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

Target Sector: Financial Services (United Kingdom Insurance Focus)

Task 1: Industry Threat Landscape

1.1: Industry Justification

The financial services sector, specifically the United Kingdom insurance industry, represents a high-value target for advanced persistent threat (APT) groups due to the volume of sensitive data, financial assets, and critical services it manages.

Insurance organisations store large amounts of personally identifiable information (PII), financial records, medical data, and risk assessment models, making them attractive targets for espionage, fraud, and long-term intelligence collection. Compromise of such data can enable identity theft, financial crime, and large-scale fraud.

From an operational perspective, insurance providers rely heavily on digital platforms, third-party integrations, and legacy systems to process claims, manage policies, and assess risk. This creates a broad attack surface that sophisticated threat actors can exploit for persistence and lateral movement.

Additionally, the insurance sector plays a critical role in national economic stability and risk management, making it a target of interest for state-sponsored actors seeking strategic intelligence or economic disruption. Regulatory frameworks such as FCA requirements, GDPR, and ISO-aligned controls further increase the impact of security incidents, as breaches can result in significant financial penalties and reputational damage.

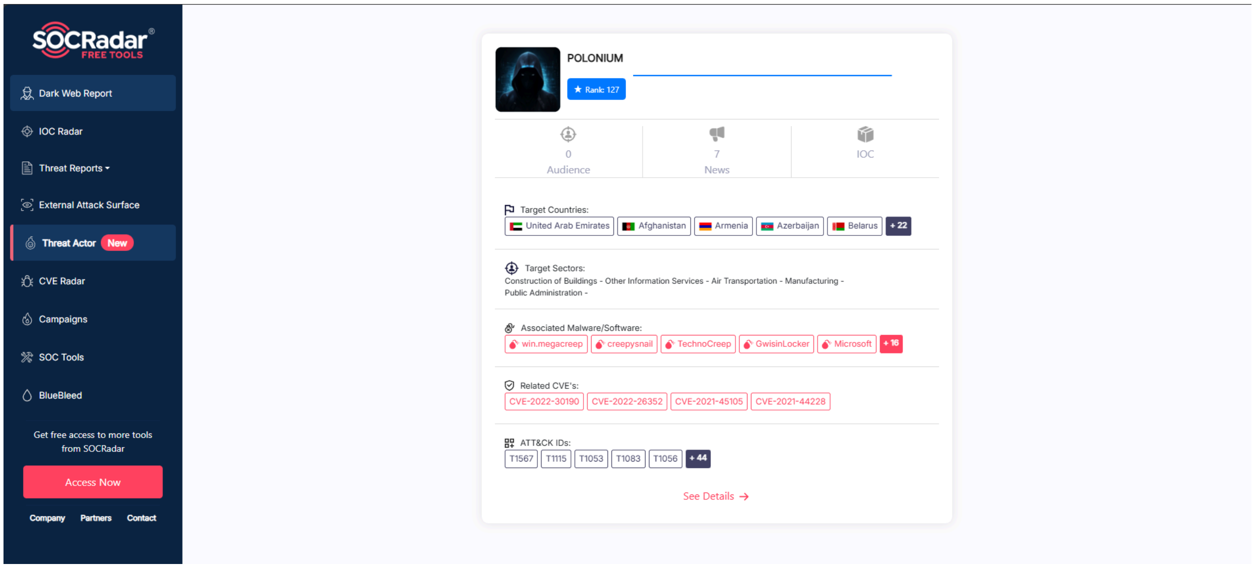
Due to its high data value, financial impact, regulatory sensitivity, and systemic importance, the UK insurance sector remains a consistent and attractive target for advanced threat actors.

1.2: Selected APT Groups

Based on open-source threat intelligence and industry-focused research using platforms such as SocRadar, three Advanced Persistent Threat (APT) groups were identified as having relevance to the financial and insurance sector. These groups have demonstrated capabilities aligned with long-term access, intelligence collection, and exploitation of trusted enterprise environments. The selected APT groups for this assessment are Polonium, Cobalt, and Windigo.

1.3: APT Threat Profiles

A. **Polonium**



POLONIUM

★ Rank: 127

0 Audience | 7 News | IOC

Target Countries:
United Arab Emirates, Afghanistan, Armenia, Azerbaijan, Belarus, + 22

Target Sectors:
Construction of Buildings - Other Information Services - Air Transportation - Manufacturing - Public Administration -

Associated Malware/Software:
win.megacreep, creepysnail, TechnoCreep, GwisinLocker, Microsoft, + 16

Related CVE's:
CVE-2022-30190, CVE-2022-26352, CVE-2021-45105, CVE-2021-44228

ATT&CK IDs:
T1567, T1115, T1053, T1083, T1056, + 44

See Details →

Polonium is an advanced persistent threat group observed conducting long-term espionage-focused operations, with activity reported by multiple security vendors. The group is known for leveraging legitimate cloud services and trusted platforms to maintain persistence and command-and-control, reducing the likelihood of detection by traditional security controls.

Polonium's primary motivation is strategic espionage, focusing on maintaining covert access to victim environments for intelligence collection. Rather than relying heavily on custom malware, the group frequently abuses legitimate services such as Microsoft OneDrive and VPN infrastructure, aligning with living-off-the-land techniques.

This tradecraft presents a significant risk to the financial and insurance sector, where cloud services, third-party integrations, and trusted identities are widely used. Abuse of legitimate platforms can enable Polonium to blend into normal enterprise traffic, making detection and attribution more challenging for SOC teams.

Threat Group	Tactics	Techniques IDs
Polonium	Collection	T1560, T1005, T1125, T1113, T1530, T1056, T1115
Polonium	Command & Control	T1090, T1071, T1095, T1571, T1572, T1573, T1102, T1105, T1132
Polonium	Credential Access	T1056
Polonium	Defense Evasion	T1036, T1070, T1574, T1078, T1127, T1140, T1218, T1027, T1134
Polonium	Discovery	T1083, T1057, T1033, T1016, T1082
Polonium	Execution	T1053, T1059, T1129, T1569
Polonium	Exfiltration	T1041, T1567

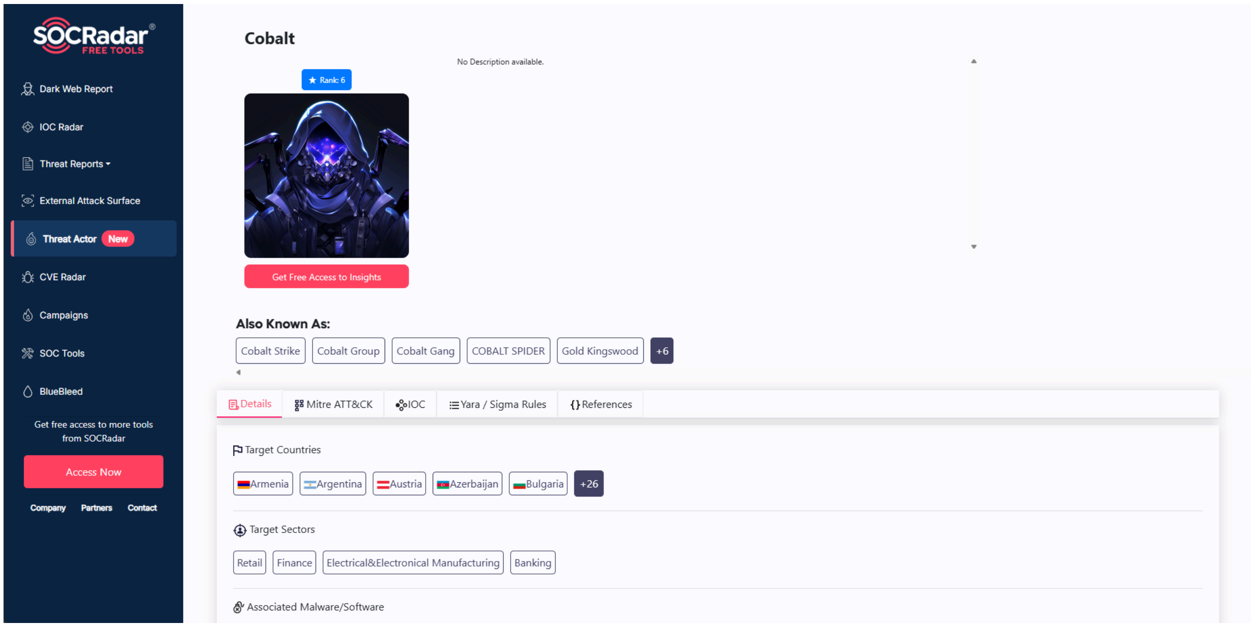
Polonium	Initial Access	T1199, T1078, T1566
Polonium	Persistence	T1547, T1053, T1574, T1078
Polonium	Privilege Escalation	T1574, T1053, T1078, T1134
Polonium	Resource Development	T1588, T1583, T1587

References:

Microsoft Security Blog – Exposing Polonium activity and infrastructure targeting organizations (2022)

Socrader Polonium TTPs

B. Cobalt Group



Cobalt

No Description available.

Also Known As:

Cobalt Strike | Cobalt Group | Cobalt Gang | COBALT SPIDER | Gold Kingswood | +6

Target Countries

Armenia | Argentina | Austria | Azerbaijan | Bulgaria | +26

Target Sectors

Retail | Finance | Electrical&Electronical Manufacturing | Banking

Associated Malware/Software

Cobalt Group is a financially motivated advanced threat actor that has primarily targeted financial institutions. According to Rapid7 and other open-source reporting, the group has conducted sophisticated intrusions aimed at stealing funds by compromising ATM infrastructure, card processing environments, payment platforms, and SWIFT systems.

The group has historically focused on banks across Eastern Europe, Central Asia, and Southeast Asia, demonstrating strong knowledge of financial transaction workflows and enterprise banking systems. Although one of the group's alleged leaders was arrested in Spain in early 2018, reporting indicates that Cobalt Group remains active and continues to pose a threat to financial-sector organisations.

Cobalt Group's operations are characterised by long-term access, credential compromise, and the abuse of legitimate administrative tools to move laterally and maintain persistence. The group has also been linked to the Carbanak malware and is believed to share tradecraft and operational overlap with the Carbanak threat group. Their ability to leverage compromised organisations as staging points to access additional victims highlights a mature and expansion-focused attack model.

This combination of financial motivation, operational sophistication, and proven impact against European organisations makes Cobalt Group highly relevant to the insurance sector, which shares similar infrastructure, trust relationships, and sensitive financial data with banking institutions.

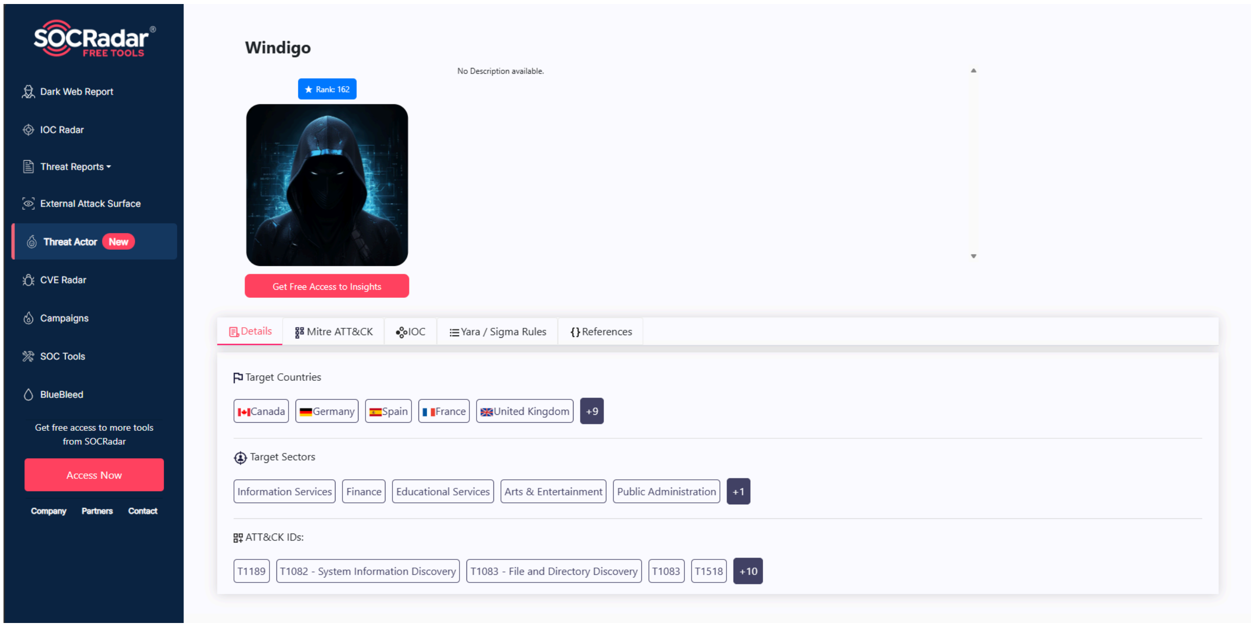
Threat Group	Tactics	Technique IDs
Cobalt	Collection	T1119, T1560, T1113, T1115, T1074, T1185, T1557, T1530, T1114, T1005, T1213, T1125, T1039, T1056, T1123, T1123
Cobalt	Command & Control	T1090, T1071, T1572, T1065, T1568, T1008, T1102, T1573, T1094, T1205, T1001, T1104, T1219, T1105, T1043,
Cobalt	Credential Access	T1528, T1003, T1558, T1552, T1503, T1539, T1557, T1187, T1110, T1555, T1081, T1556, T1179, T1056
Cobalt	Defense Evasion	T1070, T1143, T1553, T1484, T1078, T1107, T1506, T1218, T1221,T1222, T1205,T1014, T1197, T1134, T1027,
Cobalt	Discovery	T1049, T1012, T1135, T1018, T1016, T1614, T1057, T1046, T1124, T1497, T1482, T1083, T1082, T1033, T1120,
Cobalt	Execution	T1106, T1203, T1035, T1086, T1559, T1053, T1059, T1129, T1569, T1204, T1170, T1610, T1085, T1155,T1047
Cobalt	Exfiltration	T1020, T1011, T1567, T1029, T1537, T1048, T1041, T1030
Cobalt	Impact	T1485, T1491, T1489, T1565, T1490, T1486, T1496, T1498, T1529, T1561, T1531
Cobalt	Initial Access	T1189, T1078, T1190, T1133, T1195, T1199, T1566
Cobalt	Lateral Movement	T1080, T1506, T1210, T1021, T1570, T1097, T1051, T1563, T1550
Cobalt	Persistence	T1547, T1176, T1554, T1078, T1133, T1098, T1205, T1136, T1197, T1053, T1158, T1037, T1542, T1546, T1112,
Cobalt	Privilege Escalation	T1547, T1068, T1484, T1078, T1098, T1134, T1053, T1037, T1546, T1574, T1548, T1179, T1055, T1543
Cobalt	Reconnaissance	T1589, T1592, T1591, T1596, T1597, T1595, T1590, T1594, T1598
Cobalt	Resource Development	T1583, T1608, T1588, T1585, T1586, T1587, T1584

References:

Rapid7 InsightIDR – Cobalt Group

socRader Cobalt TTPs

C. Windigo Group



Windigo

No Description available.

Target Countries

Canada | Germany | Spain | France | United Kingdom | +9

Target Sectors

Information Services | Finance | Educational Services | Arts & Entertainment | Public Administration | +1

ATT&CK IDs:

T1189 | T1082 - System Information Discovery | T1083 - File and Directory Discovery | T1083 | T1518 | +10

Windigo is a cybercrime-associated threat group observed conducting broad infrastructure compromise, particularly targeting Linux and Unix servers across multiple regions. According to the *Operation Windigo* report, compromised servers were used to host malicious content, act as proxies or relays, and serve as distribution points for credential-stealing malware and spam. The campaign exploited vulnerabilities in web applications and weak server credentials to gain initial access and establish persistent footholds.

The group's primary motivation is financial gain, often achieved indirectly by compromising server infrastructure and leveraging that access for downstream malicious activity, including credential theft. The pervasive use of backdoored servers allowed Windigo operators to obscure their origin, facilitate additional intrusions, and harvest credentials at scale.

This type of compromise poses a threat to sectors such as financial services and insurance, where credential theft and unauthorized access can lead to broader network compromise and data exposure.

Threat Group	Tactics	Technique IDs
Windigo	Collection	T1005

Windigo	Command & Control	T1090
Windigo	Discovery	T1082, T1083, T1518
Windigo	Execution	T1059
Windigo	Initial Access	T1189
Windigo	Persistence	T1543
Windigo	Privilege Escalation	T1543

Reference:

ESET. Operation Windigo. (2014)

socRader Windigo TTPs

Task 2: TTP Analysis Using MITRE ATT&CK

2.1 Methodology

This section documents the Tactics, Techniques, and Procedures (TTPs) associated with the selected APT groups using the MITRE ATT&CK Enterprise framework. Techniques were identified through open-source intelligence, including MITRE ATT&CK documentation, vendor threat reports, and SOC-focused intelligence platforms. Emphasis was placed on post-compromise behavior, particularly credential access, lateral movement, command and control (C2), and persistence techniques relevant to enterprise and insurance environments.

2.2 MITRE ATT&CK Technique Mapping Overview

The following subsections map observed techniques used by Polonium, Cobalt, and Windigo across the ATT&CK lifecycle, highlighting behaviors that enable sustained access and operational impact within financial and insurance sector environments.

2.3 APT-Specific TTP Mapping

TTP ANALYSIS FOR POLONIUM

APT	Tactics	Technique ID	Technique Name
Polonium	Lateral Movement	T1199	Trusted Relationship
Polonium	Initial Access	T1078	Valid Accounts
Polonium	Command and Control	T1090	Proxy
Polonium	Exfiltration	T1567.002	Exfiltration over web service: Cloud Storage.
Polonium	Resource Development	T1588.002	Obtain Capabilities: Tools

Polonium demonstrates a strong preference for abusing legitimate cloud services and trusted relationships to blend malicious activity into normal enterprise traffic. By leveraging valid credentials, cloud-based command and control, and commercial VPN infrastructure, the group significantly reduces detection opportunities based on traditional signature-based controls.

TTP ANALYSIS FOR COBALT GROUP

APT	Tactics	Technique ID	Technique Name
Cobalt Group	Lateral Movement	T1021.001	Remote Services: Remote Desktop Protocol.
Cobalt Group	Initial Access	T1566.001	Phishing: Separating Attachment
Cobalt Group	Command and Control	T1071.001	Application layer Protocol: Web Protocols
Cobalt Group	Credential Access	T1003	OS Credential Dumping
Cobalt Group	Command and Control	T1090	Proxy

The mapped techniques show Cobalt Group's reliance on credential compromise and valid account abuse to maintain access within enterprise environments. Remote services are used to enable lateral movement toward high-value systems, while web-based command-and-control allows attacker traffic to blend with legitimate network activity.

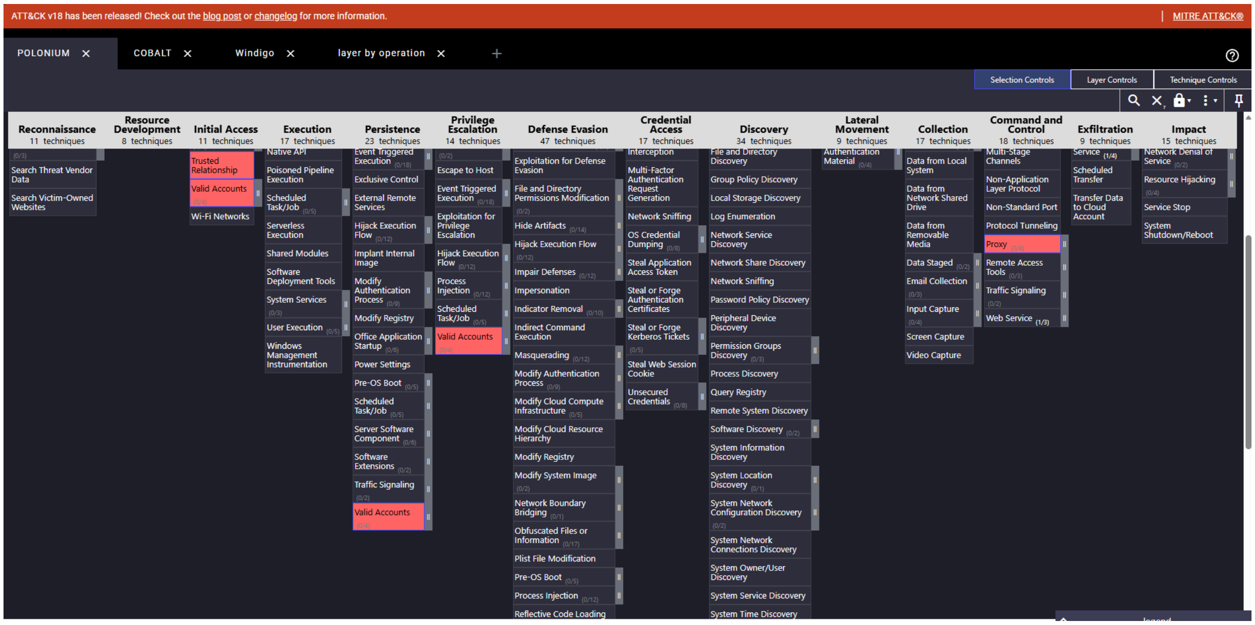
TTP ANALYSIS FOR WINDIGO GROUP

APT	Tactics	Technique ID	Technique Name
Windigo	Lateral Movement	T1021	Remote Services
Windigo	Initial Access	T1078	Valid Accounts
Windigo	Persistence	T1547	Boot or Logon Autostart Execution
Windigo	Credential Access	T1003	OS Credential Dumping
Windigo	Command and Control	T1102	Web Service

Windigo's TTPs indicate a credential-driven intrusion model focused on persistence and internal movement. The use of remote services for lateral movement and web-based command-and-control channels supports stealthy, long-term operations within compromised environments.

Task 3: ATT&CK Navigator Mapping & Overlap Analysis

3.1 ATT&CK Navigator Layer Creation



ATT&CK v18 has been released! Check out the blog post or changelog for more information. | MITRE ATT&CK®

POLONIUM × | COBALT × | Windigo × | layer by operation × | +

Selection Controls | Layer Controls | Technique Controls

Reconnaissance 11 techniques
(0/3)
Search Threat Vendor Data
Search Victim-Owned Websites

Resource Development 8 techniques

Initial Access 11 techniques
Trusted Relationship
Valid Accounts (0/4)
Wi-Fi Networks

Execution 17 techniques
Native API
Poisoned Pipeline Execution
Scheduled Task/Job (0/5)
Serverless Execution
Shared Modules
Software Deployment Tools
System Services (0/3)
User Execution (0/5)
Windows Management Instrumentation

Persistence 23 techniques
Event Triggered Execution (0/18)
Exclusive Control
External Remote Services
Hijack Execution Flow (0/12)
Implant Internal Image
Modify Authentication Process (0/9)
Modify Registry
Office Application Startup (0/6)
Power Settings
Pre-OS Boot (0/5)
Scheduled Task/Job (0/5)
Server Software Component (0/6)
Software Extensions (0/2)
Traffic Signaling (0/2)
Valid Accounts (0/4)

Privilege Escalation 14 techniques
(0/2)
Escape to Host
Event Triggered Execution (0/18)
Exploitation for Privilege Escalation
Hijack Execution Flow (0/12)
Process Injection (0/12)
Scheduled Task/Job (0/5)
Valid Accounts (0/4)

Defense Evasion 47 techniques
Exploitation for Defense Evasion
File and Directory Permissions Modification (0/2)
Hide Artifacts (0/14)
Hijack Execution Flow (0/12)
Impair Defenses (0/12)
Impersonation
Indicator Removal (0/10)
Indirect Command Execution
Masquerading (0/12)
Modify Authentication Process (0/9)
Modify Cloud Compute Infrastructure (0/5)
Modify Cloud Resource Hierarchy
Modify Registry
Modify System Image (0/2)
Network Boundary Bridging (0/1)
Obfuscated Files or Information (0/17)
Plist File Modification
Pre-OS Boot (0/5)
Process Injection (0/12)
Reflective Code Loading

Credential Access 17 techniques
Interception
Multi-Factor Authentication Request Generation
Network Sniffing
OS Credential Dumping (0/8)
Steal Application Access Token
Steal or Forge Authentication Certificates
Steal or Forge Kerberos Tickets (0/5)
Steal Web Session Cookie
Unsecured Credentials (0/8)

Discovery 34 techniques
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 (0/3)
Process Discovery
Query Registry
Remote System Discovery
Software Discovery (0/2)
System Information Discovery
System Location Discovery (0/1)
System Network Configuration Discovery (0/2)
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery

Lateral Movement 9 techniques
Authentication Material (0/4)

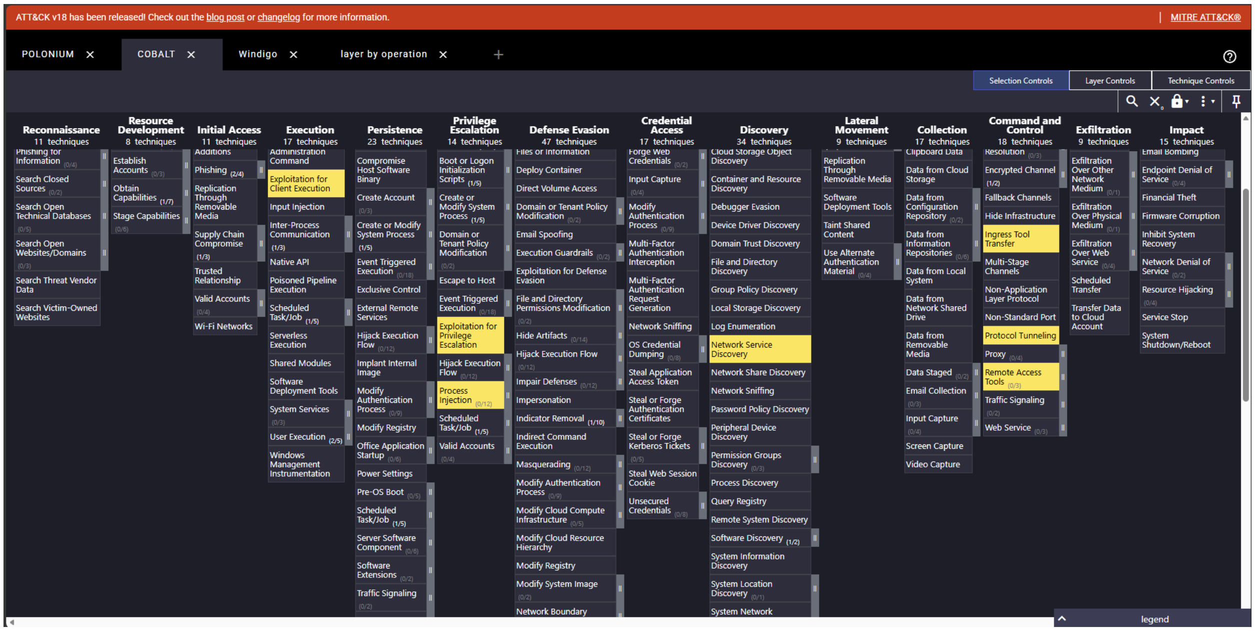
Collection 17 techniques
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged (0/2)
Email Collection (0/3)
Input Capture (0/4)
Screen Capture
Video Capture

Command and Control 18 techniques
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy (0/4)
Remote Access Tools (0/3)
Traffic Signaling (0/2)
Web Service (1/3)

Exfiltration 9 techniques
Service (1/4)
Scheduled Transfer
Transfer Data to Cloud Account

Impact 15 techniques
Network Denial of Service (0/2)
Resource Hijacking (0/4)
Service Stop
System Shutdown/Reboot

legend



ATT&CK v18 has been released! Check out the blog post or changelog for more information. | MITRE ATT&CK®

POLONIUM × | COBALT × | Windigo × | layer by operation × | +

Selection Controls | Layer Controls | Technique Controls

Reconnaissance 11 techniques
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
Establish Accounts (0/3)
Obtain Capabilities (1/7)
Stage Capabilities (0/6)

Initial Access 11 techniques
Additions
Phishing (2/4)
Replication Through Removable Media
Supply Chain Compromise (1/3)
Trusted Relationship
Valid Accounts (0/4)
Wi-Fi Networks

Execution 17 techniques
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 (0/3)
User Execution (2/5)
Windows Management Instrumentation

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

Privilege Escalation 14 techniques
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 (0/18)
Exploitation for Privilege Escalation
Hijack Execution Flow (0/12)
Process Injection (0/12)
Scheduled Task/Job (1/5)
Valid Accounts (0/4)

Defense Evasion 47 techniques
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 (0/14)
Hijack Execution Flow (0/12)
Impair Defenses (0/12)
Impersonation
Indicator Removal (1/10)
Indirect Command Execution
Masquerading (0/12)
Modify Authentication Process (0/9)
Modify Cloud Compute Infrastructure (0/5)
Modify Cloud Resource Hierarchy
Modify Registry
Modify System Image (0/2)
Network Boundary

Credential Access 17 techniques
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 (0/8)
Steal Application Access Token
Steal or Forge Authentication Certificates
Steal or Forge Kerberos Tickets (0/5)
Steal Web Session Cookie
Unsecured Credentials (0/8)

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

Lateral Movement 9 techniques
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material (0/4)

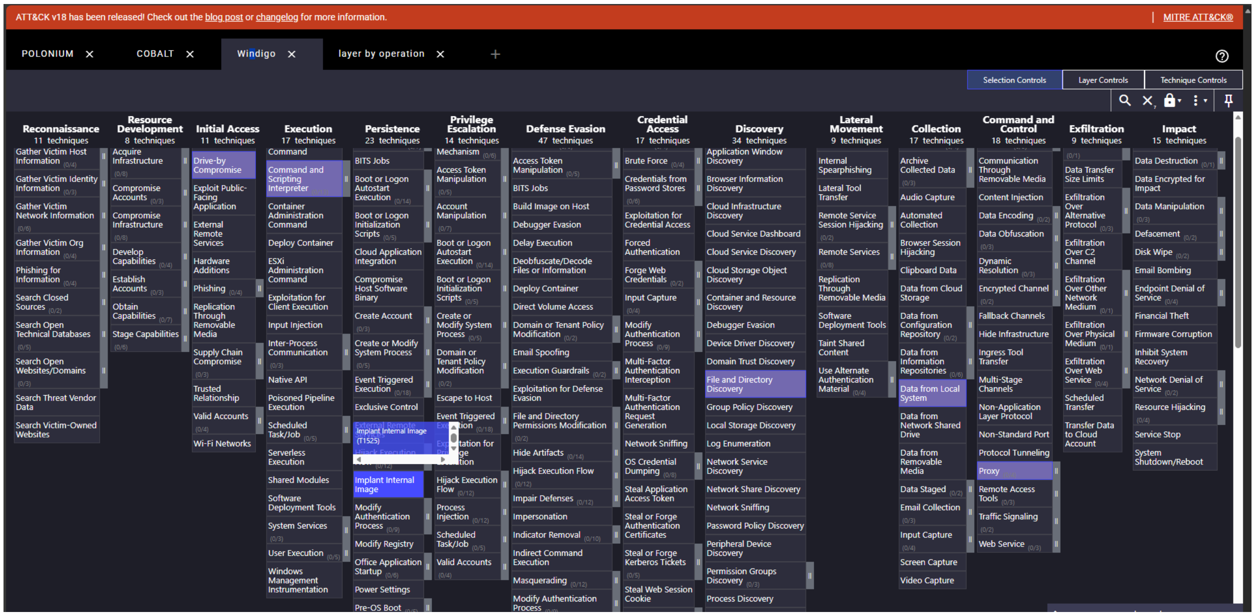
Collection 17 techniques
Clipboard Data
Data from Cloud Storage
Data from Configuration Repository (0/2)
Data from Information Repositories (0/6)
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged (0/2)
Email Collection (0/3)
Input Capture (0/4)
Screen Capture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

Command and Control 18 techniques
Resolution (0/3)
Encrypted Channel (1/2)
Fallback Channels
Hide Infrastructure
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy (0/4)
Remote Access Tools (0/3)
Traffic Signaling (0/2)
Web Service (0/3)

Exfiltration 9 techniques
Exfiltration Over Other Network Medium (0/1)
Exfiltration Over Physical Medium (0/1)
Exfiltration Over Web Service (0/4)
Scheduled Transfer
Transfer Data to Cloud Account

Impact 15 techniques
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

legend



ATT&CK v18 has been released! Check out the blog post or changelog for more information. | MITRE ATT&CK®

Reconnaissance
11 techniques
Gather Victim Host Information (0/4)
Gather Victim Identity Information (0/3)
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
Acquire Infrastructure (0/8)
Compromise Accounts (0/3)
Compromise Infrastructure (0/8)
Develop Capabilities (0/4)
Establish Accounts (0/3)
Obtain Capabilities (0/7)
Stage Capabilities (0/6)

Initial Access
11 techniques
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (0/4)
Replication Through Removable Media
Supply Chain Compromise (0/3)
Trusted Relationship
Valid Accounts (0/4)
Wi-Fi Networks

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

Persistence
23 techniques
BITS Jobs
Boot or Logon Autostart Execution (0/14)
Boot or Logon Initialization Scripts (0/5)
Cloud Application Integration
Compromise Host Software Binary
Create Account (0/3)
Create or Modify System Process (0/5)
Event Triggered Execution (0/18)
Exclusive Control
External Remote Services
Implant Internal Image (T1525)
Hijack Execution Flow (0/12)
Implant Internal Image
Modify Authentication Process (0/9)
Modify Registry
Office Application Startup (0/6)
Power Settings
Pre-OS Boot (0/5)

Privilege Escalation
14 techniques
Mechanism (0/6)
Access Token Manipulation (0/5)
Account Manipulation (0/7)
Boot or Logon Autostart Execution (0/14)
Boot or Logon Initialization Scripts (0/5)
Create or Modify System Process (0/5)
Domain or Tenant Policy Modification (0/2)
Escape to Host
Event Triggered Execution (0/18)
Exploitation for Privilege Escalation
Hijack Execution Flow (0/12)
Process Injection (0/12)
Scheduled Task/Job (0/5)
Valid Accounts (0/4)

Defense Evasion
47 techniques
Access Token Manipulation (0/5)
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 (0/2)
Email Spoofing
Execution Guardrails (0/2)
Exploitation for Defense Evasion
File and Directory Permissions Modification (0/2)
Hide Artifacts (0/14)
Hijack Execution Flow (0/12)
Impair Defenses (0/12)
Impersonation
Indicator Removal (0/10)
Indirect Command Execution
Masquerading (0/12)
Modify Authentication Process (0/9)

Credential Access
17 techniques
Brute Force (0/4)
Credentials from Password Stores (0/6)
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 (0/8)
Steal Application Access Token
Steal or Forge Authentication Certificates
Steal or Forge Kerberos Tickets (0/5)
Steal Web Session Cookie

Discovery
34 techniques
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 (0/3)
Process Discovery

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

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

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

Exfiltration
9 techniques
(0/1)
Data Transfer Size Limits
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 (0/4)
Scheduled Transfer
Transfer Data to Cloud Account

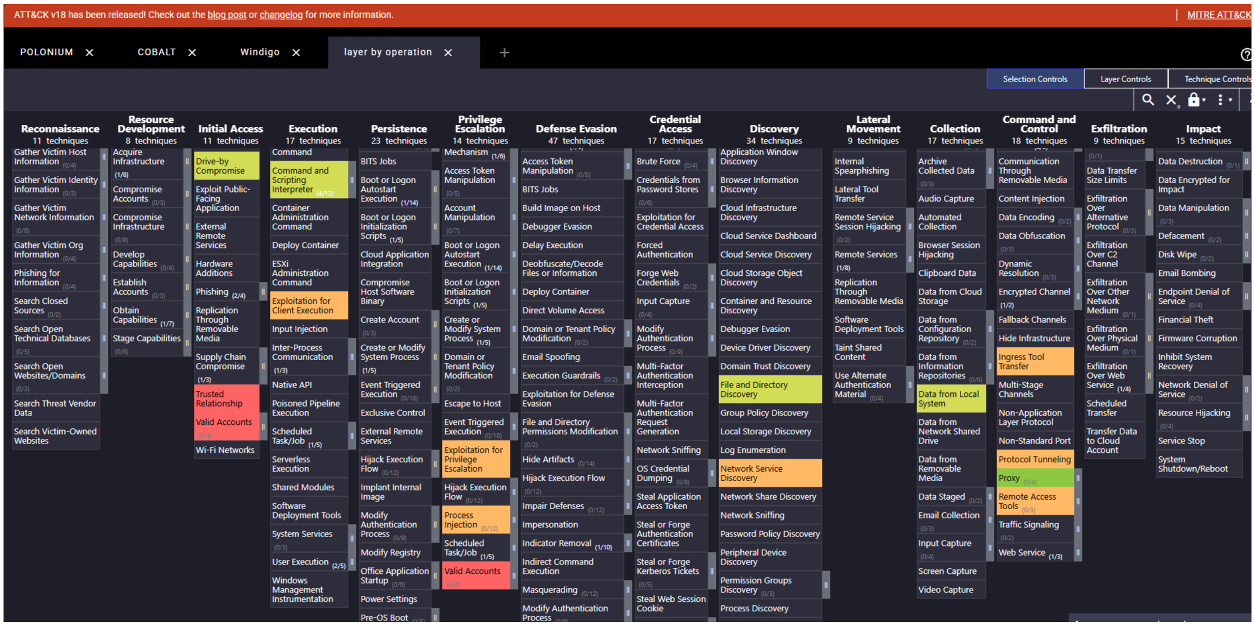
Impact
15 techniques
Data Destruction (0/1)
Data Encrypted for Impact
Data Manipulation (0/3)
Defacement (0/2)
Disk Wipe (0/2)
Email Bombing
Endpoint Denial of Service (0/4)
Financial Theft
Firmware Corruption
Inhibit System Recovery
Network Denial of Service (0/2)
Resource Hijacking (0/4)
Service Stop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

Separate MITRE ATT&CK Navigator layers were created for each identified APT group (Polonium, Cobalt, and Windigo).

Techniques were selected based on open-source intelligence and mapped to the MITRE ATT&CK Enterprise matrix to visualise each group's observed behaviour across the attack lifecycle, from initial access through command and control.

Note: Due to display limitations, the screenshot shows a partial view of the ATT&CK Navigator layer. The complete technique set is provided as an exported ATT&CK Navigator layer file in the project repository for full visibility and review.

3.2. Overlap (Combined) Layer Analysis



Reconnaissance 11 techniques
Gather Victim Host Information (0/4)
Gather Victim Identity Information (0/3)
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
Acquire Infrastructure (1/8)
Compromise Accounts (0/3)
Compromise Infrastructure (0/8)
Develop Capabilities (0/4)
Establish Accounts (0/3)
Obtain Capabilities (1/7)
Stage Capabilities (0/6)

Initial Access 11 techniques
Drive-by Compromise
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 (0/4)
Wi-Fi Networks

Execution 17 techniques
Command
Command and Scripting Interpreter (4/13)
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 (0/3)
User Execution (2/5)
Windows Management Instrumentation

Persistence 23 techniques
BITS Jobs
Boot or Logon Autostart Execution (1/14)
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 (0/18)
Exclusive Control
External Remote Services
Hijack Execution Flow (0/12)
Implant Internal Image
Modify Authentication Process (0/9)
Modify Registry
Office Application Startup (0/6)
Power Settings
Pre-OS Boot

Privilege Escalation 14 techniques
Mechanism (1/6)
Access Token Manipulation (0/5)
Account Manipulation (0/7)
Boot or Logon Autostart Execution (1/14)
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 (0/18)
Exploitation for Privilege Escalation
Hijack Execution Flow (0/12)
Process Injection (0/12)
Scheduled Task/Job (1/5)
Valid Accounts (0/4)

Defense Evasion 47 techniques
Access Token Manipulation (0/5)
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 (0/2)
Email Spoofing
Execution Guardrails (0/2)
Exploitation for Defense Evasion
File and Directory Permissions Modification (0/2)
Hide Artifacts (0/14)
Hijack Execution Flow
Impair Defenses (0/12)
Impersonation
Indicator Removal (1/10)
Indirect Command Execution
Masquerading (0/12)
Modify Authentication Process

Credential Access 17 techniques
Brute Force (0/4)
Credentials from Password Stores (0/6)
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 (0/8)
Steal Application Access Token
Steal or Forge Authentication Certificates
Steal or Forge Kerberos Tickets (0/5)
Steal Web Session Cookie

Discovery 34 techniques
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 (0/3)
Process Discovery

Lateral Movement 9 techniques
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (0/2)
Remote Services (1/8)
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material (0/4)

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

Command and Control 18 techniques
Communication Through Removable Media
Content Injection
Data Encoding (0/2)
Data Obfuscation (0/3)
Dynamic Resolution (0/3)
Encrypted Channel (1/2)
Fallback Channels
Hide Infrastructure
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy (0/4)
Remote Access Tools (0/3)
Traffic Signaling (0/2)
Web Service (1/3)

Exfiltration 9 techniques
(0/1)
Data Transfer Size Limits
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
Data Destruction (0/1)
Data Encrypted for 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

A combined ATT&CK Navigator layer was generated to identify techniques shared by two or more APT groups. This overlap analysis highlights attacker behaviours that are consistently relied upon across different threat actors targeting the financial and insurance sector.

3.3 High-Frequency and Choke Point Techniques

The overlap analysis of the combined ATT&CK Navigator layer revealed several techniques consistently used across all APT groups. These high-frequency techniques represent operational “choke points” that attackers repeatedly rely on to maintain access and operate within compromised environments.

Credential Access techniques, particularly the abuse of Valid Accounts (T1078), appeared across all APT groups. This indicates a shared reliance on stolen or compromised credentials to bypass perimeter controls and blend in with legitimate user activity.

In terms of Lateral Movement, the use of Remote Services (T1021) was commonly observed. This technique enables attackers to move between systems using standard administrative protocols, allowing them to reach high-value assets while minimising detection.

For Command and Control, several groups demonstrated the use of Web Services (T1102) and proxy-based communication methods. By leveraging legitimate cloud services and encrypted channels, attackers can disguise malicious traffic as normal business activity, complicating network-based detection.

The recurrence of these techniques across distinct APT groups suggests that defensive controls focused on credential hygiene, privileged access monitoring, and cloud service visibility can significantly reduce risk. **Prioritising detection around these shared techniques provides greater defensive coverage than actor-specific signatures.**

4.1. Overview

This section translates the identified overlapping ATT&CK techniques into actionable security controls aligned with recognised industry frameworks. By mapping high-frequency APT TTPs to the NIST Cybersecurity Framework (CSF) and ISO/IEC 27001 control domains, this analysis demonstrates how threat intelligence can directly inform detection, prevention, and governance decisions within a Security Operations Center (SOC) supporting the insurance sector.

4.2 NIST CSF Mapping Table

Mapping Overlapping APT TTPs to NIST CSF Functions

Overlapping ATTACK Technique	**Threat Description**	**NIST CSF FUNCTION**	**Control Focus**
T1078 - Valid Accounts	Abuse of legitimate credentials for access and persistence	PR.AC (Protect - Access Control)	Strong IAM, MFA, credential lifestyle management
T1199 - Trusted Relationship	Exploitation of third party or partner access	ID.SC (Identify - Supply Chain Risk)	Third party risk management and access segmentation
T1133 - External Remote Services	Remote access abuse (VPN, RDP, Cloud Services)	PR.AC	Secure remote access, Conditional access policies
T1102 - Web Services (C2)	Command and Control via legitimate cloud platforms	DE.CM (Detect - Continuous Monitoring)	Cloud traffic monitoring and anomaly detection
T1567.002 - Exfiltration to Cloud Storage	Data exfiltration Using Cloud services	DE.DP (dETECT - Data Protection)	DLP, outbound traffic inspection

Mapping these techniques to the NIST CSF highlights how common APT behaviors can be mitigated through strong access control, continuous monitoring, and supply-chain risk management. These controls directly address attacker reliance on legitimate credentials and trusted infrastructure rather than malware-heavy tradecraft.

4.3 ISO/IEC 27001 Mapping Table

Mapping Overlapping APT TTPs to ISO/IEC 27001 Control

ATTACK Technique	ISO/IEC 27001 Control	Control Objective
T1078 - Valid Accounts	Access Control	Prevent Unauthorised use of legitimate accounts
T1199 - Trusted Relationship	Supplier Relationship	Reduce third party access risk
T1133 - External Remote Services	Network Security	Secure Remote and external connections

T1102 - Web Services (C2)	Logging & Monitoring	Detect abnormal use of legitimate services
T1567.002 - Exfiltration to Cloud Storage	Information Protection	Prevent unauthorised data movement.

Aligning these TTPs to ISO/IEC 27001 control demonstrates how governance-driven security controls can reduce exposure to attacker techniques that exploit trust, credentials, and legitimate infrastructure.

Conclusion

This assessment demonstrated how industry-focused threat intelligence can be operationalised to support security decision-making within the UK insurance sector. By analysing APT groups with known relevance to financial services, mapping their behaviours to the MITRE ATT&CK framework, and identifying overlapping techniques, this project highlighted common attacker dependencies on legitimate credentials, trusted relationships, and cloud-based infrastructure.

The use of ATT&CK Navigator enabled visualisation of shared TTPs across Polonium, Cobalt Group and Windigo threat actors, revealing consistent choke points that attackers rely on for persistence, lateral movement, command and control, and data exfiltration. These findings reinforce the importance of behaviour-driven detection and continuous monitoring over signature-based approaches.

By aligning the identified techniques to NIST CSF and ISO/IEC 27001 control, the analysis demonstrated how threat intelligence can directly inform governance, detection, and risk mitigation strategies within a SOC environment. This approach supports the development of more resilient security controls, improved visibility, and informed policy decisions tailored to the insurance industry's threat landscape.

Future work could expand this analysis to include additional threat actors, deeper detection engineering use cases, and validation of controls through simulated attack scenarios.