Supporting
European
Aviation

EUROCONTROL

Data Driven APT Attribution and AI/ML Research

2022 TF-CSIRT & FIRST Virtual Symposium

Patrick MANA
EATM-CERT Manager – EUROCONTROL EATM-CERT

Bahtiar MUSTAFA
Cyber-security expert, CISSP – EUROCONTROL EATM-CERT

FOUNDING MEMBER OF sesar JOINT UNDERTAKING

NETWORK MANAGER

Why? How? What ?

- Objective: Improve attribution

- Why?
  - Aviation is a critical infrastructure – Subject to “strategic” threats (thus well identified APTs)
  - Cyber attacks on aviation are “popular” and attractive for the media
  - Very similar technologies used all over the world
  - Attribution is not an obsession … But we need to improve our prediction capability of future attacks

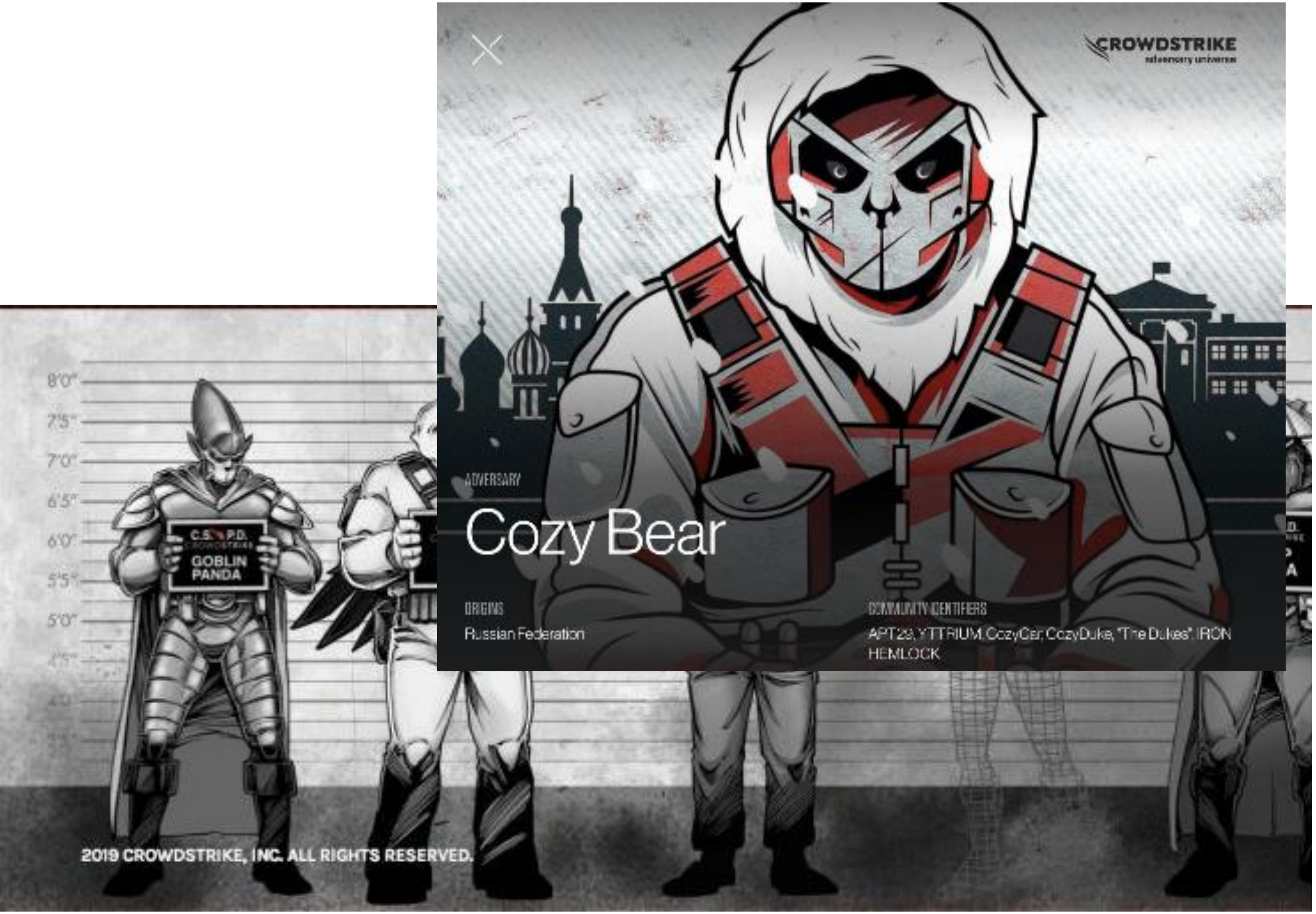
- How? Two-step approach
  - SW-based tool to identify potential APTs based on MITRE ATT&CK TTPs
  - AI/ML app to analyse the attack context in order to refine attribution

Summary

- Problem
  - Attribution

- Solution: 2-step approach
  - Step1: AFiT
  - Step2: AI/ML tool

APT Groups



ADVERSARY

Cozy Bear

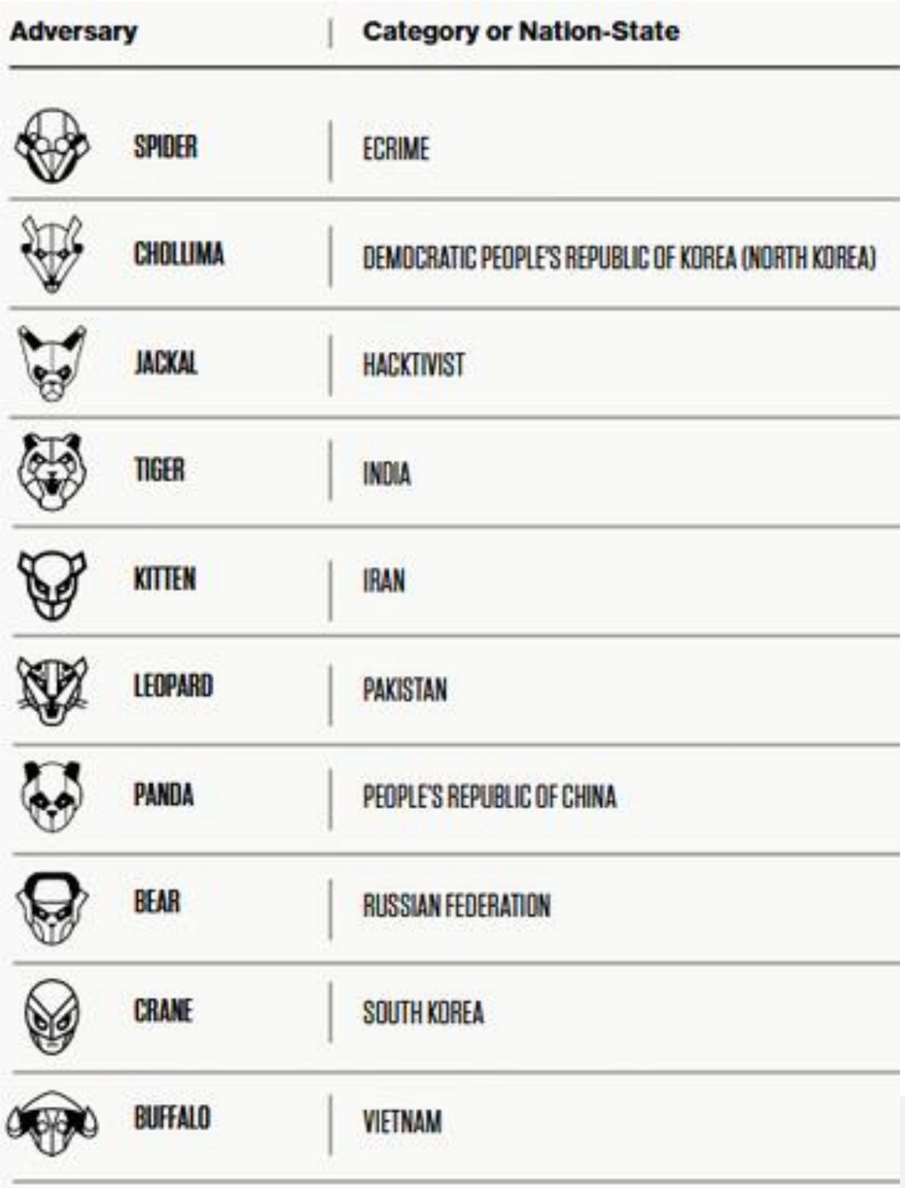
ORIGINS

Russian Federation

COMMUNITY IDENTIFIERS

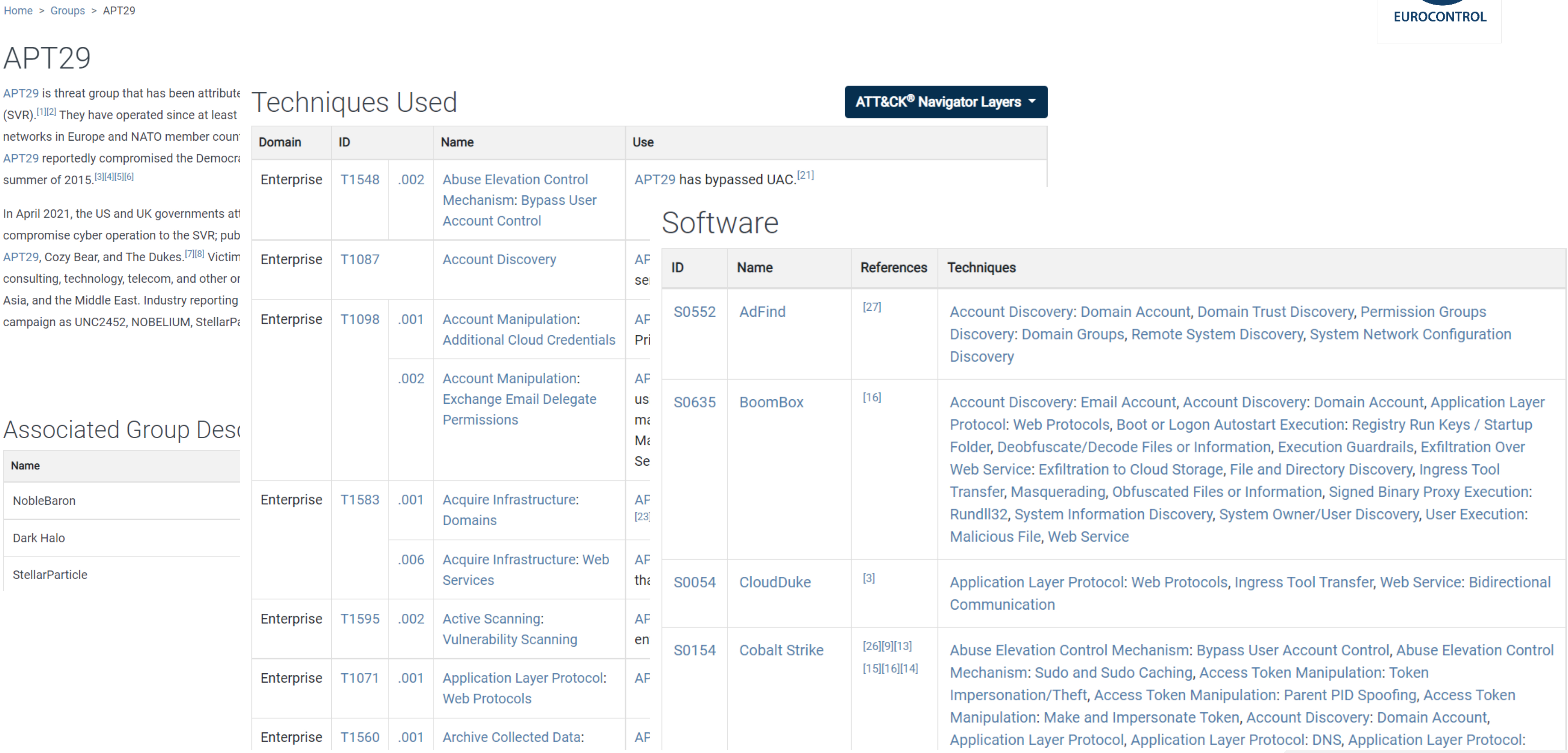
APT29, YTTRIUM, CozyCar, CozyDuke, "The Dukes", IRON HEMLOCK

2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.



Adversary	Category or Nation-State
SPIDER	ECRIME
CHOLLIMA	DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA (NORTH KOREA)
JACKAL	HACKTIVIST
TIGER	INDIA
KITTEN	IRAN
LEOPARD	PAKISTAN
PANDA	PEOPLE'S REPUBLIC OF CHINA
BEAR	RUSSIAN FEDERATION
CRANE	SOUTH KOREA
BUFFALO	VIETNAM

APT29



Home > Groups > APT29

APT29

APT29 is threat group that has been attribute
(SVR).[1][2] They have operated since at least
networks in Europe and NATO member coun
APT29 reportedly compromised the Democr
summer of 2015.[3][4][5][6]

In April 2021, the US and UK governments at
compromise cyber operation to the SVR; pub
APT29, Cozy Bear, and The Dukes.[7][8] Victim
consulting, technology, telecom, and other or
Asia, and the Middle East. Industry reporting
campaign as UNC2452, NOBELIUM, StellarP

Associated Group Desc

Name
NobleBaron
Dark Halo
StellarParticle

Techniques Used

ATT&CK® Navigator Layers

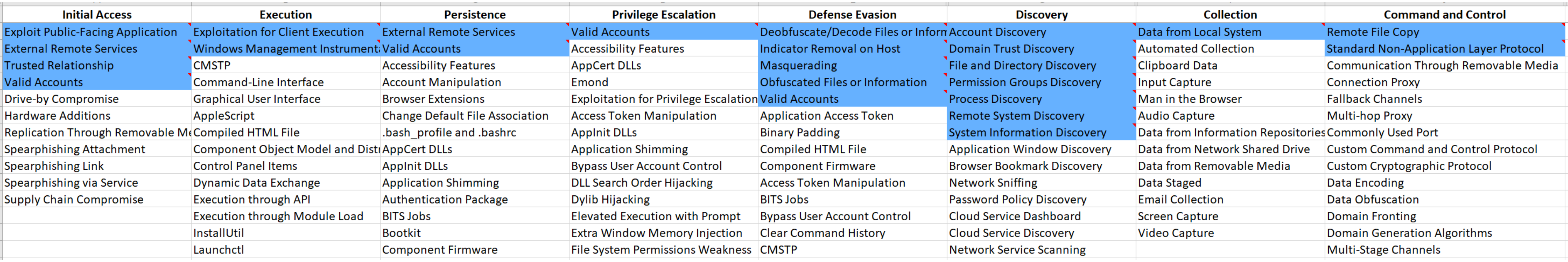
Domain	ID		Name	Use
Enterprise	T1548	.002	Abuse Elevation Control Mechanism: Bypass User Account Control	APT29 has bypassed UAC.[21]
Enterprise	T1087		Account Discovery	AP se
Enterprise	T1098	.001	Account Manipulation: Additional Cloud Credentials	AP Pri
		.002	Account Manipulation: Exchange Email Delegate Permissions	AP usi ma Ma Se
Enterprise	T1583	.001	Acquire Infrastructure: Domains	AP [23]
		.006	Acquire Infrastructure: Web Services	AP tha
Enterprise	T1595	.002	Active Scanning: Vulnerability Scanning	AP en
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	AP
Enterprise	T1560	.001	Archive Collected Data:	AP

Software

ID	Name	References	Techniques
S0552	AdFind	[27]	Account Discovery: Domain Account, Domain Trust Discovery, Permission Groups Discovery: Domain Groups, Remote System Discovery, System Network Configuration Discovery
S0635	BoomBox	[16]	Account Discovery: Email Account, Account Discovery: Domain Account, Application Layer Protocol: Web Protocols, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Deobfuscate/Decode Files or Information, Execution Guardrails, Exfiltration Over Web Service: Exfiltration to Cloud Storage, File and Directory Discovery, Ingress Tool Transfer, Masquerading, Obfuscated Files or Information, Signed Binary Proxy Execution: Rundll32, System Information Discovery, System Owner/User Discovery, User Execution: Malicious File, Web Service
S0054	CloudDuke	[3]	Application Layer Protocol: Web Protocols, Ingress Tool Transfer, Web Service: Bidirectional Communication
S0154	Cobalt Strike	[26][9][13] [15][16][14]	Abuse Elevation Control Mechanism: Bypass User Account Control, Abuse Elevation Control Mechanism: Sudo and Sudo Caching, Access Token Manipulation: Token Impersonation/Theft, Access Token Manipulation: Parent PID Spoofing, Access Token Manipulation: Make and Impersonate Token, Account Discovery: Domain Account, Application Layer Protocol, Application Layer Protocol: DNS, Application Layer Protocol:

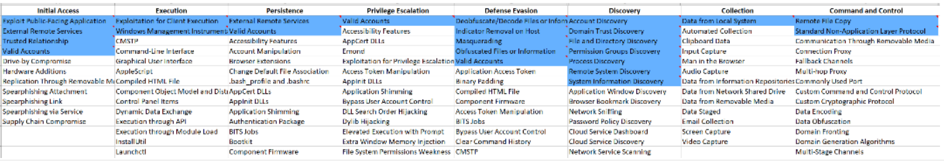
https://attack.mitre.org/groups/G0016/

MITRE ATT&CK mapping for APT29

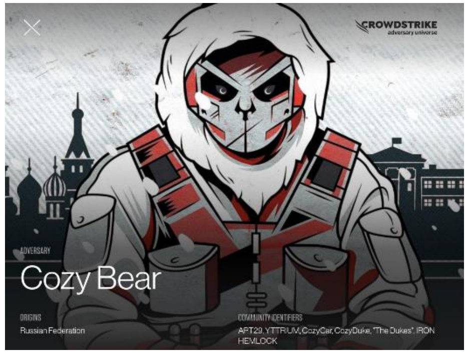


Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Collection	Command and Control
Exploit Public-Facing Application	Exploitation for Client Execution	External Remote Services	Valid Accounts	Deobfuscate/Decode Files or Inform	Account Discovery	Data from Local System	Remote File Copy
External Remote Services	Windows Management Instrumenta	Valid Accounts	Accessibility Features	Indicator Removal on Host	Domain Trust Discovery	Automated Collection	Standard Non-Application Layer Protocol
Trusted Relationship	CMSTP	Accessibility Features	AppCert DLLs	Masquerading	File and Directory Discovery	Clipboard Data	Communication Through Removable Media
Valid Accounts	Command-Line Interface	Account Manipulation	Emond	Obfuscated Files or Information	Permission Groups Discovery	Input Capture	Connection Proxy
Drive-by Compromise	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Valid Accounts	Process Discovery	Man in the Browser	Fallback Channels
Hardware Additions	AppleScript	Change Default File Association	Access Token Manipulation	Application Access Token	Remote System Discovery	Audio Capture	Multi-hop Proxy
Replication Through Removable Me	Compiled HTML File	.bash_profile and .bashrc	AppInit DLLs	Binary Padding	System Information Discovery	Data from Information Repositories	Commonly Used Port
Spearphishing Attachment	Component Object Model and Distr	AppCert DLLs	Application Shimming	Compiled HTML File	Application Window Discovery	Data from Network Shared Drive	Custom Command and Control Protocol
Spearphishing Link	Control Panel Items	AppInit DLLs	Bypass User Account Control	Component Firmware	Browser Bookmark Discovery	Data from Removable Media	Custom Cryptographic Protocol
Spearphishing via Service	Dynamic Data Exchange	Application Shimming	DLL Search Order Hijacking	Access Token Manipulation	Network Sniffing	Data Staged	Data Encoding
Supply Chain Compromise	Execution through API	Authentication Package	Dylib Hijacking	BITS Jobs	Password Policy Discovery	Email Collection	Data Obfuscation
	Execution through Module Load	BITS Jobs	Elevated Execution with Prompt	Bypass User Account Control	Cloud Service Dashboard	Screen Capture	Domain Fronting
	InstallUtil	Bootkit	Extra Window Memory Injection	Clear Command History	Cloud Service Discovery	Video Capture	Domain Generation Algorithms
	Launchctl	Component Firmware	File System Permissions Weakness	CMSTP	Network Service Scanning		Multi-Stage Channels

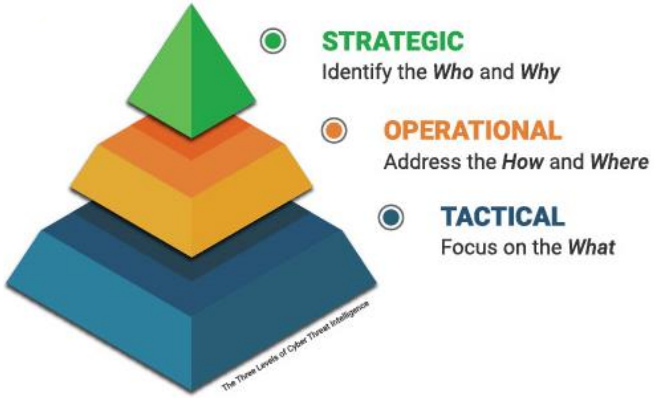
Problem : Attribution



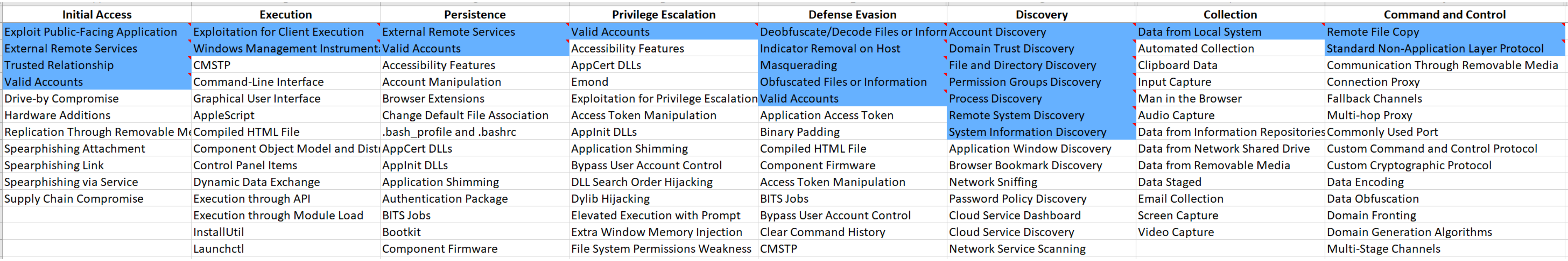
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Collection	Command and Control
Exploit Public-Facing Application	Exploitation for Client Execution	External Remote Services	Valid Accounts	Deobfuscate/Decode Files or Inform	Account Discovery	Data from Local System	Remote File Copy
External Remote Services	Windows Management Instrument	Valid Accounts	Accessibility Features	Indicator Removal on Host	Domain Trust Discovery	Automated Collection	Standard Non-Application Layer Protocol
Trusted Relationship	CMSTP	Accessibility Features	AppCert DLLs	Masquerading	File and Directory Discovery	Clipboard Data	Communication Through Removable Media
Valid Accounts	Command-Line Interface	Account Manipulation	Emond	Obfuscated Files or Information	Permission Groups Discovery	Input Capture	Connection Proxy
Drive-by Compromise	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Valid Accounts	Process Discovery	Man in the Browser	Fallback Channels
Hardware Additions	AppleScript	Change Default File Association	Access Token Manipulation	Application Access Token	Remote System Discovery	Audio Capture	Multi-hop Proxy
Replication Through Removable M	Compiled HTML File	.bash_profile and .bashrc	AppInit DLLs	Binary Padding	System Information Discovery	Data from Information Repositories	Commonly Used Port
Spearphishing Attachment	Component Object Model and Dist	AppCert DLLs	Application Shimming	Compiled HTML File	Application Window Discovery	Data from Network Shared Drive	Custom Command and Control Protocol
Spearphishing Link	Control Panel Items	AppInit DLLs	Bypass User Account Control	Component Firmware	Browser Bookmark Discovery	Data from Removable Media	Custom Cryptographic Protocol
Spearphishing via Service	Dynamic Data Exchange	Application Shimming	DLL Search Order Hijacking	Access Token Manipulation	Network Sniffing	Data Staged	Data Encoding
Supply Chain Compromise	Execution through API	Authentication Package	Dylib Hijacking	BITS Jobs	Password Policy Discovery	Email Collection	Data Obfuscation
	Execution through Module Load	BITS Jobs	Elevated Execution with Prompt	Bypass User Account Control	Cloud Service Dashboard	Screen Capture	Domain Fronting
	InstallUtil	Bootkit	Extra Window Memory Injection	Clear Command History	Cloud Service Discovery	Video Capture	Domain Generation Algorithms
	Launchctl	Component Firmware	File System Permissions Weakness	CMSTP	Network Service Scanning		Multi-Stage Channels



APT29

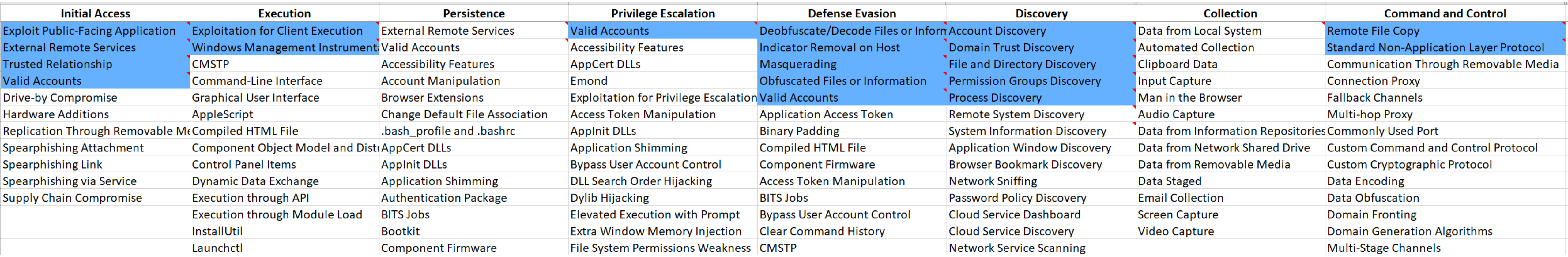

STRATEGIC
Identify the *Who* and *Why*
OPERATIONAL
Address the *How* and *Where*
TACTICAL
Focus on the *What*
The Three Levels of Cyber Threat Intelligence

Which APT Group is this ?



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Collection	Command and Control
Exploit Public-Facing Application	Exploitation for Client Execution	External Remote Services	Valid Accounts	Deobfuscate/Decode Files or Inform	Account Discovery	Data from Local System	Remote File Copy
External Remote Services	Windows Management Instrumenta	Valid Accounts	Accessibility Features	Indicator Removal on Host	Domain Trust Discovery	Automated Collection	Standard Non-Application Layer Protocol
Trusted Relationship	CMSTP	Accessibility Features	AppCert DLLs	Masquerading	File and Directory Discovery	Clipboard Data	Communication Through Removable Media
Valid Accounts	Command-Line Interface	Account Manipulation	Emond	Obfuscated Files or Information	Permission Groups Discovery	Input Capture	Connection Proxy
Drive-by Compromise	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Valid Accounts	Process Discovery	Man in the Browser	Fallback Channels
Hardware Additions	AppleScript	Change Default File Association	Access Token Manipulation	Application Access Token	Remote System Discovery	Audio Capture	Multi-hop Proxy
Replication Through Removable Me	Compiled HTML File	.bash_profile and .bashrc	AppInit DLLs	Binary Padding	System Information Discovery	Data from Information Repositories	Commonly Used Port
Spearphishing Attachment	Component Object Model and Distr	AppCert DLLs	Application Shimming	Compiled HTML File	Application Window Discovery	Data from Network Shared Drive	Custom Command and Control Protocol
Spearphishing Link	Control Panel Items	AppInit DLLs	Bypass User Account Control	Component Firmware	Browser Bookmark Discovery	Data from Removable Media	Custom Cryptographic Protocol
Spearphishing via Service	Dynamic Data Exchange	Application Shimming	DLL Search Order Hijacking	Access Token Manipulation	Network Sniffing	Data Staged	Data Encoding
Supply Chain Compromise	Execution through API	Authentication Package	Dylib Hijacking	BITS Jobs	Password Policy Discovery	Email Collection	Data Obfuscation
	Execution through Module Load	BITS Jobs	Elevated Execution with Prompt	Bypass User Account Control	Cloud Service Dashboard	Screen Capture	Domain Fronting
	InstallUtil	Bootkit	Extra Window Memory Injection	Clear Command History	Cloud Service Discovery	Video Capture	Domain Generation Algorithms
	Launchctl	Component Firmware	File System Permissions Weakness	CMSTP	Network Service Scanning		Multi-Stage Channels

What if some information is missing?



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Collection	Command and Control
Exploit Public-Facing Application	Exploitation for Client Execution	External Remote Services	Valid Accounts	Deobfuscate/Decode Files or Inforn	Account Discovery	Data from Local System	Remote File Copy
External Remote Services	Windows Management Instrument	Valid Accounts	Accessibility Features	Indicator Removal on Host	Domain Trust Discovery	Automated Collection	Standard Non-Application Layer Protocol
Trusted Relationship	CMSTP	Accessibility Features	AppCert DLLs	Masquerading	File and Directory Discovery	Clipboard Data	Communication Through Removable Media
Valid Accounts	Command-Line Interface	Account Manipulation	Emond	Obfuscated Files or Information	Permission Groups Discovery	Input Capture	Connection Proxy
Drive-by Compromise	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Valid Accounts	Process Discovery	Man in the Browser	Fallback Channels
Hardware Additions	AppleScript	Change Default File Association	Access Token Manipulation	Application Access Token	Remote System Discovery	Audio Capture	Multi-hop Proxy
Replication Through Removable Me	Compiled HTML File	.bash_profile and .bashrc	AppInit DLLs	Binary Padding	System Information Discovery	Data from Information Repositories	Commonly Used Port
Spearphishing Attachment	Component Object Model and Distr	AppCert DLLs	Application Shimming	Compiled HTML File	Application Window Discovery	Data from Network Shared Drive	Custom Command and Control Protocol
Spearphishing Link	Control Panel Items	AppInit DLLs	Bypass User Account Control	Component Firmware	Browser Bookmark Discovery	Data from Removable Media	Custom Cryptographic Protocol
Spearphishing via Service	Dynamic Data Exchange	Application Shimming	DLL Search Order Hijacking	Access Token Manipulation	Network Sniffing	Data Staged	Data Encoding
Supply Chain Compromise	Execution through API	Authentication Package	Dylib Hijacking	BITS Jobs	Password Policy Discovery	Email Collection	Data Obfuscation
	Execution through Module Load	BITS Jobs	Elevated Execution with Prompt	Bypass User Account Control	Cloud Service Dashboard	Screen Capture	Domain Fronting
	InstallUtil	Bootkit	Extra Window Memory Injection	Clear Command History	Cloud Service Discovery	Video Capture	Domain Generation Algorithms
	Launchctl	Component Firmware	File System Permissions Weakness	CMSTP	Network Service Scanning		Multi-Stage Channels

Solution

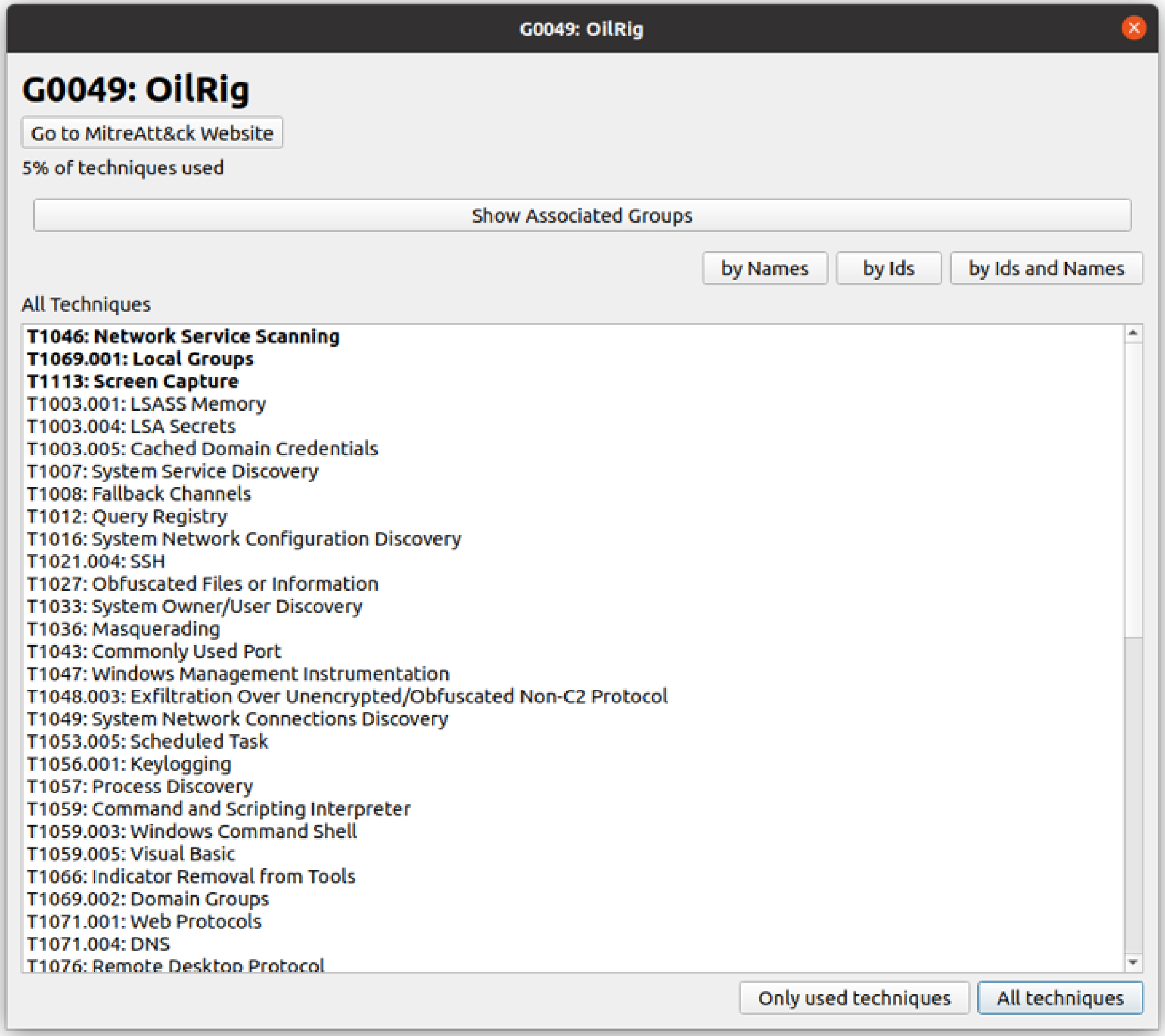
- Data driven APT attribution
- Based on observed TTPs
- 2 step approach:
  - Step 1: AFiT tool
  - Step 2: AI/ML tool for data (TTP) extraction from free text

1st step: Adversary Finder tool

1st step: SW based tool – Adversary Finder Tool (AFiT)

- Free tool developed by EATM-CERT
- APT database from MITRE ATT&CK
- Used to show how MITRE ATT&CK can be used
- Support the promotion and use of MITRE ATT&CK in aviation
- Use TTPs to predict APT group
- Support prediction based on TTP similarity

Adversary Finder Tool (AFiT)

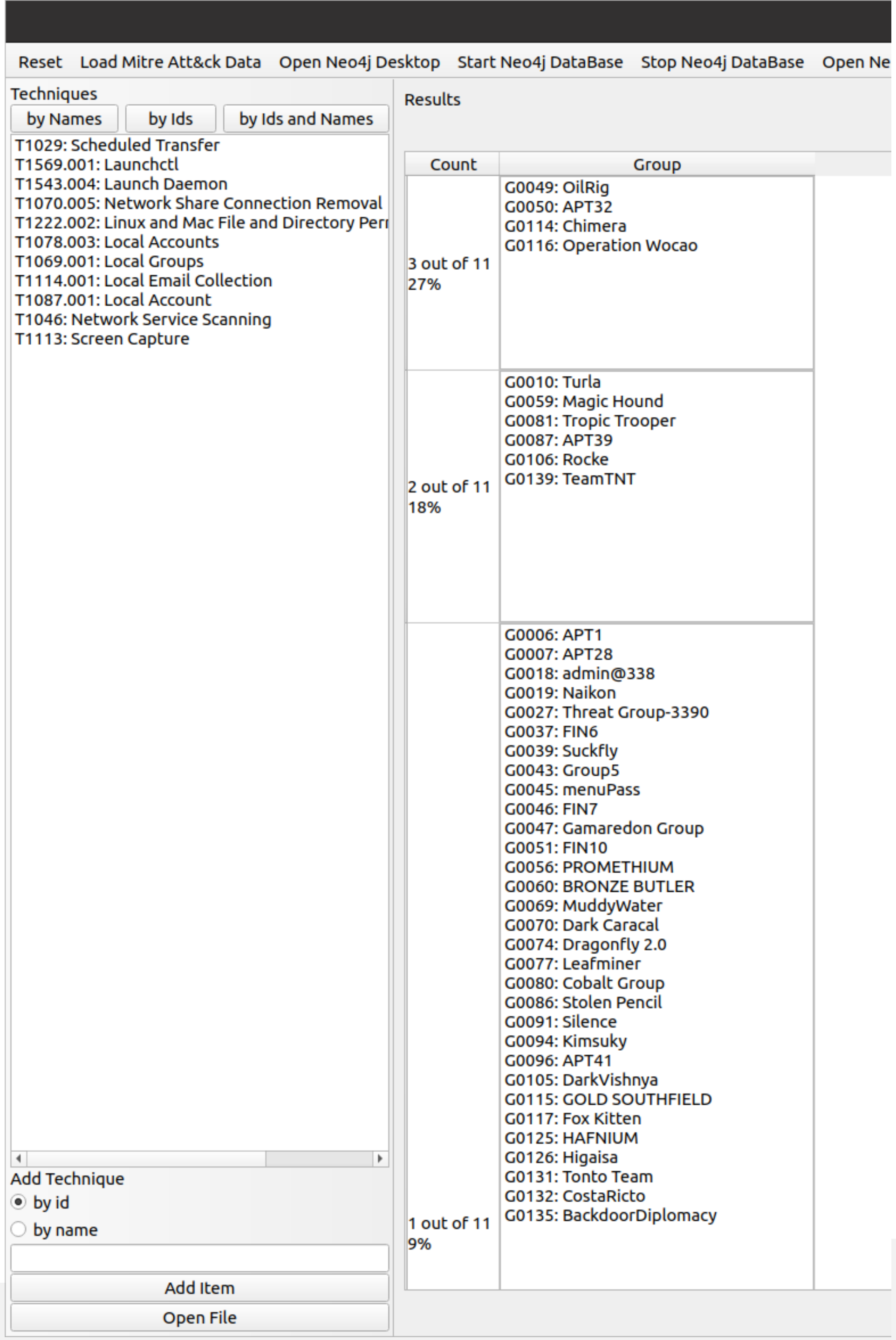


G0049: OilRig

5% of techniques used

All Techniques

T1046: Network Service Scanning
T1069.001: Local Groups
T1113: Screen Capture
T1003.001: LSASS Memory
T1003.004: LSA Secrets
T1003.005: Cached Domain Credentials
T1007: System Service Discovery
T1008: Fallback Channels
T1012: Query Registry
T1016: System Network Configuration Discovery
T1021.004: SSH
T1027: Obfuscated Files or Information
T1033: System Owner/User Discovery
T1036: Masquerading
T1043: Commonly Used Port
T1047: Windows Management Instrumentation
T1048.003: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol
T1049: System Network Connections Discovery
T1053.005: Scheduled Task
T1056.001: Keylogging
T1057: Process Discovery
T1059: Command and Scripting Interpreter
T1059.003: Windows Command Shell
T1059.005: Visual Basic
T1066: Indicator Removal from Tools
T1069.002: Domain Groups
T1071.001: Web Protocols
T1071.004: DNS
T1076: Remote Desktop Protocol



Techniques

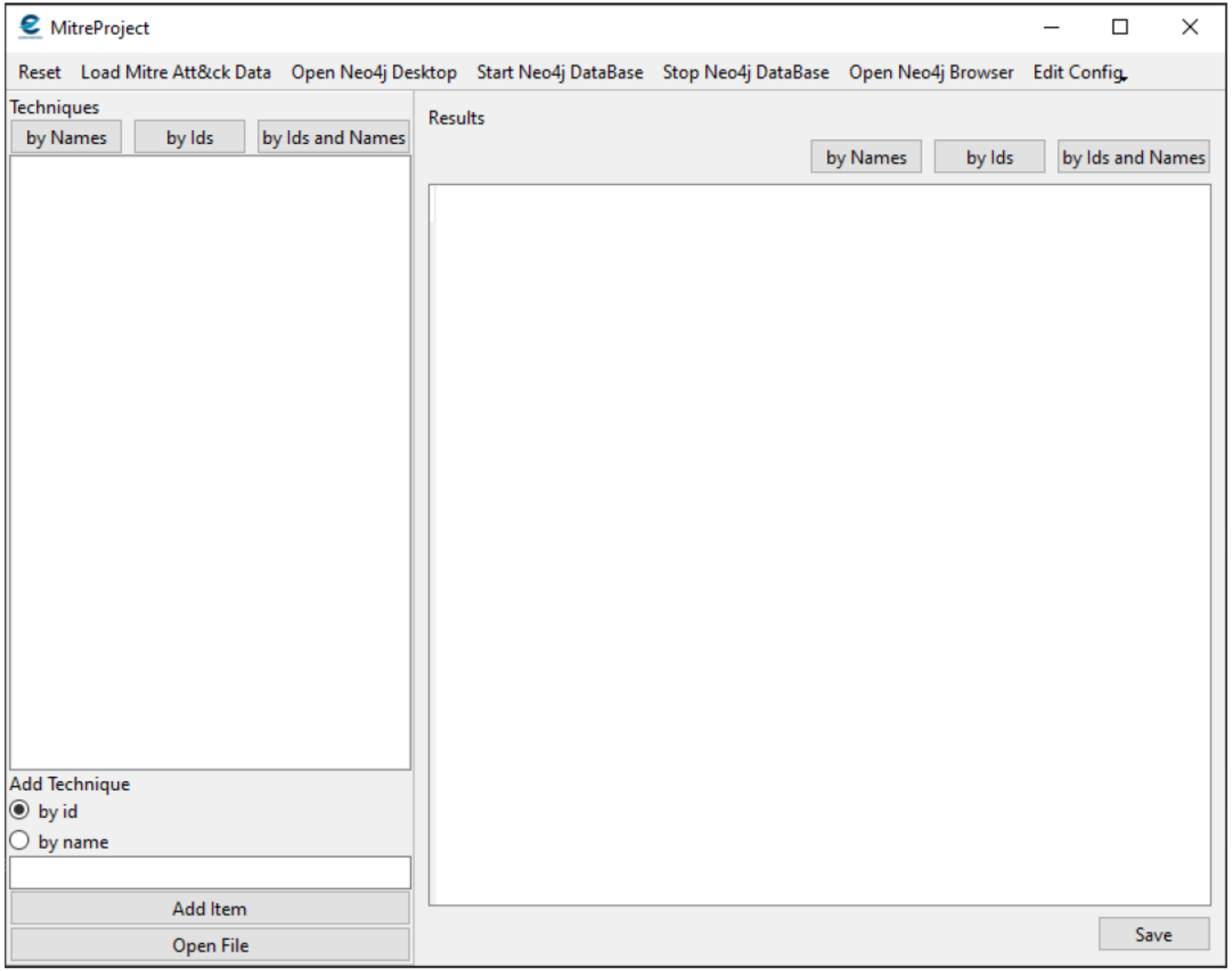
T1029: Scheduled Transfer
T1569.001: Launchctl
T1543.004: Launch Daemon
T1070.005: Network Share Connection Removal
T1222.002: Linux and Mac File and Directory Perr
T1078.003: Local Accounts
T1069.001: Local Groups
T1114.001: Local Email Collection
T1087.001: Local Account
T1046: Network Service Scanning
T1113: Screen Capture

Add Technique
● by id
○ by name

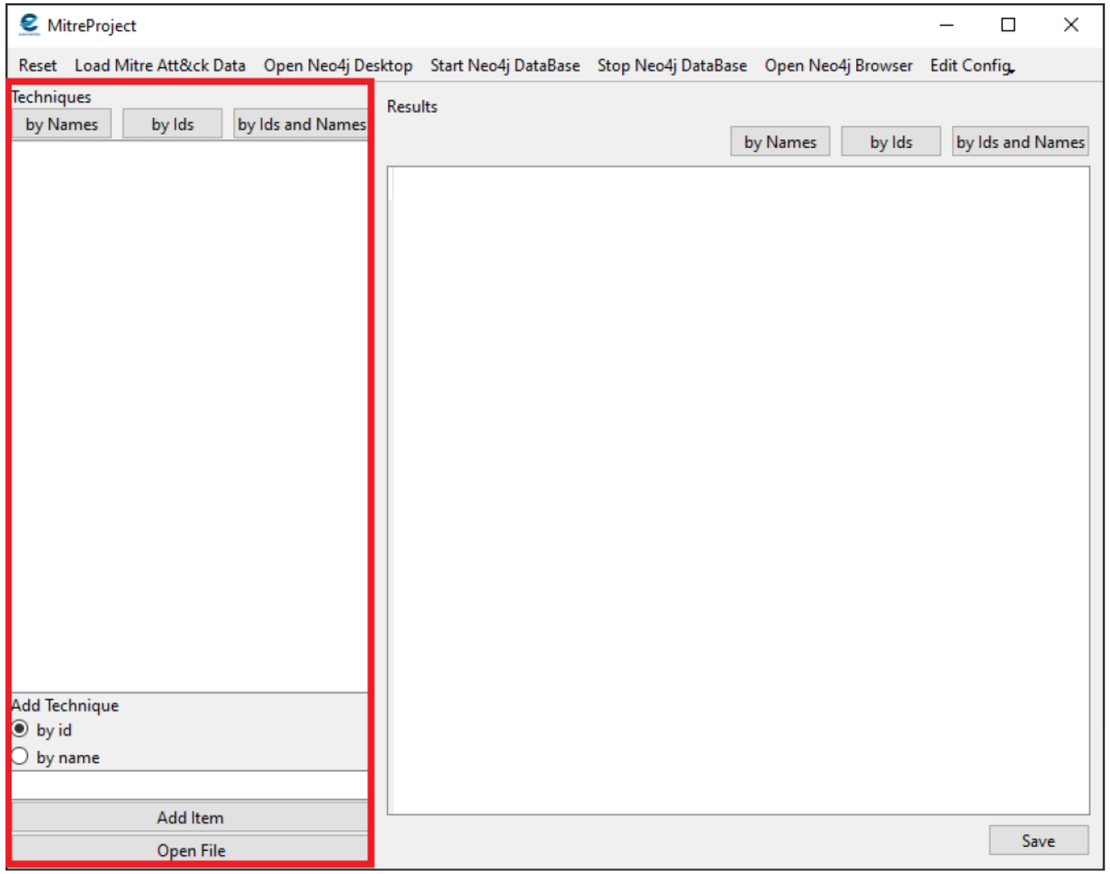
Results

Count	Group
3 out of 11 27%	G0049: OilRig G0050: APT32 G0114: Chimera G0116: Operation Wocao
2 out of 11 18%	G0010: Turla G0059: Magic Hound G0081: Tropic Trooper G0087: APT39 G0106: Rocke G0139: TeamTNT
1 out of 11 9%	G0006: APT1 G0007: APT28 G0018: admin@338 G0019: Naikon G0027: Threat Group-3390 G0037: FIN6 G0039: Suckfly G0043: Group5 G0045: menuPass G0046: FIN7 G0047: Gamaredon Group G0051: FIN10 G0056: PROMETHIUM G0060: BRONZE BUTLER G0069: MuddyWater G0070: Dark Caracal G0074: Dragonfly 2.0 G0077: Leafminer G0080: Cobalt Group G0086: Stolen Pencil G0091: Silence G0094: Kimsuky G0096: APT41 G0105: DarkVishnya G0115: GOLD SOUTHFIELD G0117: Fox Kitten G0125: HAFNIUM G0126: Higaisa G0131: Tonto Team G0132: CostaRicto G0135: BackdoorDiplomacy

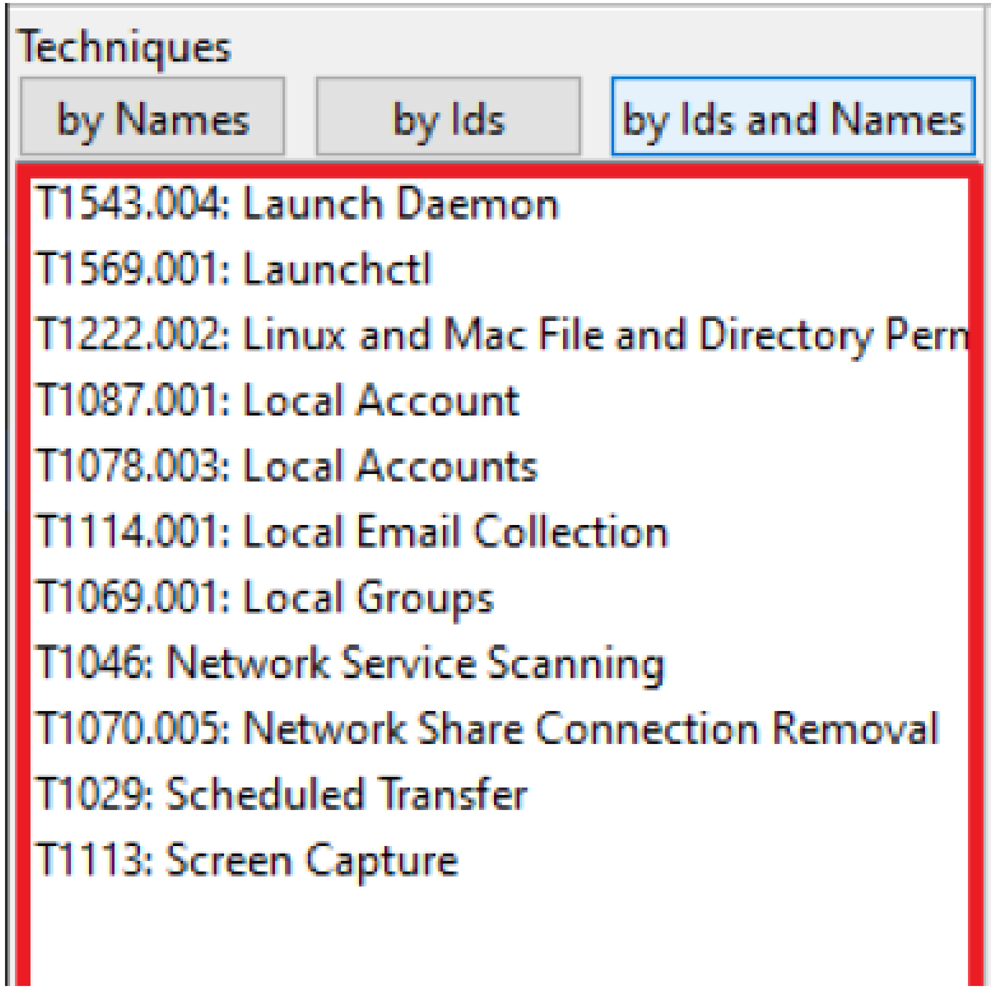
Adversary Finder Tool (AFiT)



Adversary Finder Tool (AFiT)

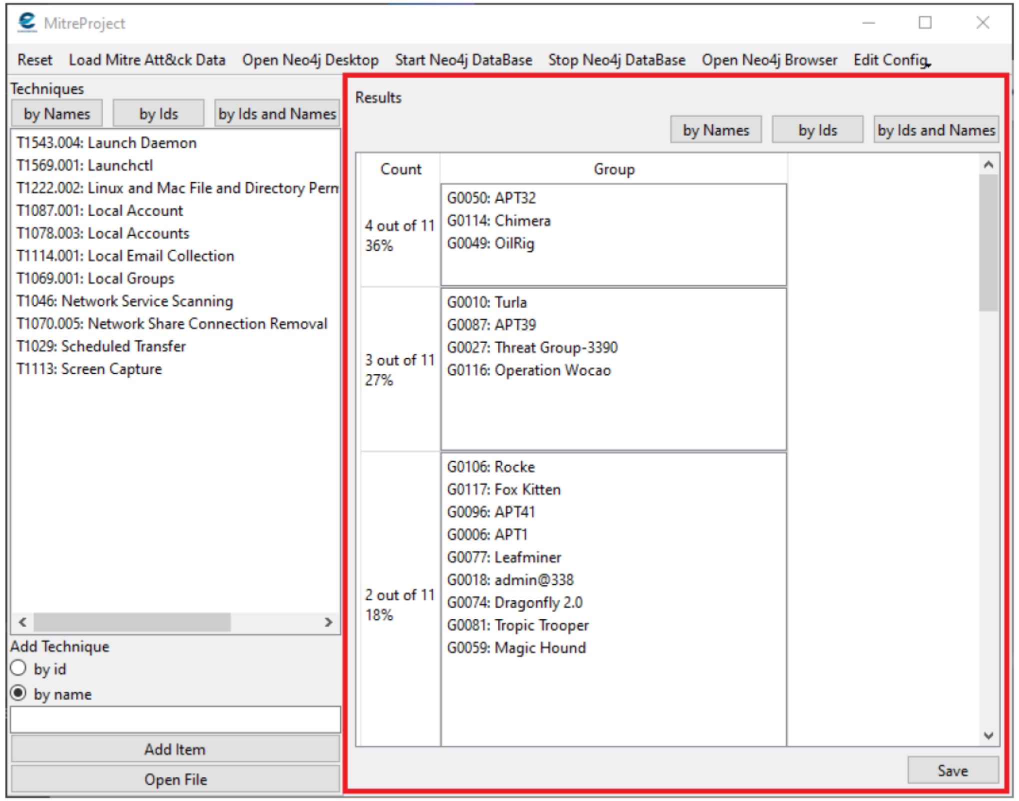


● by id
○ by name



T1543.004: Launch Daemon
T1569.001: Launchctl
T1222.002: Linux and Mac File and Directory Pern
T1087.001: Local Account
T1078.003: Local Accounts
T1114.001: Local Email Collection
T1069.001: Local Groups
T1046: Network Service Scanning
T1070.005: Network Share Connection Removal
T1029: Scheduled Transfer
T1113: Screen Capture

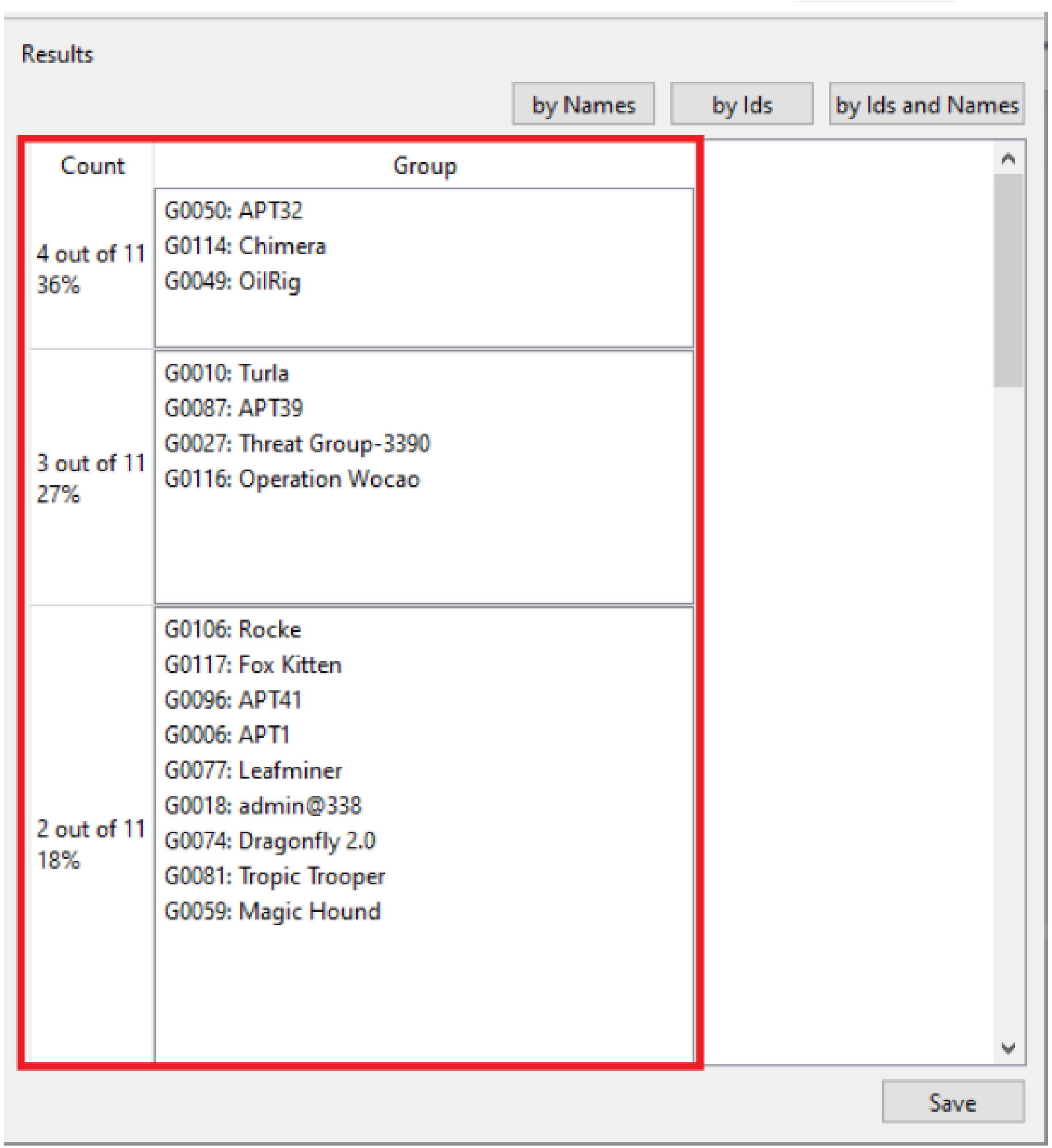
Adversary Finder Tool (AFiT)



T1543.004: Launch Daemon
T1569.001: Launchctl
T1222.002: Linux and Mac File and Directory Perm
T1087.001: Local Account
T1078.003: Local Accounts
T1114.001: Local Email Collection
T1069.001: Local Groups
T1046: Network Service Scanning
T1070.005: Network Share Connection Removal
T1029: Scheduled Transfer
T1113: Screen Capture

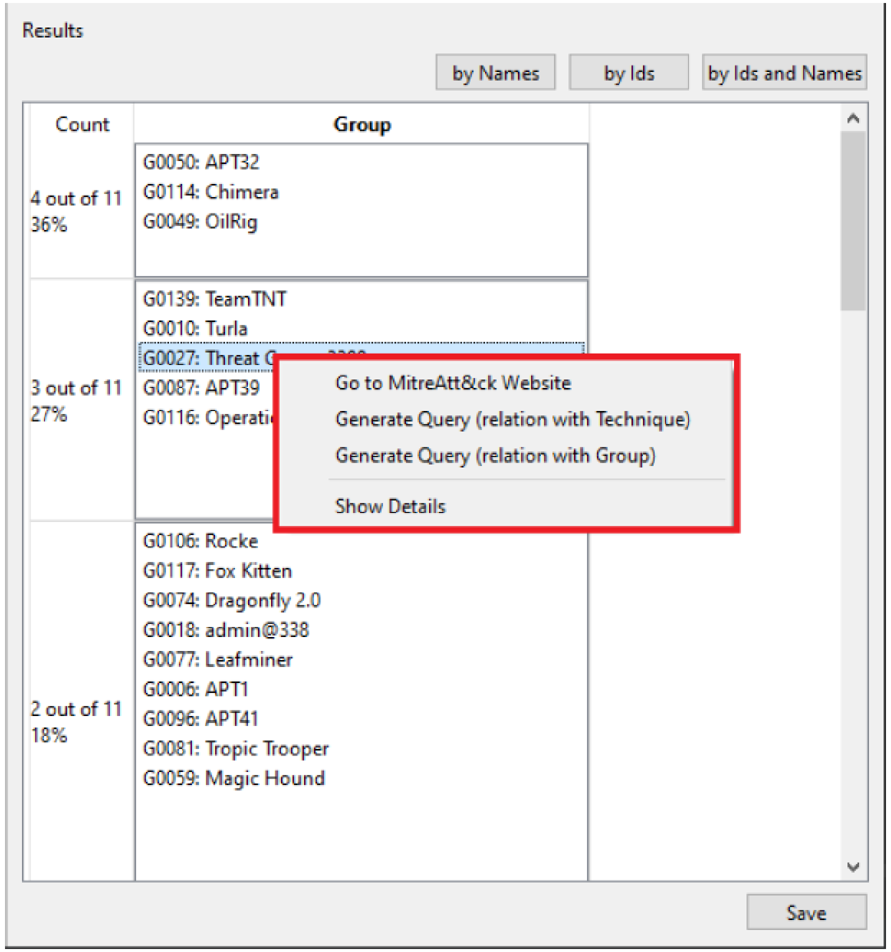
○ by id
● by name

Count	Group
4 out of 11 36%	G0050: APT32 G0114: Chimera G0049: OilRig
3 out of 11 27%	G0010: Turla G0087: APT39 G0027: Threat Group-3390 G0116: Operation Wocao
2 out of 11 18%	G0106: Rocke G0117: Fox Kitten G0096: APT41 G0006: APT1 G0077: Leafminer G0018: admin@338 G0074: Dragonfly 2.0 G0081: Tropic Trooper G0059: Magic Hound

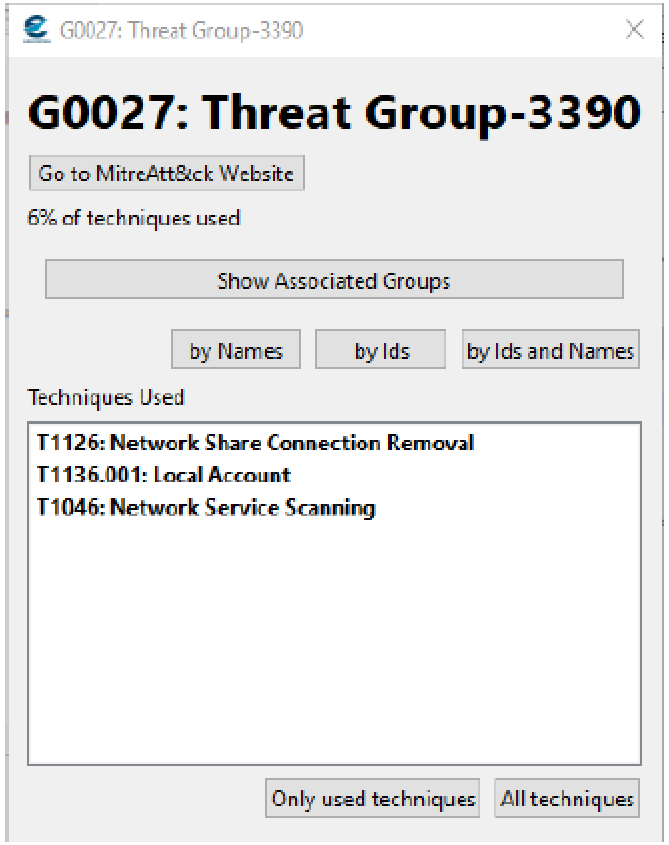


Count	Group
4 out of 11 36%	G0050: APT32 G0114: Chimera G0049: OilRig
3 out of 11 27%	G0010: Turla G0087: APT39 G0027: Threat Group-3390 G0116: Operation Wocao
2 out of 11 18%	G0106: Rocke G0117: Fox Kitten G0096: APT41 G0006: APT1 G0077: Leafminer G0018: admin@338 G0074: Dragonfly 2.0 G0081: Tropic Trooper G0059: Magic Hound

Adversary Finder Tool (AFiT)


Results
by Names
by Ids
by Ids and Names
Go to MitreAtt&ck Website
Generate Query (relation with Technique)
Generate Query (relation with Group)
Show Details
Save

Count	Group
4 out of 11 36%	G0050: APT32 G0114: Chimera G0049: OilRig
3 out of 11 27%	G0139: TeamTNT G0010: Turla G0027: Threat G G0087: APT39 G0116: Operati
2 out of 11 18%	G0106: Rocke G0117: Fox Kitten G0074: Dragonfly 2.0 G0018: admin@338 G0077: Leafminer G0006: APT1 G0096: APT41 G0081: Tropic Trooper G0059: Magic Hound



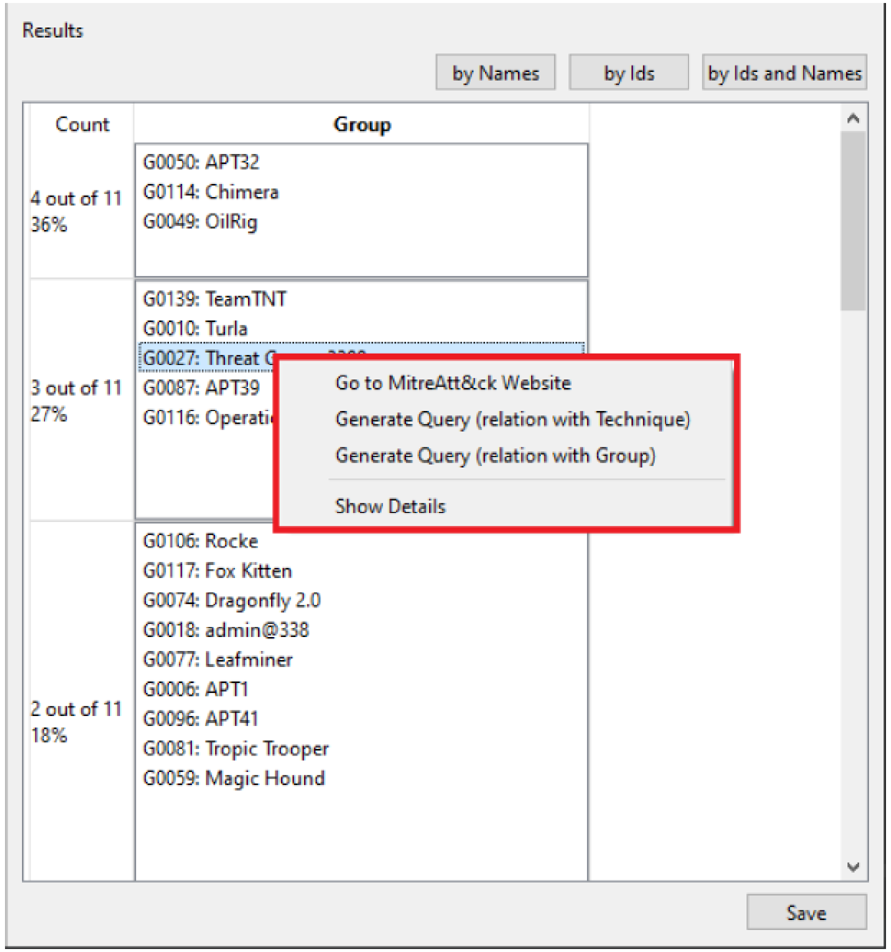
G0027: Threat Group-3390

6% of techniques used

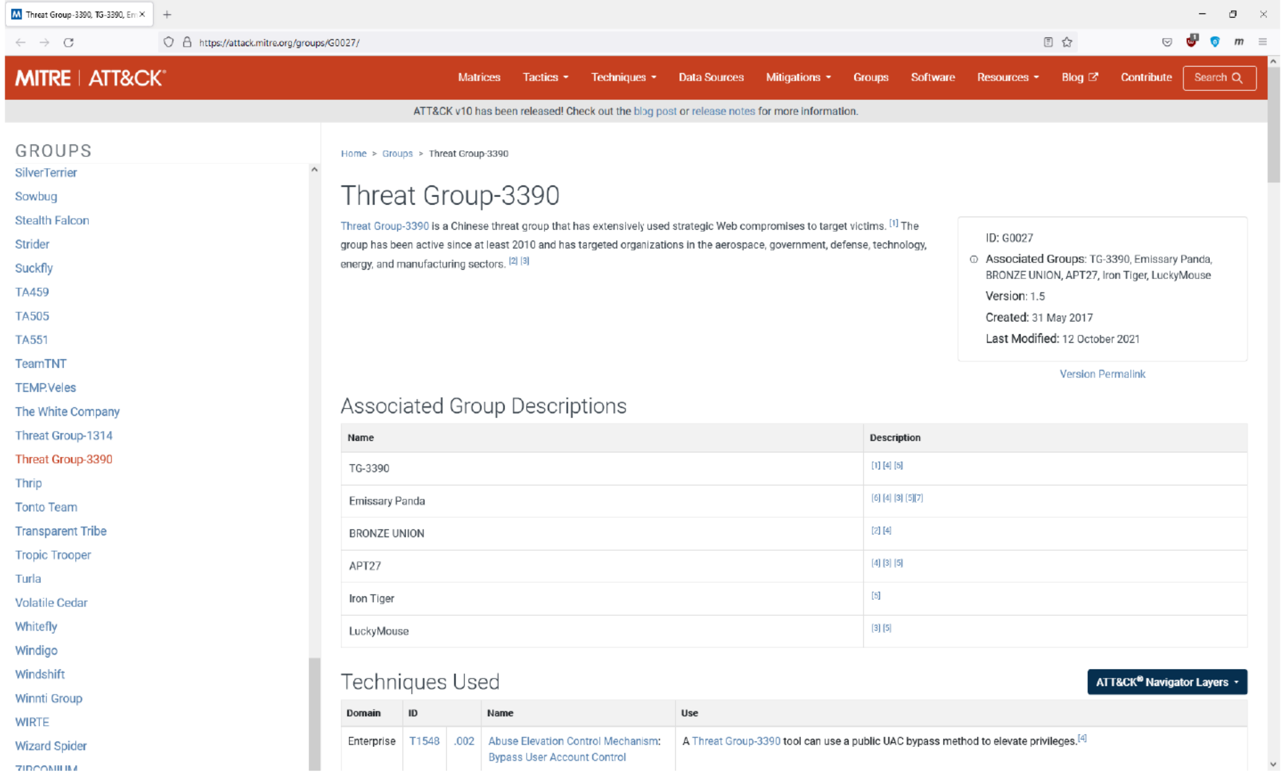
Techniques Used

T1126: Network Share Connection Removal
T1136.001: Local Account
T1046: Network Service Scanning

Adversary Finder Tool (AFiT)


Results
by Names
by Ids
by Ids and Names
Go to MitreAtt&ck Website
Generate Query (relation with Technique)
Generate Query (relation with Group)
Show Details
Save

Count	Group
4 out of 11 36%	G0050: APT32 G0114: Chimera G0049: OilRig
3 out of 11 27%	G0139: TeamTNT G0010: Turla G0027: Threat G G0087: APT39 G0116: Operati
2 out of 11 18%	G0106: Rocke G0117: Fox Kitten G0074: Dragonfly 2.0 G0018: admin@338 G0077: Leafminer G0006: APT1 G0096: APT41 G0081: Tropic Trooper G0059: Magic Hound



ATT&CK v10 has been released! Check out the blog post or release notes for more information.

GROUPS

SilverTerrier
Sowbug
Stealth Falcon
Strider
Suckfly
TA459
TA505
TA551
TeamTNT
TEMP.Veles
The White Company
Threat Group-1314
Threat Group-3390
Thrip
Tonto Team
Transparent Tribe
Tropic Trooper
Turla
Volatile Cedar
Whitefly
Windigo
Windshift
Winnti Group
WIRTE
Wizard Spider
ZIRCONIUM

Home > Groups > Threat Group-3390

Threat Group-3390

Threat Group-3390 is a Chinese threat group that has extensively used strategic Web compromises to target victims. [1] The group has been active since at least 2010 and has targeted organizations in the aerospace, government, defense, technology, energy, and manufacturing sectors. [2] [3]

ID: G0027
Associated Groups: TG-3390, Emissary Panda, BRONZE UNION, APT27, Iron Tiger, LuckyMouse
Version: 1.5
Created: 31 May 2017
Last Modified: 12 October 2021

Version Permalink

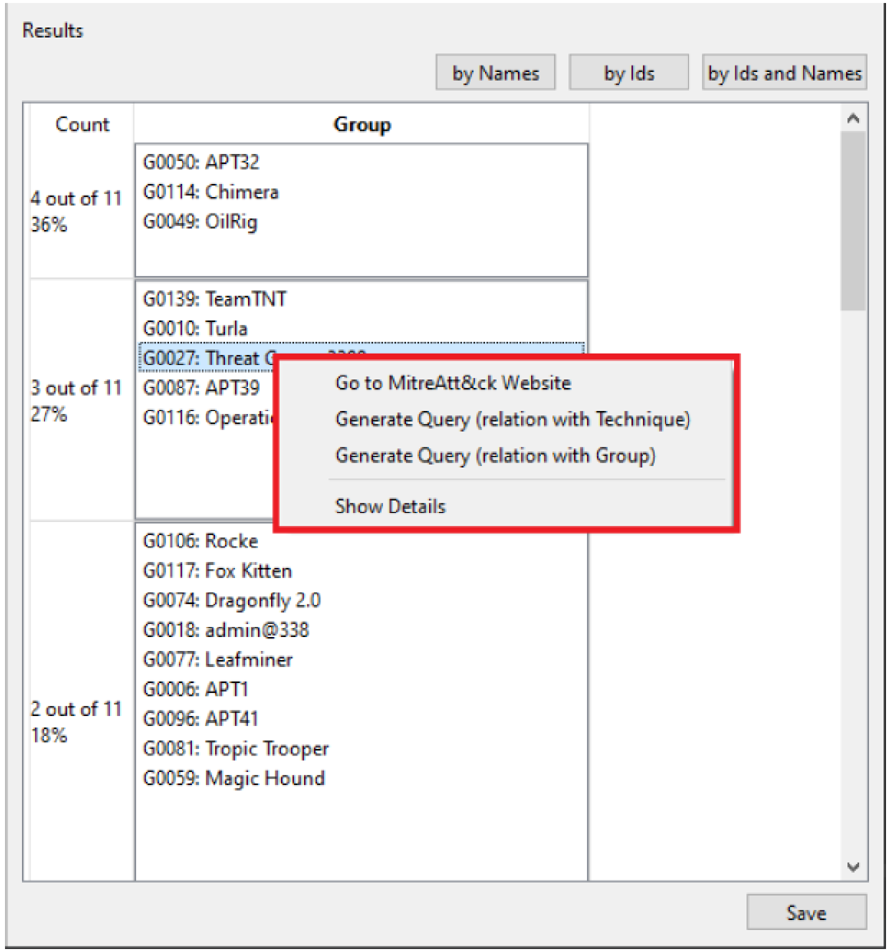
Associated Group Descriptions

Name	Description
TG-3390	[1] [4] [5]
Emissary Panda	[6] [4] [3] [5][7]
BRONZE UNION	[2] [4]
APT27	[4] [3] [5]
Iron Tiger	[5]
LuckyMouse	[3] [5]

Techniques Used

Domain	ID		Name	Use
Enterprise	T1548	.002	Abuse Elevation Control Mechanism: Bypass User Account Control	A Threat Group-3390 tool can use a public UAC bypass method to elevate privileges.[4]

Adversary Finder Tool (AFiT)

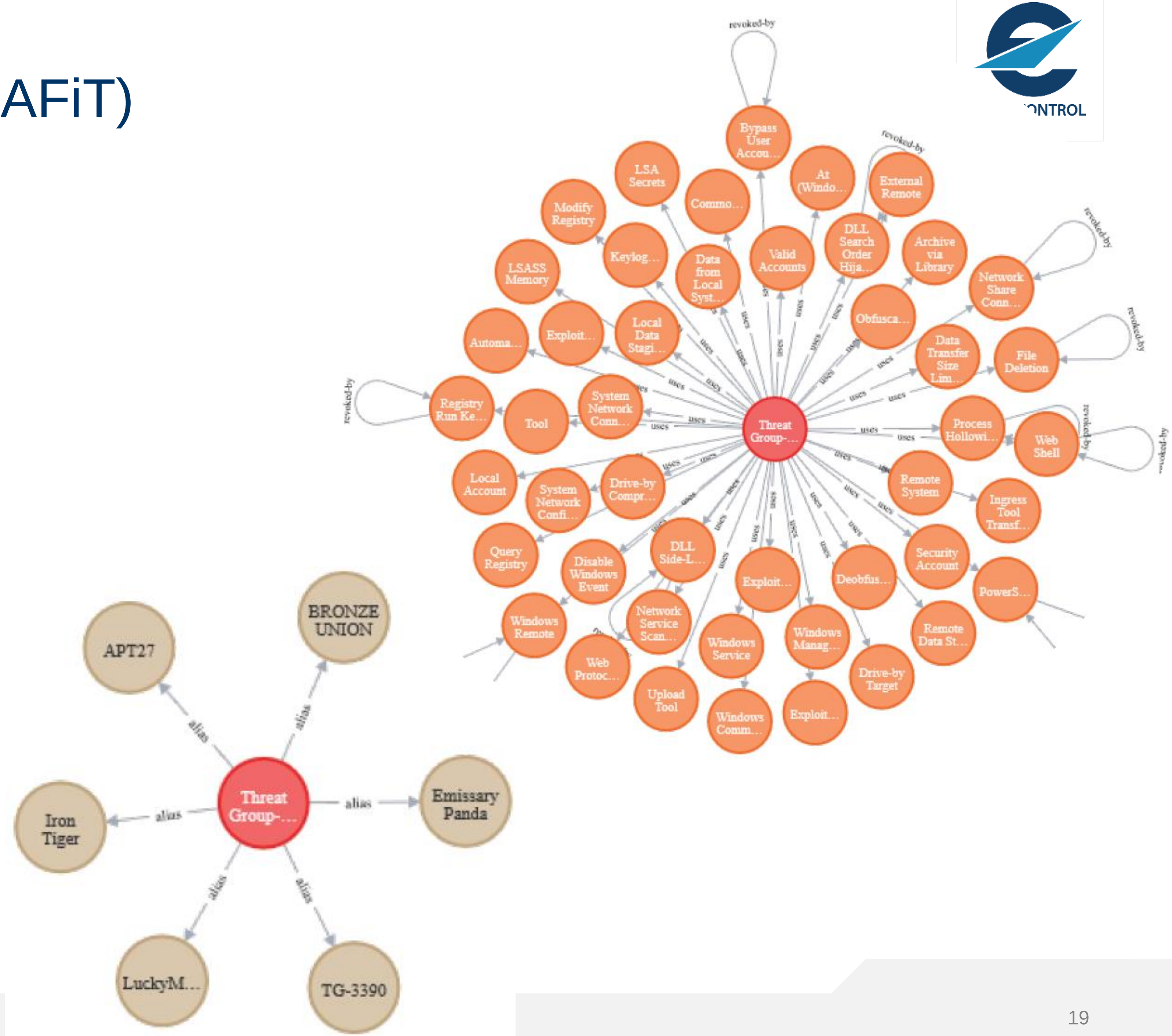


Results

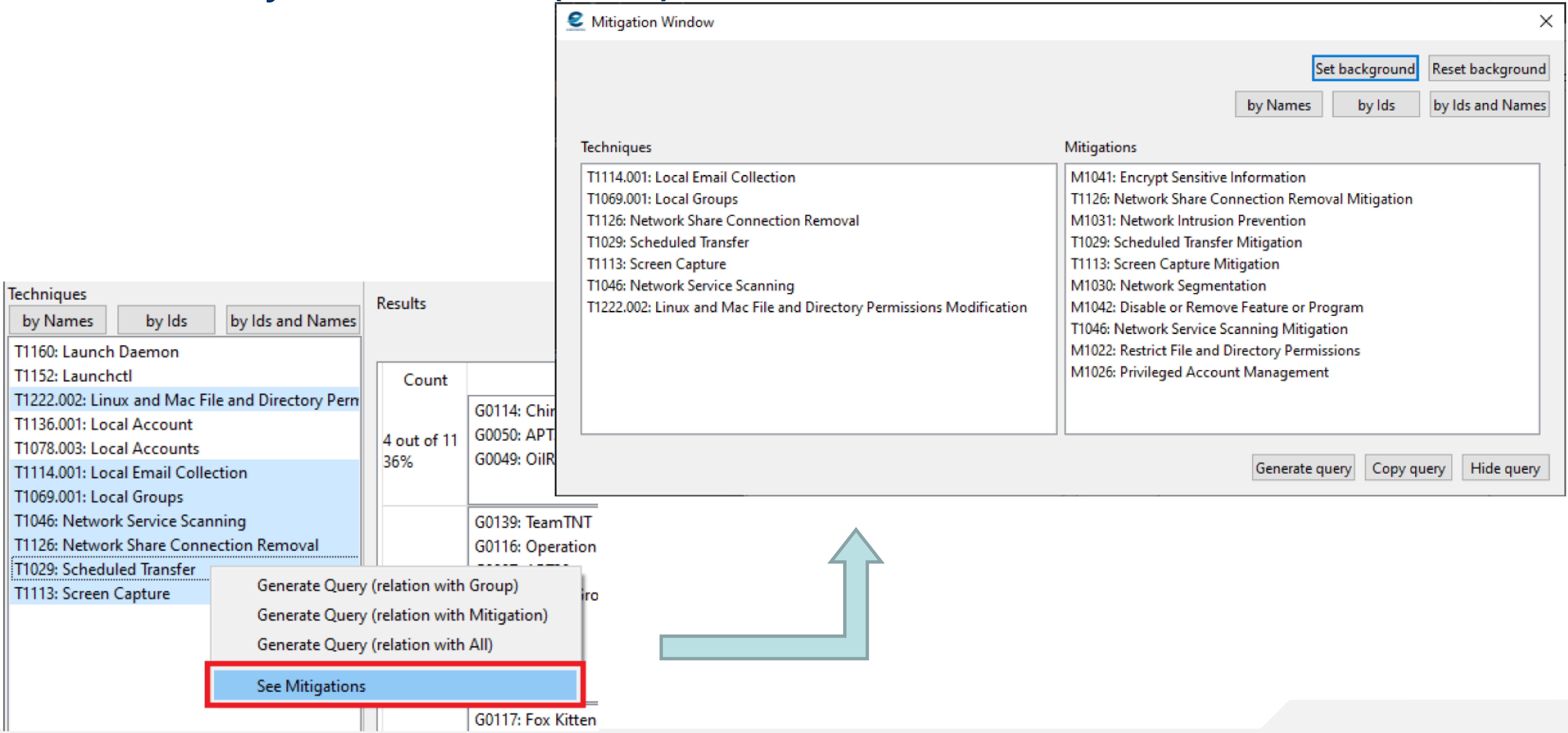
by Names | by Ids | by Ids and Names

Count	Group
4 out of 11 36%	G0050: APT32 G0114: Chimera G0049: OilRig
3 out of 11 27%	G0139: TeamTNT G0010: Turla G0027: Threat G... 3390 G0087: APT39 G0116: Operati
2 out of 11 18%	G0106: Rocke G0117: Fox Kitten G0074: Dragonfly 2.0 G0018: admin@338 G0077: Leafminer G0006: APT1 G0096: APT41 G0081: Tropic Trooper G0059: Magic Hound

Go to MitreAtt&ck Website
Generate Query (relation with Technique)
Generate Query (relation with Group)
Show Details
Save



Adversary Finder Tool (AFiT)



Techniques

- T1114.001: Local Email Collection
- T1069.001: Local Groups
- T1126: Network Share Connection Removal
- T1029: Scheduled Transfer
- T1113: Screen Capture
- T1046: Network Service Scanning
- T1222.002: Linux and Mac File and Directory Permissions Modification

Mitigations

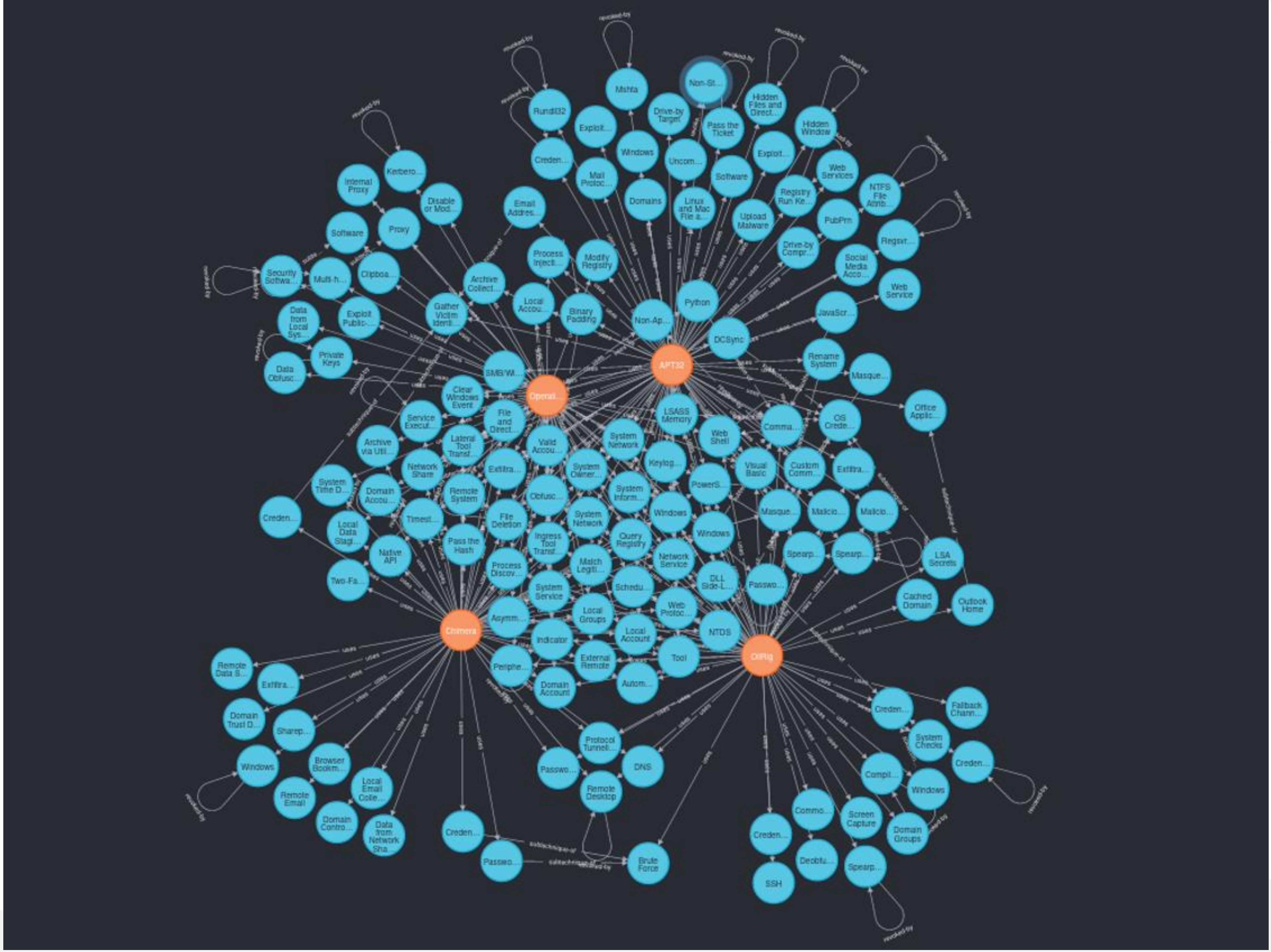
- M1041: Encrypt Sensitive Information
- T1126: Network Share Connection Removal Mitigation
- M1031: Network Intrusion Prevention
- T1029: Scheduled Transfer Mitigation
- T1113: Screen Capture Mitigation
- M1030: Network Segmentation
- M1042: Disable or Remove Feature or Program
- T1046: Network Service Scanning Mitigation
- M1022: Restrict File and Directory Permissions
- M1026: Privileged Account Management

Techniques

- T1160: Launch Daemon
- T1152: Launchctl
- T1222.002: Linux and Mac File and Directory Perm
- T1136.001: Local Account
- T1078.003: Local Accounts
- T1114.001: Local Email Collection
- T1069.001: Local Groups
- T1046: Network Service Scanning
- T1126: Network Share Connection Removal
- T1029: Scheduled Transfer
- T1113: Screen Capture

Results

Count	
4 out of 11 36%	G0114: Chir G0050: APT G0049: OilR
	G0139: TeamTNT G0116: Operation
	G0117: Fox Kitten

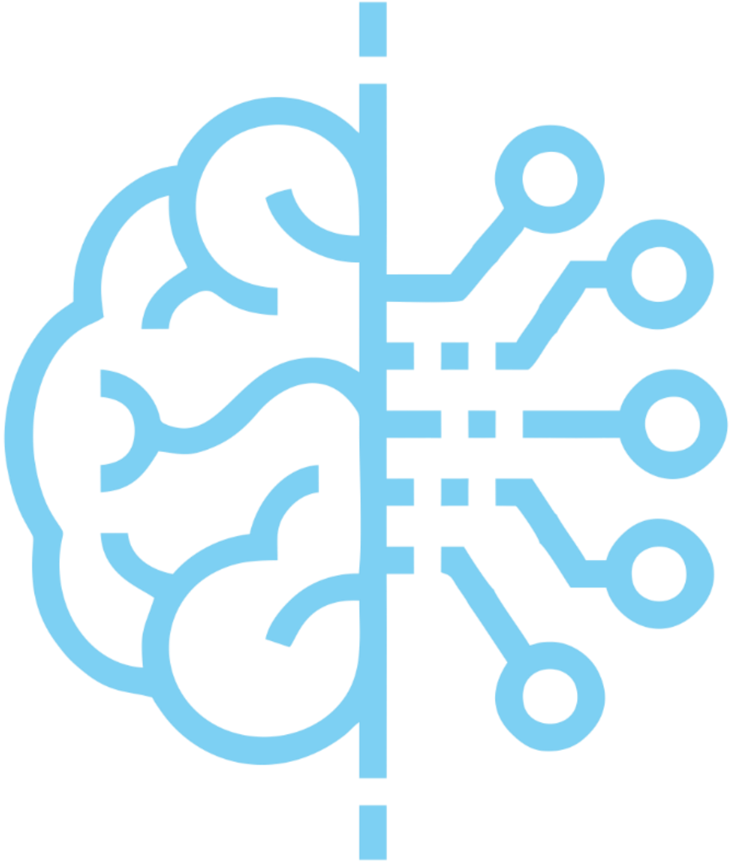

APT32
Operati...
Chimera
OilRig
Non-St...
Mshta
Rundll32
Exploit...
Drive-by Target
Pass the Ticket
Hidden Files and Direct...
Hidden Window
Creden...
Windows
Uncom...
Software
Exploit...
Web Services
NTFS File Attrib...
Kerbero...
Internal Proxy
Disable or Mod...
Mail Protoc...
Domains
Linux and Mac File a...
Upload Malware
Registry Run Ke...
PubPrn
Regsvr...
Email Addres...
Software
Proxy
Process Inject...
Modify Registry
Drive-by Compr...
Social Media Acco...
Web Service
Security Softwa...
Multi-h...
Clipboa...
Archive Collect...
Local Accou...
Binary Padding
Python
Non-Ap...
DCSync
JavaScr...
Data from Local Sys...
Exploit Public-...
Gather Victim Identi...
Private Keys
Data Obfusc...
SMB/Wi...
Rename System
Masque...
Office Applic...
Clear Windows Event
Service Execut...
File and Direct...
LSASS Memory
Web Shell
Comma...
OS Crede...
Archive via Util...
Lateral Tool Transf...
Valid Accou...
System Network
Keylog...
Visual Basic
Custom Comm...
Exfiltra...
System Time D...
Network Share
Exfiltra...
System Owner...
PowerS...
Domain Accou...
Remote System
Obfusc...
System Inform...
Windows
Masque...
Malicio...
Malicio...
Creden...
Timest...
File Deletion
System Network
Windows
Local Data Stagi...
Pass the Hash
Ingress Tool Transf...
Query Registry
Network Service
Spearp...
Spearp...
LSA Secrets
Native API
Process Discov...
Match Legiti...
Two-Fa...
System Service
Schedu...
DLL Side-L...
Passwo...
Cached Domain
Outlook Home
Asymm...
Local Groups
Web Protoc...
Indicator
Local Account
NTDS
Remote Data S...
Exfiltra...
External Remote
Tool
Periphe...
Domain Account
Autom...
Domain Trust D...
Sharep...
Protocol Tunneli...
Creden...
Fallback Chann...
System Checks
Windows
Browser Bookm...
DNS
Passwo...
Creden...
Compil...
Windows
Remote Email
Local Email Colle...
Remote Desktop
Commo...
Screen Capture
Domain Groups
Domain Contro...
Data from Network Sha...
Creden...
Creden...
Passwo...
Brute Force
Deobfu...
Spearp...
SSH
uses
revoked-by
subtechnique-of

2nd step: AI/ML based tool

AI/ML app

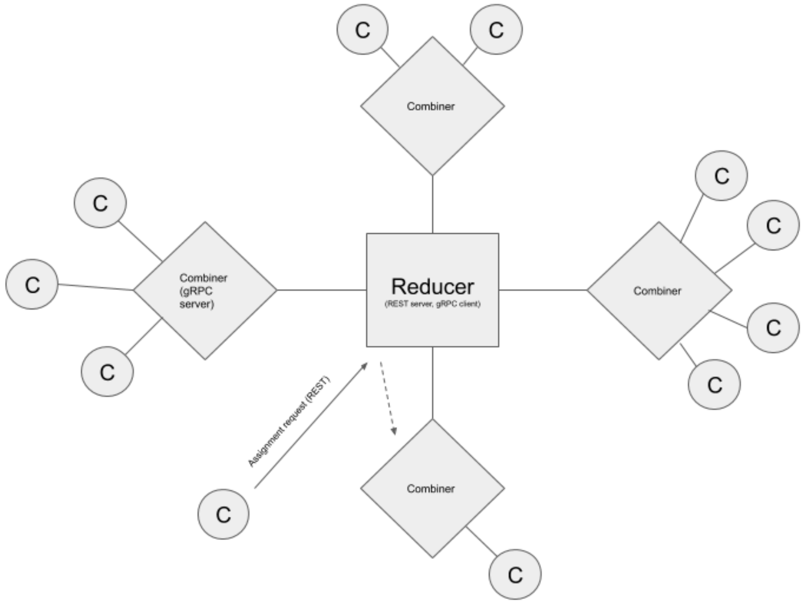
- Find and structure data (though most data cannot be shared) in free text

- Create AI/ML model that could find patterns and make better predictions
  - Improve prediction by considering contextual info provided in the cyber attack report
  - Increase likelihood for some APTs – decrease/exclude for others

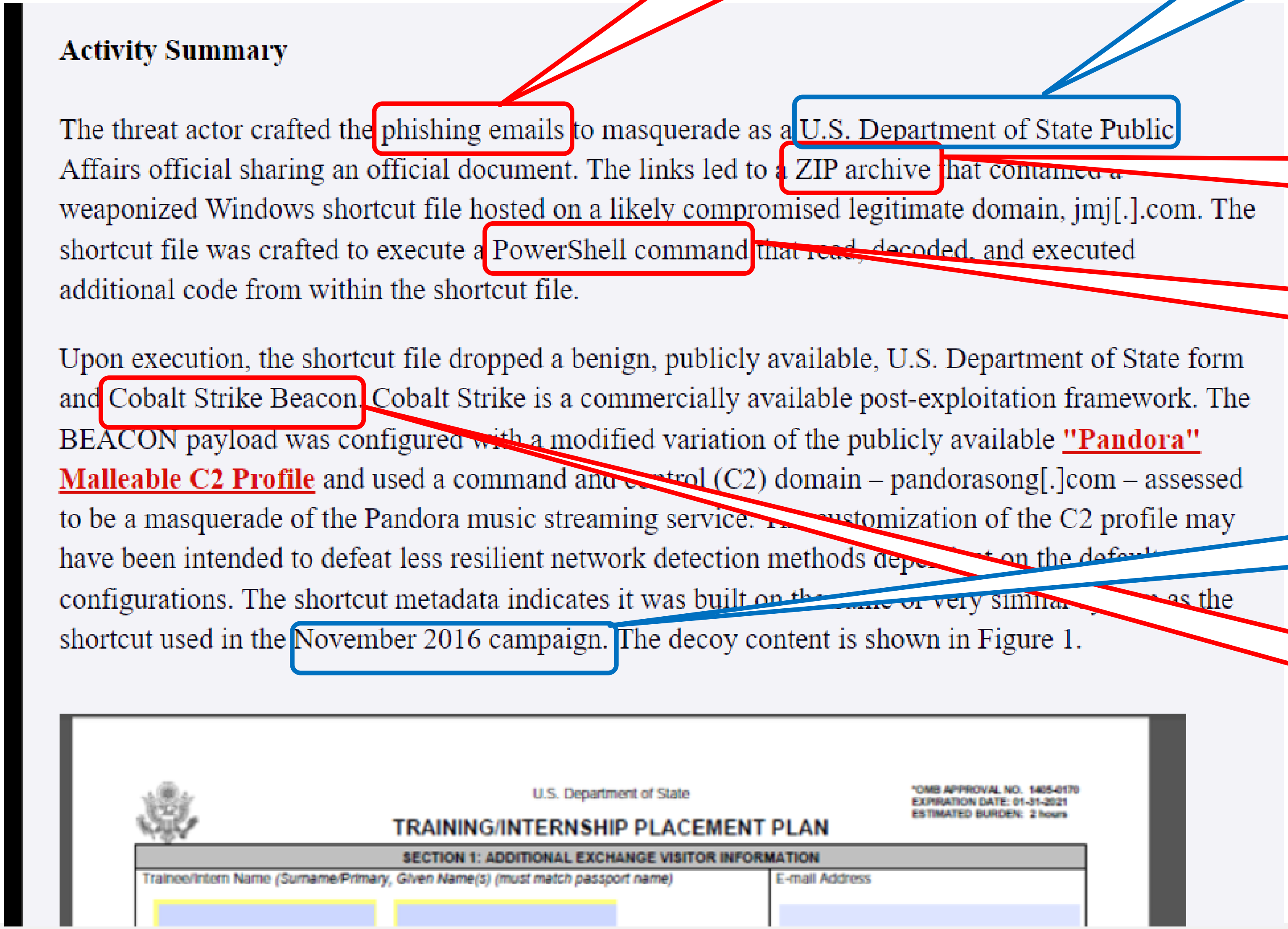


AI/ML app – Cooperation and Information sharing

- Federated machine learning
  - Share only models as **data cannot be shared**
  - FEDn Project https://scaleoutsystems.github.io/fedn/
- Two modes to use it:
  - Frozen mode: simply apply it to – without further enriching it
  - Enriching mode: apply it and further enrich the model with updated dataset



AI/ML app



Activity Summary

The threat actor crafted the phishing emails to masquerade as a U.S. Department of State Public Affairs official sharing an official document. The links led to a ZIP archive that contained a weaponized Windows shortcut file hosted on a likely compromised legitimate domain, jmj[.].com. The shortcut file was crafted to execute a PowerShell command that read, decoded, and executed additional code from within the shortcut file.

Upon execution, the shortcut file dropped a benign, publicly available, U.S. Department of State form and Cobalt Strike Beacon. Cobalt Strike is a commercially available post-exploitation framework. The BEACON payload was configured with a modified variation of the publicly available **"Pandora" Malleable C2 Profile** and used a command and control (C2) domain – pandorasong[.]com – assessed to be a masquerade of the Pandora music streaming service. The customization of the C2 profile may have been intended to defeat less resilient network detection methods dependent on the default configurations. The shortcut metadata indicates it was built on the same or very similar system as the shortcut used in the November 2016 campaign. The decoy content is shown in Figure 1.

U.S. Department of State

*OMB APPROVAL NO. 1405-0170
EXPIRATION DATE: 01-31-2021
ESTIMATED BURDEN: 2 hours

TRAINING/INTERNSHIP PLACEMENT PLAN

SECTION 1: ADDITIONAL EXCHANGE VISITOR INFORMATION

Trainee/Intern Name (Surname/Primary, Given Name(s) (must match passport name)

E-mail Address

T1566 Phishing

Context - target

T1598.002 Spearphishing Attachment

T1059.001 Powershell

Context – similar attack

T1090.004 Domain Fronting

Call for cooperation

- AFiT tool: you can use it if interested, **no need to share data with us.**
  - Report bugs, suggestions, etc..
- AI/ML app
  - Federated learning approach:
    - Train model based on your dataset
    - Enrich the “central” model based on your locally trained model
  - **No need to share data with us**

THANK YOU

Patrick MANA (patrick.mana@eurocontrol.int)
Bahtiar MUSTAFA (bahtiar.mustafa@eurocontrol.int)