/4)
- Financial Theft
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (0/2)
- Resource Hijacking (0/4)
- Service Stop
- System Shutdown/Reboot



Reconnaissance 11 techniques

Resource Development 8 techniques

Initial Access 11 techniques

Execution 17 techniques

Persistence 23 techniques
- Component (0/6)
- Software Extensions (0/2)
- Traffic Signaling (0/2)
- Valid Accounts (1/4)

Privilege Escalation 14 techniques

Defense Evasion 47 techniques
- Hierarchy
- Modify Registry
- Modify System Image (0/2)
- Network Boundary Bridging (0/1)
- Obfuscated Files or Information (5/17)
- Plist File Modification
- Pre-OS Boot (0/5)
- Process Injection (1/12)
- Reflective Code Loading
- Rogue Domain Controller
- Rootkit
- Selective Exclusion
- Subvert Trust Controls (1/6)
- System Binary Proxy Execution (5/14)
- 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 (0/4)
- Valid Accounts (1/4)
- Virtualization/Sandbox Evasion (0/3)
- Weaken Encryption (0/2)
- XSL Script Processing

Credential Access 17 techniques

Discovery 34 techniques
- System Information Discovery
- System Location Discovery (0/1)
- System Network Configuration Discovery (1/1)
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtual Machine Discovery
- Virtualization/Sandbox Evasion (0/3)

Lateral Movement 9 techniques

Collection 17 techniques

Command and Control 18 techniques

Exfiltration 9 techniques

Impact 15 techniques

Task 4: Detection & Control Mapping

4.1 NIST CSF Mapping

Key Finding	NIST CSF Function	Relevant Category	Control Example
PowerShell (T1059.001)	Protect (PR)	PR.AT, PR.PT	Security awareness training; Configuration management

OS Credential Dumping (T1003)	Protect (PR)	PR.AC	Identity management; Implement Credential Guard
Spearphishing (T1566)	Protect (PR)	PR.AT, PR.AC	Personnel training; Email filtering
Lateral Movement (T1021)	Protect (PR)	PR.AC, PR.IP	Access permission management; Network segmentation
C2 over Web Protocols (T1071)	Detect (DE)	DE.AE	Event data analysis; Network traffic analysis

4.2 ISO/IEC 27001 Mapping

Key Finding	**ISO/IEC 27001 Control Theme**	**Relevant Control (Example)**
PowerShell (T1059.001)	Operations Security (A.12)	Management of technical vulnerabilities; Application whitelisting
OS Credential Dumping (T1003)	Access Control (A.9)	Management of privileged access rights; Restrict debug privileges
Spearphishing (T1566)	Human Resource Security (A.7) & Operations Security (A.12)	Awareness training; Controls against malware
Lateral Movement (T1021)	Access Control (A.9) & Communications Security (A.13)	Network access control; Network segmentation
C2 over Web Protocols (T1071)	Operations Security (A.12) & Communications Security (A.13)	Event logging; Information transfer policies

4.3 Justification

The mapped controls directly address the common techniques used by the analyzed APT groups. Implementing these NIST CSF and ISO 27001 controls creates a layered defense that reduces exposure to the overlapping TTPs. For instance, restricting PowerShell through application control (NIST PR.PT-3, ISO A.12.6.1) limits a key execution method for four of the five groups. Similarly, enforcing strong access controls and network segmentation (NIST PR.AC-4, ISO A.9.1.2) impedes lateral movement, a critical phase for all groups. By aligning with these recognized frameworks, the government organization can adopt a comprehensive, risk-based cybersecurity approach that is both effective and compliant with sector standards. This translation of threat intelligence into concrete controls enables the SOC to move from awareness to actionable defense, focusing resources on mitigating the techniques most likely to be encountered from multiple threat actors.