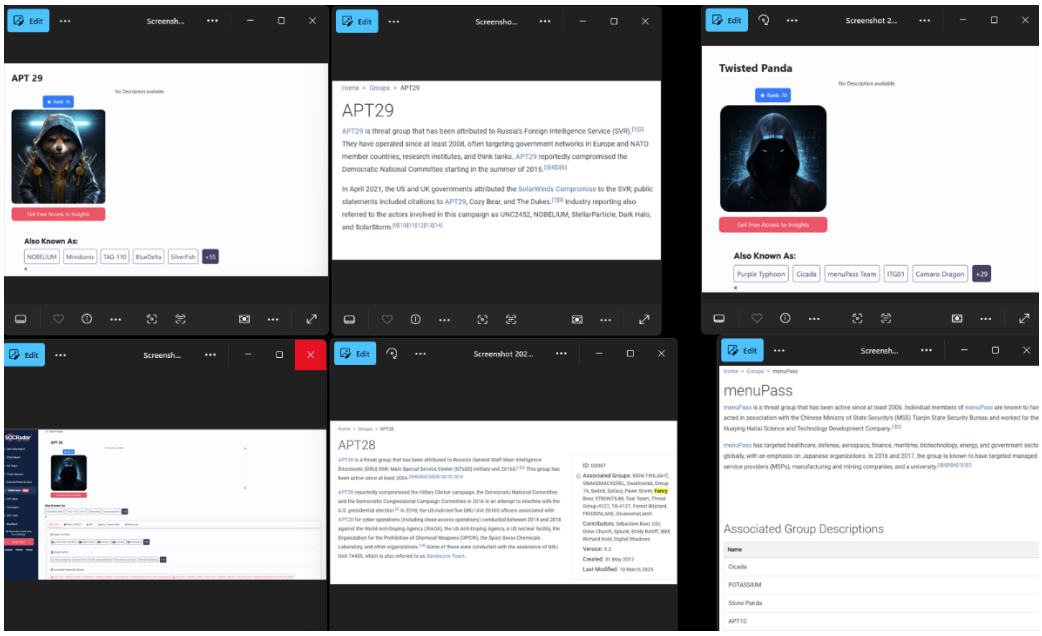
Government/Public Sector Threat Hunting Report: APT TTP Mapping & Control Alignment

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

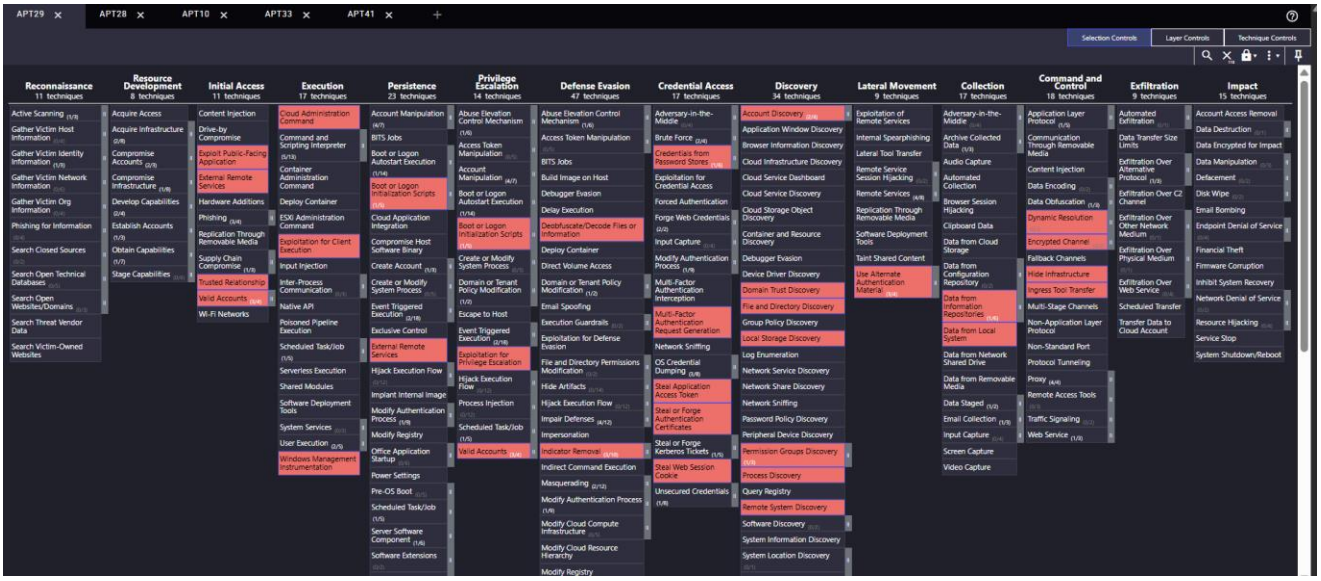
Key Focus Areas:

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

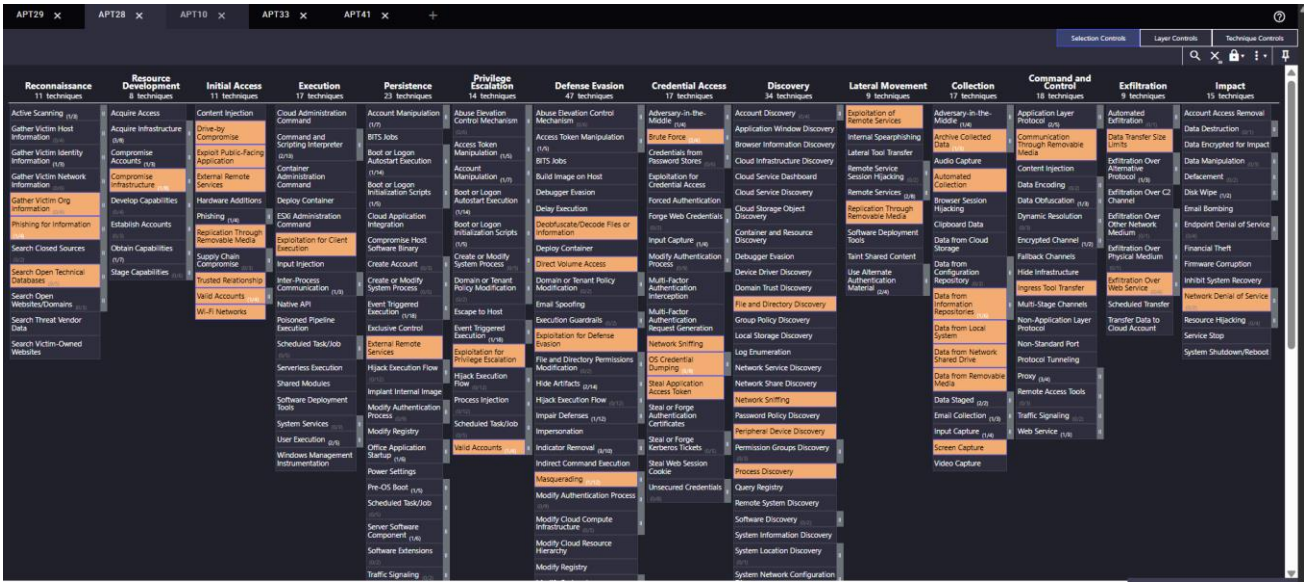
Task 3: ATT&CK Navigator Mapping & Overlap Analysis

3.1 Navigator Layers Created:

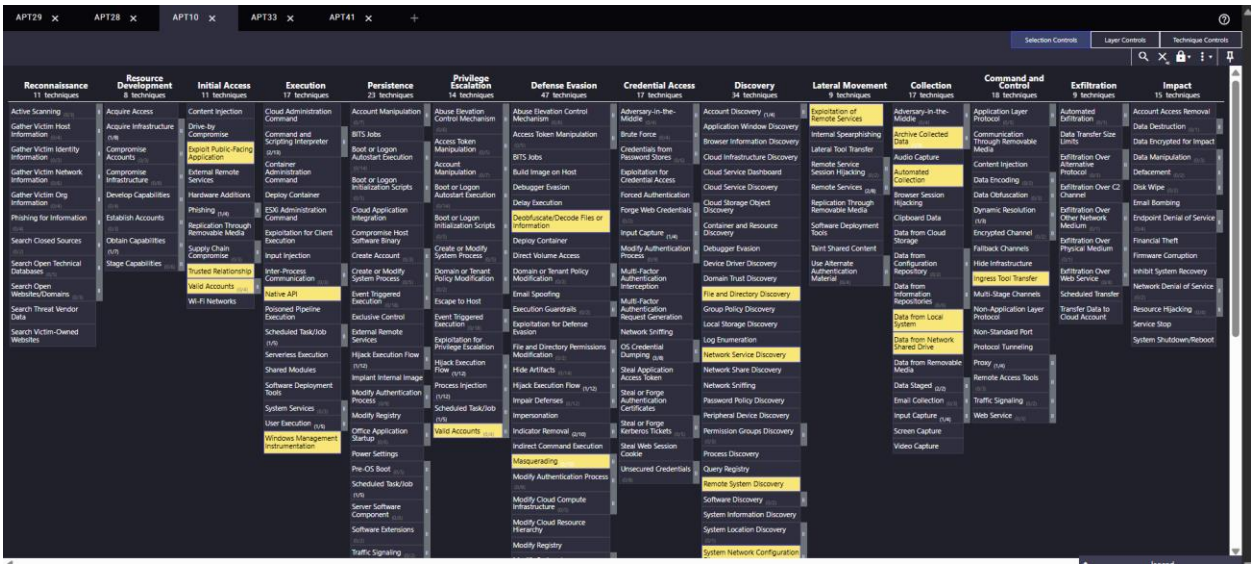
1. APT29 Layer (Cozy Bear)



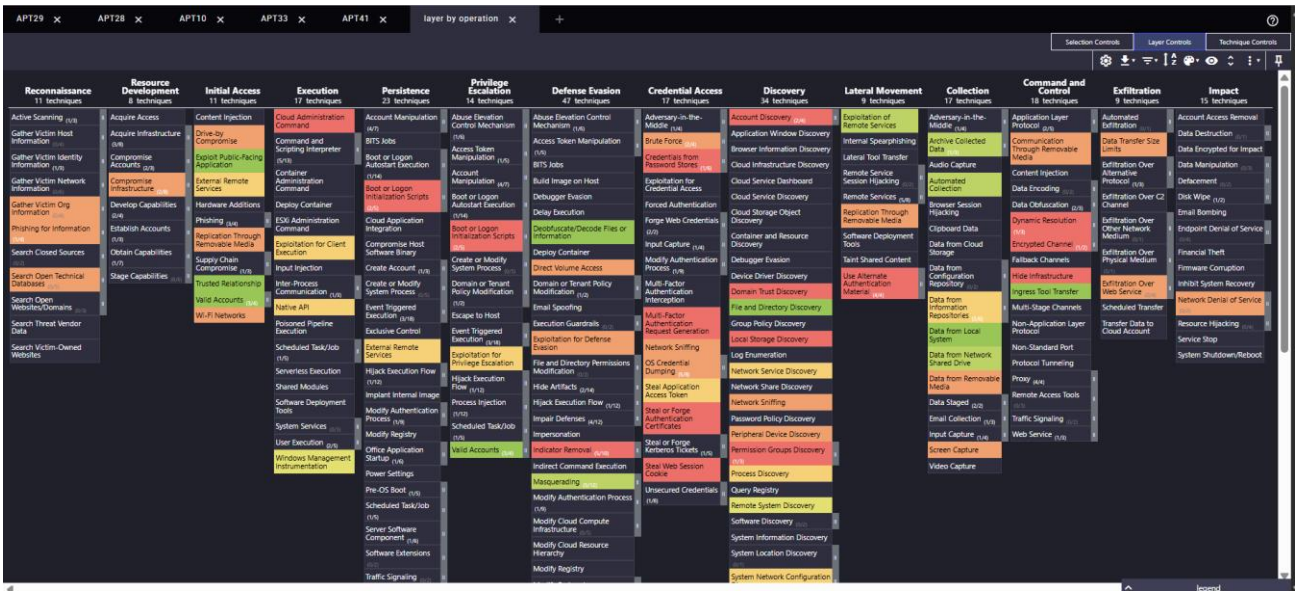
2. APT28 Layer (Fancy Bear)



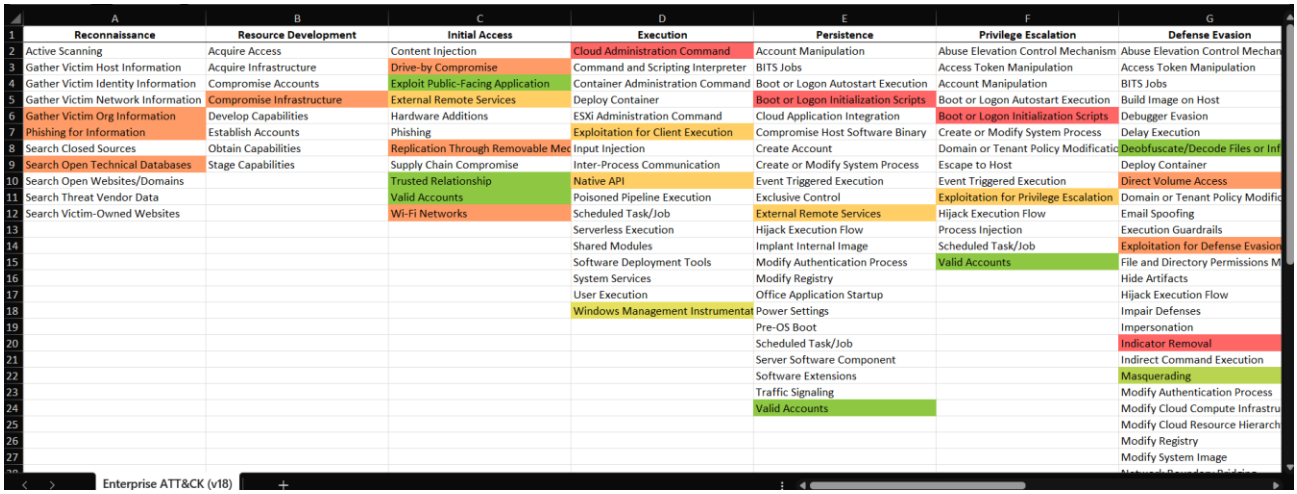
3. APT10 Layer (MenuPass)



4. Overlap Layer (Shared Techniques)



1.4 Overlap Analysis:



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
Active Scanning	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechan
Gather Victim Host Information	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	BITS Jobs	Access Token Manipulation	Access Token Manipulation
Gather Victim Identity Information	Compromise Accounts	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution	Account Manipulation	BITS Jobs
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
Gather Victim Org Information	Develop Capabilities	Hardware Additions	ESXi Administration Command	Cloud Application Integration	Boot or Logon Initialization Scripts	Debugger Evasion
Phishing for Information	Establish Accounts	Phishing	Exploitation for Client Execution	Compromise Host Software Binary	Create or Modify System Process	Delay Execution
Search Closed Sources	Obtain Capabilities	Replication Through Removable Mec	Input Injection	Create Account	Domain or Tenant Policy Modificatic	Deobfuscate/Decode Files or Inf
Search Open Technical Databases	Stage Capabilities	Supply Chain Compromise	Inter-Process Communication	Create or Modify System Process	Escape to Host	Deploy Container
Search Open Websites/Domains		Trusted Relationship	Native API	Event Triggered Execution	Event Triggered Execution	Direct Volume Access
Search Threat Vendor Data		Valid Accounts	Poisoned Pipeline Execution	Exclusive Control	Exploitation for Privilege Escalation	Domain or Tenant Policy Modific
Search Victim-Owned Websites		Wi-Fi Networks	Scheduled Task/Job	External Remote Services	Hijack Execution Flow	Email Spoofing
			Serverless Execution	Hijack Execution Flow	Process Injection	Execution Guardrails
			Shared Modules	Implant Internal Image	Scheduled Task/Job	Exploitation for Defense Evasion
			Software Deployment Tools	Modify Authentication Process	Valid Accounts	File and Directory Permissions M
			System Services	Modify Registry		Hide Artifacts
			User Execution	Office Application Startup		Hijack Execution Flow
			Windows Management Instrumentat	Power Settings		Impair Defenses
				Pre-OS Boot		Impersonation
				Scheduled Task/Job		Indicator Removal
				Server Software Component		Indirect Command Execution
				Software Extensions		Masquerading
				Traffic Signaling		Modify Authentication Process
				Valid Accounts		Modify Cloud Compute Infrastru
						Modify Cloud Resource Hierarch
						Modify Registry
						Modify System Image

Enterprise ATT&CK (v18)

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.