

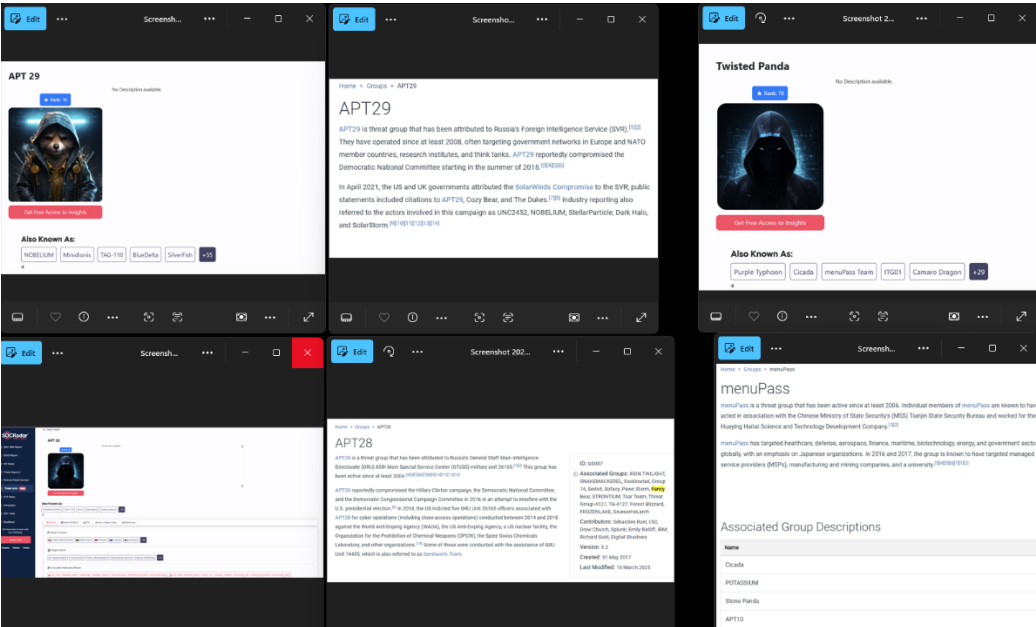
Government/Public Sector Threat Hunting Report: APT TTP Mapping & Control Alignment

Task 1: Industry Threat Landscape (Threat Intelligence)

1.1 Chosen Industry: Government/Public Sector.

Justification: The government/public sector is a high-value target due to its role in national security, governance, infrastructure, and public trust. Government agencies hold sensitive data, including national secrets, citizen records, defense information, and critical infrastructure control systems. This makes them prime targets for espionage, political influence, sabotage, and financial theft.

1.2 Selected APT Groups: APT29 (Cozy Bear), APT28 (Fancy Bear), APT10 (MenuPass), APT41 (Winnti), Lazarus Group



1.3 APT Documentation:

APT Group	Primary Motivation	Typical Targets	Known Campaigns
APT29 (Cozy Bear)	Espionage, Intelligence Gathering	Government agencies, defense contractors, research institutes	Operation Ghost, SolarWinds supply chain attack (2020)

APT Group	Primary Motivation	Typical Targets	Known Campaigns
APT28 (Fancy Bear)	Espionage, Disinformation	Military, government, political organizations	DNC hack (2016), German Parliament breach (2015)
APT10 (MenuPass)	Espionage, Intellectual Property Theft	Government, aerospace, technology, healthcare	Cloud Hopper campaign (targeting MSPs and government clients)
Lazarus Group	Financial, Disruption, Espionage	Financial systems, government entities, critical infrastructure	Sony Pictures hack (2014), WannaCry ransomware (2017)
APT41 (Winnti)	Espionage + Financial Gain	Government, healthcare, gaming, telecommunications	Operation ShadowPad, attacks on COVID-19 research entities

Task 2: TTP Analysis Using MITRE ATT&CK

APT Group	Tactic	Technique ID	Technique Name
APT29	Initial Access	T1195	Supply Chain Compromise
	Execution	T1059	Command and Scripting Interpreter
	Persistence	T1547	Boot or Logon Autostart Execution

APT Group	Tactic	Technique ID	Technique Name
	Credential Access	T1003	OS Credential Dumping
	Lateral Movement	T1021	Remote Services
	C2	T1071	Application Layer Protocol
	Exfiltration	T1041	Exfiltration Over C2 Channel
APT28	Initial Access	T1566	Phishing
	Execution	T1204	User Execution
	Persistence	T1136	Create Account
	Credential Access	T1110	Brute Force
	Lateral Movement	T1570	Lateral Tool Transfer
	C2	T1095	Non-Application Layer Protocol
	Impact	T1486	Data Encrypted for Impact
APT10	Initial Access	T1190	Exploit Public-Facing Application

APT Group	Tactic	Technique ID	Technique Name
	Persistence	T1505	Server Software Component
	Credential Access	T1555	Credentials from Password Stores
	Lateral Movement	T1210	Exploitation of Remote Services
	C2	T1105	Ingress Tool Transfer
	Exfiltration	T1048	Exfiltration Over Alternative Protocol

Key Focus Areas:

- **Credential Access:** T1003, T1110, T1555
- **Lateral Movement:** T1021, T1570, T1210
- **Command & Control:** T1071, T1095, T1105

Task 3: ATT&CK Navigator Mapping & Overlap Analysis

3.1 Navigator Layers Created:

1. APT29 Layer (Cozy Bear)

Reconnaissance 11 techniques	Resource Development 8 techniques	Initial Access 11 techniques	Execution 17 techniques	Persistence 23 techniques	Privilege Escalation 14 techniques	Defense Evasion 47 techniques	Credential Access 17 techniques	Discovery 34 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 15 techniques
Active Scanning (1/1)	Acquire Access (1/1)	Content Injection (1/1)	Cloud Administration Command (1/1)	Account Manipulation (1/1)	Abuse Elevation Control Mechanism (1/1)	Abuse Elevation Control Mechanism (1/1)	Adversary-in-the-Middle (1/1)	Account Discovery (1/1)	Exploitation of Remote Services (1/1)	Adversary-in-the-Middle (1/1)	Application Layer Protocol (1/1)	Automated Exfiltration (1/1)	Account Access Removal (1/1)
Gather Victim Host Information (1/1)	Acquire Infrastructure (1/1)	Drive-by Compromise (1/1)	Command and Scripting Interpreter (1/1)	BITS Jobs (1/1)	Access Token Manipulation (1/1)	Access Token Manipulation (1/1)	Brute Force (1/1)	Browser Information Discovery (1/1)	Internal Spearphishing (1/1)	Archive Collected Data (1/1)	Communication Through Removable Media (1/1)	Data Transfer Size Limits (1/1)	Data Destruction (1/1)
Gather Victim Identity Information (1/1)	Compromise Accounts (1/1)	Exploit Public-Facing Application (1/1)	Container Administration Command (1/1)	Boot or Logon Autostart Execution (1/1)	Account Manipulation (1/1)	Debugger Evasion (1/1)	Credentials from Password Stores (1/1)	Cloud Infrastructure Discovery (1/1)	Lateral Tool Transfer (1/1)	Audio Capture (1/1)	Content Injection (1/1)	Data Manipulation (1/1)	Data Encrypted for Impact (1/1)
Gather Victim Network Information (1/1)	Compromise Infrastructure (1/1)	External Remote Services (1/1)	Container Administration Command (1/1)	Boot or Logon Autostart Execution (1/1)	Boot or Logon Autostart Execution (1/1)	Debugger Evasion (1/1)	Exploitation of Credential Access (1/1)	Cloud Service Dashboard (1/1)	Remote Service Session Hijacking (1/1)	Automated Collection (1/1)	Content Injection (1/1)	Data Manipulation (1/1)	Defacement (1/1)
Gather Victim Org Information (1/1)	Develop Capabilities (1/1)	Hardware Additions (1/1)	Deploy Container (1/1)	Cloud Application Integration (1/1)	Boot or Logon Autostart Execution (1/1)	Delay Execution (1/1)	Forged Authentication (1/1)	Cloud Storage Object Discovery (1/1)	Remote Services (1/1)	Browser Session Hijacking (1/1)	Data Obfuscation (1/1)	Exfiltration Over C2 Channel (1/1)	Disk Wipe (1/1)
Phishing for Information (1/1)	Establish Accounts (1/1)	Phishing (1/1)	ESK Administration Command (1/1)	Cloud Application Integration (1/1)	Boot or Logon Autostart Execution (1/1)	Deobfuscate/Decode Files or Information (1/1)	Forge Web Credentials (1/1)	Container and Resource Discovery (1/1)	Application Through Removable Media (1/1)	Clipboard Data (1/1)	Dynamic Resolution (1/1)	Exfiltration Over Other Network Medium (1/1)	Email Bombing (1/1)
Search Closed Sources (1/1)	Obtain Capabilities (1/1)	Supply Chain Compromise (1/1)	Exploitation for Client Execution (1/1)	Compromise Host Software Binary (1/1)	Create or Modify System Process (1/1)	Deploy Container (1/1)	Input Capture (1/1)	Debugger Evasion (1/1)	Software Deployment Tools (1/1)	Data from Cloud Storage (1/1)	Encrypted Channel (1/1)	Exfiltration Over Physical Medium (1/1)	Endpoint Denial of Service (1/1)
Search Open Technical Databases (1/1)	Stage Capabilities (1/1)	Trusted Relationship (1/1)	Inter-Process Communication (1/1)	Create Account (1/1)	Domain or Tenant Policy Modification (1/1)	Direct Volume Access (1/1)	Multi-Factor Authentication Interception (1/1)	Device Driver Discovery (1/1)	Taint Shared Content (1/1)	Data from Configuration Repository (1/1)	Fallback Channels (1/1)	Exfiltration Over Web Service (1/1)	Financial Theft (1/1)
Search Threat Vendor Data (1/1)	Native API (1/1)	Wi-Fi Networks (1/1)	Poisoned Pipeline Execution (1/1)	Event Triggered Execution (1/1)	Escape to Host (1/1)	Execution Guards (1/1)	Request Generation (1/1)	File and Directory Discovery (1/1)	Use Alternate Authentication Material (1/1)	Data from Information Repositories (1/1)	Hide Infrastructure (1/1)	Exfiltration Over Web Service (1/1)	Fireware Corruption (1/1)
Search Victim-Owned Websites (1/1)	Search Closed Sources (1/1)	Search Open Technical Databases (1/1)	Scheduled Task/Job (1/1)	External Remote Services (1/1)	Event Triggered Execution (1/1)	File and Directory Permissions Modification (1/1)	Local Storage Discovery (1/1)	Log Enumeration (1/1)	Network Service Discovery (1/1)	Data from Network Shared Drive (1/1)	Ingress Tool Transfer (1/1)	Exfiltration Over Web Service (1/1)	Network Denial of Service (1/1)
	Search Open Technical Databases (1/1)	Search Threat Vendor Data (1/1)	Shared Modules (1/1)	Hijack Execution Flow (1/1)	Hijack Execution Flow (1/1)	Hide Artifacts (1/1)	Network Sniffing (1/1)	Network Share Discovery (1/1)	Network Service Discovery (1/1)	Data from Removable Media (1/1)	Multi-Stage Channels (1/1)	Exfiltration Over Web Service (1/1)	Resource Hijacking (1/1)
	Search Open Technical Databases (1/1)	Search Threat Vendor Data (1/1)	Software Deployment Tools (1/1)	Implant Internal Image (1/1)	Hijack Execution Flow (1/1)	Hijack Execution Flow (1/1)	OS Credential Dumping (1/1)	Network Sniffing (1/1)	Network Service Discovery (1/1)	Data from Removable Media (1/1)	Non-Standard Port (1/1)	Exfiltration Over Web Service (1/1)	Service Stop (1/1)
	Search Open Technical Databases (1/1)	Search Threat Vendor Data (1/1)	System Services (1/1)	Modify Authentication Process (1/1)	Process Injection (1/1)	Impair Defenses (1/1)	Steal or Forge Authentication Certificates (1/1)	Password Policy Discovery (1/1)	Peripheral Device Discovery (1/1)	Data Staged (1/1)	Remote Access Tools (1/1)	Exfiltration Over Web Service (1/1)	System Shutdown/Reboot (1/1)
	Search Open Technical Databases (1/1)	Search Threat Vendor Data (1/1)	User Execution (1/1)	Modify Registry (1/1)	Scheduled Task/Job (1/1)	Impersonation (1/1)	Steal or Forge Kerberos Tickets (1/1)	Remote System Discovery (1/1)	Screen Capture (1/1)	Email Collection (1/1)	Traffic Signaling (1/1)	Exfiltration Over Web Service (1/1)	
	Search Open Technical Databases (1/1)	Search Threat Vendor Data (1/1)	Windows Management Instrumentation (1/1)	Office Application Startup (1/1)	Event Triggered Execution (1/1)	Indicator Removal (1/1)	Unsecured Credentials (1/1)	Query Registry (1/1)	Video Capture (1/1)	Input Capture (1/1)	Web Service (1/1)	Exfiltration Over Web Service (1/1)	
	Search Open Technical Databases (1/1)	Search Threat Vendor Data (1/1)		Power Settings (1/1)	Event Triggered Execution (1/1)	Indirect Command Execution (1/1)		Remote System Discovery (1/1)		Screen Capture (1/1)		Exfiltration Over Web Service (1/1)	
	Search Open Technical Databases (1/1)	Search Threat Vendor Data (1/1)		Pre-OS Boot (1/1)	Event Triggered Execution (1/1)	Masquerading (1/1)		System Information Discovery (1/1)		Screen Capture (1/1)		Exfiltration Over Web Service (1/1)	
	Search Open Technical Databases (1/1)	Search Threat Vendor Data (1/1)		Scheduled Task/Job (1/1)	Event Triggered Execution (1/1)	Modify Authentication Process (1/1)		System Location Discovery (1/1)		Screen Capture (1/1)		Exfiltration Over Web Service (1/1)	
	Search Open Technical Databases (1/1)	Search Threat Vendor Data (1/1)		Server Software Component (1/1)	Event Triggered Execution (1/1)	Modify Cloud Compute Infrastructure (1/1)				Screen Capture (1/1)		Exfiltration Over Web Service (1/1)	
	Search Open Technical Databases (1/1)	Search Threat Vendor Data (1/1)		Software Extensions (1/1)	Event Triggered Execution (1/1)	Modify Cloud Resource Hierarchy (1/1)				Screen Capture (1/1)		Exfiltration Over Web Service (1/1)	
	Search Open Technical Databases (1/1)	Search Threat Vendor Data (1/1)			Event Triggered Execution (1/1)	Modify Registry (1/1)				Screen Capture (1/1)		Exfiltration Over Web Service (1/1)	

2. APT28 Layer (Fancy Bear)

Reconnaissance 11 techniques	Resource Development 8 techniques	Initial Access 11 techniques	Execution 17 techniques	Persistence 23 techniques	Privilege Escalation 14 techniques	Defense Evasion 47 techniques	Credential Access 17 techniques	Discovery 34 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 15 techniques
Active Scanning (1/1)	Acquire Access (1/1)	Content Injection (1/1)	Cloud Administration Command (1/1)	Account Manipulation (1/1)	Abuse Elevation Control Mechanism (1/1)	Abuse Elevation Control Mechanism (1/1)	Adversary-in-the-Middle (1/1)	Account Discovery (1/1)	Exploitation of Remote Services (1/1)	Adversary-in-the-Middle (1/1)	Application Layer Protocol (1/1)	Automated Exfiltration (1/1)	Account Access Removal (1/1)
Gather Victim Host Information (1/1)	Acquire Infrastructure (1/1)	Drive-by Compromise (1/1)	Command and Scripting Interpreter (1/1)	BITS Jobs (1/1)	Access Token Manipulation (1/1)	Access Token Manipulation (1/1)	Brute Force (1/1)	Browser Information Discovery (1/1)	Internal Spearphishing (1/1)	Archive Collected Data (1/1)	Communication Through Removable Media (1/1)	Data Transfer Size Limits (1/1)	Data Destruction (1/1)
Gather Victim Identity Information (1/1)	Compromise Accounts (1/1)	Exploit Public-Facing Application (1/1)	Container Administration Command (1/1)	Boot or Logon Autostart Execution (1/1)	Account Manipulation (1/1)	Debugger Evasion (1/1)	Credentials from Password Stores (1/1)	Cloud Infrastructure Discovery (1/1)	Lateral Tool Transfer (1/1)	Audio Capture (1/1)	Content Injection (1/1)	Data Manipulation (1/1)	Data Encrypted for Impact (1/1)
Gather Victim Network Information (1/1)	Compromise Infrastructure (1/1)	External Remote Services (1/1)	Container Administration Command (1/1)	Boot or Logon Autostart Execution (1/1)	Boot or Logon Autostart Execution (1/1)	Debugger Evasion (1/1)	Exploitation of Credential Access (1/1)	Cloud Service Dashboard (1/1)	Remote Service Session Hijacking (1/1)	Automated Collection (1/1)	Content Injection (1/1)	Data Manipulation (1/1)	Defacement (1/1)
Gather Victim Org Information (1/1)	Develop Capabilities (1/1)	Hardware Additions (1/1)	Deploy Container (1/1)	Cloud Application Integration (1/1)	Boot or Logon Autostart Execution (1/1)	Delay Execution (1/1)	Forged Authentication (1/1)	Cloud Storage Object Discovery (1/1)	Remote Services (1/1)	Browser Session Hijacking (1/1)	Data Obfuscation (1/1)	Exfiltration Over C2 Channel (1/1)	Disk Wipe (1/1)
Phishing for Information (1/1)	Establish Accounts (1/1)	Phishing (1/1)	ESK Administration Command (1/1)	Cloud Application Integration (1/1)	Boot or Logon Autostart Execution (1/1)	Deobfuscate/Decode Files or Information (1/1)	Forge Web Credentials (1/1)	Container and Resource Discovery (1/1)	Application Through Removable Media (1/1)	Clipboard Data (1/1)	Dynamic Resolution (1/1)	Exfiltration Over Other Network Medium (1/1)	Email Bombing (1/1)
Search Closed Sources (1/1)	Obtain Capabilities (1/1)	Supply Chain Compromise (1/1)	Exploitation for Client Execution (1/1)	Compromise Host Software Binary (1/1)	Create or Modify System Process (1/1)	Deploy Container (1/1)	Input Capture (1/1)	Debugger Evasion (1/1)	Software Deployment Tools (1/1)	Data from Cloud Storage (1/1)	Encrypted Channel (1/1)	Exfiltration Over Physical Medium (1/1)	Endpoint Denial of Service (1/1)
Search Open Technical Databases (1/1)	Stage Capabilities (1/1)	Trusted Relationship (1/1)	Inter-Process Communication (1/1)	Create Account (1/1)	Domain or Tenant Policy Modification (1/1)	Direct Volume Access (1/1)	Multi-Factor Authentication Interception (1/1)	Device Driver Discovery (1/1)	Use Alternate Authentication Material (1/1)	Data from Configuration Repository (1/1)	Fallback Channels (1/1)	Exfiltration Over Web Service (1/1)	Financial Theft (1/1)
Search Threat Vendor Data (1/1)	Native API (1/1)	Wi-Fi Networks (1/1)	Poisoned Pipeline Execution (1/1)	Event Triggered Execution (1/1)	Escape to Host (1/1)	Execution Guards (1/1)	Request Generation (1/1)	File and Directory Discovery (1/1)	Use Alternate Authentication Material (1/1)	Data from Information Repositories (1/1)	Hide Infrastructure (1/1)	Exfiltration Over Web Service (1/1)	Fireware Corruption (1/1)
Search Victim-Owned Websites (1/1)	Search Closed Sources (1/1)	Search Open Technical Databases (1/1)	Scheduled Task/Job (1/1)	External Remote Services (1/1)	Event Triggered Execution (1/1)	File and Directory Permissions Modification (1/1)	Local Storage Discovery (1/1)	Log Enumeration (1/1)	Network Service Discovery (1/1)	Data from Network Shared Drive (1/1)	Ingress Tool Transfer (1/1)	Exfiltration Over Web Service (1/1)	Network Denial of Service (1/1)
	Search Open Technical Databases (1/1)	Search Threat Vendor Data (1/1)	Shared Modules (1/1)	Hijack Execution Flow (1/1)	Hijack Execution Flow (1/1)	Hide Artifacts (1/1)	Network Sniffing (1/1)	Network Share Discovery (1/1)	Network Service Discovery (1/1)	Data from Removable Media (1/1)	Multi-Stage Channels (1/1)	Exfiltration Over Web Service (1/1)	Resource Hijacking (1/1)
	Search Open Technical Databases (1/1)	Search Threat Vendor Data (1/1)	Software Deployment Tools (1/1)	Implant Internal Image (1/1)	Hijack Execution Flow (1/1)	Hijack Execution Flow (1/1)	OS Credential Dumping (1/1)	Network Sniffing (1/1)	Network Service Discovery (1/1)	Data from Removable Media (1/1)	Non-Standard Port (1/1)	Exfiltration Over Web Service (1/1)	Service Stop (1/1)
	Search Open Technical Databases (1/1)	Search Threat Vendor Data (1/1)	System Services (1/1)	Modify Authentication Process (1/1)	Process Injection (1/1)	Impair Defenses (1/1)	Steal or Forge Authentication Certificates (1/1)	Password Policy Discovery (1/1)	Peripheral Device Discovery (1/1)	Data Staged (1/1)	Remote Access Tools (1/1)	Exfiltration Over Web Service (1/1)	System Shutdown/Reboot (1/1)
	Search Open Technical Databases (1/1)	Search Threat Vendor Data (1/1)	User Execution (1/1)	Modify Registry (1/1)	Scheduled Task/Job (1/1)	Impersonation (1/1)	Steal or Forge Kerberos Tickets (1/1)	Remote System Discovery (1/1)	Screen Capture (1/1)	Email Collection (1/1)	Traffic Signaling (1/1)	Exfiltration Over Web Service (1/1)	
	Search Open Technical Databases (1/1)	Search Threat Vendor Data (1/1)	Windows Management Instrumentation (1/1)	Office Application Startup (1/1)	Event Triggered Execution (1/1)	Indicator Removal (1/1)	Unsecured Credentials (1/1)	Query Registry (1/1)	Video Capture (1/1)	Input Capture (1/1)	Web Service (1/1)	Exfiltration Over Web Service (1/1)	
	Search Open Technical Databases (1/1)	Search Threat Vendor Data (1/1)		Power Settings (1/1)	Event Triggered Execution (1/1)	Indirect Command Execution (1/1)		Remote System Discovery (1/1)		Screen Capture (1/1)		Exfiltration Over Web Service (1/1)	
	Search Open Technical Databases (1/1)	Search Threat Vendor Data (1/1)		Pre-OS Boot (1/1)	Event Triggered Execution (1/1)	Masquerading (1/1)		System Information Discovery (1/1)		Screen Capture (1/1)		Exfiltration Over Web Service (1/1)	
	Search Open Technical Databases (1/1)	Search Threat Vendor Data (1/1)		Scheduled Task/Job (1/1)	Event Triggered Execution (1/1)	Modify Authentication Process (1/1)		System Location Discovery (1/1)		Screen Capture (1/1)		Exfiltration Over Web Service (1/1)	
	Search Open Technical Databases (1/1)	Search Threat Vendor Data (1/1)		Server Software Component (1/1)	Event Triggered Execution (1/1)	Modify Cloud Compute Infrastructure (1/1)				Screen Capture (1/1)		Exfiltration Over Web Service (1/1)	
	Search Open Technical Databases (1/1)	Search Threat Vendor Data (1/1)		Software Extensions (1/1)	Event Triggered Execution (1/1)	Modify Cloud Resource Hierarchy (1/1)				Screen Capture (1/1)		Exfiltration Over Web Service (1/1)	
	Search Open Technical Databases (1/1)	Search Threat Vendor Data (1/1)			Event Triggered Execution (1/1)	Modify Registry (1/1)				Screen Capture (1/1)		Exfiltration Over Web Service (1/1)	

3. APT10 Layer (MenuPass)

APT19 × APT28 × APT10 × APT33 × APT41 × +														
Selection Controls Layer Controls Technique Controls														
Reconnaissance 11 techniques	Resource Development 8 techniques	Initial Access 13 techniques	Execution 17 techniques	Persistence 23 techniques	Privilege Escalation 14 techniques	Defense Evasion 47 techniques	Credential Access 17 techniques	Discovery 34 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 15 techniques	
Active Scanning (1/11)	Acquire Access (1/8)	Content Injection (1/13)	Cloud Administration Command (1/17)	Account Manipulation (1/23)	Abuse Elevation Control Mechanism (1/14)	Abuse Elevation Control Mechanism (1/47)	Adversary-in-the-Middle (1/17)	Account Discovery (1/34)	Exploitation of Remote Services (1/9)	Adversary-in-the-Middle (1/17)	Application Layer Protocol (1/18)	Automated Exfiltration (1/9)	Account Access Removal (1/15)	
Gather Victim Host Information (1/11)	Acquire Infrastructure (1/8)	Drive-by Compromise (1/13)	Command and Scripting Interpreter (1/17)	BITS Jobs (1/23)	Access Token Manipulation (1/14)	Access Token Manipulation (1/47)	Brute Force (1/17)	Application Window Discovery (1/34)	Internal Spearphishing (1/9)	Archive Collected Data (1/17)	Communication Through Removable Media (1/18)	Data Transfer Size Limits (1/9)	Data Destruction (1/15)	
Gather Victim Identity Information (1/11)	Compromise Accounts (1/8)	Exploit Public-Facing Application (1/13)	Container Administration Command (1/17)	Root or Logon Autostart Execution (1/23)	Account Manipulation (1/14)	Account Manipulation (1/47)	Credentials from Password Stores (1/17)	Cloud Infrastructure Discovery (1/34)	Lateral Tool Transfer (1/9)	Audio Capture (1/17)	Content Injection (1/18)	Data Encrypted for Impact (1/9)	Data Encrypted for Impact (1/15)	
Gather Victim Network Information (1/11)	Compromise Infrastructure (1/8)	External Remote Services (1/13)	Container Administration Command (1/17)	Root or Logon Autostart Execution (1/23)	Account Manipulation (1/14)	Account Manipulation (1/47)	Exploitation for Credential Access (1/17)	Cloud Service Dashboard (1/34)	Remote Service Session Hijacking (1/9)	Automated Collection (1/17)	Content Injection (1/18)	Defacement (1/9)	Data Manipulation (1/15)	
Gather Victim Org Information (1/11)	Develop Capabilities (1/8)	Hardware Additions (1/13)	Deploy Container (1/17)	Cloud Application Integration (1/23)	Boot or Logon Autostart Execution (1/14)	Boot or Logon Autostart Execution (1/47)	Delayed Execution (1/17)	Cloud Storage Object Discovery (1/34)	Remote Services (1/9)	Browser Session Hijacking (1/17)	Data Encoding (1/18)	Disk Wipe (1/9)	Disk Wipe (1/15)	
Phishing for Information (1/11)	Establish Accounts (1/8)	Phishing (1/13)	Exploit Administration Command (1/17)	Compromise Host Software Binary (1/23)	Boot or Logon Autostart Execution (1/14)	Boot or Logon Autostart Execution (1/47)	DeepFusca/Decode Files or Information (1/17)	Container and Resource Discovery (1/34)	Replication Through Removable Media (1/9)	Clipboard Data (1/17)	Dynamic Resolution (1/18)	Email Bombing (1/9)	Endpoint Denial of Service (1/15)	
Search Closed Sources (1/11)	Obtain Capabilities (1/8)	Supply Chain Compromise (1/13)	Input Injection (1/17)	Create Account (1/23)	Create or Modify System Process (1/14)	Create or Modify System Process (1/47)	Input Capture (1/17)	Debugger Evasion (1/34)	Software Deployment Tools (1/9)	Data from Cloud Storage (1/17)	Encrypted Channel (1/18)	Financial Theft (1/9)	Financial Theft (1/15)	
Search Open Technical Databases (1/11)	Stage Capabilities (1/8)	Trusted Relationships (1/13)	Inter-Process Communication (1/17)	Create or Modify System Process (1/23)	Domain or Tenant Policy Modification (1/14)	Domain or Tenant Policy Modification (1/47)	Modify Authentication Process (1/17)	Device Driver Discovery (1/34)	Taint Shared Content (1/9)	Data from Configuration Repository (1/17)	Fallback Channels (1/18)	Inhibit System Recovery (1/9)	Inhibit System Recovery (1/15)	
Search Open Websites/Domains (1/11)		Valid Accounts (1/13)	Native API (1/17)	Event Triggered Execution (1/23)	Escape to Host (1/14)	Escape to Host (1/47)	Multi-Factor Authentication Request Generation (1/17)	Domain Trust Discovery (1/34)	Use Alternate Authentication Material (1/9)	Data from Information Repository (1/17)	Hide Infrastructure (1/18)	Network Denial of Service (1/9)	Network Denial of Service (1/15)	
Search Threat Vendor Data (1/11)			Poisoned Pipeline Execution (1/17)	Event Triggered Execution (1/23)	Event Triggered Execution (1/14)	Event Triggered Execution (1/47)	Execution Guardrails (1/17)	Group Policy Discovery (1/34)	File and Directory Discovery (1/9)	Data from Local System (1/17)	Ingress Tool Transfer (1/18)	Resource Hijacking (1/9)	Resource Hijacking (1/15)	
Search Victim-Owned Websites (1/11)			Scheduled Task/Job (1/17)	External Remote Services (1/23)	Event Triggered Execution (1/14)	Event Triggered Execution (1/47)	Exploitation for Defense Evasion (1/17)	Local Storage Discovery (1/34)	Log Enumeration (1/9)	Data from Network Shared Drive (1/17)	Non-Application Layer Protocol (1/18)	Service Stop (1/9)	Service Stop (1/15)	
			Serverless Execution (1/17)	Hijack Execution Flow (1/23)	Exploitation for Privilege Escalation (1/14)	Exploitation for Privilege Escalation (1/47)	File and Directory Permissions Modification (1/17)	Network Service Discovery (1/34)	Network Service Discovery (1/9)	Data from Removable Media (1/17)	Protocol Tunneling (1/18)	System Shutdown/Reboot (1/9)	System Shutdown/Reboot (1/15)	
			Shared Modules (1/17)	Hijack Execution Flow (1/23)	Hijack Execution Flow (1/14)	Hijack Execution Flow (1/47)	Hide Artifacts (1/17)	Network Sniffing (1/34)	Proxy (1/9)	Data from Removable Media (1/17)	Remote Access Tools (1/18)			
			Software Deployment Tools (1/17)	Implant Internal Image (1/23)	Hijack Execution Flow (1/14)	Hijack Execution Flow (1/47)	Impair Defenses (1/17)	Network Sniffing (1/34)	Proxies (1/9)	Data Staged (1/17)	Traffic Signaling (1/18)			
			System Services (1/17)	Modify Authentication Process (1/23)	Impair Defenses (1/14)	Impair Defenses (1/47)	Impersonation (1/17)	Password Policy Discovery (1/34)	Screen Capture (1/9)	Email Collection (1/17)	Web Service (1/18)			
			User Execution (1/17)	Modify Registry (1/23)	Indicator Removal (1/14)	Indicator Removal (1/47)	Steal or Forge Kerberos Tickets (1/17)	Peripheral Device Discovery (1/34)	Video Capture (1/9)	Input Capture (1/17)				
			Windows Management Instrumentation (1/17)	Office Application Startup (1/23)	Indirect Command Execution (1/14)	Indirect Command Execution (1/47)	Steal Web Session Cookie (1/17)	Permission Groups Discovery (1/34)		Screen Capture (1/17)				
				Power Settings (1/23)	Masquerading (1/14)	Masquerading (1/47)	Unsecured Credentials (1/17)	Process Discovery (1/34)		Video Capture (1/17)				
				Pre-OS Boot (1/23)	Modify Authentication Process (1/14)	Modify Authentication Process (1/47)		Query Registry (1/34)						
				Scheduled Task/Job (1/23)	Modify Cloud Compute Infrastructure (1/14)	Modify Cloud Compute Infrastructure (1/47)		Remote System Discovery (1/34)						
				Server Software Component (1/23)	Modify Cloud Resource Hierarchy (1/14)	Modify Cloud Resource Hierarchy (1/47)		Software Discovery (1/34)						
				Software Extensions (1/23)	Modify Registry (1/14)	Modify Registry (1/47)		System Information Discovery (1/34)						
				Traffic Signaling (1/23)				System Location Discovery (1/34)						
								System Network Configuration (1/34)						

4. Overlap Layer (Shared Techniques)

APT19 × APT28 × APT10 × APT33 × APT41 × layer by operation × +														
Selection Controls Layer Controls Technique Controls														
Reconnaissance 11 techniques	Resource Development 8 techniques	Initial Access 13 techniques	Execution 17 techniques	Persistence 23 techniques	Privilege Escalation 14 techniques	Defense Evasion 47 techniques	Credential Access 17 techniques	Discovery 34 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 15 techniques	
Active Scanning (1/11)	Acquire Access (1/8)	Content Injection (1/13)	Cloud Administration Command (1/17)	Account Manipulation (1/23)	Abuse Elevation Control Mechanism (1/14)	Abuse Elevation Control Mechanism (1/47)	Adversary-in-the-Middle (1/17)	Account Discovery (1/34)	Exploitation of Remote Services (1/9)	Adversary-in-the-Middle (1/17)	Application Layer Protocol (1/18)	Automated Exfiltration (1/9)	Account Access Removal (1/15)	
Gather Victim Host Information (1/11)	Acquire Infrastructure (1/8)	Drive-by Compromise (1/13)	Command and Scripting Interpreter (1/17)	BITS Jobs (1/23)	Access Token Manipulation (1/14)	Access Token Manipulation (1/47)	Brute Force (1/17)	Application Window Discovery (1/34)	Internal Spearphishing (1/9)	Archive Collected Data (1/17)	Communication Through Removable Media (1/18)	Data Transfer Size Limits (1/9)	Data Destruction (1/15)	
Gather Victim Identity Information (1/11)	Compromise Accounts (1/8)	Exploit Public-Facing Application (1/13)	Container Administration Command (1/17)	Root or Logon Autostart Execution (1/23)	Account Manipulation (1/14)	Account Manipulation (1/47)	Credentials from Password Stores (1/17)	Cloud Infrastructure Discovery (1/34)	Lateral Tool Transfer (1/9)	Audio Capture (1/17)	Content Injection (1/18)	Data Encrypted for Impact (1/9)	Data Encrypted for Impact (1/15)	
Gather Victim Network Information (1/11)	Compromise Infrastructure (1/8)	External Remote Services (1/13)	Container Administration Command (1/17)	Root or Logon Autostart Execution (1/23)	Account Manipulation (1/14)	Account Manipulation (1/47)	Exploitation for Credential Access (1/17)	Cloud Service Dashboard (1/34)	Remote Service Session Hijacking (1/9)	Automated Collection (1/17)	Content Injection (1/18)	Defacement (1/9)	Data Manipulation (1/15)	
Gather Victim Org Information (1/11)	Develop Capabilities (1/8)	Hardware Additions (1/13)	Deploy Container (1/17)	Cloud Application Integration (1/23)	Boot or Logon Autostart Execution (1/14)	Boot or Logon Autostart Execution (1/47)	Delayed Execution (1/17)	Cloud Storage Object Discovery (1/34)	Remote Services (1/9)	Browser Session Hijacking (1/17)	Data Encoding (1/18)	Disk Wipe (1/9)	Disk Wipe (1/15)	
Phishing for Information (1/11)	Establish Accounts (1/8)	Phishing (1/13)	Exploit Administration Command (1/17)	Compromise Host Software Binary (1/23)	Boot or Logon Autostart Execution (1/14)	Boot or Logon Autostart Execution (1/47)	DeepFusca/Decode Files or Information (1/17)	Container and Resource Discovery (1/34)	Replication Through Removable Media (1/9)	Clipboard Data (1/17)	Dynamic Resolution (1/18)	Email Bombing (1/9)	Endpoint Denial of Service (1/15)	
Search Closed Sources (1/11)	Obtain Capabilities (1/8)	Supply Chain Compromise (1/13)	Input Injection (1/17)	Create Account (1/23)	Create or Modify System Process (1/14)	Create or Modify System Process (1/47)	Input Capture (1/17)	Debugger Evasion (1/34)	Software Deployment Tools (1/9)	Data from Cloud Storage (1/17)	Encrypted Channel (1/18)	Financial Theft (1/9)	Financial Theft (1/15)	
Search Open Technical Databases (1/11)	Stage Capabilities (1/8)	Trusted Relationships (1/13)	Inter-Process Communication (1/17)	Create or Modify System Process (1/23)	Domain or Tenant Policy Modification (1/14)	Domain or Tenant Policy Modification (1/47)	Modify Authentication Process (1/17)	Device Driver Discovery (1/34)	Taint Shared Content (1/9)	Data from Configuration Repository (1/17)	Fallback Channels (1/18)	Inhibit System Recovery (1/9)	Inhibit System Recovery (1/15)	
Search Open Websites/Domains (1/11)		Valid Accounts (1/13)	Native API (1/17)	Event Triggered Execution (1/23)	Escape to Host (1/14)	Escape to Host (1/47)	Multi-Factor Authentication Request Generation (1/17)	Domain Trust Discovery (1/34)	Use Alternate Authentication Material (1/9)	Data from Information Repository (1/17)	Hide Infrastructure (1/18)	Network Denial of Service (1/9)	Network Denial of Service (1/15)	
Search Threat Vendor Data (1/11)			Poisoned Pipeline Execution (1/17)	Event Triggered Execution (1/23)	Event Triggered Execution (1/14)	Event Triggered Execution (1/47)	Execution Guardrails (1/17)	Group Policy Discovery (1/34)	File and Directory Discovery (1/9)	Data from Local System (1/17)	Ingress Tool Transfer (1/18)	Resource Hijacking (1/9)	Resource Hijacking (1/15)	
Search Victim-Owned Websites (1/11)			Scheduled Task/Job (1/17)	External Remote Services (1/23)	Event Triggered Execution (1/14)	Event Triggered Execution (1/47)	Exploitation for Defense Evasion (1/17)	Local Storage Discovery (1/34)	Log Enumeration (1/9)	Data from Network Shared Drive (1/17)	Non-Application Layer Protocol (1/18)	Service Stop (1/9)	Service Stop (1/15)	
			Serverless Execution (1/17)	Hijack Execution Flow (1/23)	Exploitation for Privilege Escalation (1/14)	Exploitation for Privilege Escalation (1/47)	File and Directory Permissions Modification (1/17)	Network Service Discovery (1/34)	Network Service Discovery (1/9)	Data from Removable Media (1/17)	Protocol Tunneling (1/18)	System Shutdown/Reboot (1/9)	System Shutdown/Reboot (1/15)	
			Shared Modules (1/17)	Hijack Execution Flow (1/23)	Hijack Execution Flow (1/14)	Hijack Execution Flow (1/47)	Hide Artifacts (1/17)	Network Sniffing (1/34)	Proxies (1/9)	Data from Removable Media (1/17)	Remote Access Tools (1/18)			
			Software Deployment Tools (1/17)	Implant Internal Image (1/23)	Hijack Execution Flow (1/14)	Hijack Execution Flow (1/47)	Impair Defenses (1/17)	Network Sniffing (1/34)	Proxies (1/9)	Data Staged (1/17)	Traffic Signaling (1/18)			
			System Services (1/17)	Modify Authentication Process (1/23)	Impair Defenses (1/14)	Impair Defenses (1/47)	Impersonation (1/17)	Password Policy Discovery (1/34)	Screen Capture (1/9)	Email Collection (1/17)	Web Service (1/18)			
			User Execution (1/17)	Modify Registry (1/23)	Indicator Removal (1/14)	Indicator Removal (1/47)	Steal or Forge Kerberos Tickets (1/17)	Peripheral Device Discovery (1/34)	Video Capture (1/9)	Input Capture (1/17)				
			Windows Management Instrumentation (1/17)	Office Application Startup (1/23)	Indirect Command Execution (1/14)	Indirect Command Execution (1/47)	Steal Web Session Cookie (1/17)	Permission Groups Discovery (1/34)		Screen Capture (1/17)				
				Power Settings (1/23)	Masquerading (1/14)	Masquerading (1/47)	Unsecured Credentials (1/17)	Process Discovery (1/34)		Video Capture (1/17)				
				Pre-OS Boot (1/23)	Modify Authentication Process (1/14)	Modify Authentication Process (1/47)		Query Registry (1/34)						
				Scheduled Task/Job (1/23)	Modify Cloud Compute Infrastructure (1/14)	Modify Cloud Compute Infrastructure (1/47)		Remote System Discovery (1/34)						
				Server Software Component (1/23)	Modify Cloud Resource Hierarchy (1/14)	Modify Cloud Resource Hierarchy (1/47)		Software Discovery (1/34)						
				Software Extensions (1/23)	Modify Registry (1/14)	Modify Registry (1/47)		System Information Discovery (1/34)						
				Traffic Signaling (1/23)				System Location Discovery (1/34)						
								System Network Configuration (1/34)						

1.4 Overlap Analysis:

	A	B	C	D	E	F	G
	Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
1	Active Scanning	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism
2	Gather Victim Host Information	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	BITS Jobs	Access Token Manipulation	Access Token Manipulation
3	Gather Victim Identity Information	Compromise Accounts	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution	Account Manipulation	BITS Jobs
4	Gather Victim Network Information	Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts	Boot or Logon Autostart Execution	Build Image on Host
5	Gather Victim Org Information	Develop Capabilities	Hardware Additions	ESXi Administration Command	Cloud Application Integration	Boot or Logon Initialization Scripts	Debugger Evasion
6	Phishing for Information	Establish Accounts	Phishing	Exploitation for Client Execution	Compromise Host Software Binary	Create or Modify System Process	Delay Execution
7	Search Closed Sources	Obtain Capabilities	Replication Through Removable Media	Input Injection	Create Account	Domain or Tenant Policy Modification	Deobfuscate/Decode Files or Data
8	Search Open Technical Databases	Stage Capabilities	Supply Chain Compromise	Inter-Process Communication	Create or Modify System Process	Escape to Host	Deploy Container
9	Search Open Websites/Domains		Trusted Relationship	Native API	Event Triggered Execution	Event Triggered Execution	Direct Volume Access
10	Search Threat Vendor Data		Valid Accounts	Poisoned Pipeline Execution	Exclusive Control	Exploitation for Privilege Escalation	Domain or Tenant Policy Modification
11	Search Victim-Owned Websites		Wi-Fi Networks	Scheduled Task/Job	External Remote Services	Hijack Execution Flow	Email Spoofing
12				Serverless Execution	Hijack Execution Flow	Process Injection	Execution Guardrails
13				Shared Modules	Implant Internal Image	Scheduled Task/Job	Exploitation for Defense Evasion
14				Software Deployment Tools	Modify Authentication Process	Valid Accounts	File and Directory Permissions Manipulation
15				System Services	Modify Registry		Hide Artifacts
16				User Execution	Office Application Startup		Hijack Execution Flow
17				Windows Management Instrumentation	Power Settings		Impair Defenses
18					Pre-OS Boot		Impersonation
19					Scheduled Task/Job		Indicator Removal
20					Server Software Component		Indirect Command Execution
21					Software Extensions		Masquerading
22					Traffic Signaling		Modify Authentication Process
23					Valid Accounts		Modify Cloud Compute Infrastructure
24							Modify Cloud Resource Hierarchy
25							Modify Registry
26							Modify System Image
27							Network Bandwidth Optimization

The combined Navigator layer revealed significant overlap across APTs targeting the government sector.

3.3 High-frequency techniques include:

- **T1059 (Command and Scripting Interpreter)** – Used by all three APTs for execution
- **T1021 (Remote Services)** – Common for lateral movement
- **T1071 (Application Layer Protocol)** – Prevalent C2 method
- **T1566 (Phishing)** – Primary initial access vector for APT28 and observed in APT10 campaigns

Choke Point Techniques:

Attackers consistently rely on:

- **Credential dumping (T1003)** and **phishing (T1566)** to gain and escalate access
- **Remote services (T1021)** for lateral movement within government networks
- **C2 over standard protocols (T1071)** to blend with legitimate traffic

Significance:

These overlaps indicate that while APTs may have different motivations and origins, they employ similar post-compromise TTPs. This allows defenders to develop unified detection and mitigation strategies targeting these shared behaviors, rather than focusing on individual threat actors.

Task 4: Detection & Control Mapping (NIST & ISO)

4.1 NIST CSF Mapping

NIST CSF Function	Relevant Overlapping TTPs	Recommended Controls
Identify	T1566, T1195, T1190	Asset management, risk assessment, supply chain risk management
Protect	T1003, T1110, T1555	Identity management, access control, awareness training
Detect	T1059, T1021, T1071	Continuous monitoring, anomaly detection, log analysis
Respond	T1570, T1210, T1486	Response planning, communications, analysis
Recover	T1486, T1041, T1048	Recovery planning, improvements, communications

ISO/IEC 27001 Mapping

ISO 27001 Control Theme	Relevant TTPs	Justification
A.9 Access Control	T1003, T1110, T1555	Limits credential exposure and unauthorized access
A.12 Operations Security	T1059, T1021, T1071	Monitors and controls execution, lateral movement, and C2
A.13 Communications Security	T1071, T1105, T1048	Protects against C2 and exfiltration over network protocols
A.14 System Acquisition & Development	T1195, T1190	Ensures secure development and supply chain integrity

ISO 27001 Control Theme	Relevant TTPs	Justification
A.16 Information Security Incident Management	T1570, T1210, T1486	Enables effective detection, response, and recovery

4.2 Control Justification:

By implementing NIST CSF and ISO 27001 controls aligned with overlapping TTPs, government agencies can reduce exposure to common attack patterns. For example, enforcing strict access controls (ISO A.9) mitigates credential dumping and brute force attacks. Continuous monitoring and anomaly detection (NIST Detect) help identify suspicious command execution and lateral movement. Together, these controls create a layered defense that addresses the most prevalent techniques used by APTs targeting the public sector.

Report Prepared By: Temitayo Olanrewaju
Date: January 2026
Sources: MITRE ATT&CK, SOCRadre, CISA Alerts, OSINT Reports.