AFiT

Estelle 'GMicka' Deharvengt

Jan 17, 2022

CONTENTS

1 Welcome to AFiT (Adversary Finder Tool) Manual! 1
- 1.1 First Steps . . . 1
- 1.2 Exploring AFiT . . . 5
- 1.3 New version of Mitre Att&ck . . . 9
- 1.4 Closing AFiT . . . 9
- 1.5 Additional Information . . . 10

2 Menu 11
- 2.1 Reset . . . 11
- 2.2 Load Mitre Att&ck Data . . . 11
- 2.3 Open Neo4j Desktop . . . 13
- 2.4 Start Neo4j Database . . . 14
- 2.5 Stop Neo4j Database . . . 16
- 2.6 Open Neo4j Browser . . . 16
- 2.7 Edit Config . . . 18

3 Techniques Section 21
- 3.1 Display . . . 22
- 3.2 Adding Techniques . . . 25
- 3.3 Techniques Options . . . 33
- 3.4 Go to Mitre Att&ck Website . . . 34
- 3.5 Generate Query . . . 36
- 3.6 Remove . . . 40
- 3.7 See Mitigation . . . 42

4 Results Section 55
- 4.1 Display . . . 56
- 4.2 Group Options . . . 59
- 4.3 Link to Mitre Att&ck Website . . . 62
- 4.4 Generate Query . . . 63
- 4.5 Show Details . . . 65
- 4.6 Save . . . 84

CHAPTER

ONE

WELCOME TO AFIT (ADVERSARY FINDER TOOL) MANUAL!

1.1 First Steps

This section will guide you to install and launch AFiT[1].

1.1.1 Requirements

AFiT runs with Python[2] 3.9. Make sure it is installed before following the installation steps.

It also requires having Neo4j[3] installed and running as it will connect to Neo4j database.
Neo4j Community Edition or Neo4j Desktop are sufficient.
The ip address is `127.0.0.1`, the bolt port is `7687` and the authentication is neo4j(username), mitre(password).
These settings are defined directly into python script.

1.1.2 Setting Neo4j Database

Install Neo4j Community Edition

Install Neo4j Community edition by running installNeo4j.sh script.

```
$ ./installNeo4j.sh
```

If the installation was not successful, follow the instruction from Neo4j Website

[1] AFiT stands for Adversary Finder Tool.

[2] Python is an interpreted high-level general-purpose programming language. More information and downloads on the Python's website.

[3] Neo4j is an open-source, NoSQL, native graph database that provides an ACID-compliant transactional backend for applications. More information and downloads on Neo4j's website.

Checking installation

Start Neo4j with the following command.

```
$ sudo systemctl start neo4j.service
```

Display Neo4j status.

```
$ sudo systemctl status neo4j.service
```

The output should be the following:

```
 neo4j.service - Neo4j Graph Database
     Loaded: loaded (/lib/systemd/system/neo4j.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2020-08-07 01:43:00 UTC; 6min ago
   Main PID: 21915 (java)
      Tasks: 45 (limit: 1137)
     Memory: 259.3M
     CGroup: /system.slice/neo4j.service
. . .
```

Setting Neo4j new password

Run to following command to start neo4j cypher shell

```
$ cypher-shell
```

You will be asked to set a new password. The password define in AFiT's source code is *mitre*. If you choose to use another password, you should modify it in the code otherwise AFiT won't be able to connect to Neo4j Database.

```
cypher-shell prompt
username: neo4j
password: neo4j                          # Default password
Password change required
new password: mitre                      # Set new password
confirm password: mitre                  # Confirm new password
Connected to Neo4j 4.1.0 at neo4j://localhost:7687 as user neo4j.
Type :help for a list of available commands or :exit to exit the shell.
Note that Cypher queries must end with a semicolon.
```

Exit cypher-shell with the following command.

```
neo4j@neo4j> :exit
```

1.1.3 Run AFiT in a python virtual environment (Optional)

Create

Create a new python virtual environment to run AFiT.

With Venv

```
$ python3.9 -m venv /path/to/new/environment/env_name
```

If the following error is displayed,

```
Error: Command '['/home/trainees/Desktop/AFiT/AFIT/bin/python3.9', '-Im', 'ensurepip', '-
↪-upgrade', '--default-pip']' returned non-zero exit status 1.
```

install venv lib for python 3.9.

```
$ sudo apt-get install python3.9-dev python3.9-venv
```

With Conda

```
$ conda create --name env_name python=3.9
```

Activate

Activate the virtual environment.

With Venv

```
$ source /path/to/new/environment/env_name/bin/activate
```

With Conda

```
$ conda activate env_name
```

Deactivate

Once you are finished using AFiT, you can deactivate the environment.

With Venv

```
$ deactivate
```

With Conda

```
$ conda deactivate
```

1.1.4 Start AFiT

To start the program, run AFiT.sh script.

```
$ ./AFiT.sh
```

This script will install the requirements of the program in the current virtual environment and launch AFiT.

If the requirements are already installed, the following message will be displayed.

```
Requirement already satisfied: GitPython==3.1.24 in ./Test1/lib/python3.8/site-packages␣
↪(from -r requirements.txt (line 1)) (3.1.24)
Requirement already satisfied: neo4j==4.3.4 in ./Test1/lib/python3.8/site-packages (from␣
↪-r requirements.txt (line 2)) (4.3.4)
Requirement already satisfied: py2neo==2021.2.0 in ./Test1/lib/python3.8/site-packages␣
↪(from -r requirements.txt (line 3)) (2021.2.0)
Requirement already satisfied: PySide6==6.2.1 in ./Test1/lib/python3.8/site-packages␣
↪(from -r requirements.txt (line 4)) (6.2.1)
Requirement already satisfied: gitdb<5,>=4.0.1 in ./Test1/lib/python3.8/site-packages␣
↪(from GitPython==3.1.24->-r requirements.txt (line 1)) (4.0.9)
Requirement already satisfied: typing-extensions>=3.7.4.3 in ./Test1/lib/python3.8/site-
↪packages (from GitPython==3.1.24->-r requirements.txt (line 1)) (4.0.1)
Requirement already satisfied: pytz in ./Test1/lib/python3.8/site-packages (from␣
↪neo4j==4.3.4->-r requirements.txt (line 2)) (2021.3)
Requirement already satisfied: packaging in ./Test1/lib/python3.8/site-packages (from␣
↪py2neo==2021.2.0->-r requirements.txt (line 3)) (21.3)
Requirement already satisfied: interchange~=2021.0.3 in ./Test1/lib/python3.8/site-
↪packages (from py2neo==2021.2.0->-r requirements.txt (line 3)) (2021.0.4)
Requirement already satisfied: pygments>=2.0.0 in ./Test1/lib/python3.8/site-packages␣
↪(from py2neo==2021.2.0->-r requirements.txt (line 3)) (2.11.2)
Requirement already satisfied: monotonic in ./Test1/lib/python3.8/site-packages (from␣
↪py2neo==2021.2.0->-r requirements.txt (line 3)) (1.6)
Requirement already satisfied: urllib3 in ./Test1/lib/python3.8/site-packages (from␣
↪py2neo==2021.2.0->-r requirements.txt (line 3)) (1.26.8)
Requirement already satisfied: pansi>=2020.7.3 in ./Test1/lib/python3.8/site-packages␣
↪(from py2neo==2021.2.0->-r requirements.txt (line 3)) (2020.7.3)
Requirement already satisfied: six>=1.15.0 in ./Test1/lib/python3.8/site-packages (from␣
↪py2neo==2021.2.0->-r requirements.txt (line 3)) (1.16.0)
Requirement already satisfied: certifi in ./Test1/lib/python3.8/site-packages (from␣
↪py2neo==2021.2.0->-r requirements.txt (line 3)) (2021.10.8)
Requirement already satisfied: shiboken6==6.2.1 in ./Test1/lib/python3.8/site-packages␣
↪(from PySide6==6.2.1->-r requirements.txt (line 4)) (6.2.1)
```

(continues on next page)

(continued from previous page)

```
Requirement already satisfied: smmap<6,>=3.0.1 in ./Test1/lib/python3.8/site-packages␣
↪(from gitdb<5,>=4.0.1->GitPython==3.1.24->-r requirements.txt (line 1)) (5.0.0)
Requirement already satisfied: pyparsing!=3.0.5,>=2.0.2 in ./Test1/lib/python3.8/site-
↪packages (from packaging->py2neo==2021.2.0->-r requirements.txt (line 3)) (3.0.6)
```

If so, you may want to run AFiT without installing the requirement. To do so, run the following command.

```
$ python3.9 AFiT.py
```

First use

On first use of AFiT, it is highly recommended to *load MitreAttack* data to have the database up to date.

1.2 Exploring AFiT

This section provides a brief presentation of the software and its areas.

AFiT contains three main area: the *Menu* on the top, the *Techniques Section* on the left and the *Results Section* on the right.

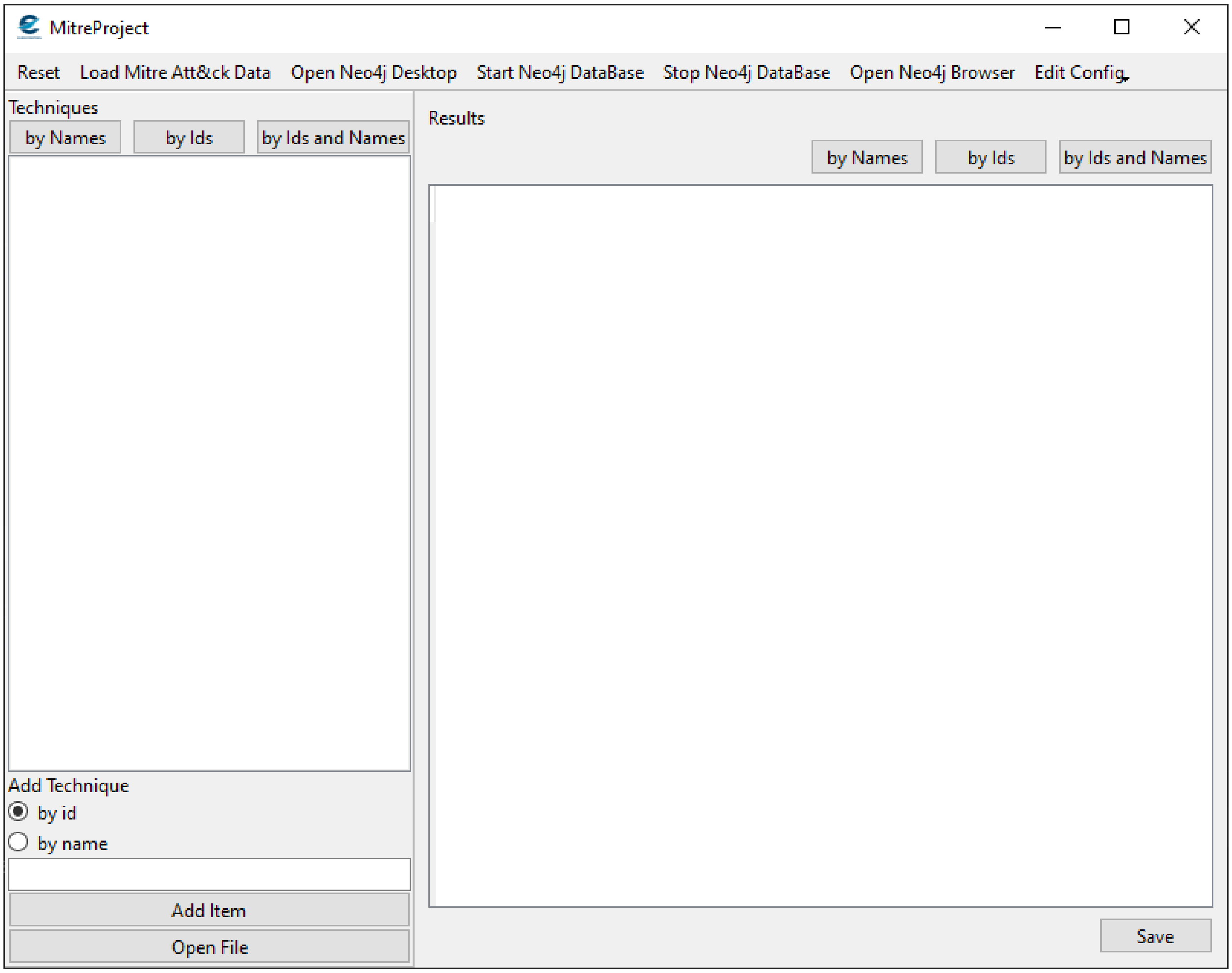


Fig. 1: AFiT's main window.
This window is displayed when AFiT is running.

1.2.1 Menu

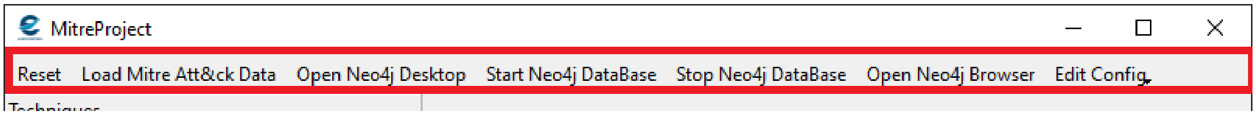


Fig. 2: AFiT's Menu.

AFiT Menu section contains general features of the software.

Read more about the Menu

1.2.2 Techniques Section

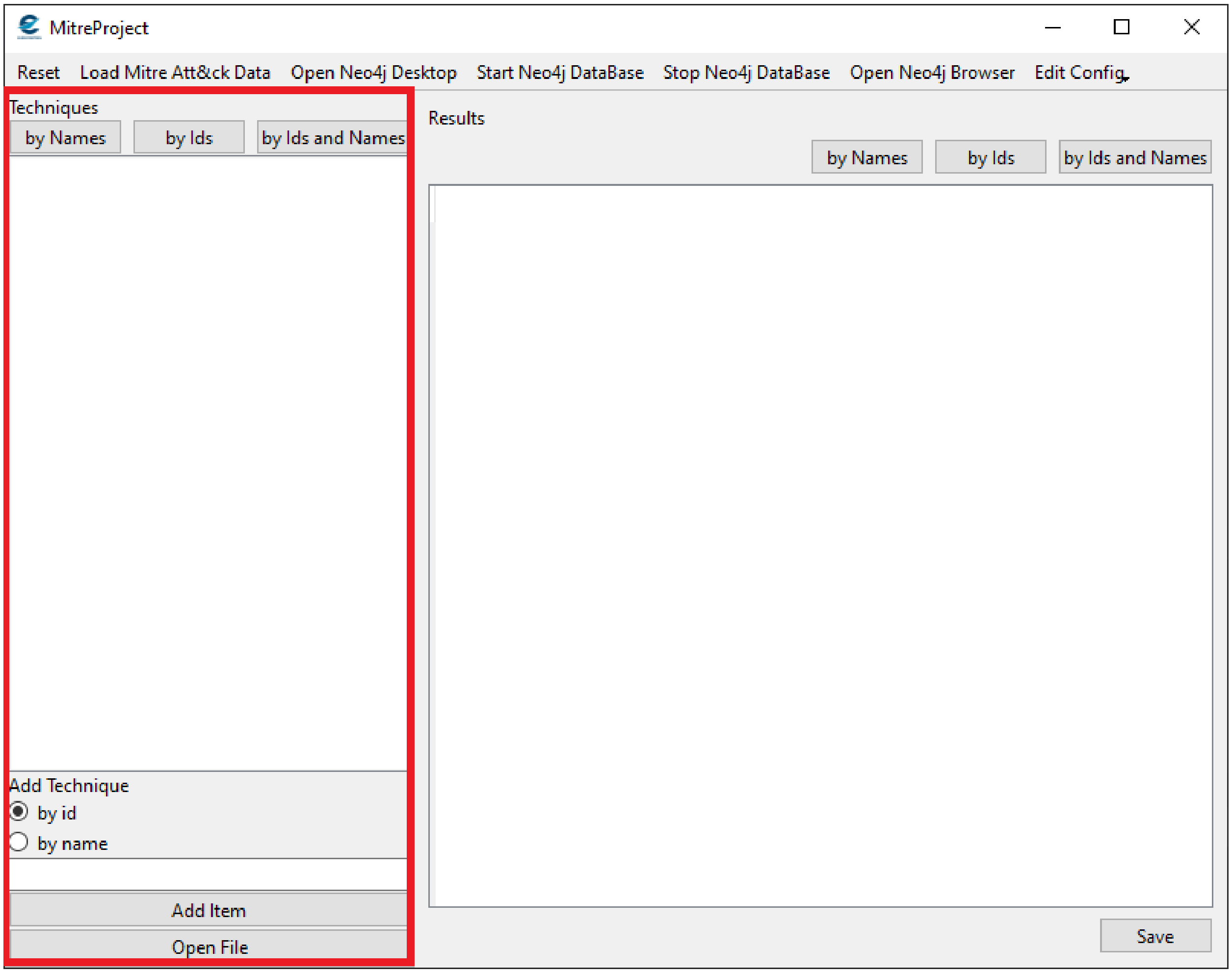
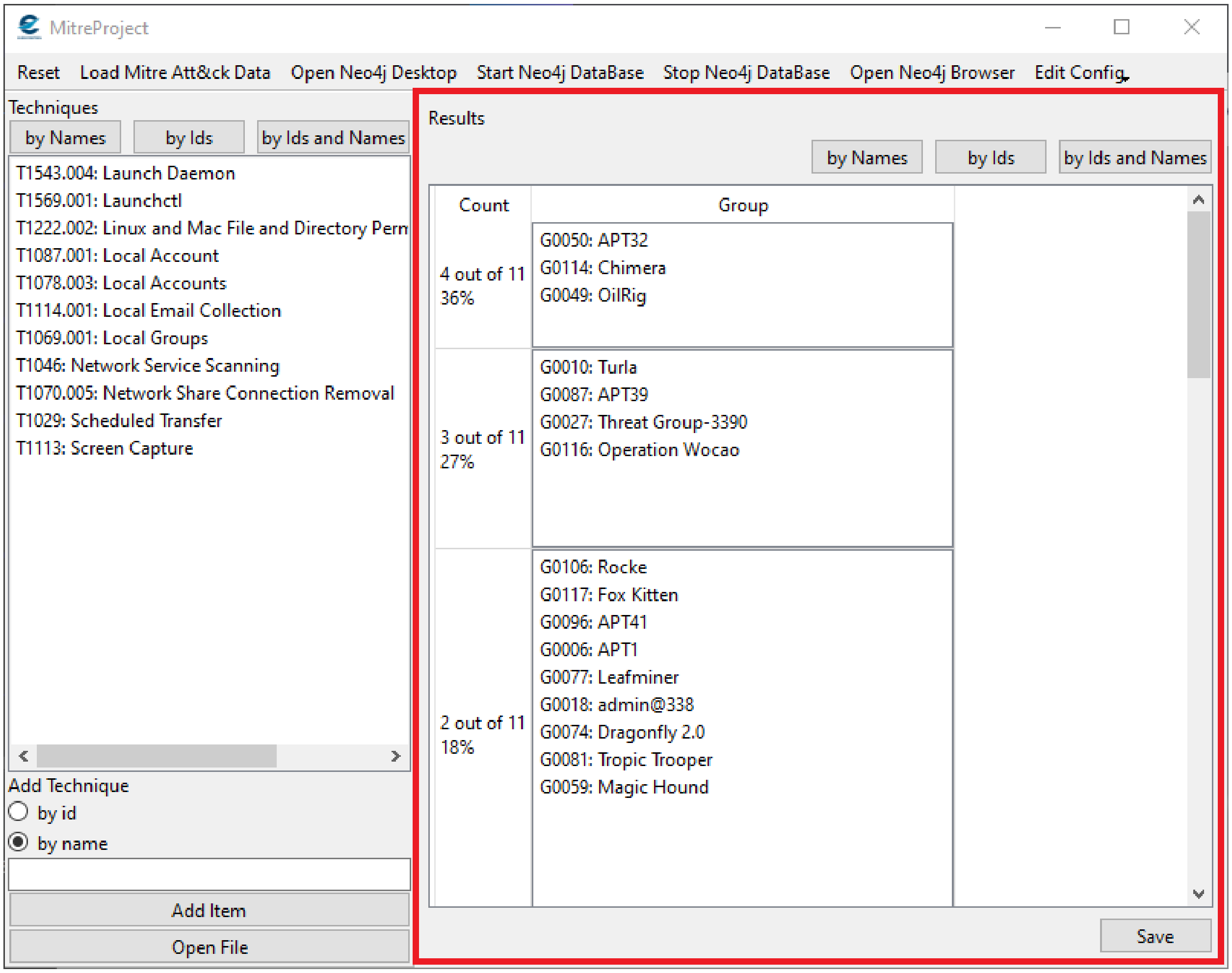


Fig. 3: AFiT's Techniques Section

AFiT Techniques Section contains features to display and manage the techniques given as input.
Read more about the Techniques Section

1.2.3 Results Section



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

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

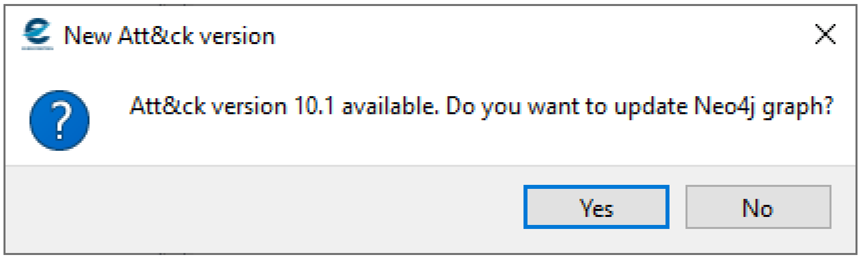
Fig. 4: AFiT's Results Section

AFiT Results Section contains the information about the groups retrieved from the database based on the given techniques. This section also contains the display options for the groups and a *Save* option.

Read more about the Results Section

1.3 New version of Mitre Att&ck

If a new version of Mitre Att&ck is detected, the following pop up will be displayed.

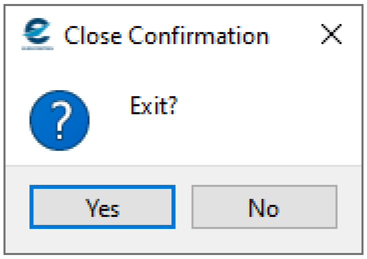


Att&ck version 10.1 available. Do you want to update Neo4j graph?

Fig. 5: By clicking `Yes` Neo4j graph will be updated

1.4 Closing AFiT

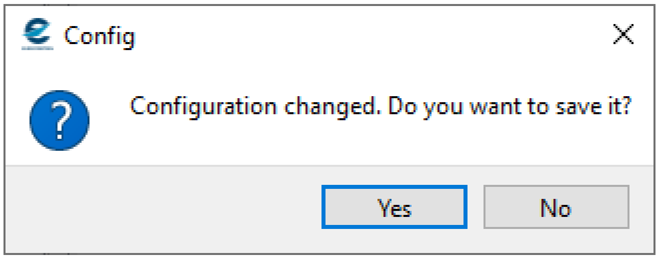
When the main window is closed, a confirm message will be displayed. If you want to close AFiT click `Yes`.



Exit?

Fig. 6: Confirmation Message to exit AFiT

If the configuration of AFiT changed, a message will be displayed to confirm if this new configuration must be saved.



Configuration changed. Do you want to save it?

Fig. 7: Confirmation Message to save the new configuration

1.5 Additional Information

Mitre Att&ck[6] enterprise-attack data is imported from a json file in the Cti repository of Mitre's Github.

For the development of this software, the tool attack2neo was used and slightly modified.

[6] MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. More information on Mitre Att&ck's website.

MENU

AFiT Menu contains general features of the software.

You will find a description for each feature in this section.

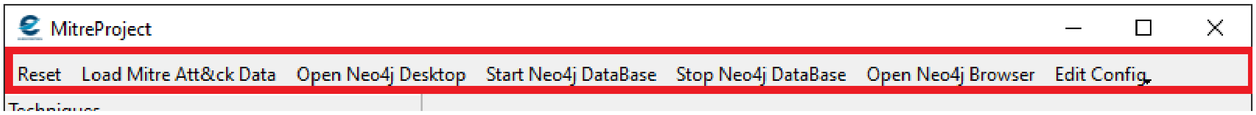


Fig. 1: AFiT's Menu.

2.1 Reset

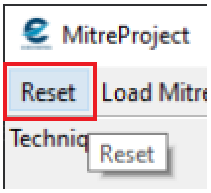


Fig. 2: Reset Button.

Clicking this button will remove all techniques and groups in the *Techniques* and *Results Section*.

2.2 Load Mitre Att&ck Data

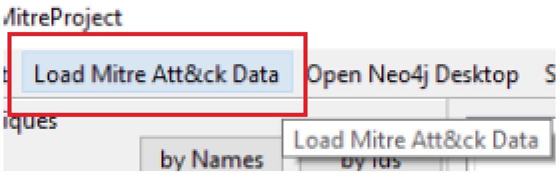
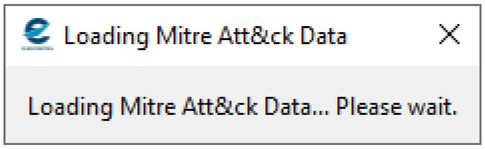


Fig. 3: Load Mitre Att&ck Data Button.

This feature is used to create a Neo4j Graph based on the Mitre Att&ck Enterprise Attack data.
First it loads enterprise-attack.json from Mitre/Cti repository.
Then, it opens a Neo4j Graph connection and deletes all existing nodes and edges.
Finally it reads the data from the json file and creates the nodes in the Neo4j Graph.

This feature can take some time to be completed. While it is still running you will see the following window.

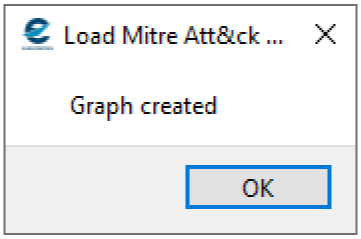


Loading Mitre Att&ck Data

Loading Mitre Att&ck Data... Please wait.

Fig. 4: This window means that the data is still being loaded in the Graph. This step can take some time.

Once the Graph is complete a new window will be shown stating that the Graph is created.

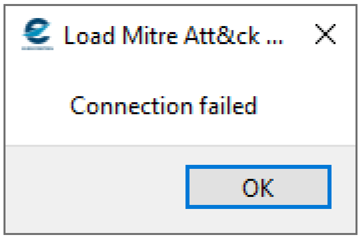


Load Mitre Att&ck ...

Graph created

Fig. 5: This window means that the data has been successfully loaded in the Graph.

If an error occurs, a new window will show up to inform that the creation of the Graph has not been completed.



Load Mitre Att&ck ...

Connection failed

Fig. 6: Example of failure during the creation of Graph.

Warning: Do not forget to start Neo4j Database before loading Mitre Att&ck Data.

2.3 Open Neo4j Desktop

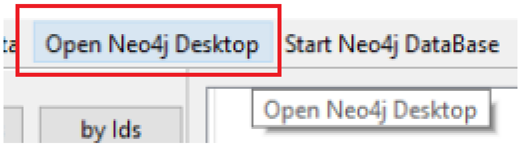


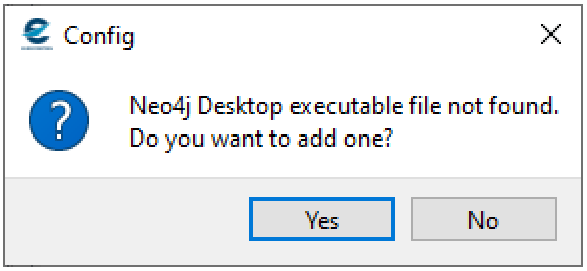
Fig. 7: Open Neo4j Desktop Button.

This button will open Neo4j Desktop[1].

Warning: This feature will not work if Neo4j Desktop is not installed.

Note: This is the only feature that will not work if Neo4j Desktop is not installed. Any other version of Neo4j is sufficient to run the rest of the features of AFiT.

If AFiT can not find it, a new window will show up asking if you want to select the executable file manually.

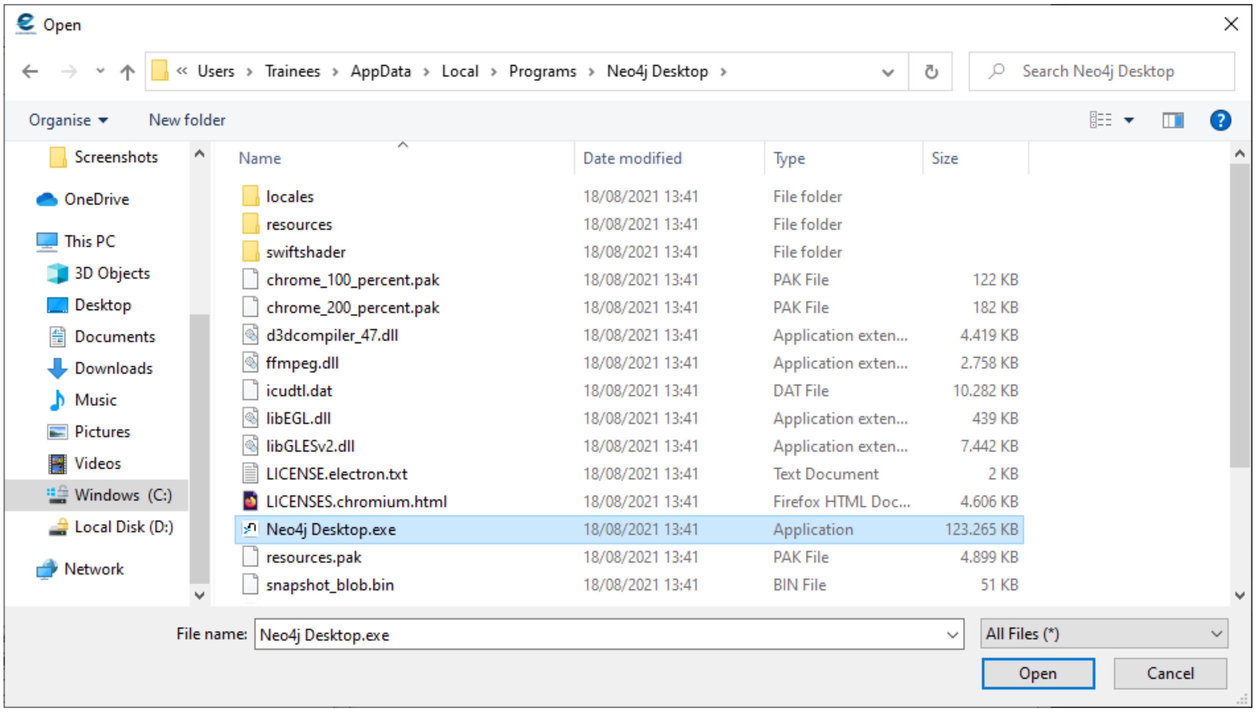


Neo4j Desktop executable file not found.
Do you want to add one?

Fig. 8: This Window is displayed if AFiT was unable to find Neo4j Desktop executable file.

If you select 'Yes' option, a File Dialog window will show up to select Neo4j Desktop executable file.

[1] Neo4j Desktop is an installable application to help you work with Neo4j. Read more about Neo4j Desktop.



Name	Date modified	Type	Size
locales	18/08/2021 13:41	File folder	
resources	18/08/2021 13:41	File folder	
swiftshader	18/08/2021 13:41	File folder	
chrome_100_percent.pak	18/08/2021 13:41	PAK File	122 KB
chrome_200_percent.pak	18/08/2021 13:41	PAK File	182 KB
d3dcompiler_47.dll	18/08/2021 13:41	Application exten...	4.419 KB
ffmpeg.dll	18/08/2021 13:41	Application exten...	2.758 KB
icudtl.dat	18/08/2021 13:41	DAT File	10.282 KB
libEGL.dll	18/08/2021 13:41	Application exten...	439 KB
libGLESv2.dll	18/08/2021 13:41	Application exten...	7.442 KB
LICENSE.electron.txt	18/08/2021 13:41	Text Document	2 KB
LICENSES.chromium.html	18/08/2021 13:41	Firefox HTML Doc...	4.606 KB
Neo4j Desktop.exe	18/08/2021 13:41	Application	123.265 KB
resources.pak	18/08/2021 13:41	PAK File	4.899 KB
snapshot_blob.bin	18/08/2021 13:41	BIN File	51 KB

File name: Neo4j Desktop.exe

Fig. 9: Select Neo4j Desktop executable file with this file dialog window.

After selecting the executable file, AFiT will open Neo4j Desktop.

2.4 Start Neo4j Database

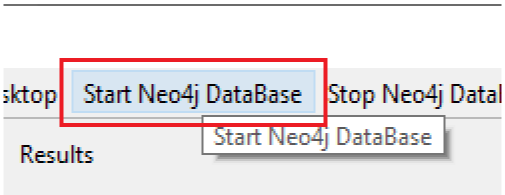
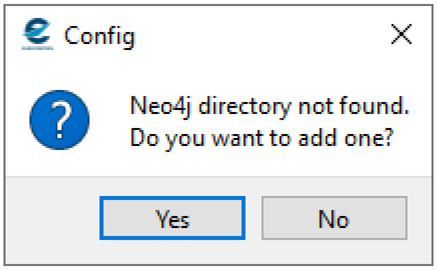


Fig. 10: Start Neo4j Database Button.

This button will start Neo4j Database.

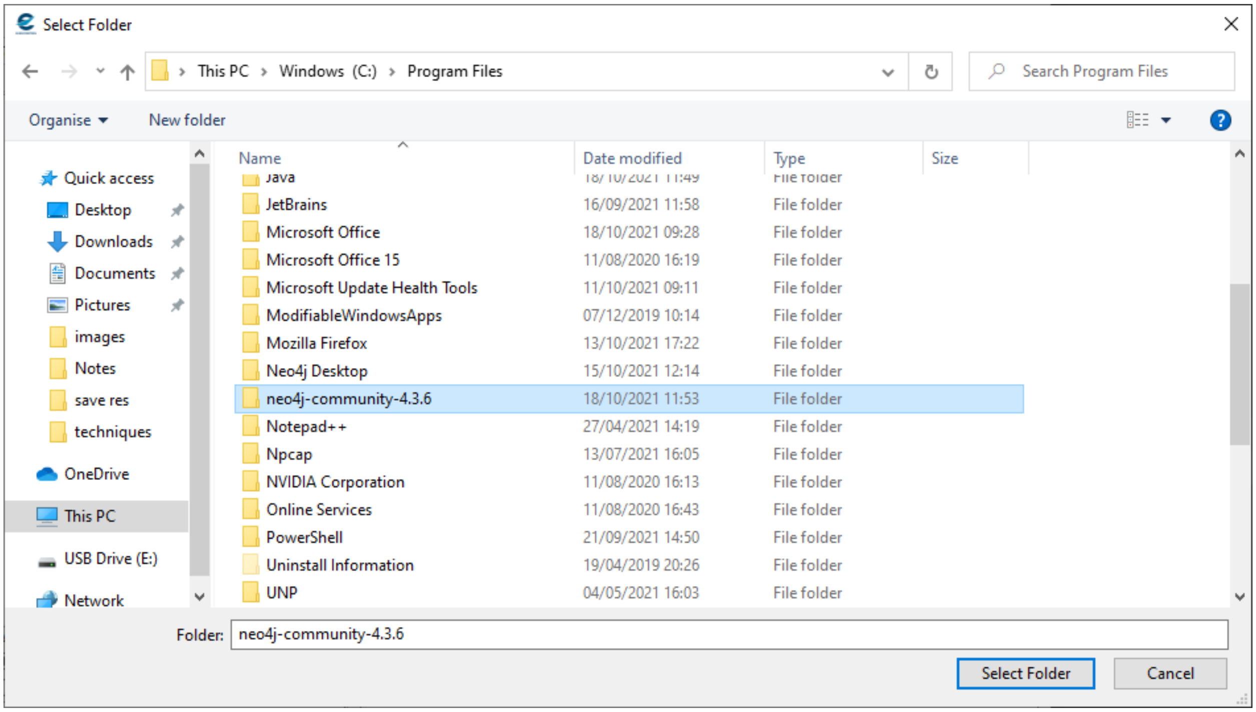
If Neo4j's directory is not found, a new window will show up asking if you want to select the directory manually.



Neo4j directory not found.
Do you want to add one?

Fig. 11: This Window is displayed if AFiT was unable to find Neo4j directory.

If you select `Yes` option, a File Dialog window will show up to select Neo4j directory.



Name	Date modified	Type	Size
Java	18/10/2021 11:49	File folder	
JetBrains	16/09/2021 11:58	File folder	
Microsoft Office	18/10/2021 09:28	File folder	
Microsoft Office 15	11/08/2020 16:19	File folder	
Microsoft Update Health Tools	11/10/2021 09:11	File folder	
ModifiableWindowsApps	07/12/2019 10:14	File folder	
Mozilla Firefox	13/10/2021 17:22	File folder	
Neo4j Desktop	15/10/2021 12:14	File folder	
neo4j-community-4.3.6	18/10/2021 11:53	File folder	
Notepad++	27/04/2021 14:19	File folder	
Npcap	13/07/2021 16:05	File folder	
NVIDIA Corporation	11/08/2020 16:13	File folder	
Online Services	11/08/2020 16:43	File folder	
PowerShell	21/09/2021 14:50	File folder	
Uninstall Information	19/04/2019 20:26	File folder	
UNP	04/05/2021 16:03	File folder	

Folder: neo4j-community-4.3.6

Fig. 12: Select Neo4j directory with this file dialog window.

After selecting the directory, AFiT will start Neo4j Database.

2.5 Stop Neo4j Database

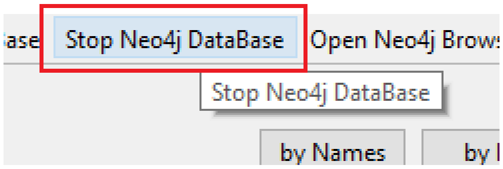


Fig. 13: Stop Neo4j Database Button.

This button will stop Neo4j Database.

If Neo4j directory is not found, this feature has the same behaviour as *Start Neo4j Database*

2.6 Open Neo4j Browser

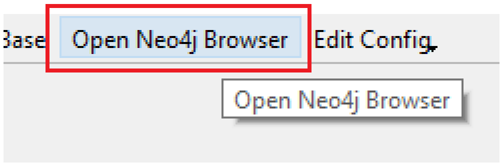
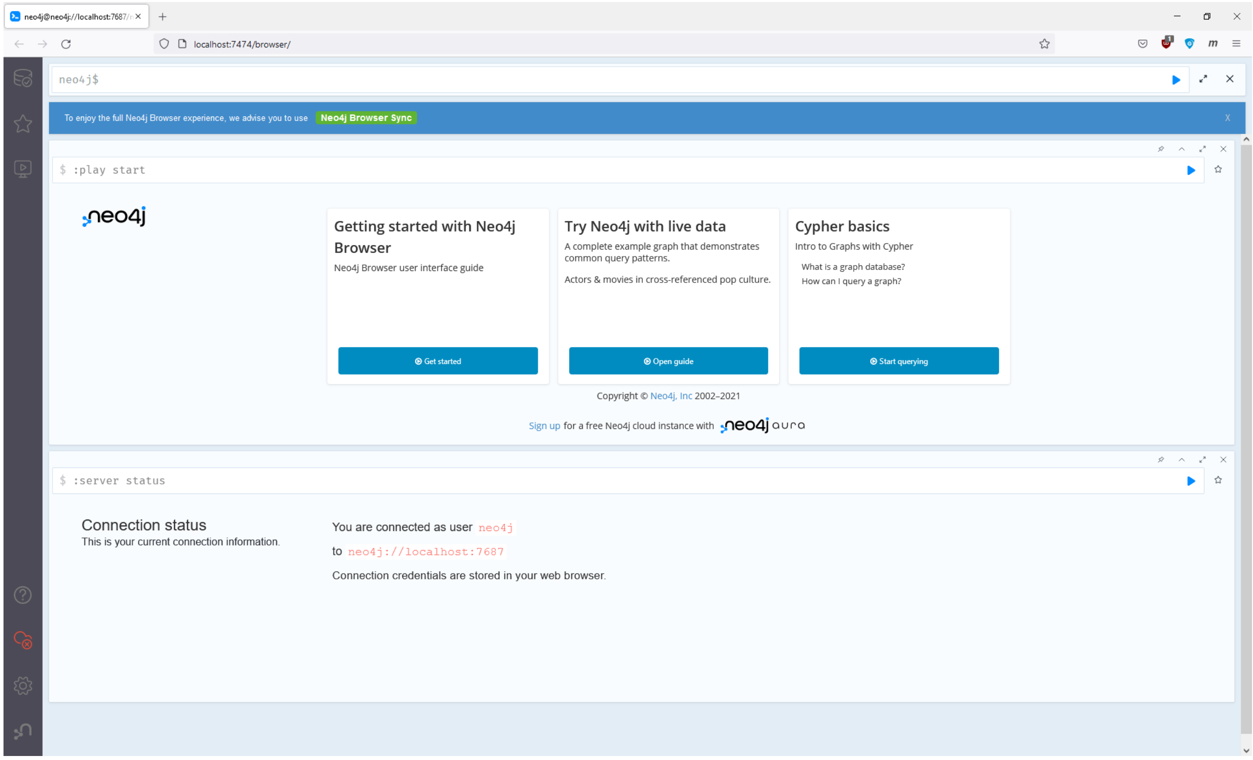


Fig. 14: Open Neo4j Browser Button.

This button will open Neo4j Browser.



To enjoy the full Neo4j Browser experience, we advise you to use Neo4j Browser Sync

```
$ :play start
```

Getting started with Neo4j Browser

Neo4j Browser user interface guide

Try Neo4j with live data

A complete example graph that demonstrates common query patterns.

Actors & movies in cross-referenced pop culture.

Cypher basics

Intro to Graphs with Cypher

What is a graph database?

How can I query a graph?

Copyright © Neo4j, Inc 2002–2021

Sign up for a free Neo4j cloud instance with neo4j aura

```
$ :server status
```

Connection status

This is your current connection information.

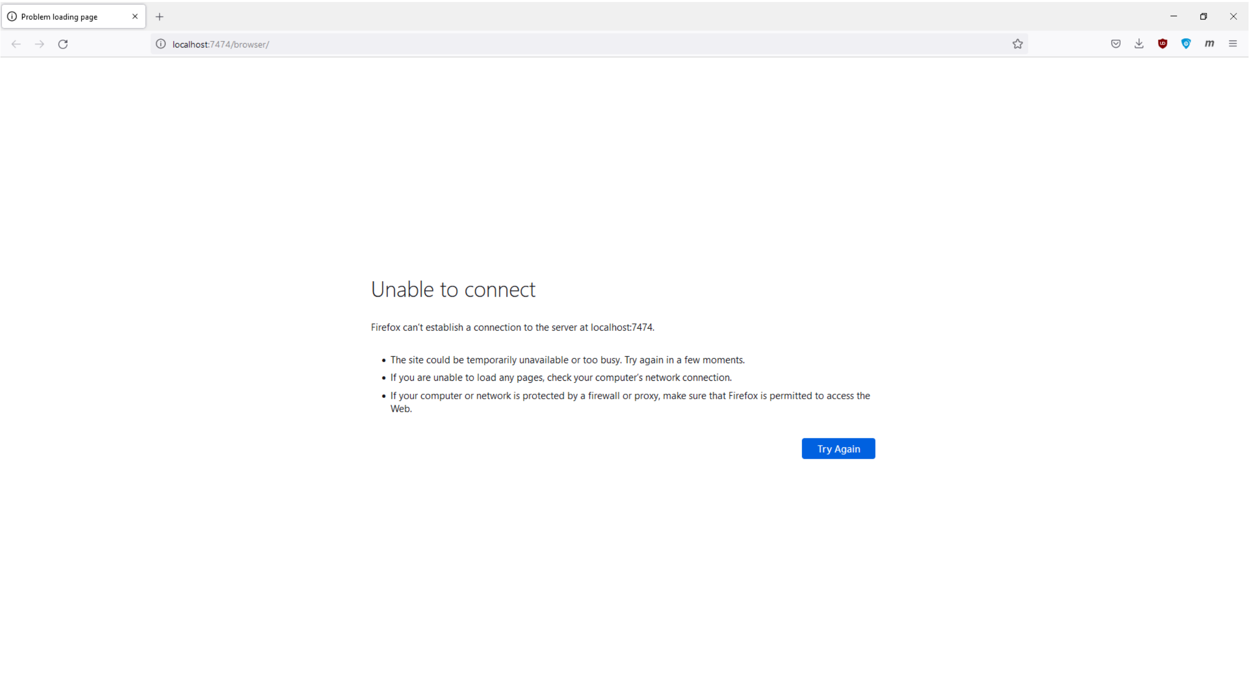
You are connected as user neo4j

to neo4j://localhost:7687

Connection credentials are stored in your web browser.

Fig. 15: Neo4j Browser.

Note: Make sure that Neo4j Database is started or the browser will not load.



Unable to connect

Firefox can't establish a connection to the server at localhost:7474.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Fig. 16: Neo4j Database is not running and the browser is not loading.

2.7 Edit Config

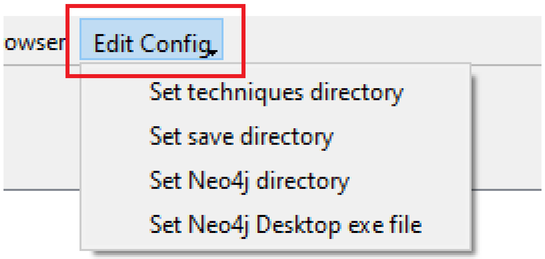


Fig. 17: Edit Config Button.

This button contains a menu to edit the configuration of AFiT.

2.7.1 Set techniques directory

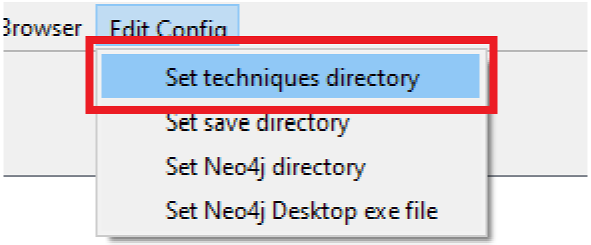


Fig. 18: Set Techniques Directory.

This option allows to set a working directory for the techniques files. (see *Add Multiple Items*)

2.7.2 Set save directory

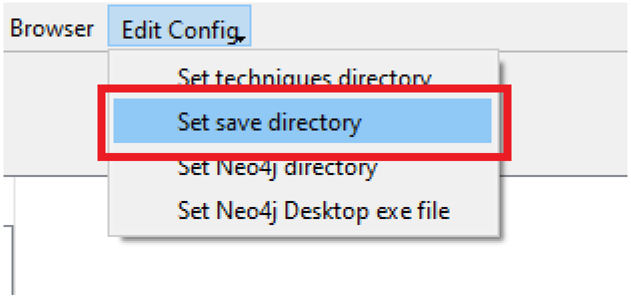


Fig. 19: Set save directory.

This option allows to set a working directory for the save option. (see *Save Results*)

2.7.3 Set Neo4j directory

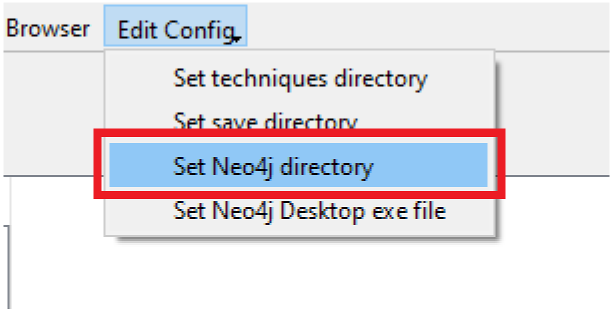


Fig. 20: Set Neo4j Directory.

This option allows to set the Neo4j directory. (see *Start Neo4j Database* and *Stop Neo4j Database*)

2.7.4 Set Neo4j Desktop Executable File

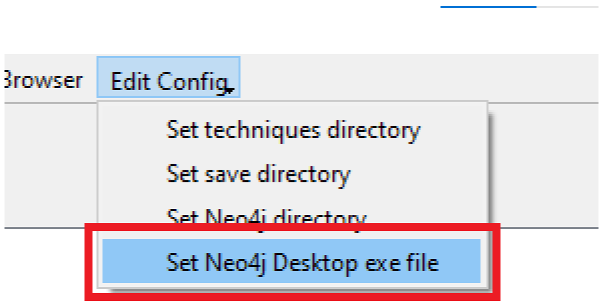


Fig. 21: Set Neo4j Desktop Executable File.

This option allows to set the Neo4j Desktop Executable File. (see *Open Neo4j Desktop*)

CHAPTER THREE

TECHNIQUES SECTION

AFiT Techniques Section contains features to display and manage the techniques given as input.
You will find a detailed description of all the areas in this section.

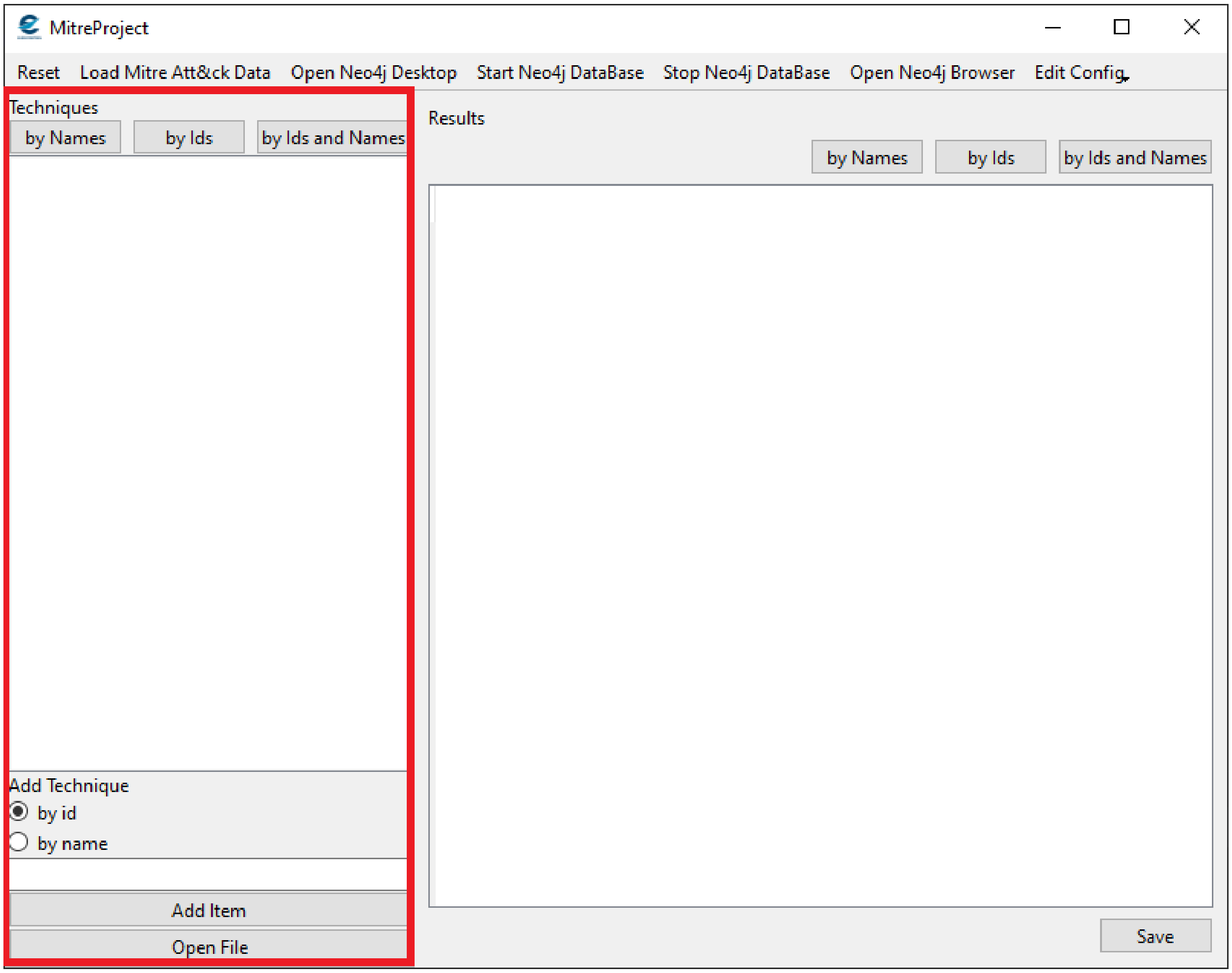


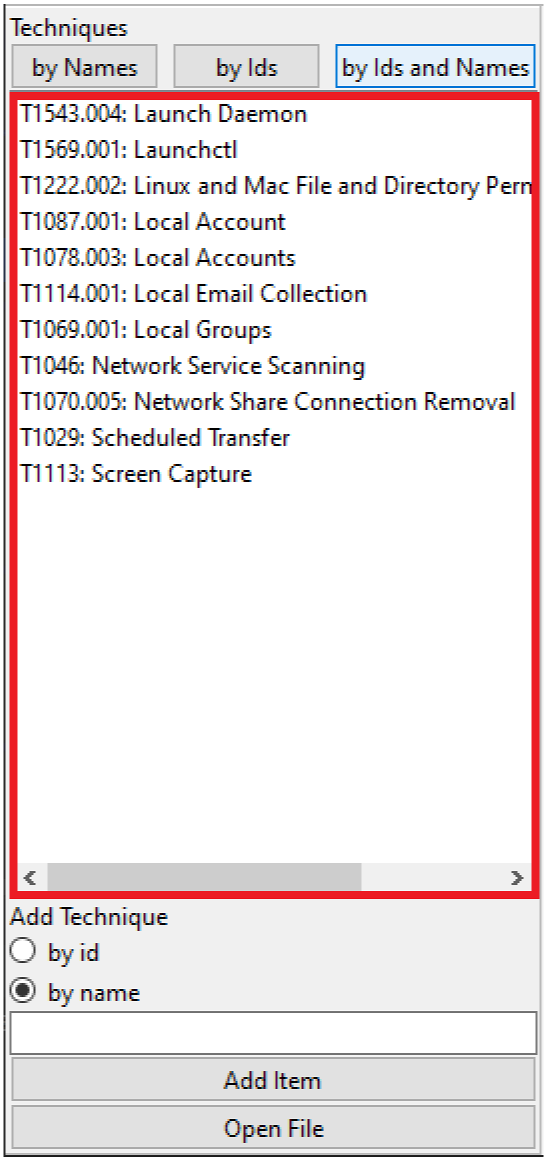
Fig. 1: AFiT's Techniques Section

3.1 Display

In the following paragraphs, the display options are listed and explained.

3.1.1 Where are the techniques listed ?

In the center of the section, you will find a list view that displays all the techniques used as input.



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

○ by id
● by name

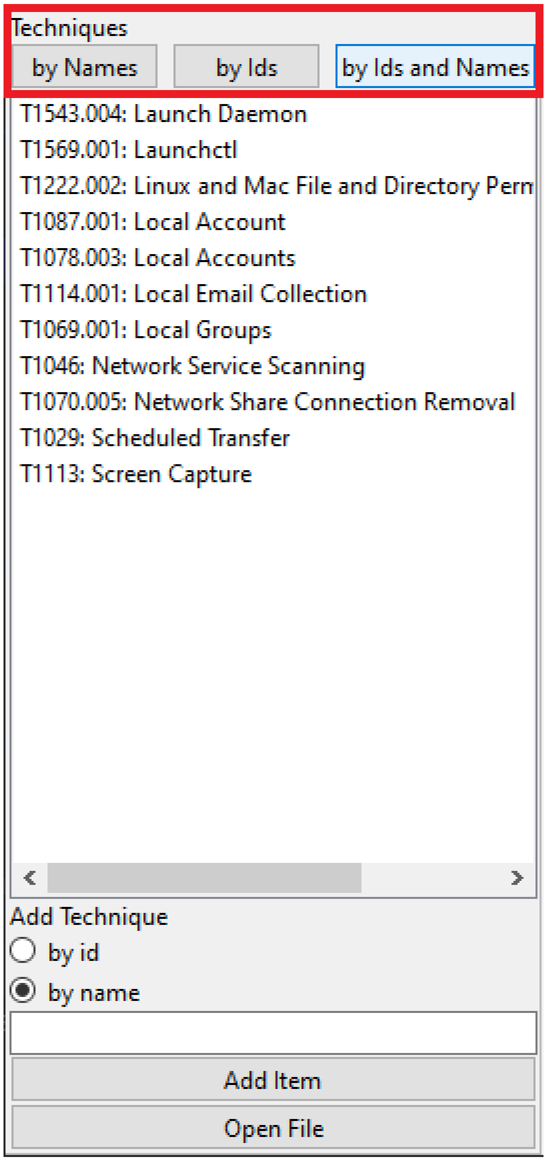
Fig. 2: List View where the techniques are displayed

Techniques will be labeled either by their names, by their id or both of them. For example, the technique *Screen Capture* will be appear either by its name (Screen Capture), by its id (T1113) or by both of them (T1113: Screen Capture).

3.1.2 Choose how the techniques are displayed

You can choose how the techniques will appear in the *list view*.
There are three options: techniques can either be shown *by name*, *by id* or *by id and name*.

Those option are available on the top of the *list view*.

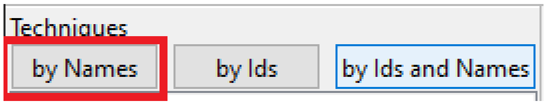


T1543.004: Launch Daemon
T1569.001: Launchctl
T1222.002: Linux and Mac File and Directory Pern
T1087.001: Local Account
T1078.003: Local Accounts
T1114.001: Local Email Collection
T1069.001: Local Groups
T1046: Network Service Scanning
T1070.005: Network Share Connection Removal
T1029: Scheduled Transfer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

○ by id
● by name

Fig. 3: Techniques Display Options

To see the techniques by their names, click the button `by Names`.



Techniques

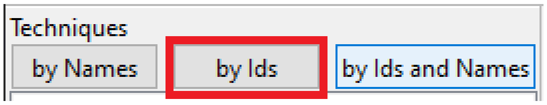
by Names

by Ids

by Ids and Names

Fig. 4: This button allows to display techniques by their names

To see the techniques by their ids, click the button `by Ids`.



Techniques

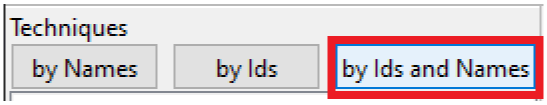
by Names

by Ids

by Ids and Names

Fig. 5: This button allows to display techniques by their ids

To see the techniques by their ids and names, click the button `by Ids and Names`.



Techniques

by Names

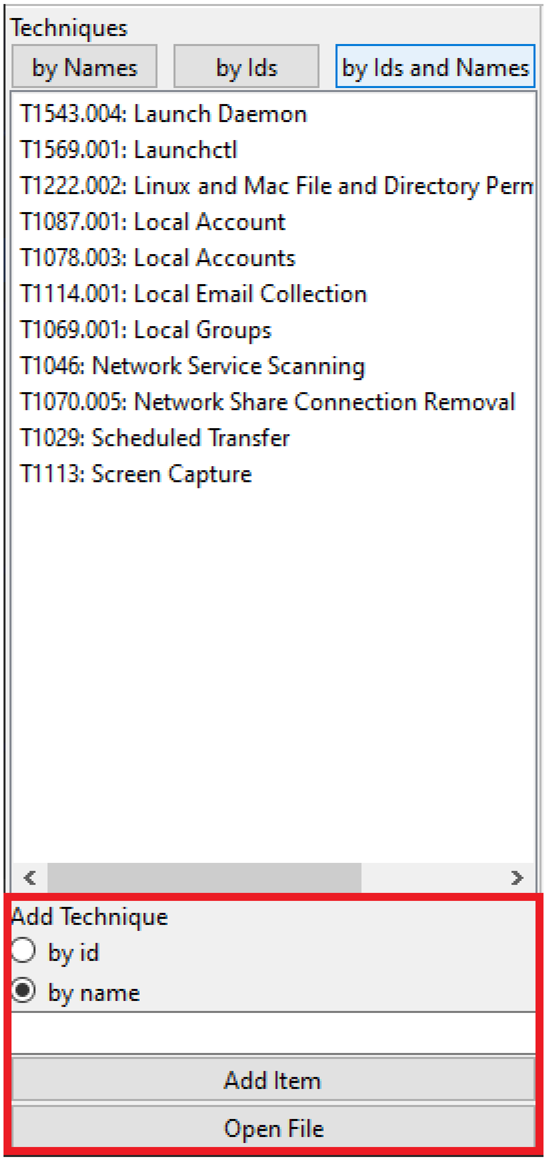
by Ids

by Ids and Names

Fig. 6: This button allows to display techniques by their ids and names

3.2 Adding Techniques

The area dedicated to add techniques is located bellow the *list view*



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

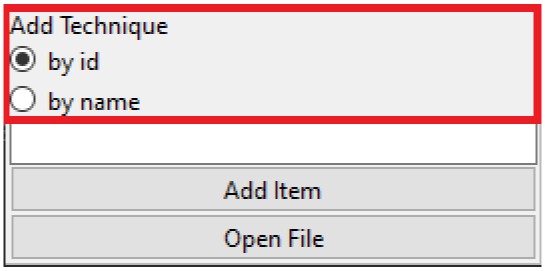
Add Technique
○ by id
● by name

Fig. 7: Add technique area

3.2.1 Add One Item

1. Choose how you want to add the new technique.

   You can add a technique by its name or by its id.



Add Technique

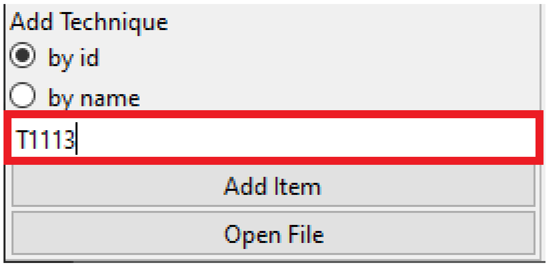
● by id

○ by name

Fig. 8: Add a technique by its type

2. Enter the technique.

   Write the name or the id of the technique in the text editor box.



Add Technique

● by id

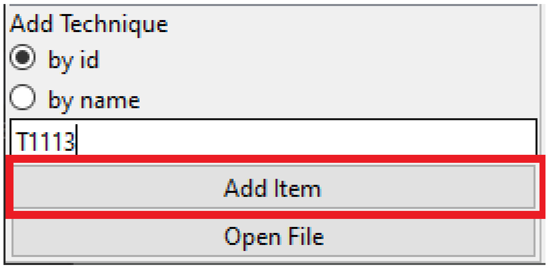
○ by name

T1113

Fig. 9: Adding Technique T1113 by Id

3. Add the Item.

   Add the new technique by clicking the button `Add Item`.



Add Technique

● by id

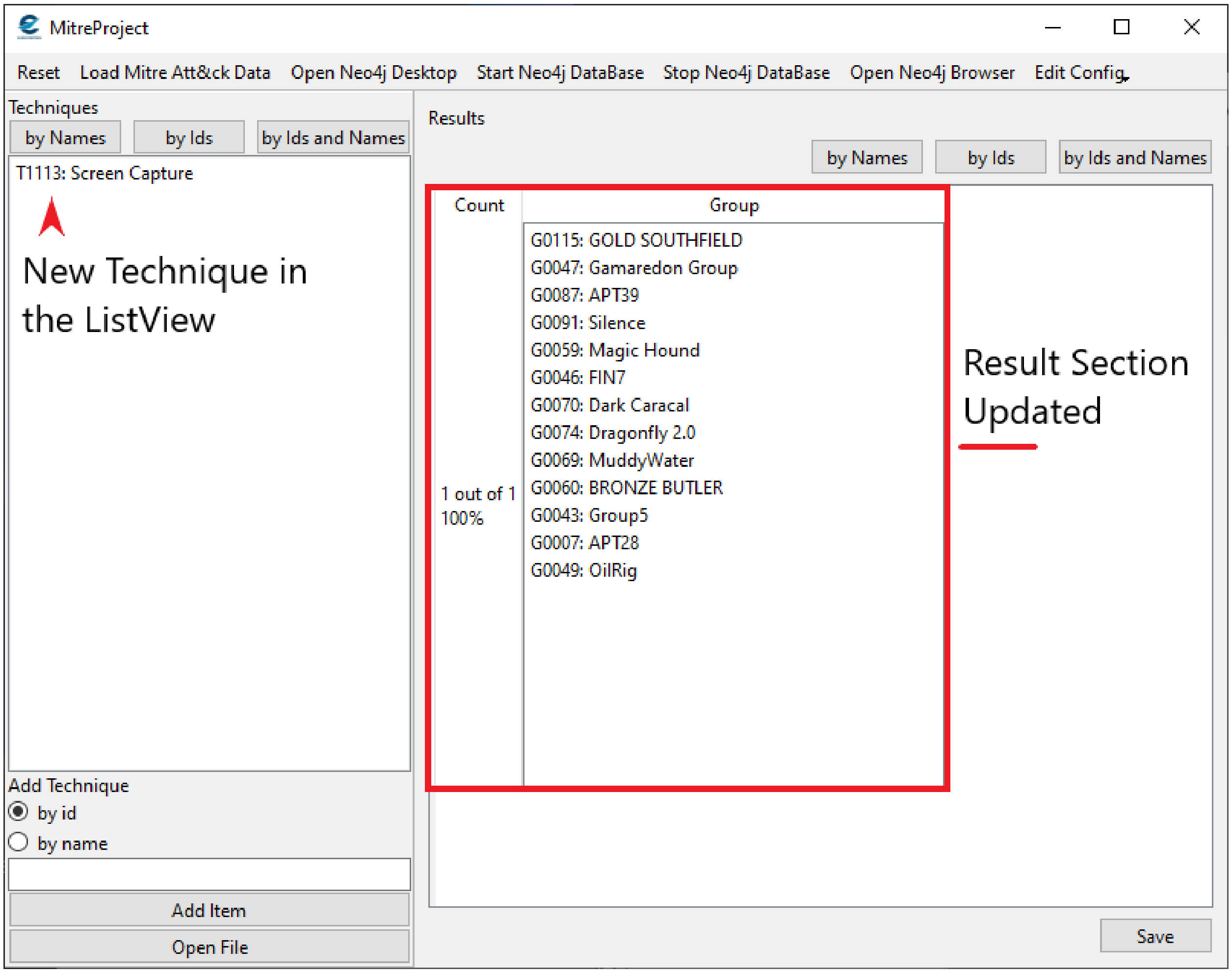
○ by name

T1113

Fig. 10: Adding Technique T1113 by Id

4. Result.

   The new Technique is added to the list of techniques and the result section is automatically updated.



T1113: Screen Capture

New Technique in the ListView

Count	Group
1 out of 1 100%	G0115: GOLD SOUTHFIELD G0047: Gamaredon Group G0087: APT39 G0091: Silence G0059: Magic Hound G0046: FIN7 G0070: Dark Caracal G0074: Dragonfly 2.0 G0069: MuddyWater G0060: BRONZE BUTLER G0043: Group5 G0007: APT28 G0049: OilRig

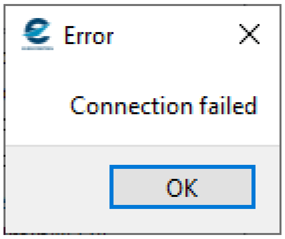
Result Section Updated

Fig. 11: Technique T1113 is added to the list view and the Result Section is automatically updated

5. Errors that might occur.

   If the technique can not be added to the list a new window will appear explaining the nature of the failure. Hereunder, examples of error are explained.

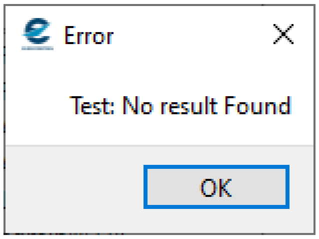
   Example 1



Connection failed

Fig. 12: This window will be displayed if AFiT can not connect with Neo4j Graph. This might occur if the database is not active.

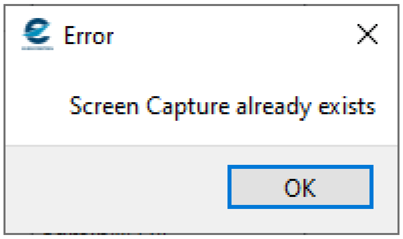
Example 2



Test: No result Found

Fig. 13: This window will be displayed the technique can not be found in the database

Example 3



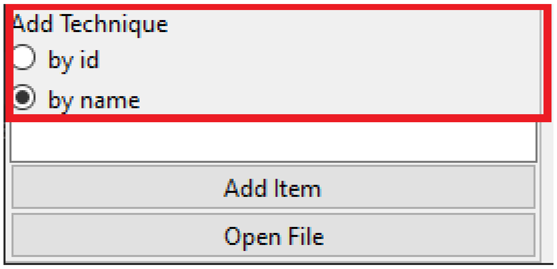
Screen Capture already exists

Fig. 14: This window will be displayed the technique is already in the list

3.2.2 Add Multiple Items

1. Choose how you want to add the new techniques.

   You can add techniques by their name or by their id.



Add Technique
○ by id
● by name

Fig. 15: Add techniques by their type

2. Click *Open File*

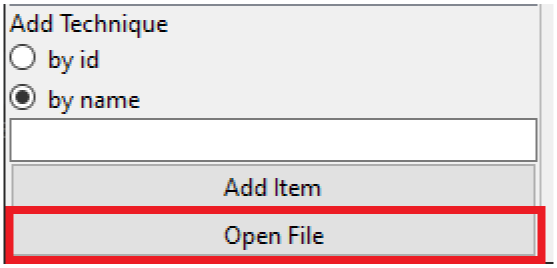
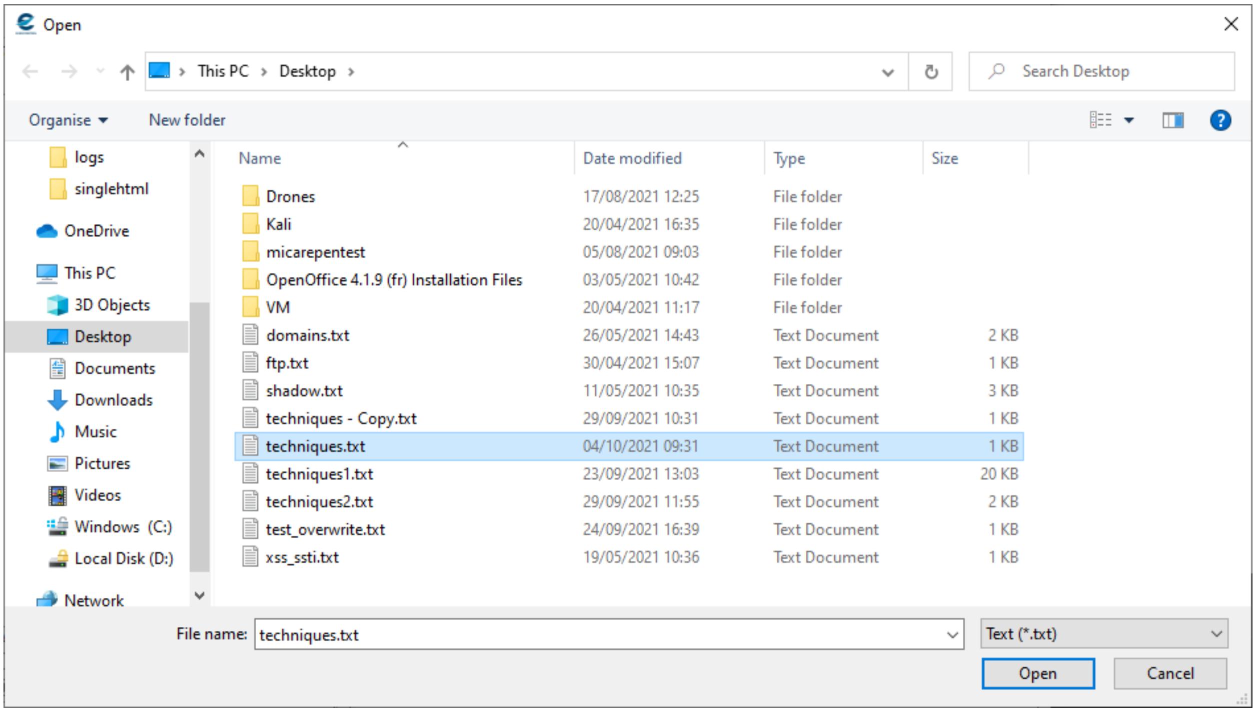


Fig. 16: *Open File* Button

3. Select a file.

   Select a .txt file containing techniques.



Name	Date modified	Type	Size
Drones	17/08/2021 12:25	File folder	
Kali	20/04/2021 16:35	File folder	
micarepentest	05/08/2021 09:03	File folder	
OpenOffice 4.1.9 (fr) Installation Files	03/05/2021 10:42	File folder	
VM	20/04/2021 11:17	File folder	
domains.txt	26/05/2021 14:43	Text Document	2 KB
ftp.txt	30/04/2021 15:07	Text Document	1 KB
shadow.txt	11/05/2021 10:35	Text Document	3 KB
techniques - Copy.txt	29/09/2021 10:31	Text Document	1 KB
techniques.txt	04/10/2021 09:31	Text Document	1 KB
techniques1.txt	23/09/2021 13:03	Text Document	20 KB
techniques2.txt	29/09/2021 11:55	Text Document	2 KB
test_overwrite.txt	24/09/2021 16:39	Text Document	1 KB
xss_ssti.txt	19/05/2021 10:36	Text Document	1 KB

File name: techniques.txt

Text (*.txt)

Fig. 17: Selecting techniques.txt

4. File format to add multiple techniques.

   A file used to add multiple techniques should be a .txt file with one technique per line. (Empty lines containing only a line break will be ignored)

   File example (if the selected type to add techniques is *name*):

```
Launch Daemon
Launchctl
```

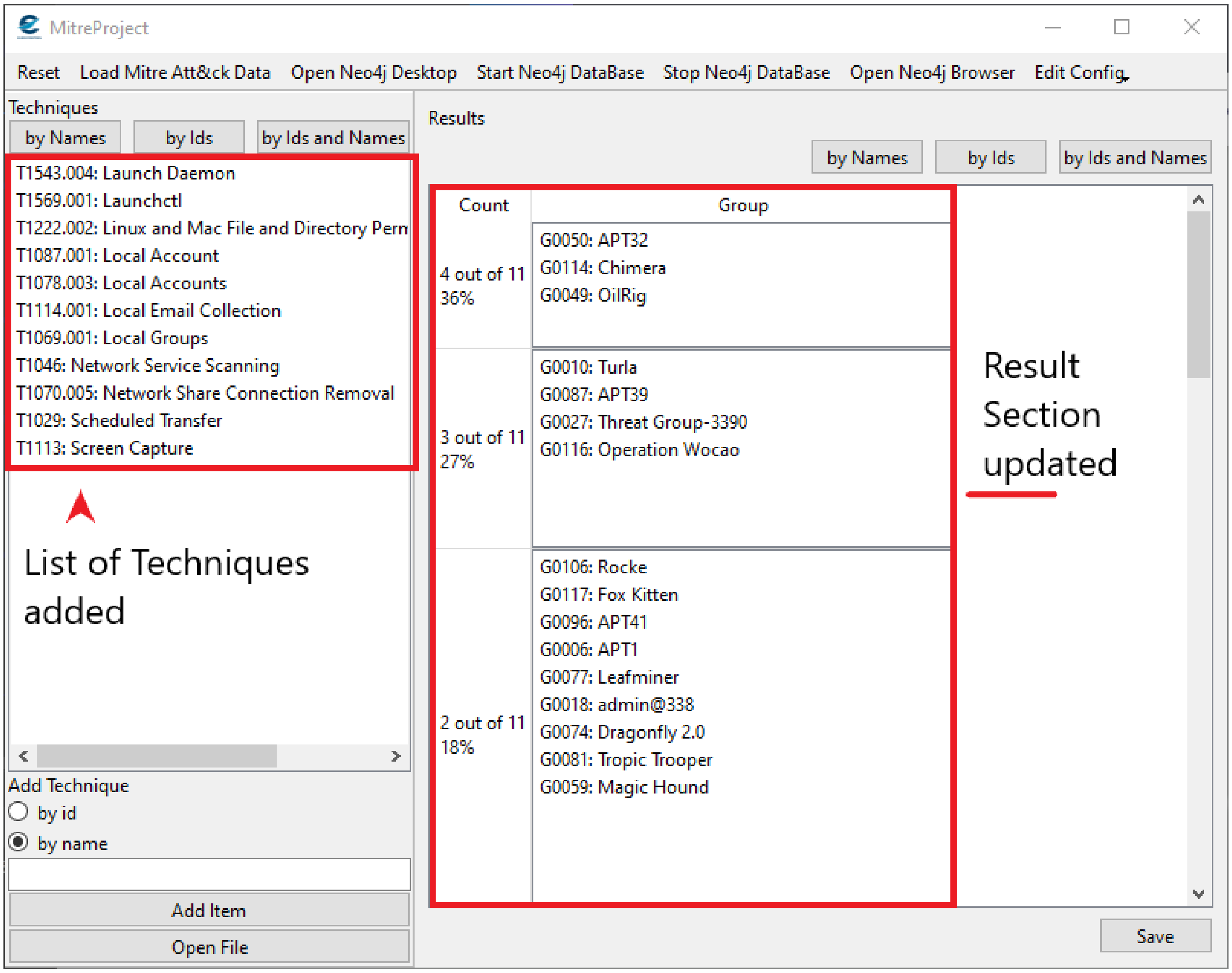
(continues on next page)

(continued from previous page)

```
Linux and Mac File and Directory Permissions Modification
Local Account
Local Accounts
Local Email Collection
Local Groups
Network Service Scanning
Network Share Connection Removal
Scheduled Transfer
Screen Capture
```

5. Result.

   New Techniques are added to the list of techniques and the result section is automatically updated.



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

List of Techniques added

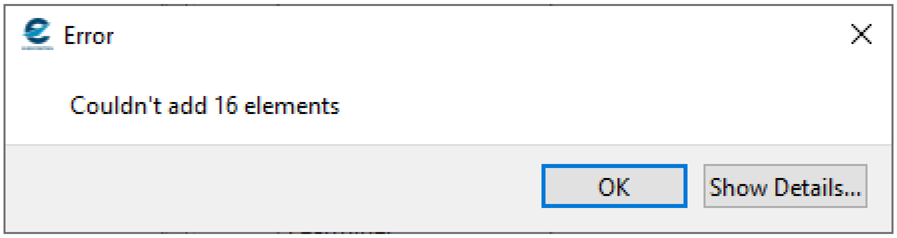
Count	Group
4 out of 11 36%	G0050: APT32 G0114: Chimera G0049: OilRig
3 out of 11 27%	G0010: Turla G0087: APT39 G0027: Threat Group-3390 G0116: Operation Wocao
2 out of 11 18%	G0106: Rocke G0117: Fox Kitten G0096: APT41 G0006: APT1 G0077: Leafminer G0018: admin@338 G0074: Dragonfly 2.0 G0081: Tropic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

Result Section updated

Fig. 18: New techniques are added to the list view and the Result Section is updated

6. Errors that might occur.

   If some or all the techniques of the file can not be added to the list a new window will appear.

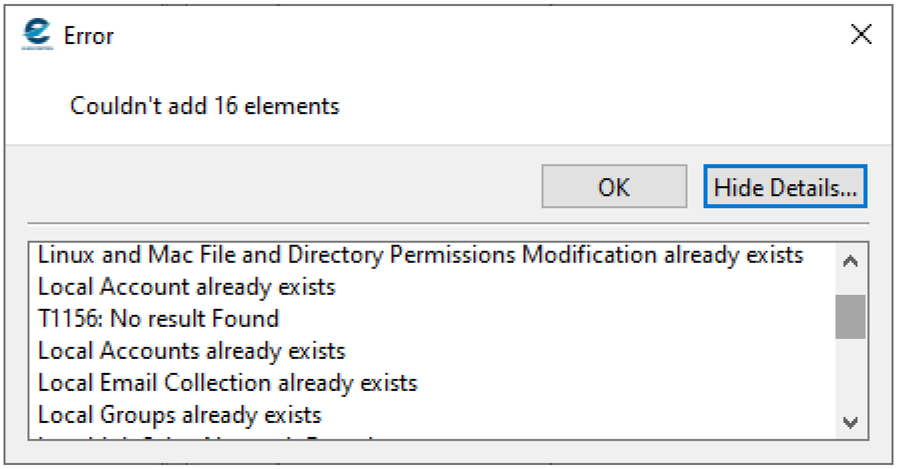


Error

Couldn't add 16 elements

Fig. 19: This window is displayed because 16 techniques can not be added to the technique list

By clicking *Show Details*, the list of all techniques that can not be added will be displayed with the reason it failed.



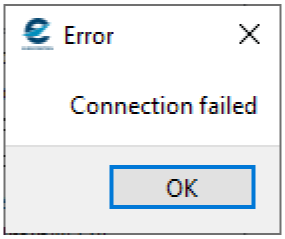
Error

Couldn't add 16 elements

Linux and Mac File and Directory Permissions Modification already exists
Local Account already exists
T1156: No result Found
Local Accounts already exists
Local Email Collection already exists
Local Groups already exists

Fig. 20: In this example, *T1156* was not added because no result was found in the database and *Local Accounts* was not added because it is already in the list.

If none of the technique were added because AFiT can not connect with Neo4j Graph, a window will be displayed with the label *Connection failed*.



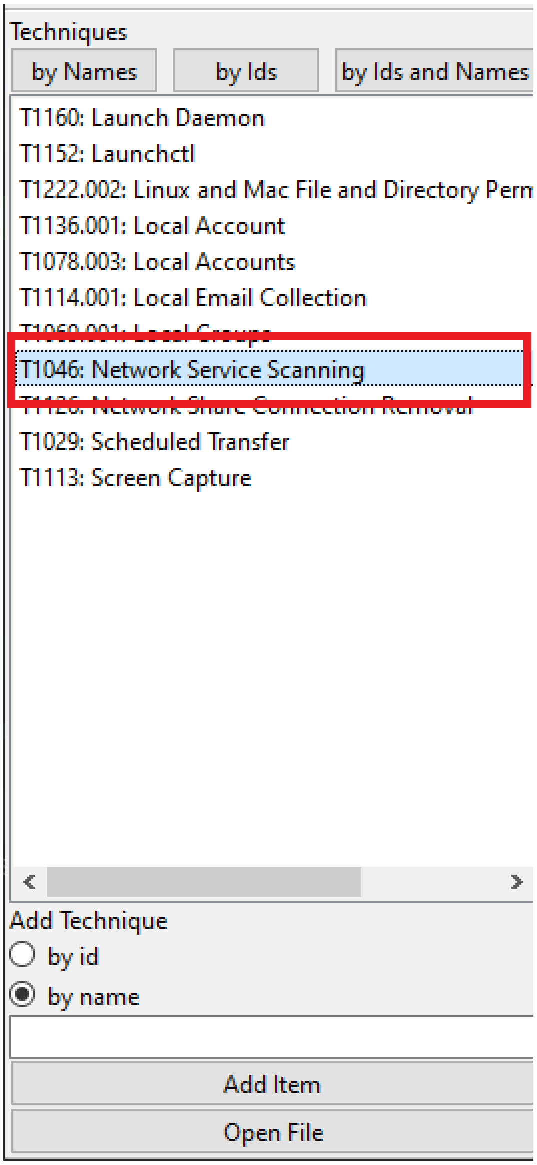
Error

Connection failed

Fig. 21: This window will be displayed if AFiT can not connect with Neo4j Graph. This might occur if the database is not active.

3.3 Techniques Options

Select one or more technique in the table view.



T1160: Launch Daemon
T1152: Launchctl
T1222.002: Linux and Mac File and Directory Pern
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

Add Technique
○ by id
● by name

Fig. 22: Selecting Network Service Scanning

Click right to display the technique options.

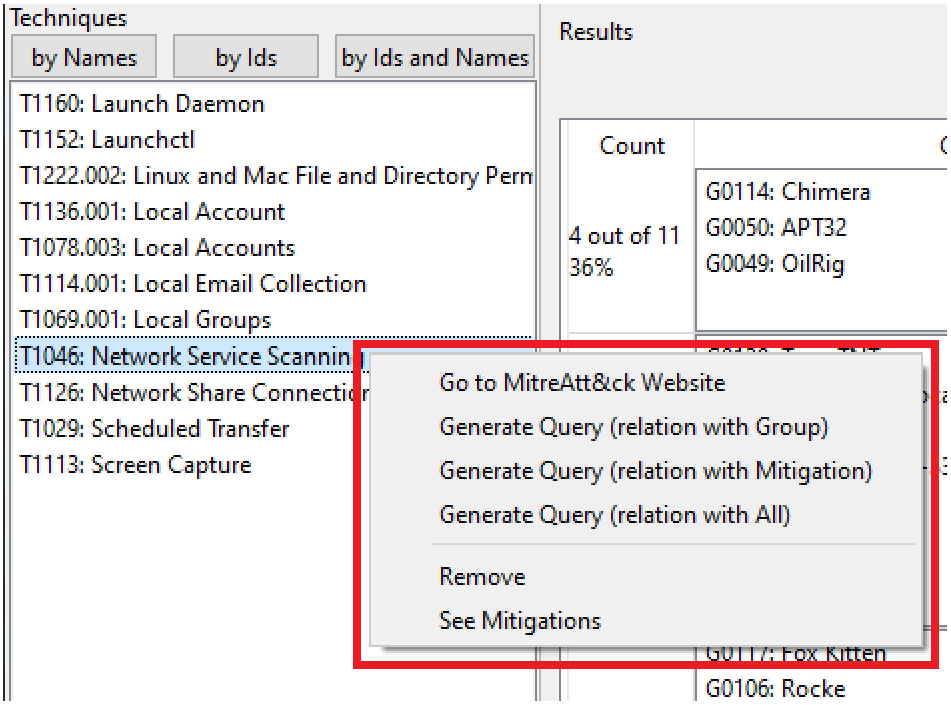
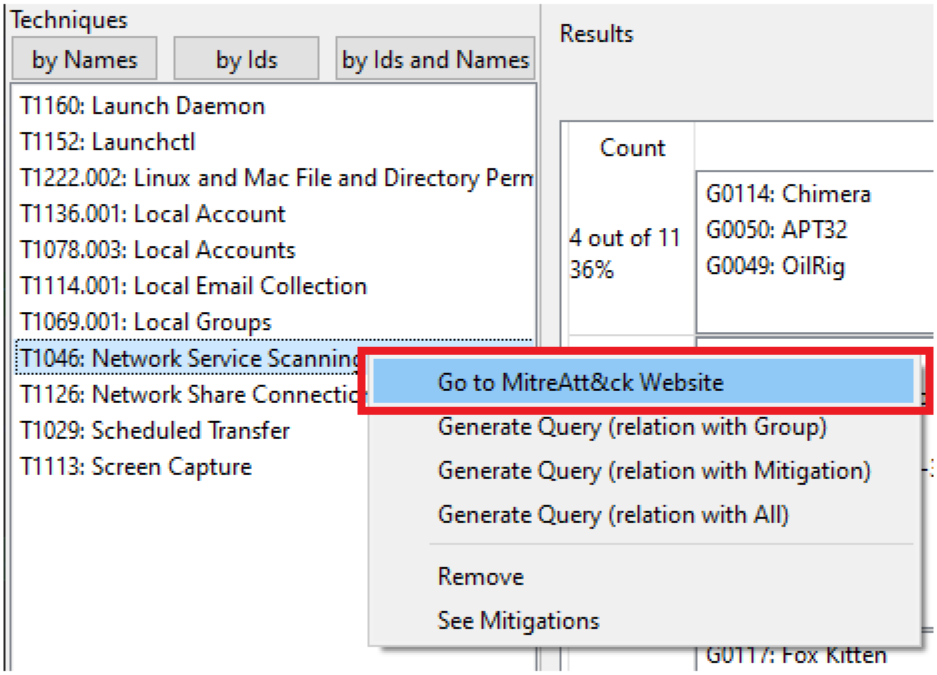

Techniques
by Names
by Ids
by Ids and Names
T1160: Launch Daemon
T1152: Launchctl
T1222.002: Linux and Mac File and Directory Perm
T1136.001: Local Account
T1078.003: Local Accounts
T1114.001: Local Email Collection
T1069.001: Local Groups
T1046: Network Service Scannin
T1126: Network Share Connectio
T1029: Scheduled Transfer
T1113: Screen Capture
Results
Count
4 out of 11
36%
G0114: Chimera
G0050: APT32
G0049: OilRig
Go to MitreAtt&ck Website
Generate Query (relation with Group)
Generate Query (relation with Mitigation)
Generate Query (relation with All)
Remove
See Mitigations
G0117: Fox Kitten
G0106: Rocke

Fig. 23: Technique Options

1. *Go to Mitre Att&ck Website*
2. *Generate Query*
3. *Remove*
4. *See Mitigation*

3.4 Go to Mitre Att&ck Website

This option is a link to the corresponding page of Mitre Attack Website.

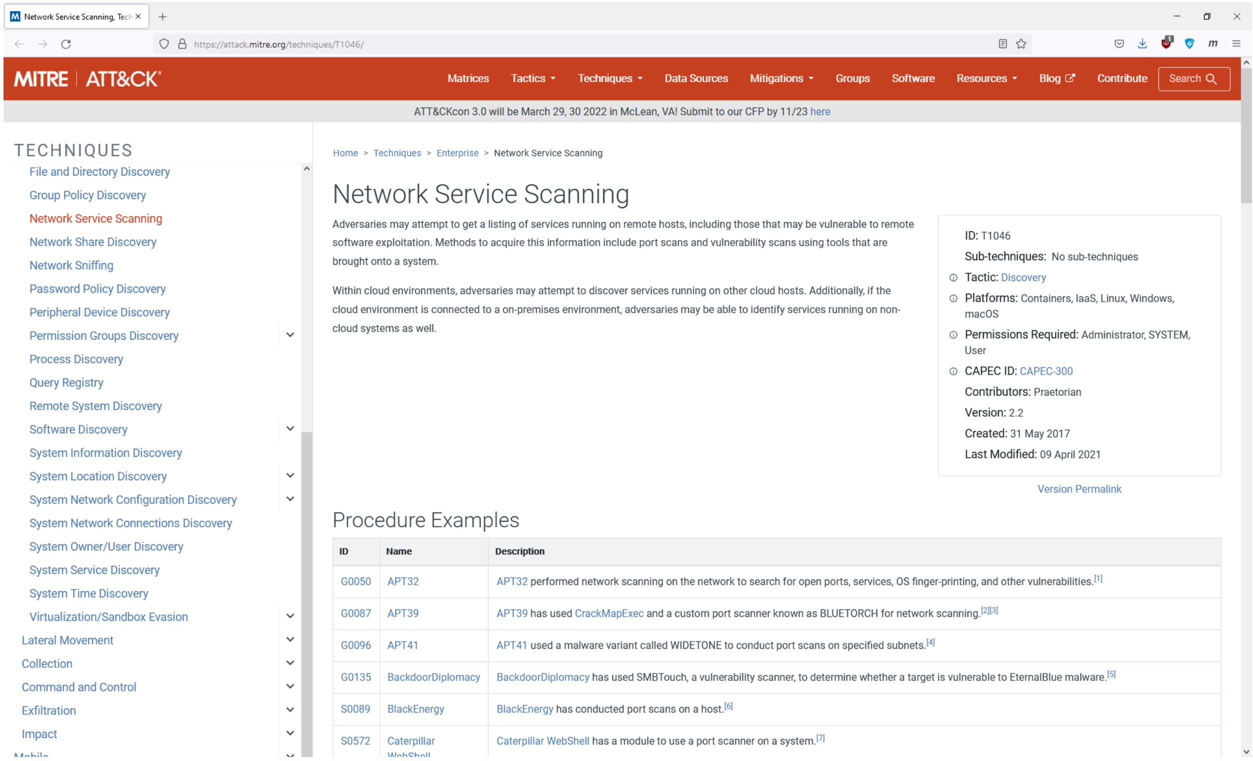

Techniques
by Names
by Ids
by Ids and Names
Results
Count
Go to MitreAtt&ck Website
Generate Query (relation with Group)
Generate Query (relation with Mitigation)
Generate Query (relation with All)
Remove
See Mitigations

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 Connectic
T1029: Scheduled Transfer
T1113: Screen Capture

4 out of 11
36%

G0114: Chimera
G0050: APT32
G0049: OilRig
G0117: Fox Kitten

Fig. 24: The option `Go to MitreAtt&ck Website` is a link to the Network Service Scanning's page of Mitre Att&ck Website.


Network Service Scanning, Tech
https://attack.mitre.org/techniques/T1046/
MITRE | ATT&CK
Matrices
Tactics
Techniques
Data Sources
Mitigations
Groups
Software
Resources
Blog
Contribute
Search
TECHNIQUES
File and Directory Discovery
Group Policy Discovery
Network Service Scanning
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery
Process Discovery
Query Registry
Remote System Discovery
Software Discovery
System Information Discovery
System Location Discovery
System Network Configuration Discovery
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery
Virtualization/Sandbox Evasion
Lateral Movement
Collection
Command and Control
Exfiltration
Impact
Mobile
Home > Techniques > Enterprise > Network Service Scanning
Version Permalink

ATT&CKcon 3.0 will be March 29, 30 2022 in McLean, VA! Submit to our CFP by 11/23 here

Network Service Scanning

Adversaries may attempt to get a listing of services running on remote hosts, including those that may be vulnerable to remote software exploitation. Methods to acquire this information include port scans and vulnerability scans using tools that are brought onto a system.

Within cloud environments, adversaries may attempt to discover services running on other cloud hosts. Additionally, if the cloud environment is connected to a on-premises environment, adversaries may be able to identify services running on non-cloud systems as well.

ID: T1046
Sub-techniques: No sub-techniques
Tactic: Discovery
Platforms: Containers, IaaS, Linux, Windows, macOS
Permissions Required: Administrator, SYSTEM, User
CAPEC ID: CAPEC-300
Contributors: Praetorian
Version: 2.2
Created: 31 May 2017
Last Modified: 09 April 2021

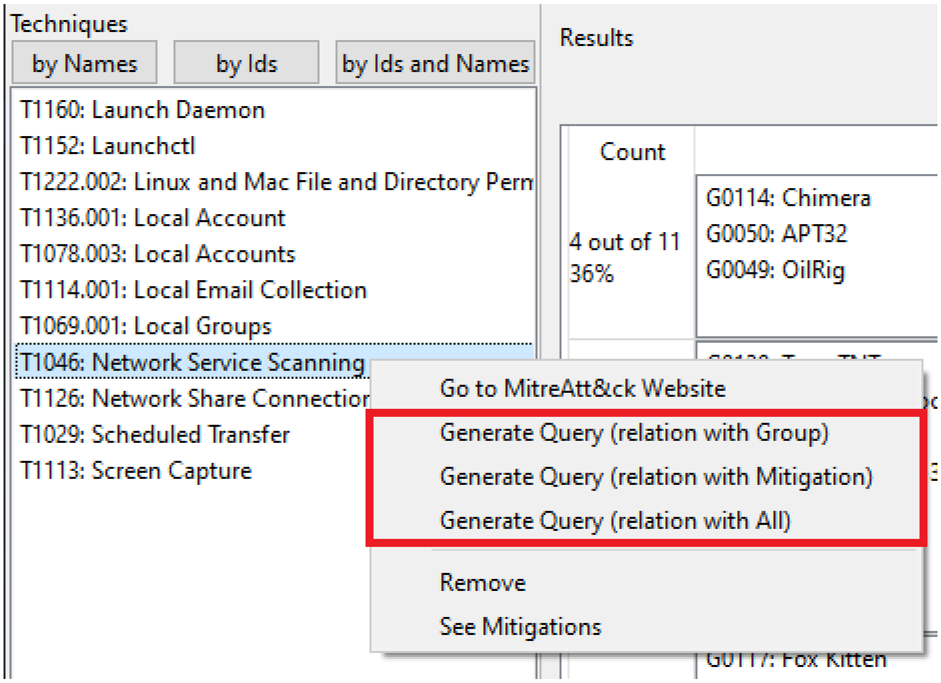
Procedure Examples

ID	Name	Description
G0050	APT32	APT32 performed network scanning on the network to search for open ports, services, OS finger-printing, and other vulnerabilities.[1]
G0087	APT39	APT39 has used CrackMapExec and a custom port scanner known as BLUETORCH for network scanning.[2][3]
G0096	APT41	APT41 used a malware variant called WIDETONE to conduct port scans on specified subnets.[4]
G0135	BackdoorDiplomacy	BackdoorDiplomacy has used SMBTouch, a vulnerability scanner, to determine whether a target is vulnerable to EternalBlue malware.[5]
S0089	BlackEnergy	BlackEnergy has conducted port scans on a host.[6]
S0572	Caterpillar WebShell	Caterpillar WebShell has a module to use a port scanner on a system.[7]

Fig. 25: Network Service Scanning details in Mitre Att&ck Website

3.5 Generate Query

The options Generate Query create a query to get the data directly from Neo4j. The Query is automatically copied and can be used, for example, with Neo4j browser.


Techniques
by Names
by Ids
by Ids and Names
Results
Count
Go to MitreAtt&ck Website
Generate Query (relation with Group)
Generate Query (relation with Mitigation)
Generate Query (relation with All)
Remove
See Mitigations

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

4 out of 11
36%

G0114: Chimera
G0050: APT32
G0049: OilRig

G0117: Fox Kitten

Fig. 26: Generate Query Options for Network Service Scanning

3.5.1 Relation with Group

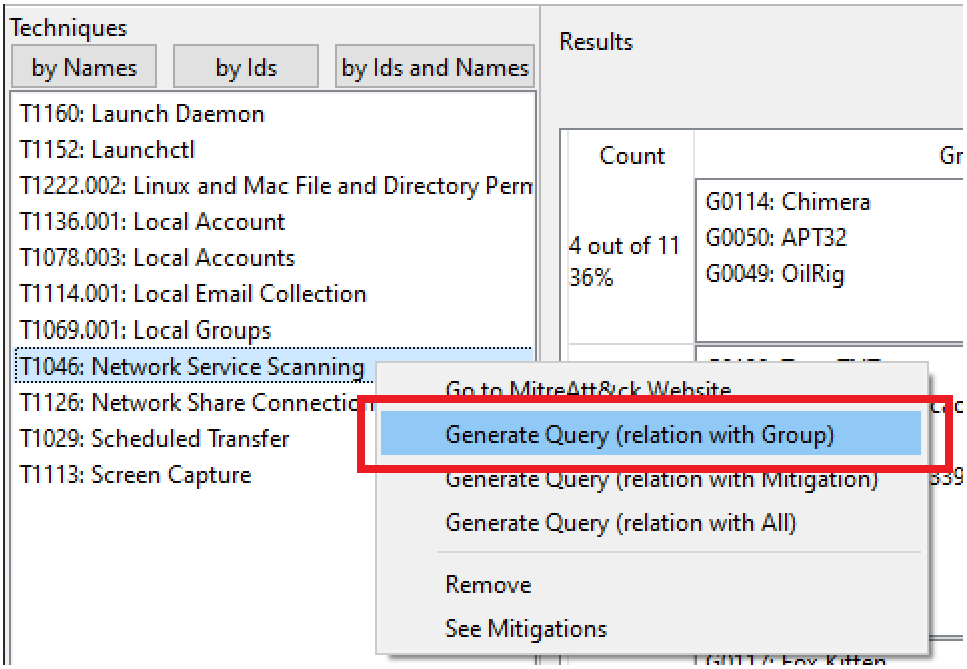

Techniques
by Names
by Ids
by Ids and Names
T1160: Launch Daemon
T1152: Launchctl
T1222.002: Linux and Mac File and Directory Perm
T1136.001: Local Account
T1078.003: Local Accounts
T1114.001: Local Email Collection
T1069.001: Local Groups
T1046: Network Service Scanning
T1126: Network Share Connectio
T1029: Scheduled Transfer
T1113: Screen Capture
Results
Count
Gr
4 out of 11
36%
G0114: Chimera
G0050: APT32
G0049: OilRig
Go to MitreAtt&ck Website
Generate Query (relation with Group)
Generate Query (relation with Mitigation)
Generate Query (relation with All)
Remove
See Mitigations
G0117: Fox Kitten

Fig. 27: Generate a query for Network Service Scanning

This query gets all the group related with one or more technique.

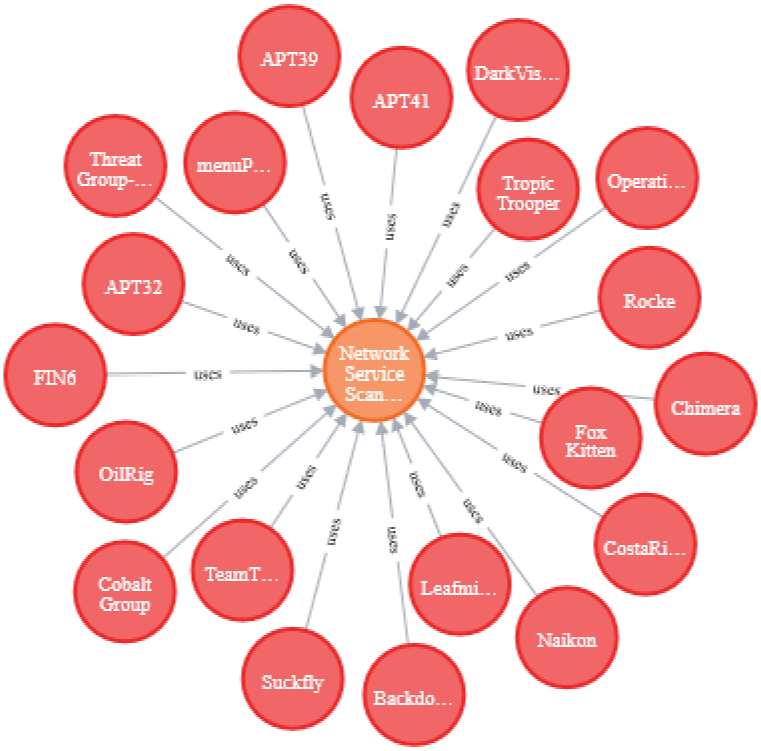
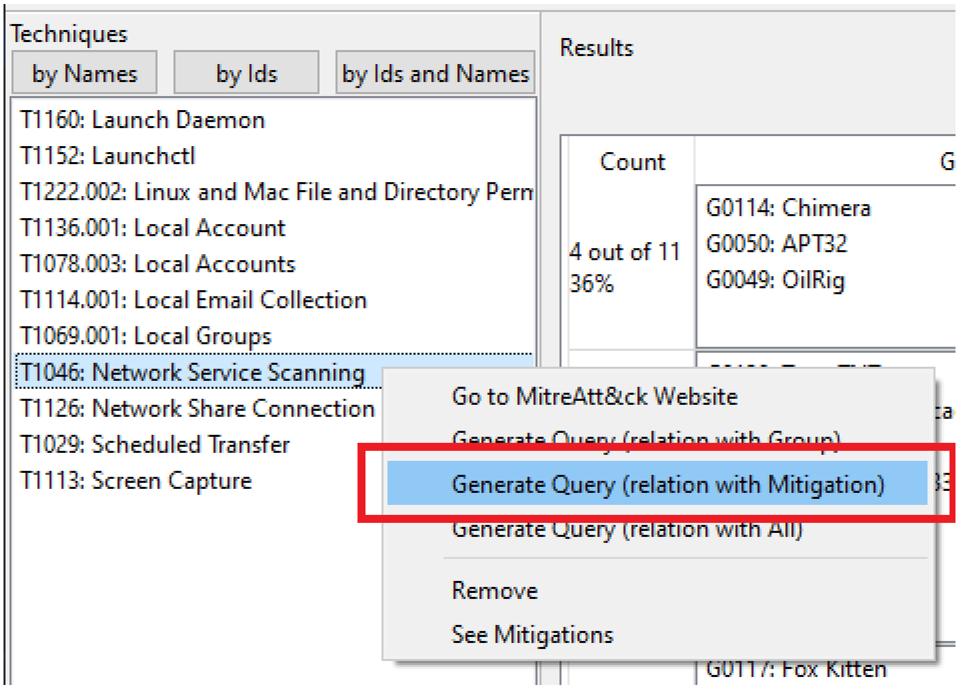


Fig. 28: Results of the query in Neo4j

3.5.2 Relation with Mitigation


Techniques
by Names
by Ids
by Ids and Names
Results
Go to MitreAtt&ck Website
Generate Query (relation with Group)
Generate Query (relation with Mitigation)
Generate Query (relation with All)
Remove
See Mitigations

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
T1029: Scheduled Transfer
T1113: Screen Capture

Count	G
4 out of 11 36%	G0114: Chimera G0050: APT32 G0049: OilRig
	G0117: Fox Kitten

Fig. 29: Generate a query for Network Service Scanning

This query gets all the mitigations related with one or more technique.

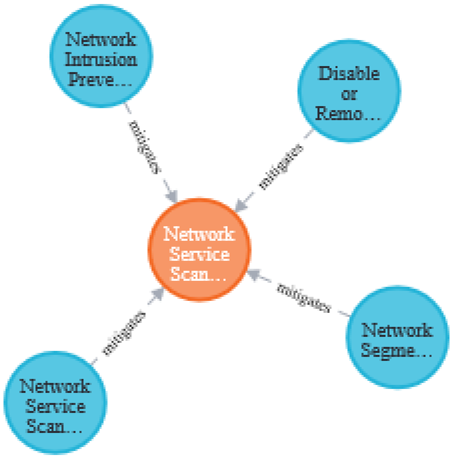
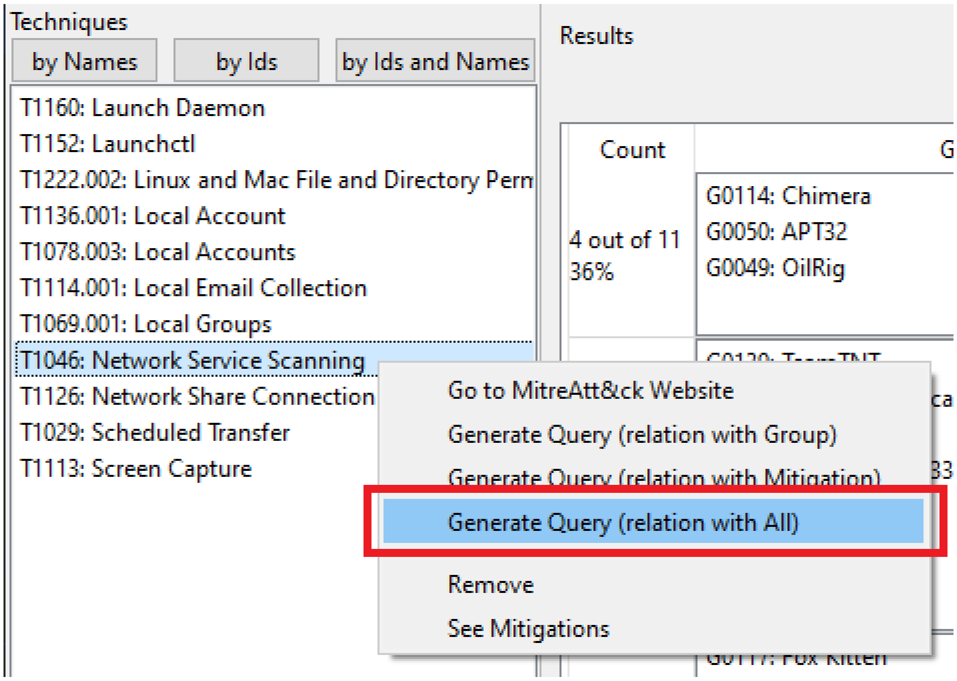


Fig. 30: Results of the query in Neo4j

3.5.3 Relation with All


Techniques
by Names
by Ids
by Ids and Names
Results
Go to MitreAtt&ck Website
Generate Query (relation with Group)
Generate Query (relation with Mitigation)
Generate Query (relation with All)
Remove
See Mitigations

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
T1029: Scheduled Transfer
T1113: Screen Capture

Count	G
4 out of 11 36%	G0114: Chimera G0050: APT32 G0049: OilRig
	G0139: TeamTNT … G0117: Fox Kitten

Fig. 31: Generate a query for Network Service Scanning

This query gets all the nodes related with one or more technique.

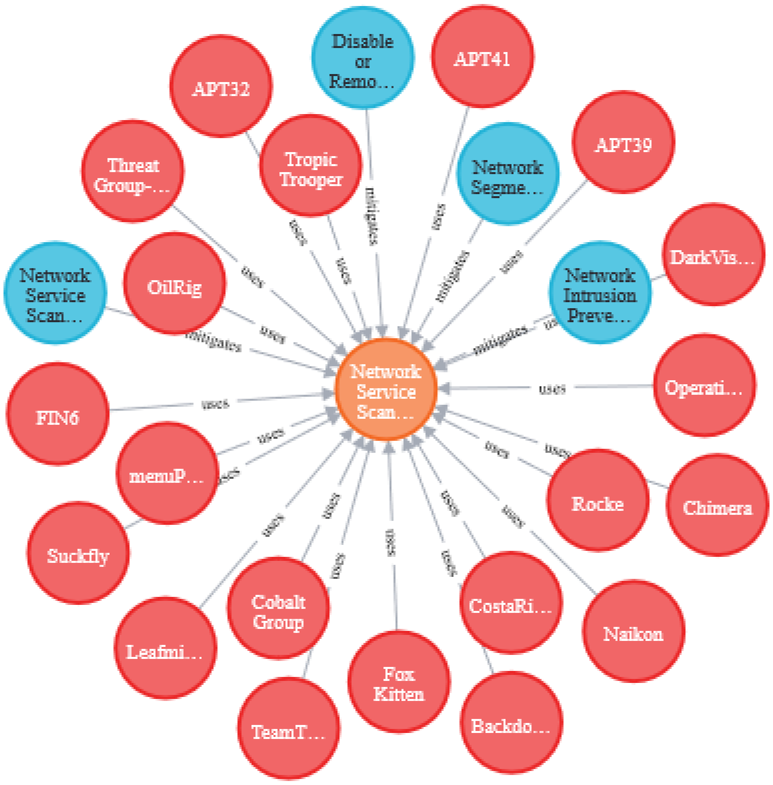


Fig. 32: Results of the query in Neo4j

3.6 Remove

This option removes the techniques selected. The remove option is displayed only if one technique is selected.

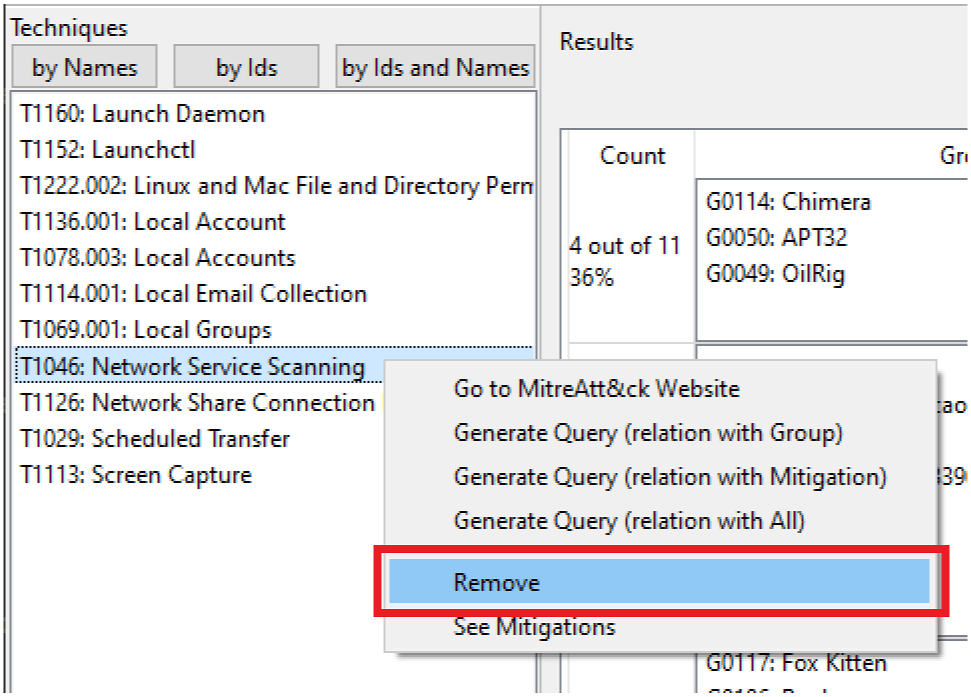
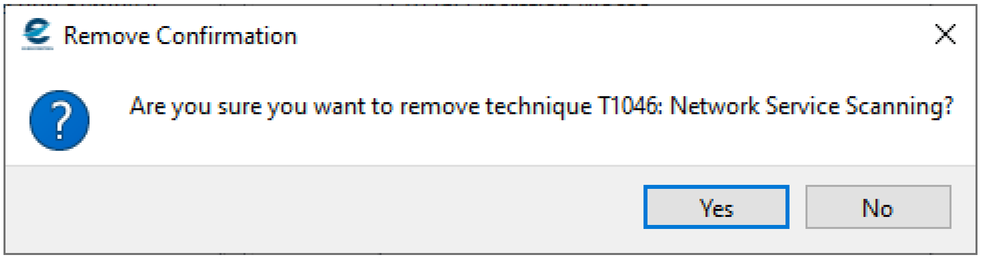
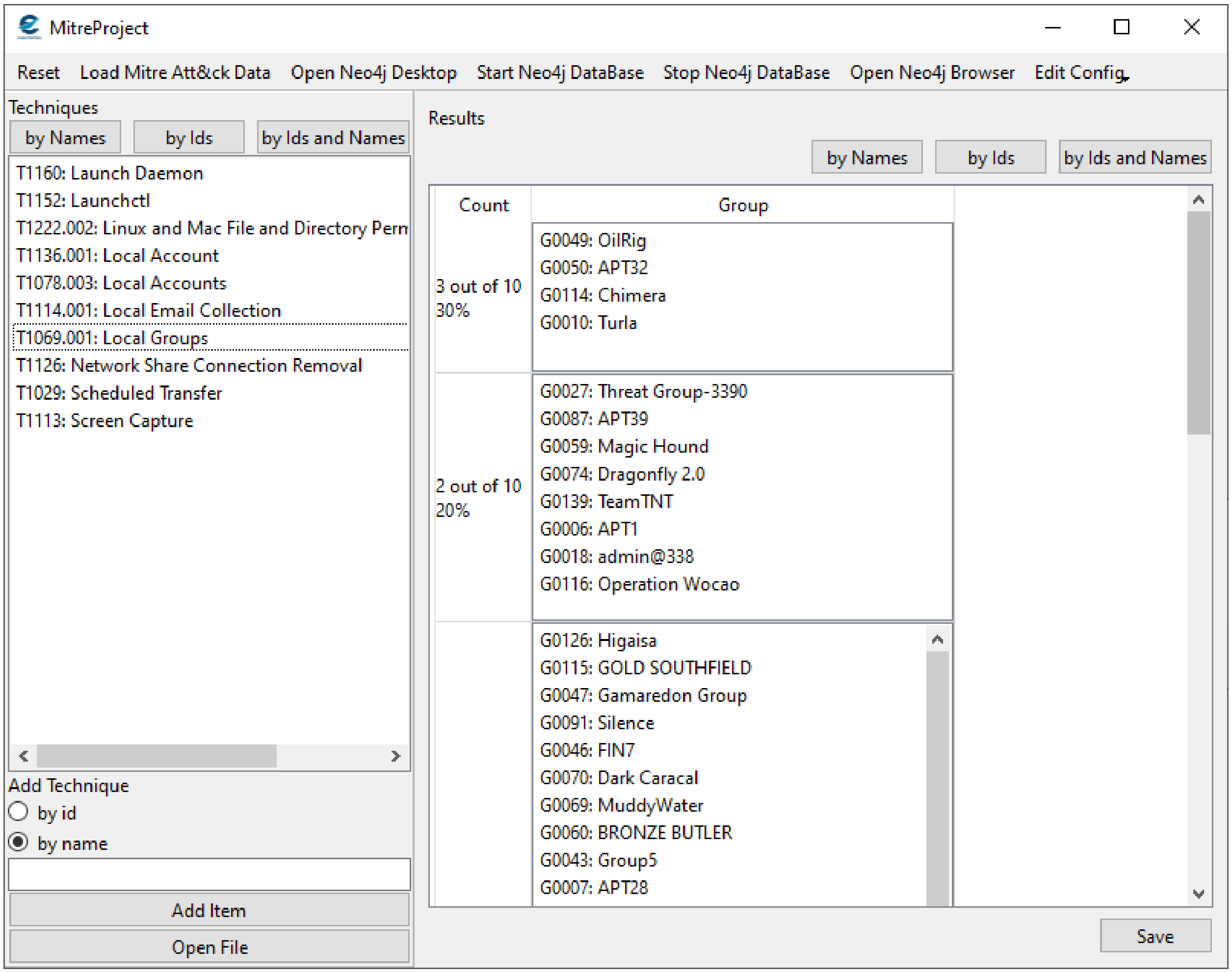

Techniques
by Names
by Ids
by Ids and Names
T1160: Launch Daemon
T1152: Launchctl
T1222.002: Linux and Mac File and Directory Perm
T1136.001: Local Account
T1078.003: Local Accounts
T1114.001: Local Email Collection
T1069.001: Local Groups
T1046: Network Service Scanning
T1126: Network Share Connection
T1029: Scheduled Transfer
T1113: Screen Capture
Results
Count
Gr
4 out of 11
36%
G0114: Chimera
G0050: APT32
G0049: OilRig
Go to MitreAtt&ck Website
Generate Query (relation with Group)
Generate Query (relation with Mitigation)
Generate Query (relation with All)
Remove
See Mitigations
G0117: Fox Kitten

Fig. 33: Remove option



Are you sure you want to remove technique T1046: Network Service Scanning?

Fig. 34: This message is displayed to confirm that the technique should be removed.



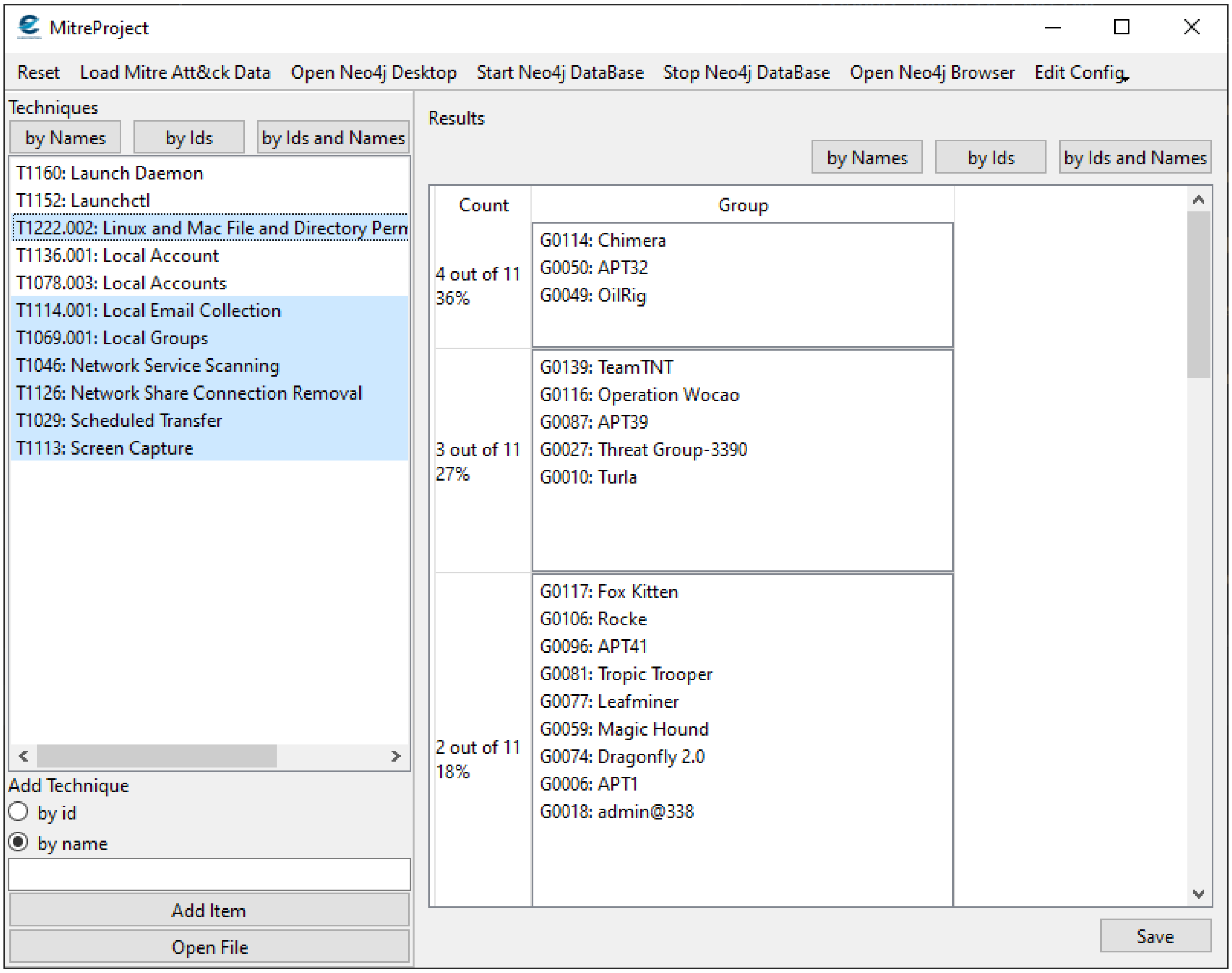
T1160: Launch Daemon
T1152: Launchctl
T1222.002: Linux and Mac File and Directory Perm
T1136.001: Local Account
T1078.003: Local Accounts
T1114.001: Local Email Collection
T1069.001: Local Groups
T1126: Network Share Connection Removal
T1029: Scheduled Transfer
T1113: Screen Capture

Count	Group
3 out of 10 30%	G0049: OilRig G0050: APT32 G0114: Chimera G0010: Turla
2 out of 10 20%	G0027: Threat Group-3390 G0087: APT39 G0059: Magic Hound G0074: Dragonfly 2.0 G0139: TeamTNT G0006: APT1 G0018: admin@338 G0116: Operation Wocao
	G0126: Higaisa G0115: GOLD SOUTHFIELD G0047: Gamaredon Group G0091: Silence G0046: FIN7 G0070: Dark Caracal G0069: MuddyWater G0060: BRONZE BUTLER G0043: Group5 G0007: APT28

Fig. 35: *Network Service Scanning* technique is removed and the results are updated.

3.7 See Mitigation

This option provides all the mitigations related to the selected techniques in a new window.



Techniques

- T1160: Launch Daemon
- T1152: Launchctl
- T1222.002: Linux and Mac File and Directory Pern
- 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

Add Technique

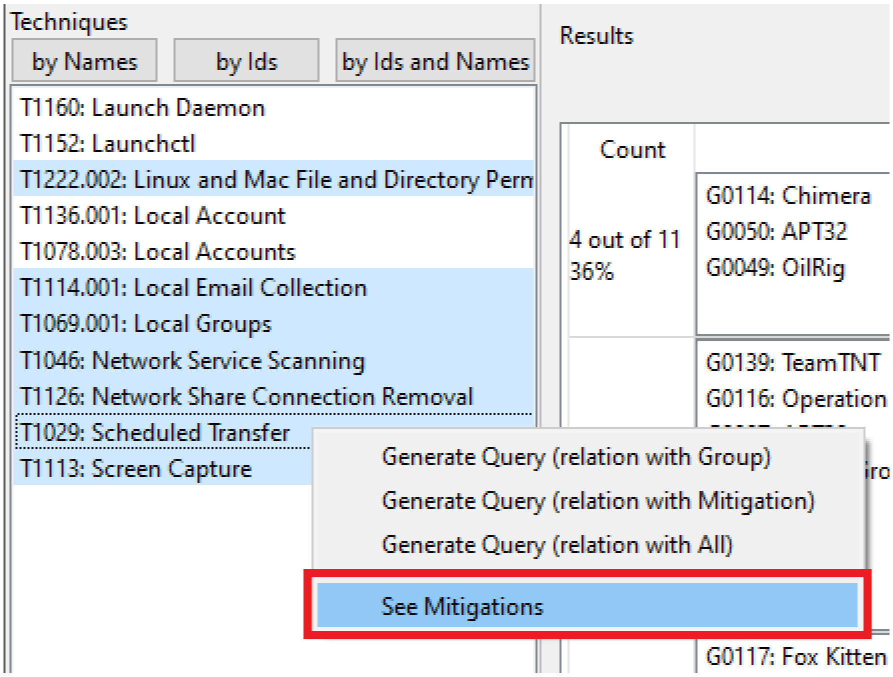
○ by id

● by name

Results

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

Fig. 36: Selecting techniques


Techniques
by Names
by Ids
by Ids and Names
Results
Count
Generate Query (relation with Group)
Generate Query (relation with Mitigation)
Generate Query (relation with All)
See Mitigations

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

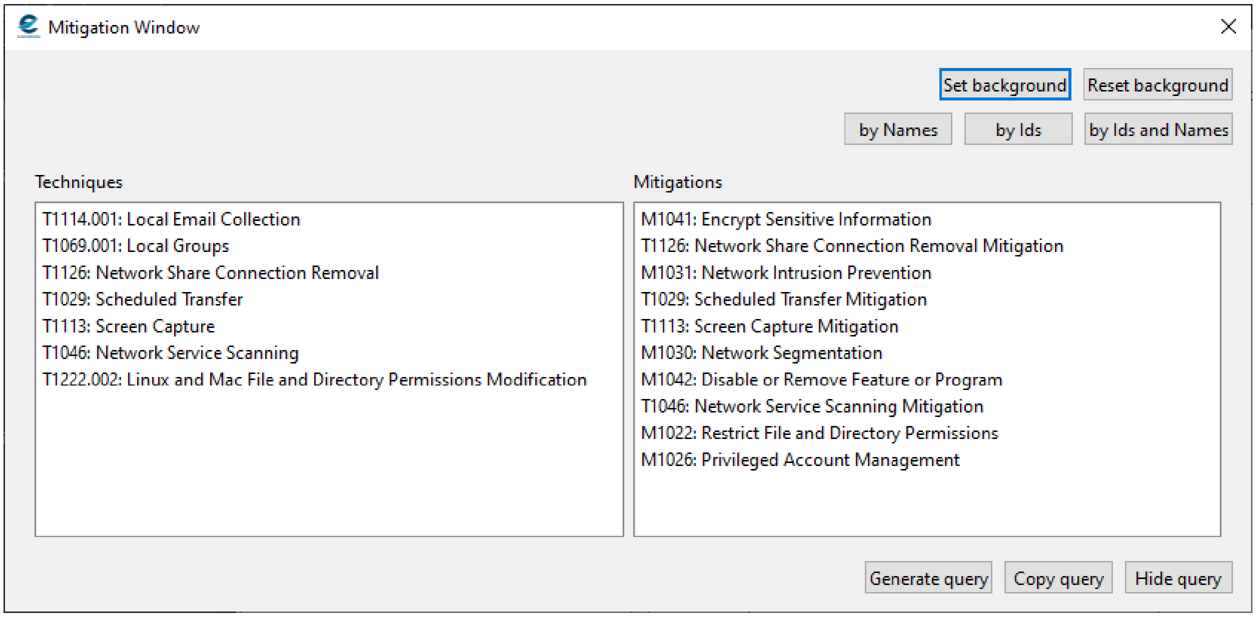
4 out of 11
36%

G0114: Chimera
G0050: APT32
G0049: OilRig

G0139: TeamTNT
G0116: Operation

G0117: Fox Kitten

Fig. 37: See mitigations option



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:

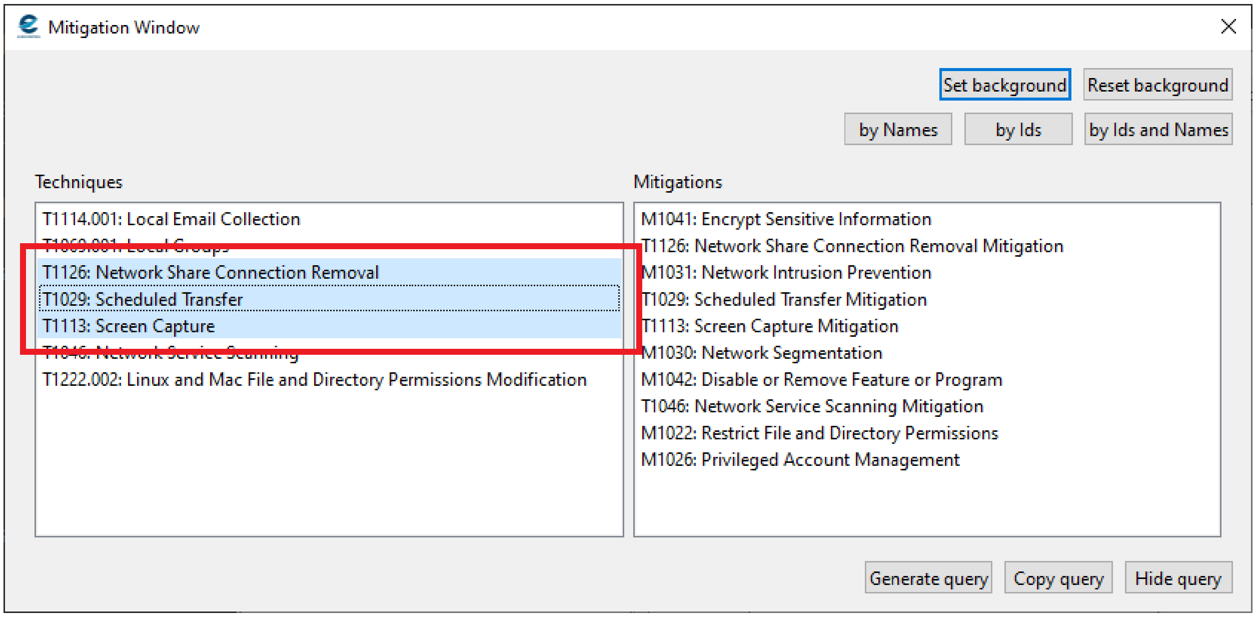
M1041: Encrypt Sensitive Information
T1126: Network Share Connection Removal Mitigation
M1031: Network Intrusion Prevention
T1029: Scheduled Transfer Mitigation
T1113: Screen Capture Mitigation
M1030: Network Segmentation
M1042: Disable or Remove Feature or Program
T1046: Network Service Scanning Mitigation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

Fig. 38: Mitigation Window

3.7.1 Set Background

This option is used to change the color of the background of the techniques and the mitigations in the *listviews*

1. Select one or more technique in the left list.



Techniques

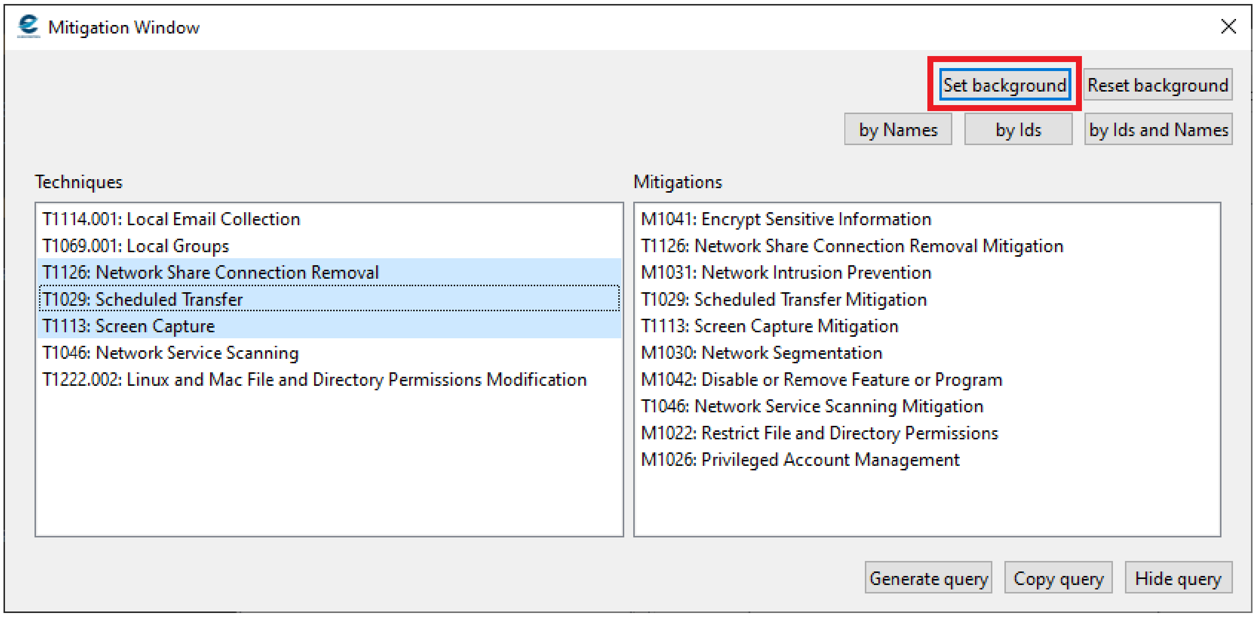
T1114.001: Local Email Collection
T1069.001: Local Groups
T1126: Network Share Connection Removal
T1029: Scheduled Transfer
T1113: Screen Capture
T1046: Network Service Scanning
T1222.002: Linux and Mac File and Directory Permissions Modification

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

Fig. 39: Selecting Network Share Connection Removal, Scheduled Transfer and Screen Capture

2. Click the option `Set background`.



Techniques

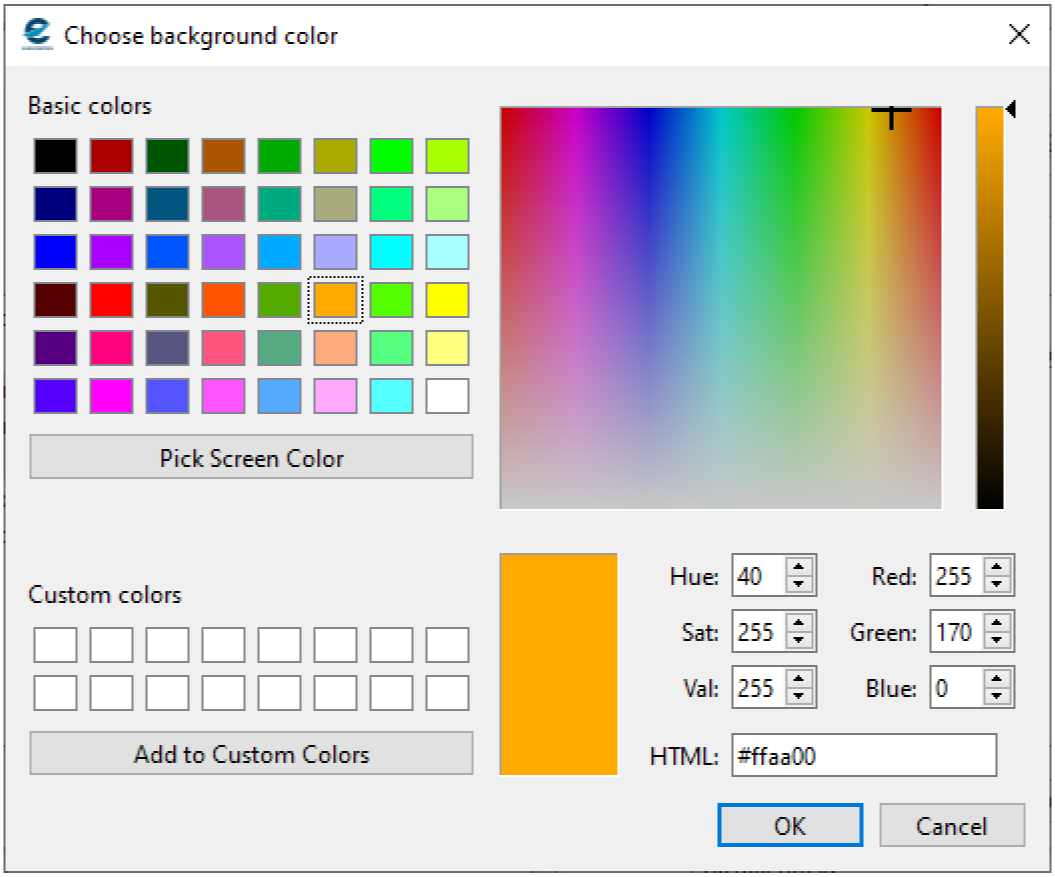
T1114.001: Local Email Collection
T1069.001: Local Groups
T1126: Network Share Connection Removal
T1029: Scheduled Transfer
T1113: Screen Capture
T1046: Network Service Scanning
T1222.002: Linux and Mac File and Directory Permissions Modification

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

Fig. 40: Set background button

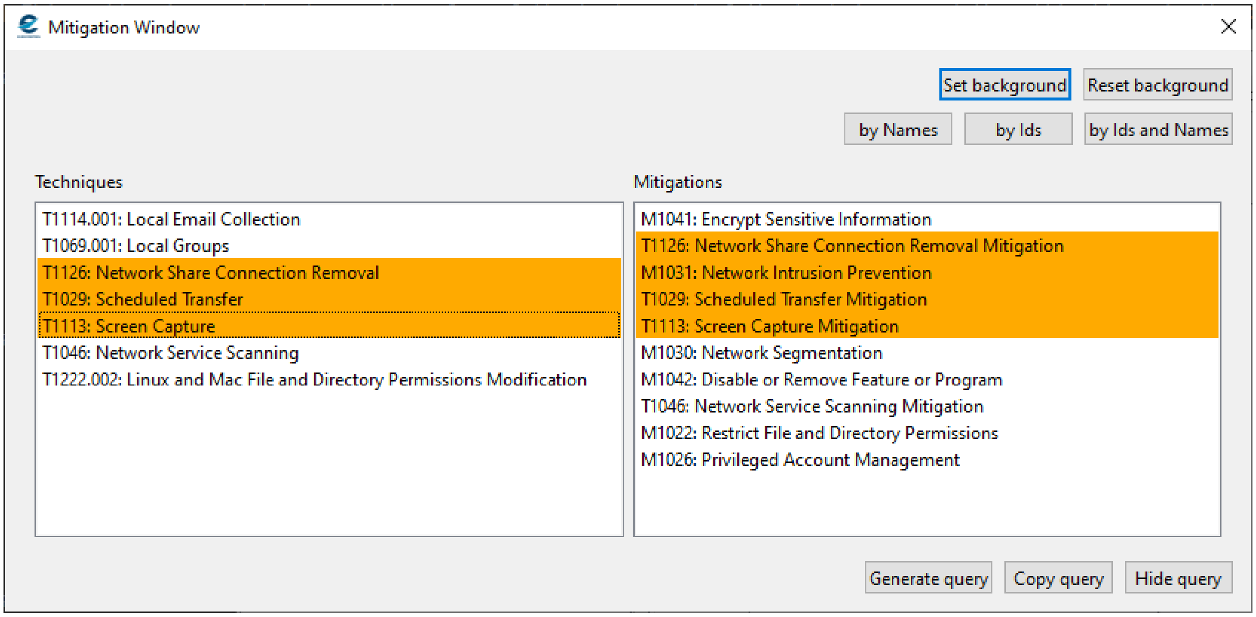
3. Select the color.



Hue: 40
Sat: 255
Val: 255
Red: 255
Green: 170
Blue: 0
HTML: #ffaa00

Fig. 41: Select the new color for the background

4. The techniques selected and their related mitigation have their background set to the chosen color.



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

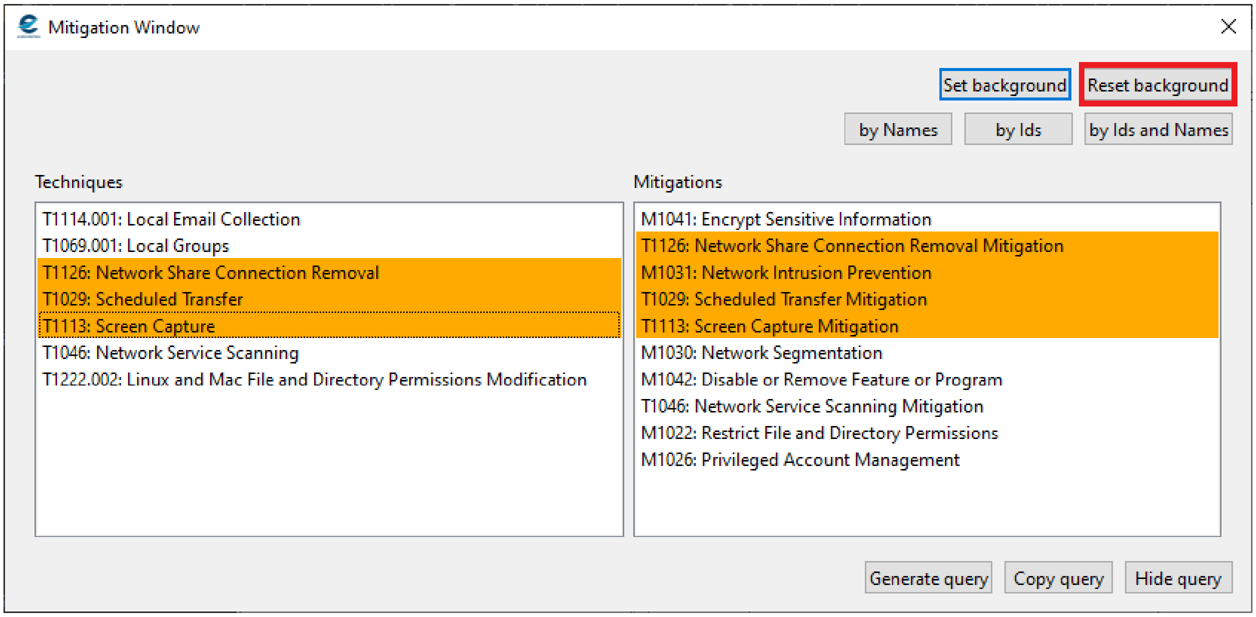
Mitigations

- 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

Fig. 42: The background of the techniques Network Share Connection Removal, Scheduled Transfer and Screen Capture and their related mitigation changed

3.7.2 Reset Background

This option reset the background color of all the items of the listviews to their original color.



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

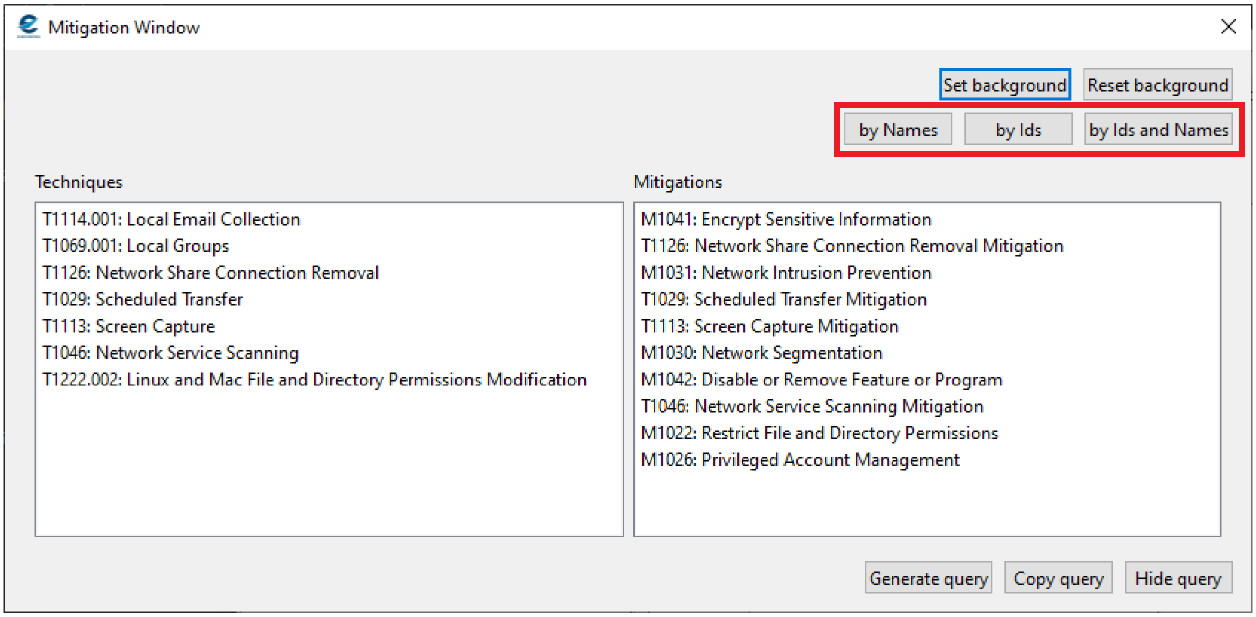
Mitigations

- 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

Fig. 43: Reset Background option

3.7.3 Display Options

You can choose how the techniques and mitigations will appear in the *listviews*.
There are three options: techniques can either be shown by name, by id or by id and name.



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

Fig. 44: Techniques Display Options

To see the techniques by their names, click the button `by Names`.

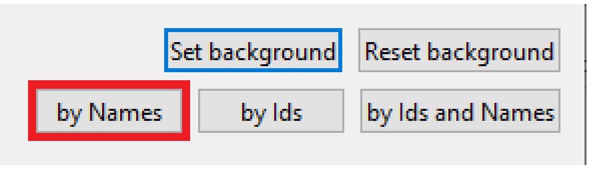


Fig. 45: This button allows to display techniques by their names

To see the techniques by their ids, click the button `by Ids`.

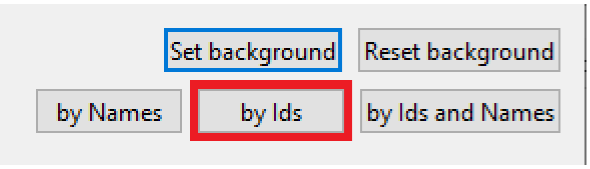


Fig. 46: This button allows to display techniques by their ids

To see the techniques by their ids and names, click the button `by Ids and Names`.

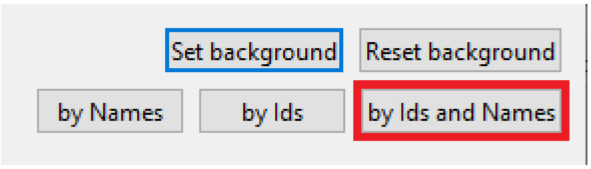
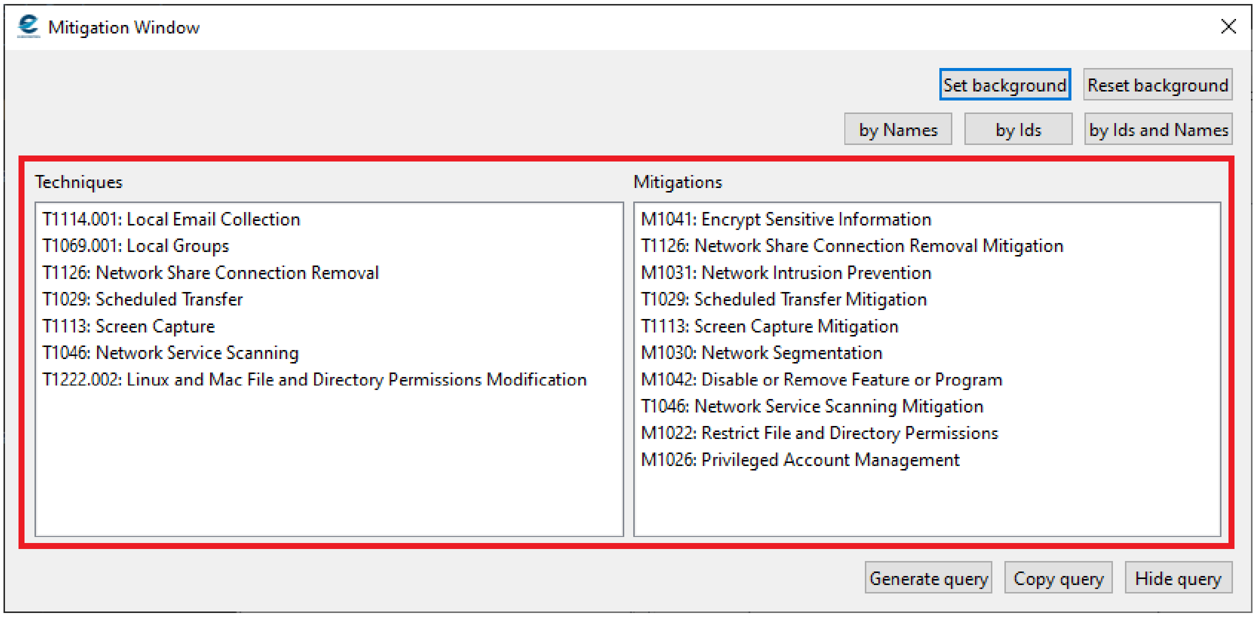


Fig. 47: This button allows to display techniques by their ids and names

3.7.4 ListViews

The listviews contain the techniques and their related mitigations



Techniques

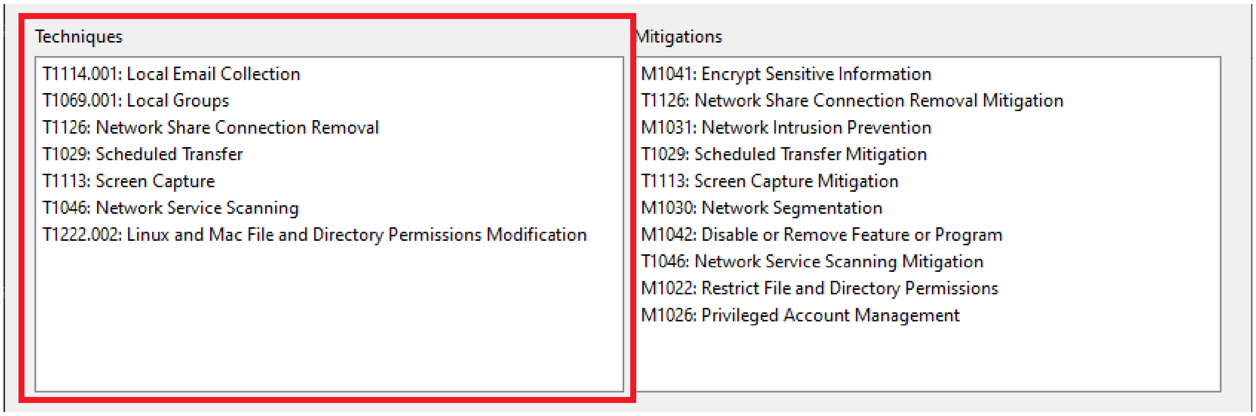
T1114.001: Local Email Collection
T1069.001: Local Groups
T1126: Network Share Connection Removal
T1029: Scheduled Transfer
T1113: Screen Capture
T1046: Network Service Scanning
T1222.002: Linux and Mac File and Directory Permissions Modification

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

Fig. 48: Listviews Area

The techniques are displayed in the left listview.



Techniques

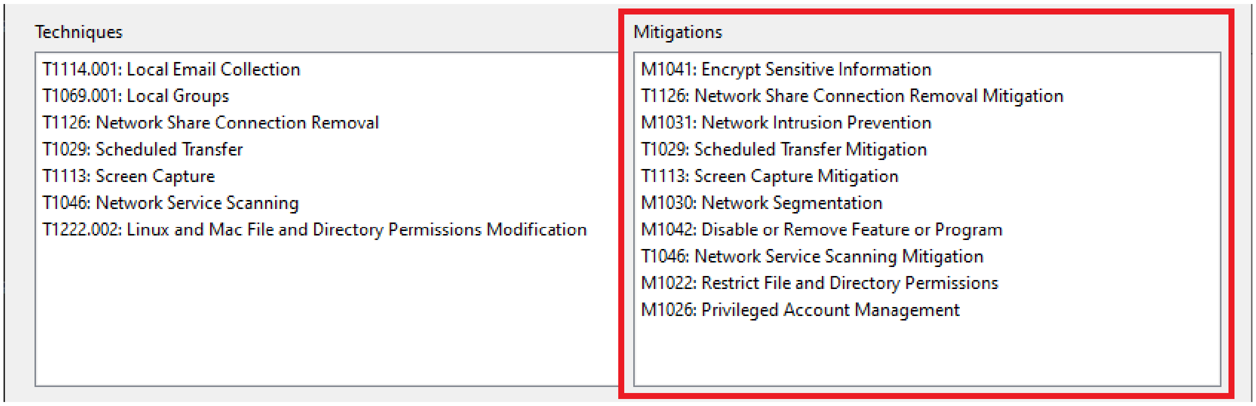
T1114.001: Local Email Collection
T1069.001: Local Groups
T1126: Network Share Connection Removal
T1029: Scheduled Transfer
T1113: Screen Capture
T1046: Network Service Scanning
T1222.002: Linux and Mac File and Directory Permissions Modification

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

Fig. 49: Technique Listview

The mitigations related with the techniques are displayed in the right listview.



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

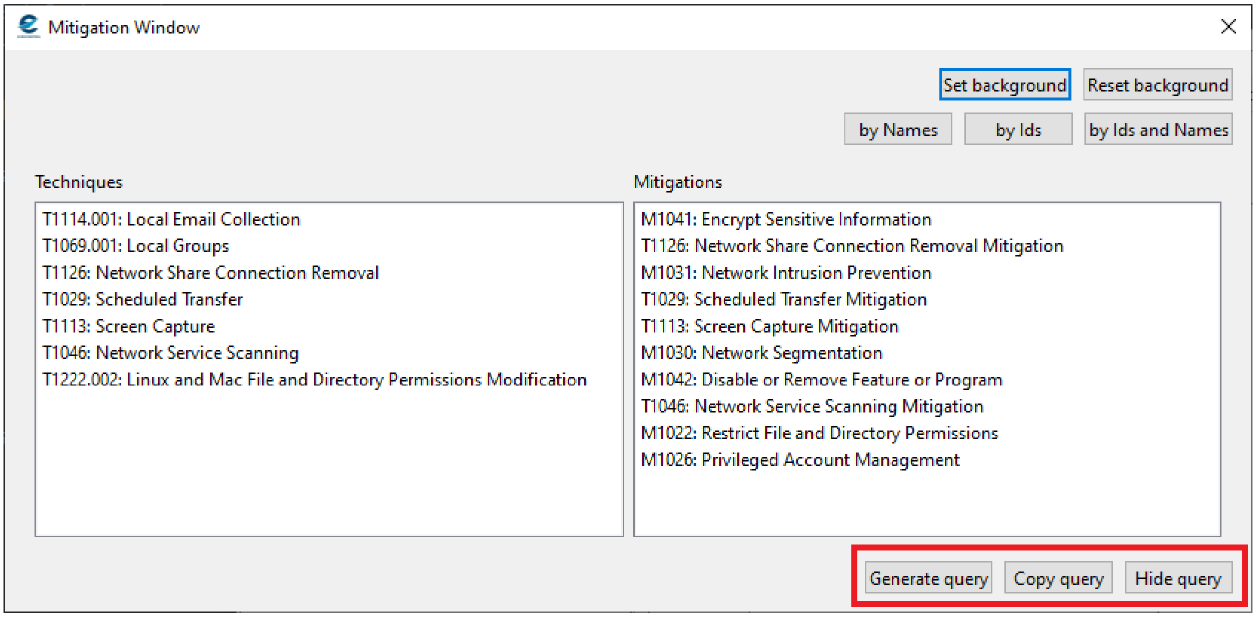
M1041: Encrypt Sensitive Information
T1126: Network Share Connection Removal Mitigation
M1031: Network Intrusion Prevention
T1029: Scheduled Transfer Mitigation
T1113: Screen Capture Mitigation
M1030: Network Segmentation
M1042: Disable or Remove Feature or Program
T1046: Network Service Scanning Mitigation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

Fig. 50: Mitigation Listview

Note: See *Techniques Options* for the options of both listviews.

3.7.5 Query Options

This area contains all the options concerning the query linking techniques and their mitigations.



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

Fig. 51: Query Options area

Generate Query

Generate the query for the selected techniques and display it by clicking the button `Generate query`. If no technique is selected, the query will be generated for all of them.

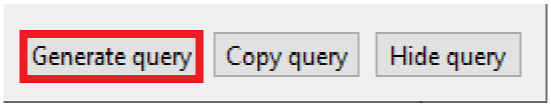
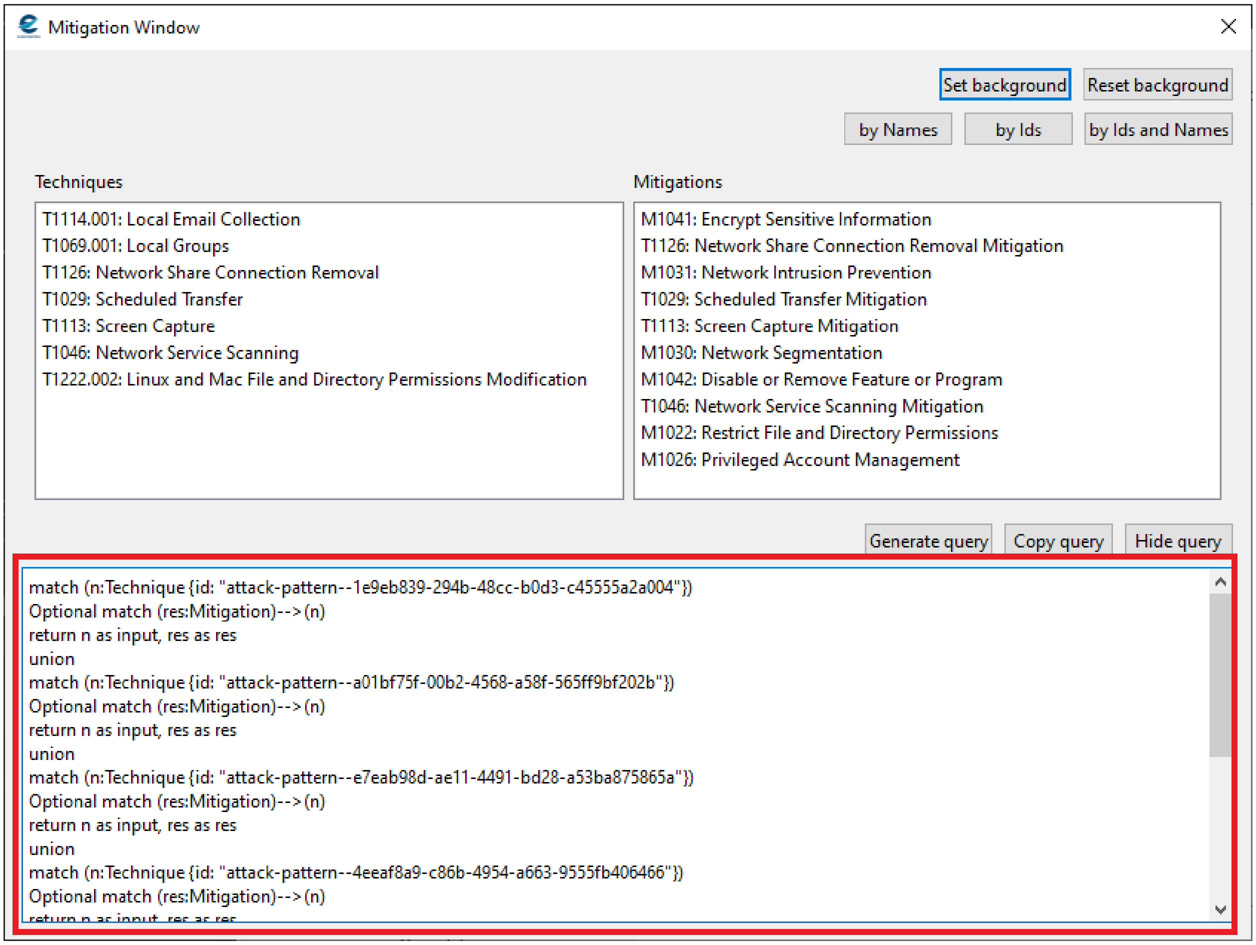


Fig. 52: Generate Query button



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

```
match (n:Technique {id: "attack-pattern--1e9eb839-294b-48cc-b0d3-c45555a2a004"})
Optional match (res:Mitigation)-->(n)
return n as input, res as res
union
match (n:Technique {id: "attack-pattern--a01bf75f-00b2-4568-a58f-565ff9bf202b"})
Optional match (res:Mitigation)-->(n)
return n as input, res as res
union
match (n:Technique {id: "attack-pattern--e7eab98d-ae11-4491-bd28-a53ba875865a"})
Optional match (res:Mitigation)-->(n)
return n as input, res as res
union
match (n:Technique {id: "attack-pattern--4eeaf8a9-c86b-4954-a663-9555fb406466"})
Optional match (res:Mitigation)-->(n)
return n as input, res as res
```

Fig. 53: The Query is created and displayed in a text area

Copy Query

This button copies the query displayed in the text area.

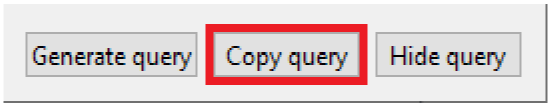


Fig. 54: Copy Query button

Hide Query

This option removes the query and hides the text area.

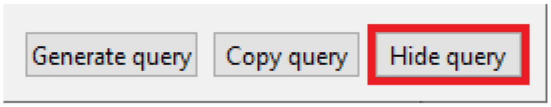


Fig. 55: Hide Query button

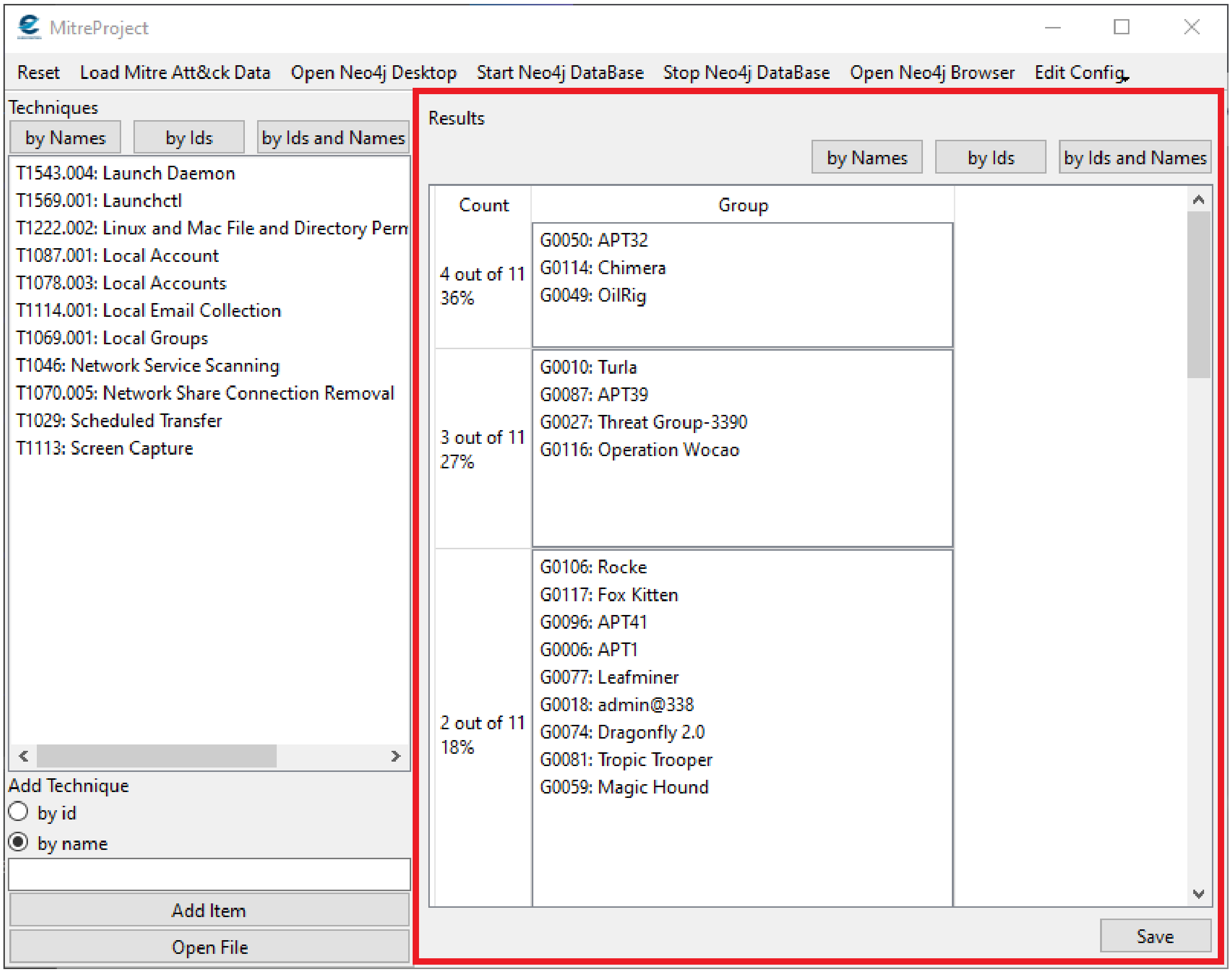
CHAPTER

FOUR

RESULTS SECTION

AFiT Results Section contains the information about the groups retrieved from the database based on the given techniques.

Hereunder, you will find information about all the areas of the Results section.



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

○ 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

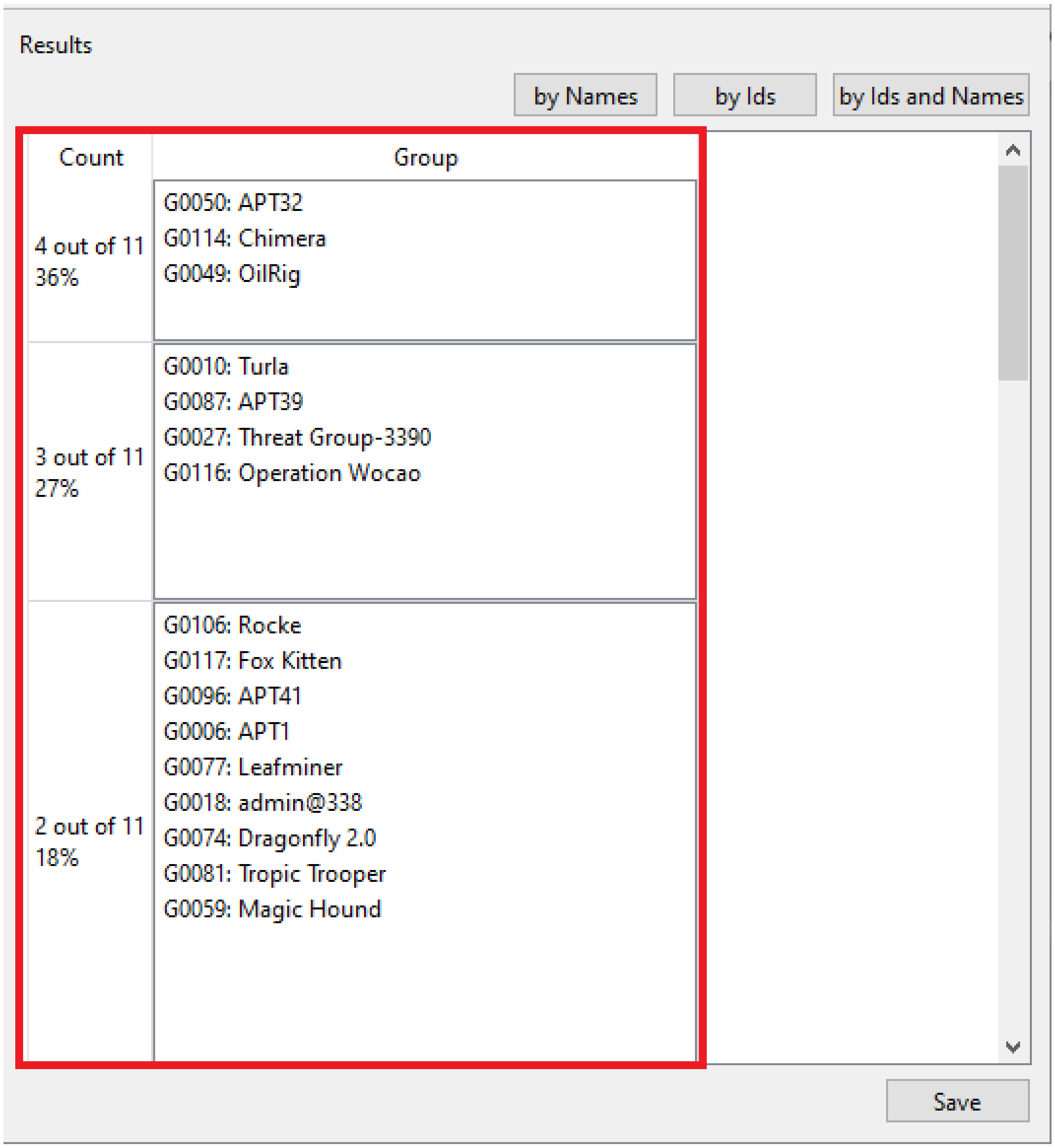
Fig. 1: AFiT's Results Section

4.1 Display

The following paragraphs describe how results are displayed.

4.1.1 Where are the results displayed ?

Results are displayed in a table view in the right part of the main window.

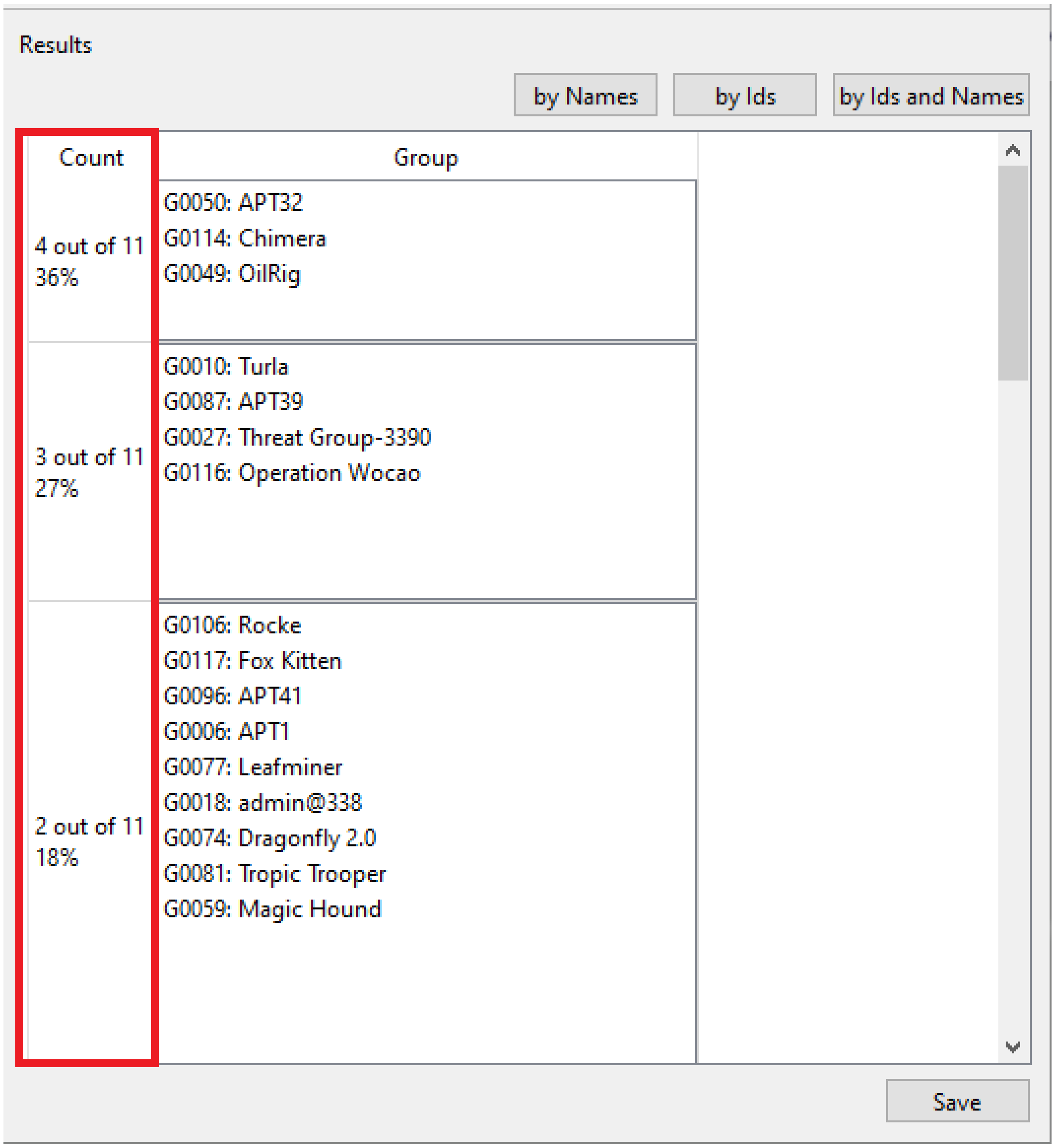


Count	Group
4 out of 11 36%	G0050: APT32 G0114: Chimera G0049: OilRig
3 out of 11 27%	G0010: Turla G0087: APT39 G0027: Threat Group-3390 G0116: Operation Wocao
2 out of 11 18%	G0106: Rocke G0117: Fox Kitten G0096: APT41 G0006: APT1 G0077: Leafminer G0018: admin@338 G0074: Dragonfly 2.0 G0081: Tropic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

Fig. 2: Results are listed in this Table View

4.1.2 What does *Count* column mean ?

Numbers in the *Count* column represent the number of technique used by the groups and listed in the Techniques Section.

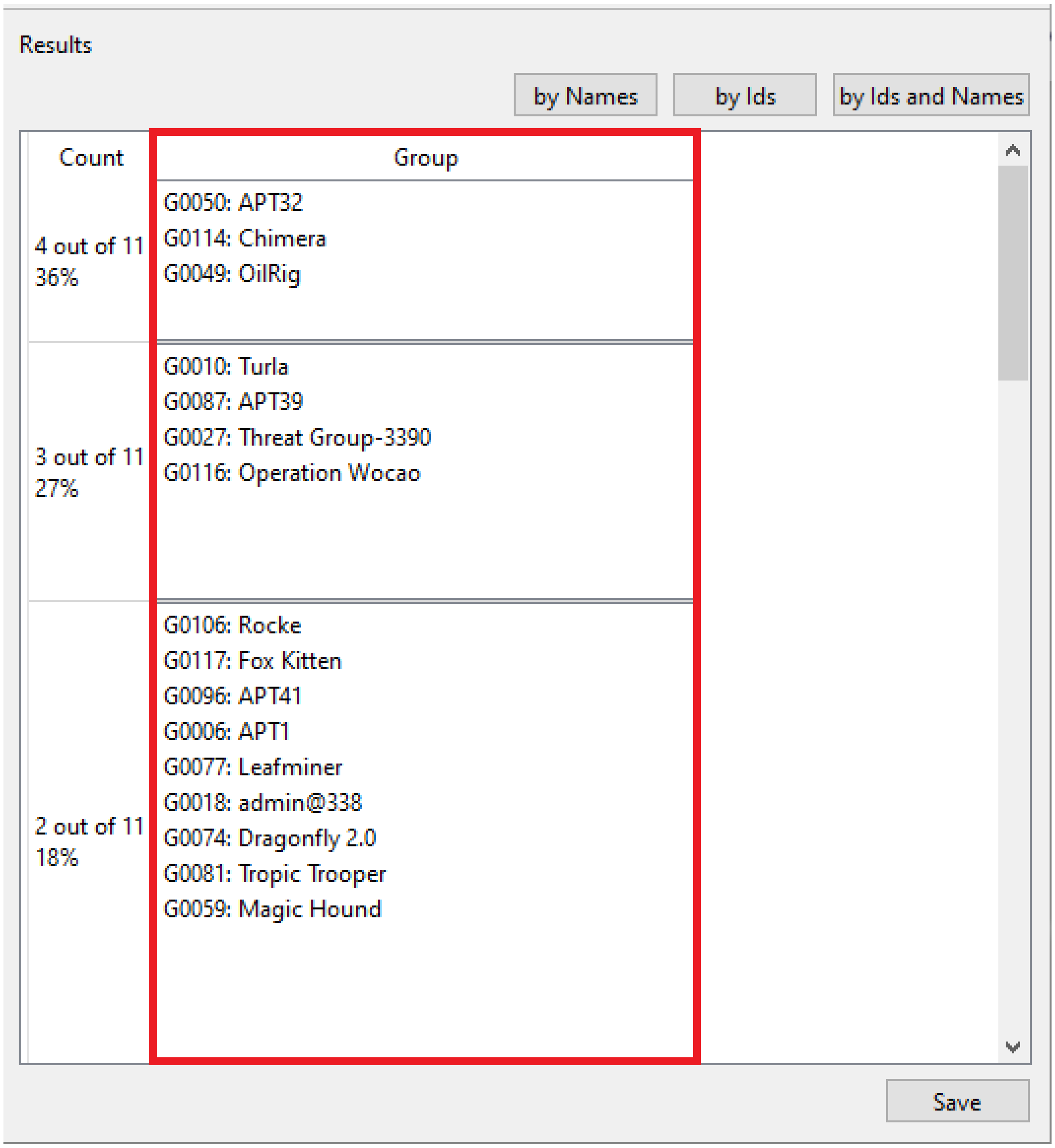


Count	Group
4 out of 11 36%	G0050: APT32 G0114: Chimera G0049: OilRig
3 out of 11 27%	G0010: Turla G0087: APT39 G0027: Threat Group-3390 G0116: Operation Wocao
2 out of 11 18%	G0106: Rocke G0117: Fox Kitten G0096: APT41 G0006: APT1 G0077: Leafminer G0018: admin@338 G0074: Dragonfly 2.0 G0081: Tropic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

Fig. 3: In the first row of this example, the groups have 4 common techniques with the list in Techniques Section.

4.1.3 What does *Group* column mean ?

Groups column contains the name and id of the groups that uses some of the techniques contained in Techniques Section.



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

Fig. 4: In the first row of this example, *APT32*, *Chimera* and *OilRig* used 4 techniques contained in Techniques Section.

4.1.4 How do I change the display mode of the groups ?

Groups column display mode can be changed by clicking the three button located on the top right part of the Result Section.

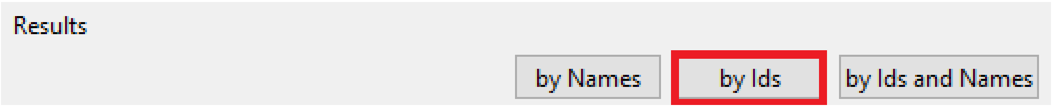


Fig. 5: This button allows to display the groups by their id.

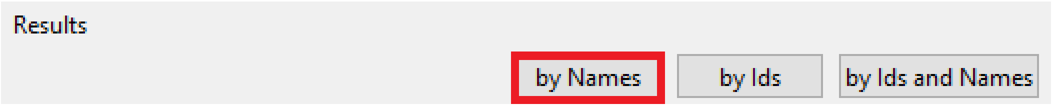


Fig. 6: This button allows to display the groups by their name.

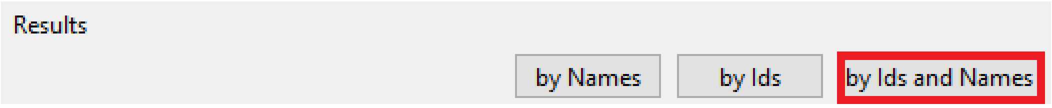
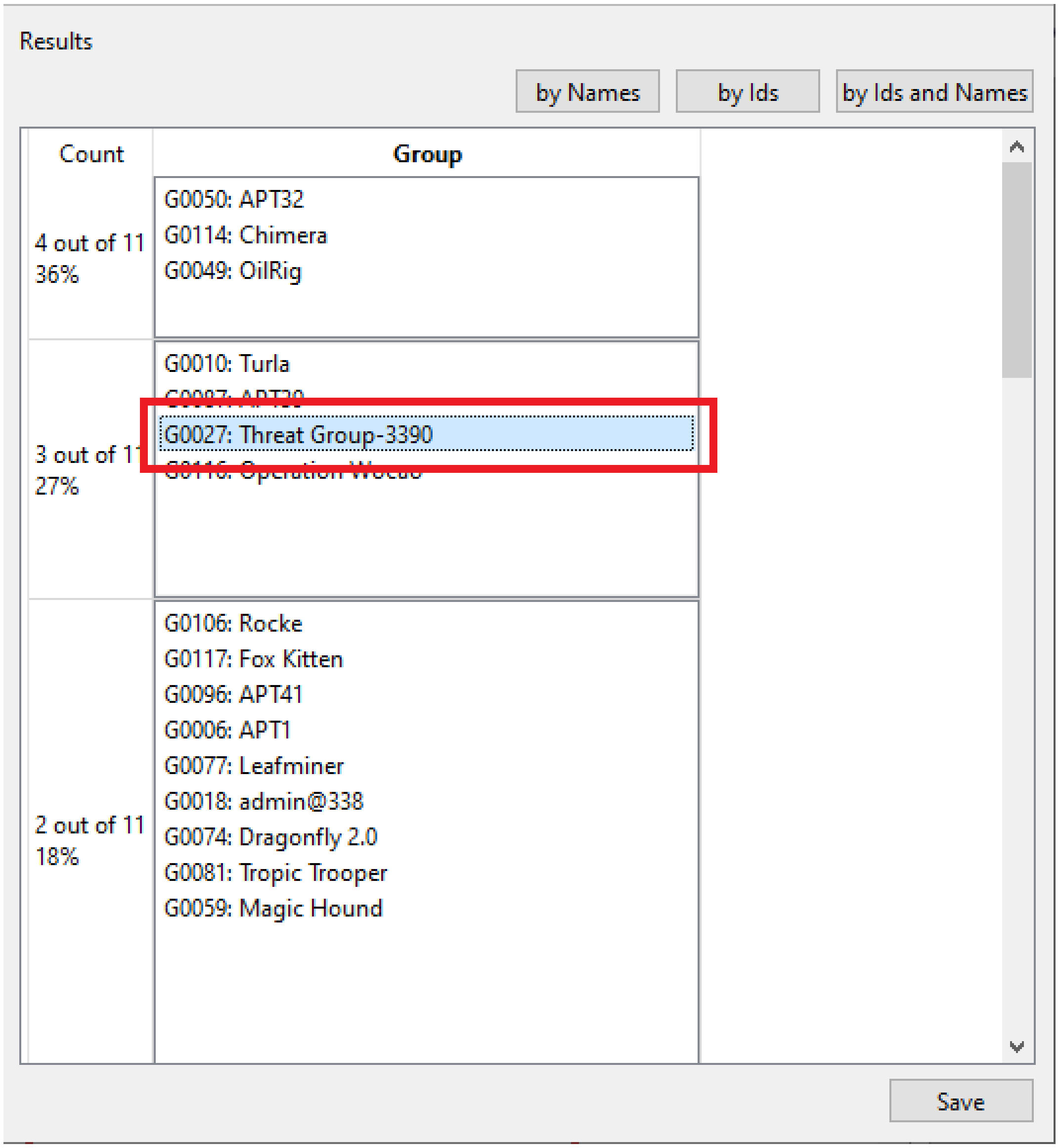


Fig. 7: This button allows to display the groups by their id and name.

4.2 Group Options

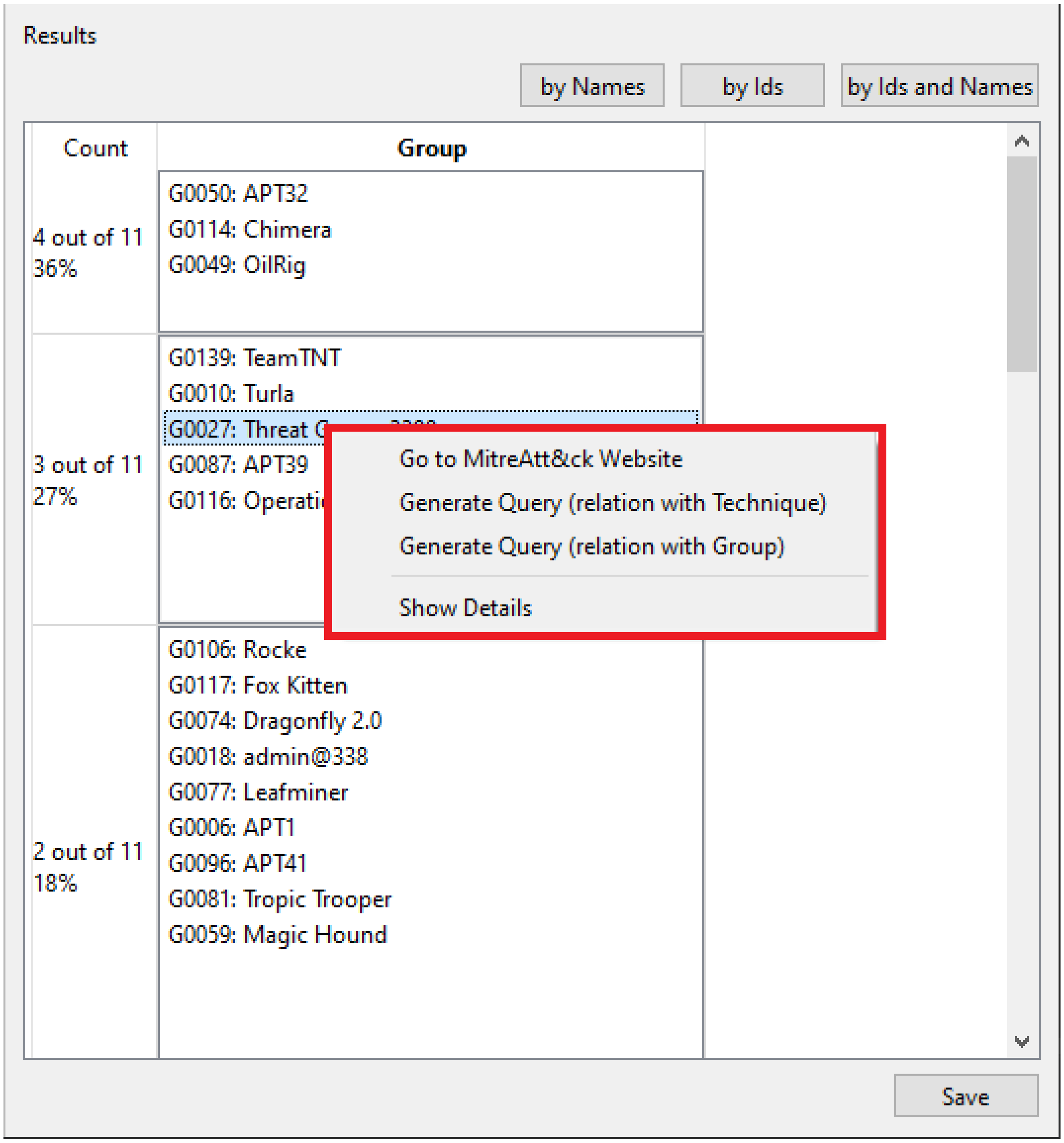
Select one or more group in the table view.



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

Fig. 8: Selecting Threat Group-3390

Click right to display the group options.


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

Fig. 9: Group options for the selection

1. *Go to Mitre Att&ck Website*
2. *Generate Query*
3. *Show Details*

Note: `Go to Mitre Att&ck Website` and `Show Details` options are available only for one item selected.

4.3 Link to Mitre Att&ck Website

This option is a link to the corresponding page of Mitre Attack Website.

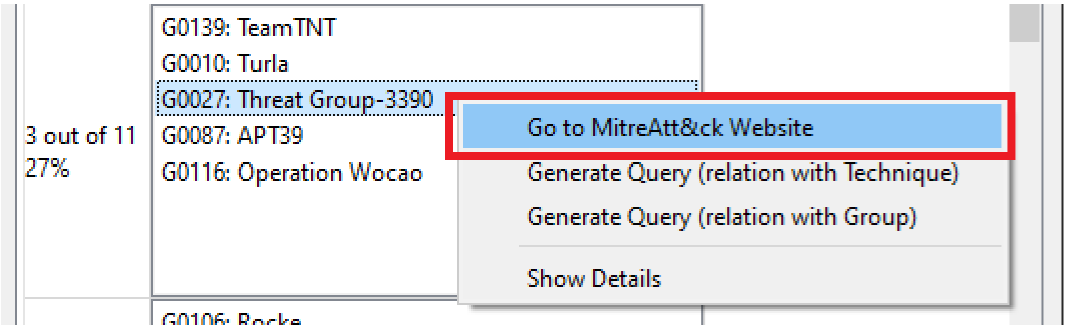
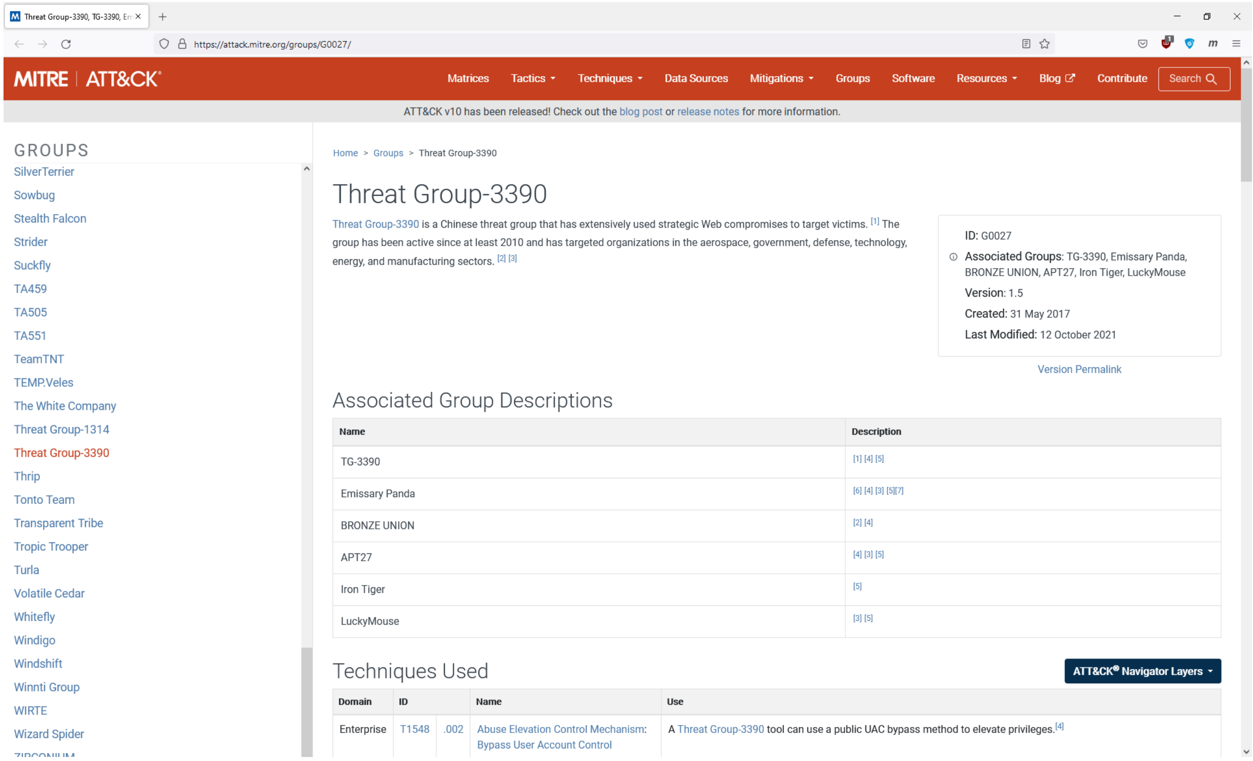


Fig. 10: The option `Go to MitreAtt&ck Website` is a link to the Threat Group-3390's page of Mitre Att&ck Website.



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

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]

Fig. 11: Threat Group-3390 details in Mitre Att&ck Website

4.4 Generate Query

The options Generate Query create a query to get the data directly from Neo4j. The Query is automatically copied and can be used, for example, with Neo4j browser.

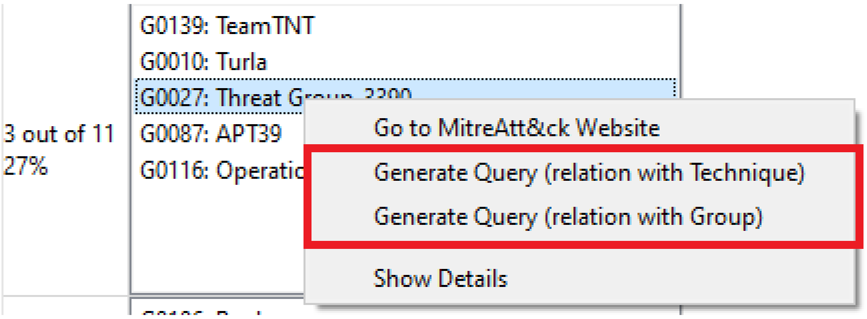


Fig. 12: Generate Query Options for Threat Group-3390

4.4.1 Relation with Technique

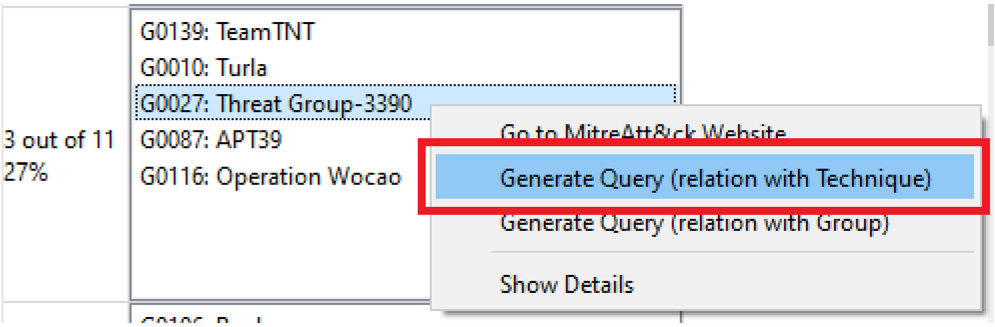


Fig. 13: Generate a query for Threat Group-3390

This query gets all the Techniques related with one or more group.

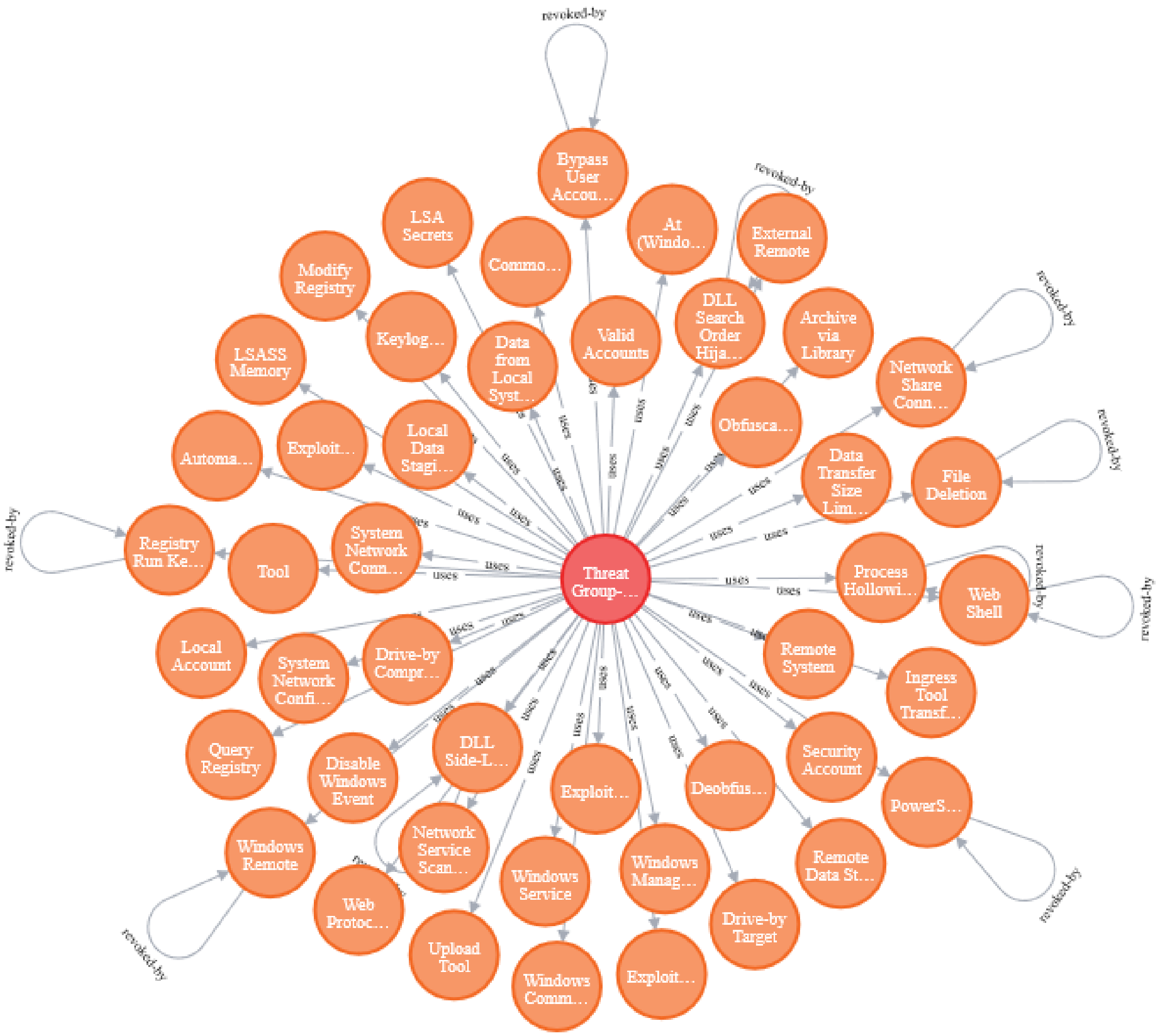
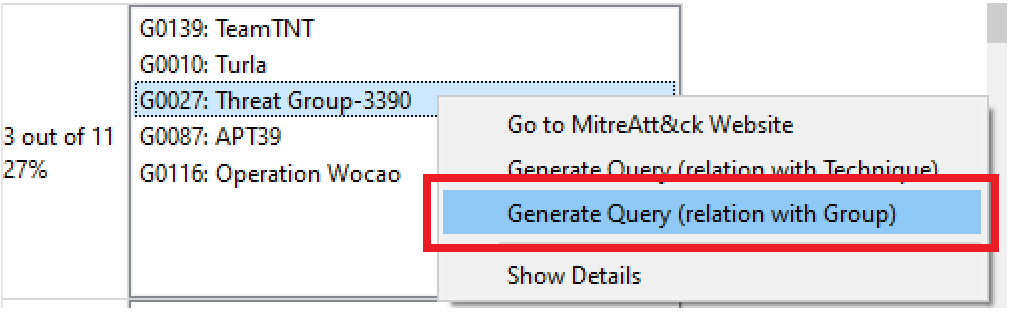


Fig. 14: Results of the query in Neo4j

4.4.2 Relation with Group


3 out of 11
27%

G0139: TeamTNT
G0010: Turla
G0027: Threat Group-3390
G0087: APT39
G0116: Operation Wocao

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

Fig. 15: Generate a query for Threat Group-3390

This query gets all the associated groups of one or more group.

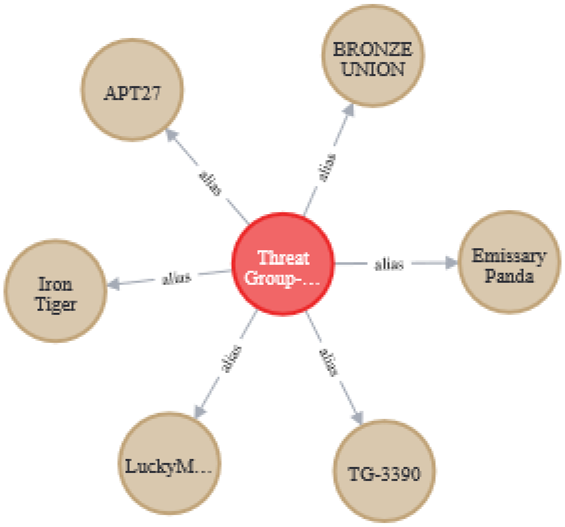


Fig. 16: Results of the query in Neo4j

4.5 Show Details

This option provides details about techniques used by a specific group in a new window.

> **Warning:** If the list of the Techniques Section is updated, details contained in the *Show Details* windows currently opened will not be updated. To get the details updated you must close the window and open it again.

4.5.1 How to open a *Show Details* window ?

Select the *Show Detail* option.

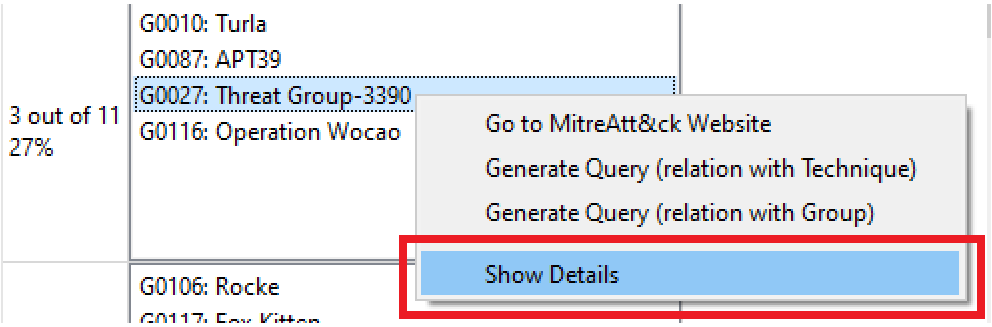
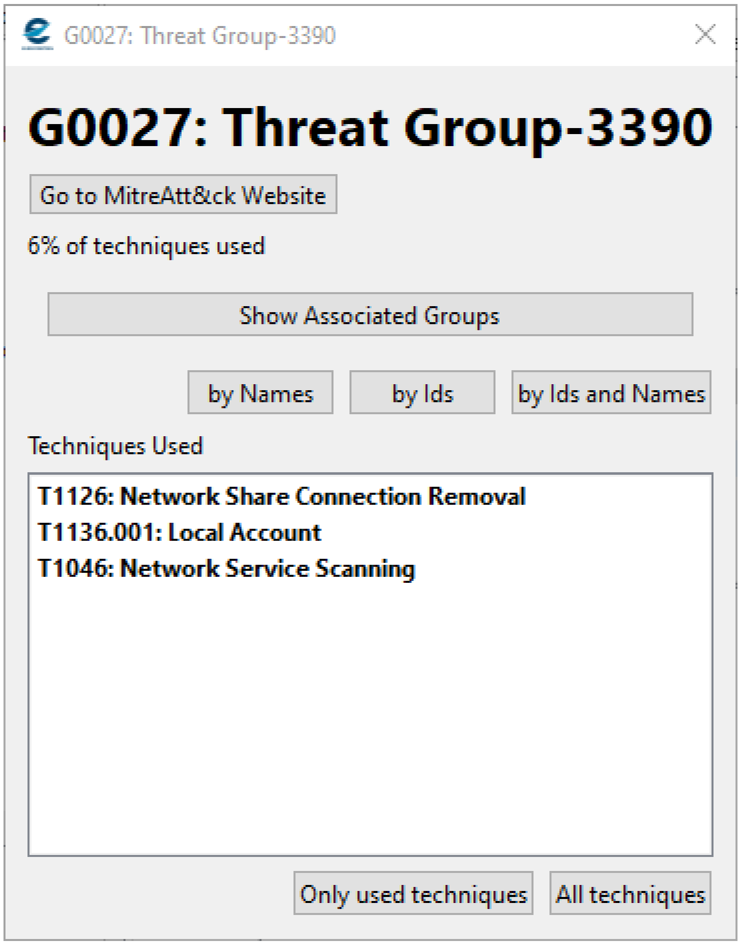


Fig. 17: *Show Detail* Option

The new window is displayed.



G0027: Threat Group-3390

6% of techniques used

Techniques Used

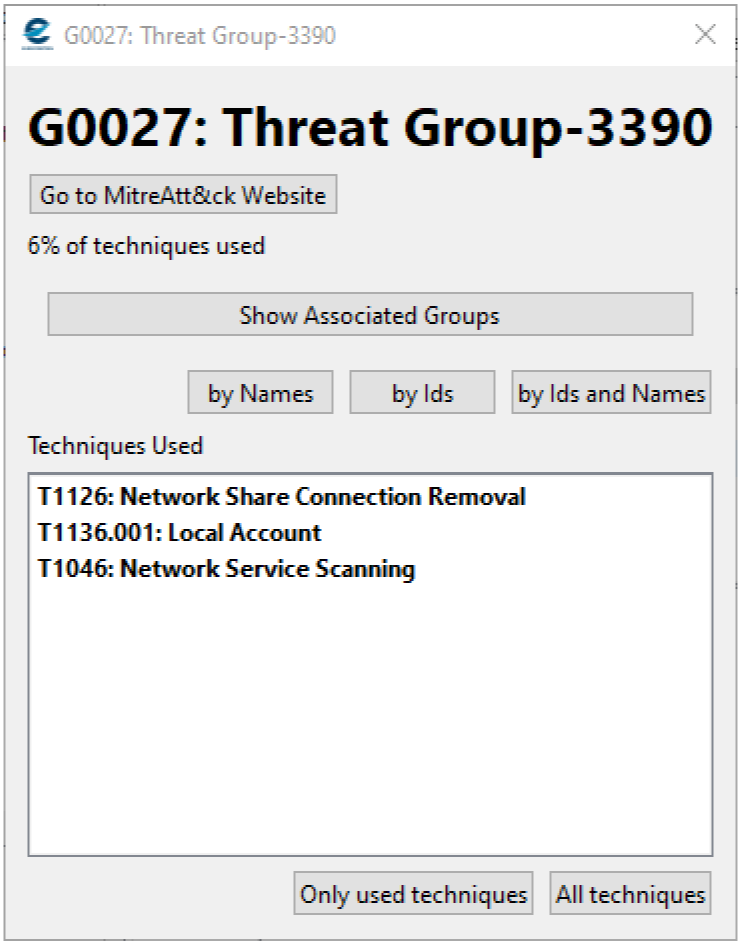
T1126: Network Share Connection Removal
T1136.001: Local Account
T1046: Network Service Scanning

Fig. 18: Show Details Window for Threat Group-3390

4.5.2 *Show Details* Window

The *Show Details* Window contains:

1. A *Title*
2. A *button link* to Mitre Att&ck Website
3. The *percentage* of techniques used
4. The *Associated Group*
5. *Display Options*
6. A *label*
7. A *list view*
8. *Techniques buttons*



G0027: Threat Group-3390

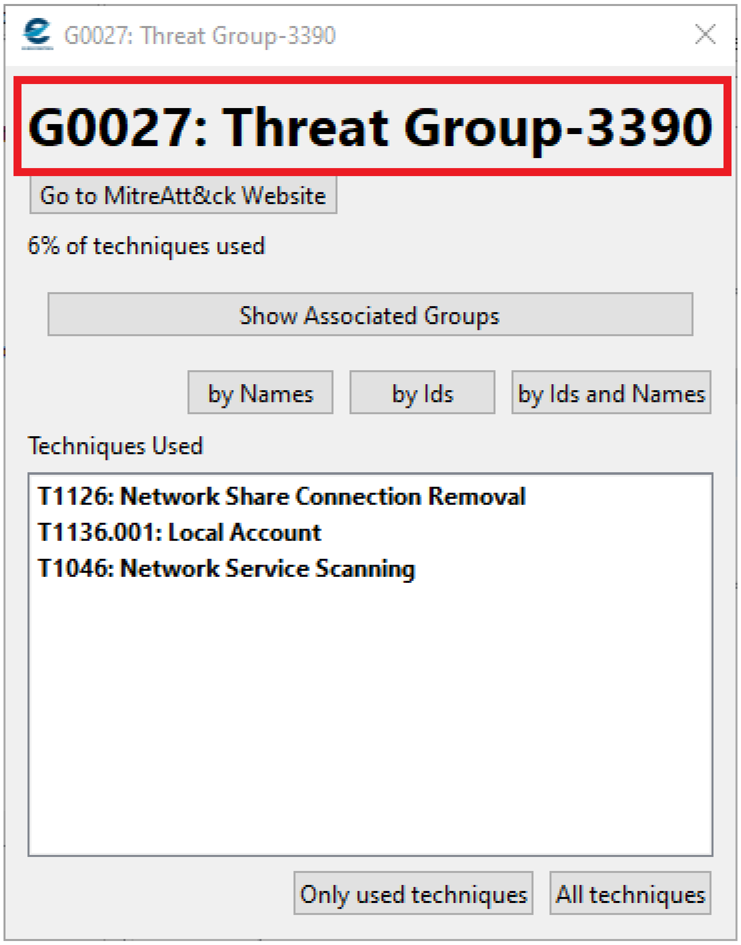
6% of techniques used

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

Fig. 19: Show Details Window for Threat Group-3390

Title

The title of the window is the id and the name of the group.



G0027: Threat Group-3390

G0027: Threat Group-3390

6% of techniques used

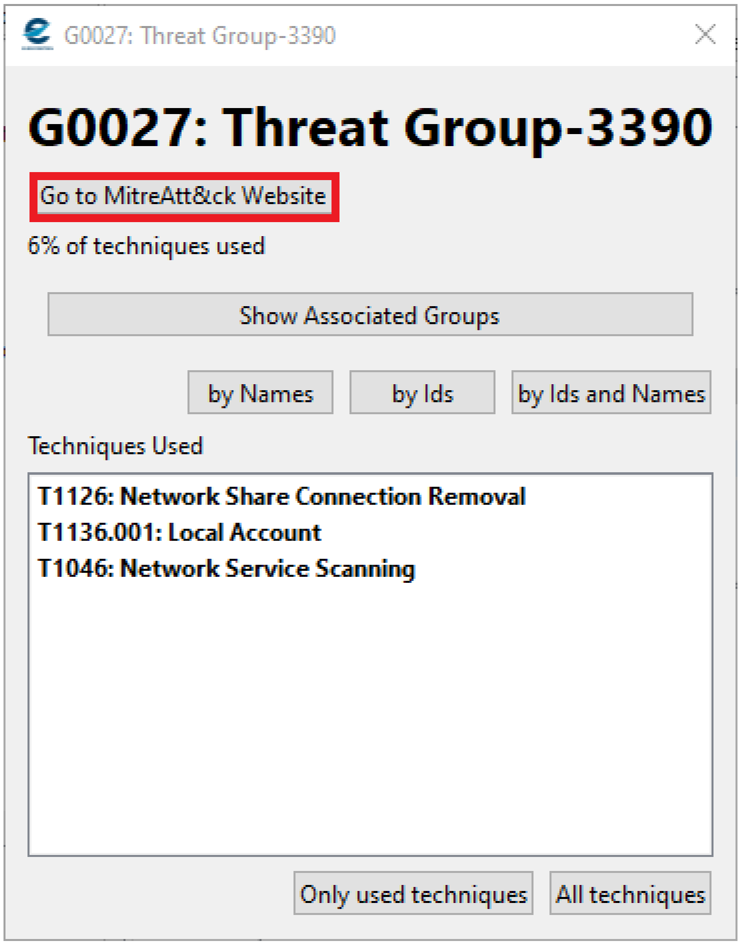
Techniques Used

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

Fig. 20: Show Details Title (G0027: Threat Group-3390)

Button Link to Mitre Att&ck Website

This button is a link to the corresponding page of Mitre Attack Website.



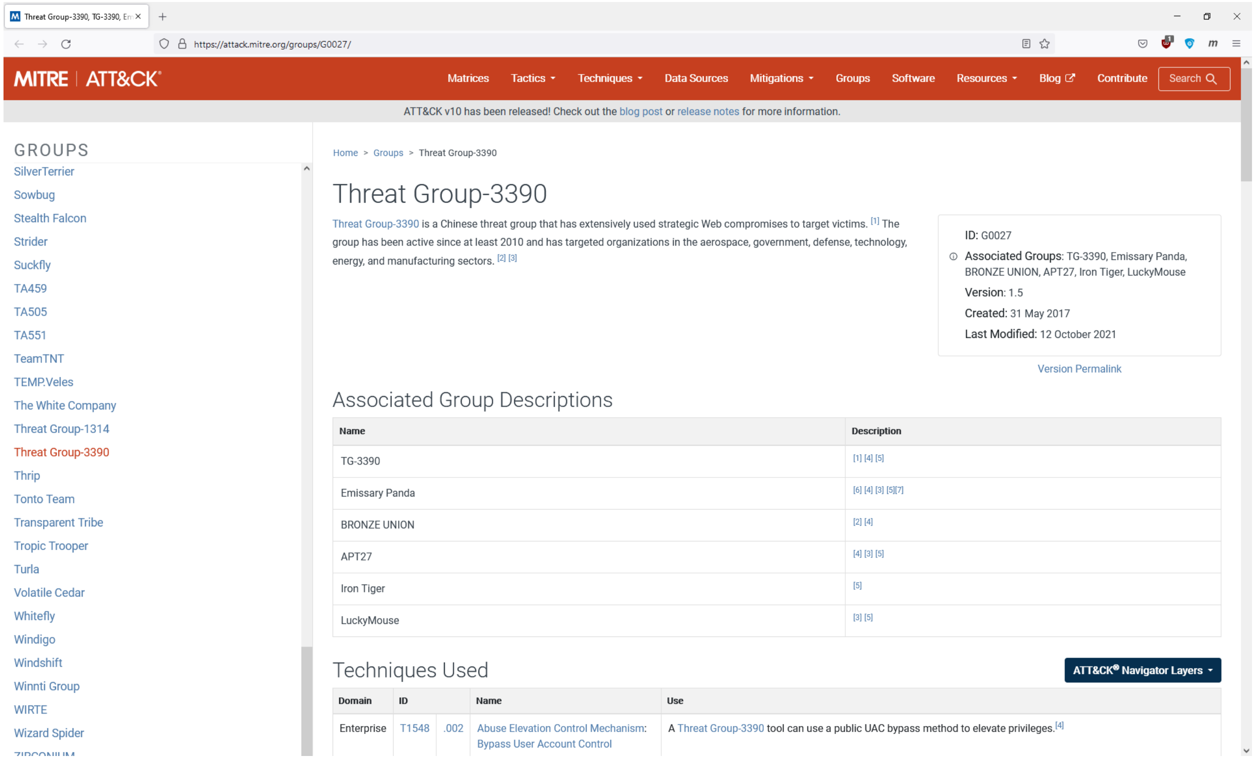
G0027: Threat Group-3390

6% of techniques used

Techniques Used

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

Fig. 21: The button `Go to MitreAtt&ck Website` is a link to the Threat Group-3390's page of Mitre Att&ck Website.



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

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]

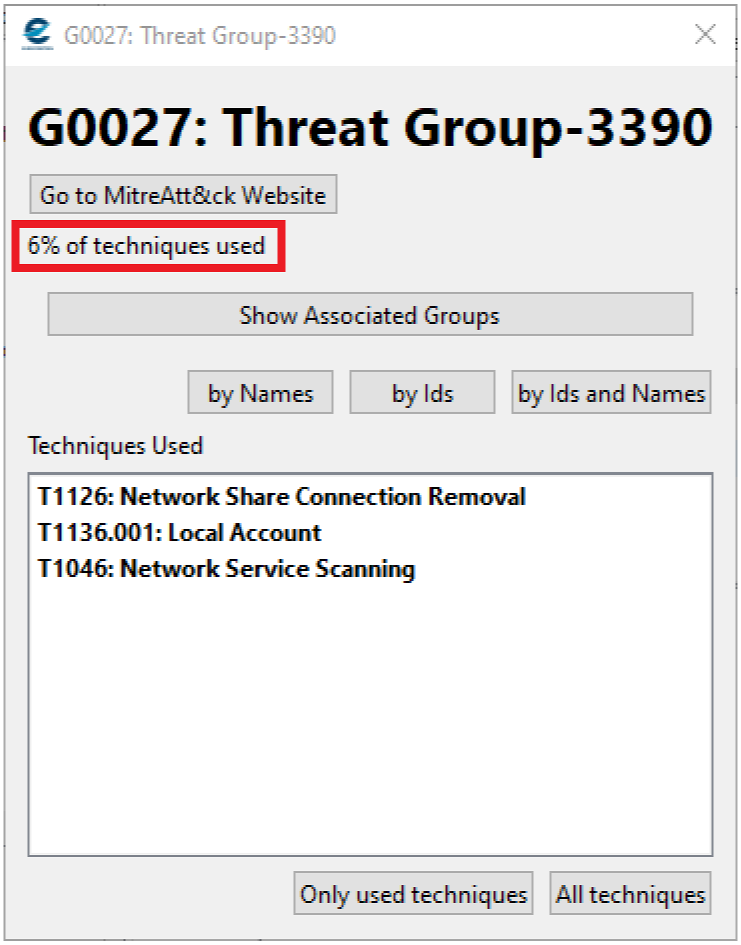
Techniques Used

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]

Fig. 22: Threat Group-3390 details in Mitre Att&ck Website

Percentage of techniques used

This Label gives the percentage of techniques used by this group as per the input list.



G0027: Threat Group-3390

6% of techniques used

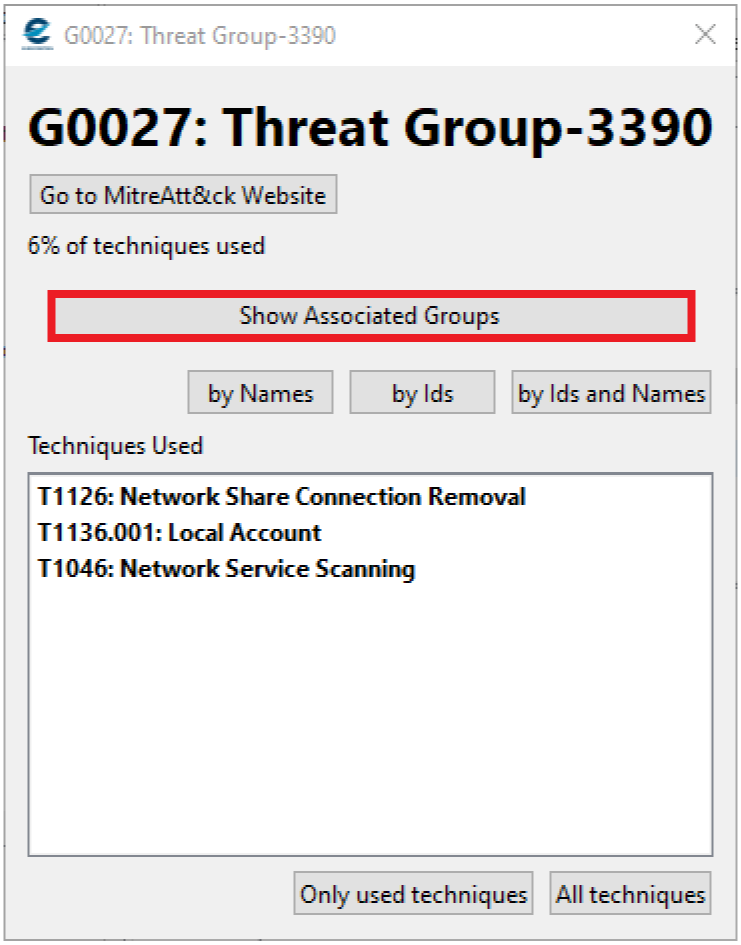
Techniques Used

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

Fig. 23: 6% of the techniques used by Thread Group-3390 are in the input list

Associated Groups

Some groups have associated groups. If so, the list of the associated groups can be displayed by clicking the button `Show Associated Groups`.

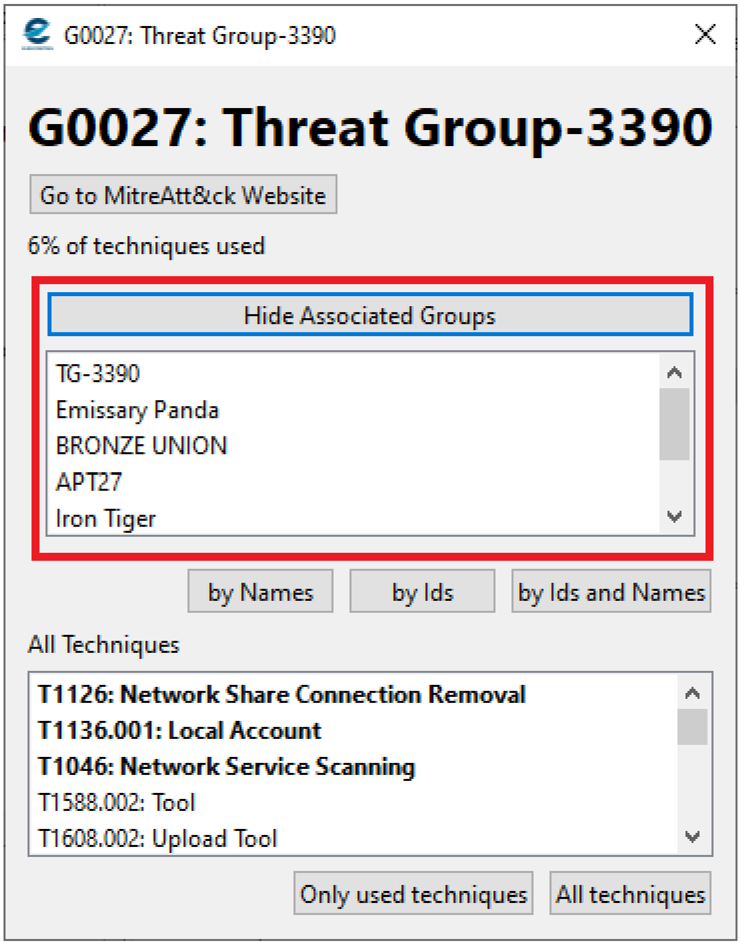


G0027: Threat Group-3390

6% of techniques used

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

Fig. 24: This button will display the names of the associated groups



G0027: Threat Group-3390

6% of techniques used

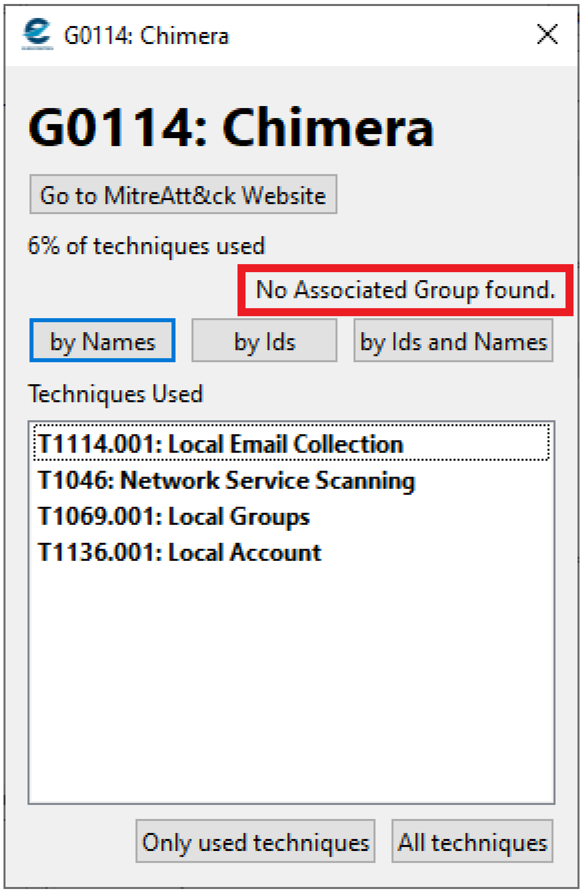
TG-3390
Emissary Panda
BRONZE UNION
APT27
Iron Tiger

All Techniques

T1126: Network Share Connection Removal
T1136.001: Local Account
T1046: Network Service Scanning
T1588.002: Tool
T1608.002: Upload Tool

Fig. 25: List of the associated groups of Threat Group-3390

If the group has no associated group, the button `Show Associated Groups` will be replaced by a label `No associated group found`.



G0114: Chimera

6% of techniques used

No Associated Group found.

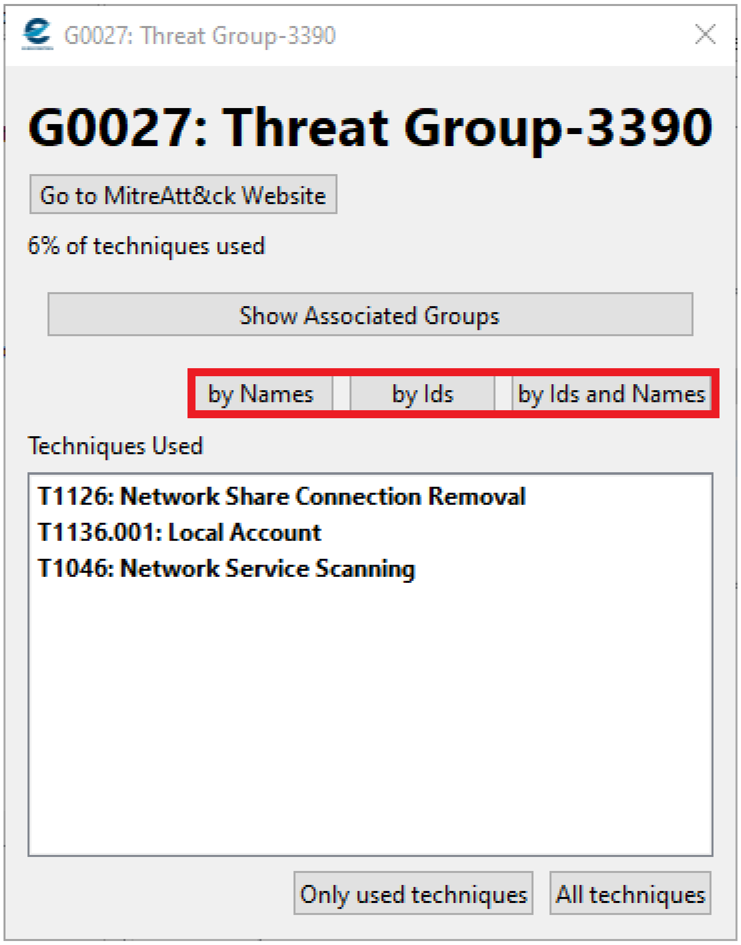
Techniques Used

T1114.001: Local Email Collection
T1046: Network Service Scanning
T1069.001: Local Groups
T1136.001: Local Account

Fig. 26: Chimera have no associated group

Display Options

You can choose how the techniques will appear in the *list view*.
There are three options: techniques can either be shown by name, by id or by id and name.



G0027: Threat Group-3390

G0027: Threat Group-3390

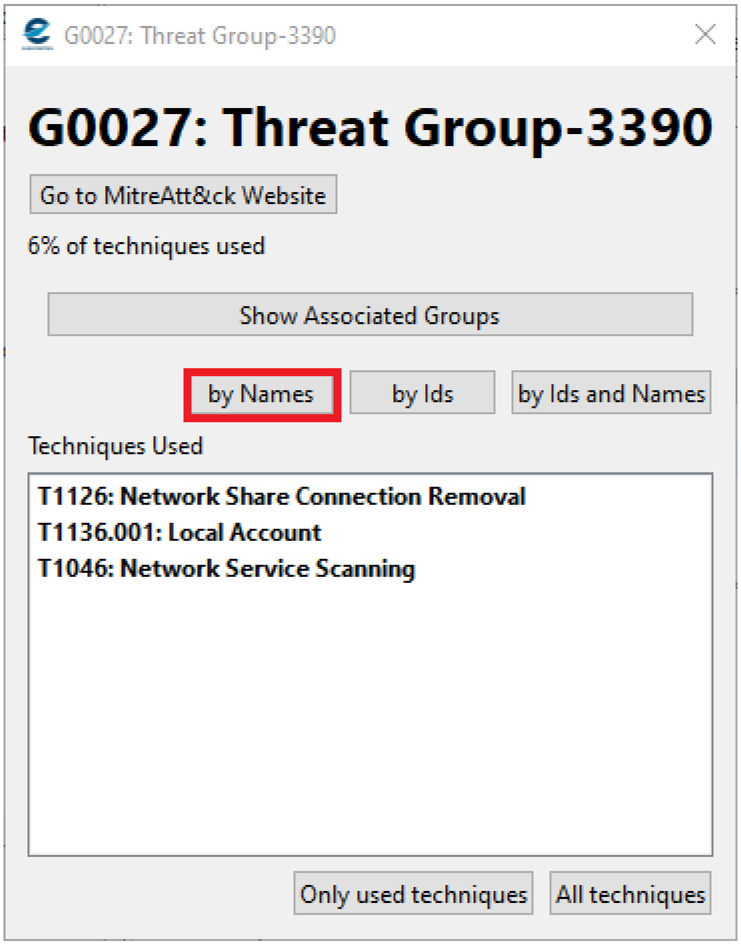
6% of techniques used

Techniques Used

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

Fig. 27: Techniques Display Options

To see the techniques by their names, click the button `by Names`.



G0027: Threat Group-3390

G0027: Threat Group-3390

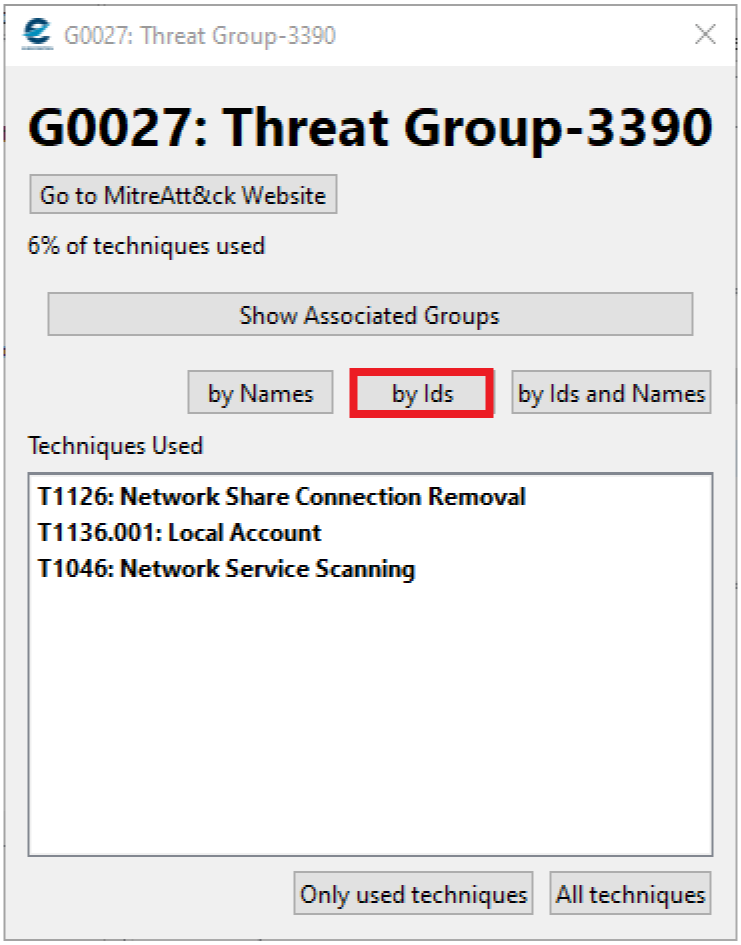
6% of techniques used

Techniques Used

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

Fig. 28: This button allows to display techniques by their names

To see the techniques by their ids, click the button `by Ids`.

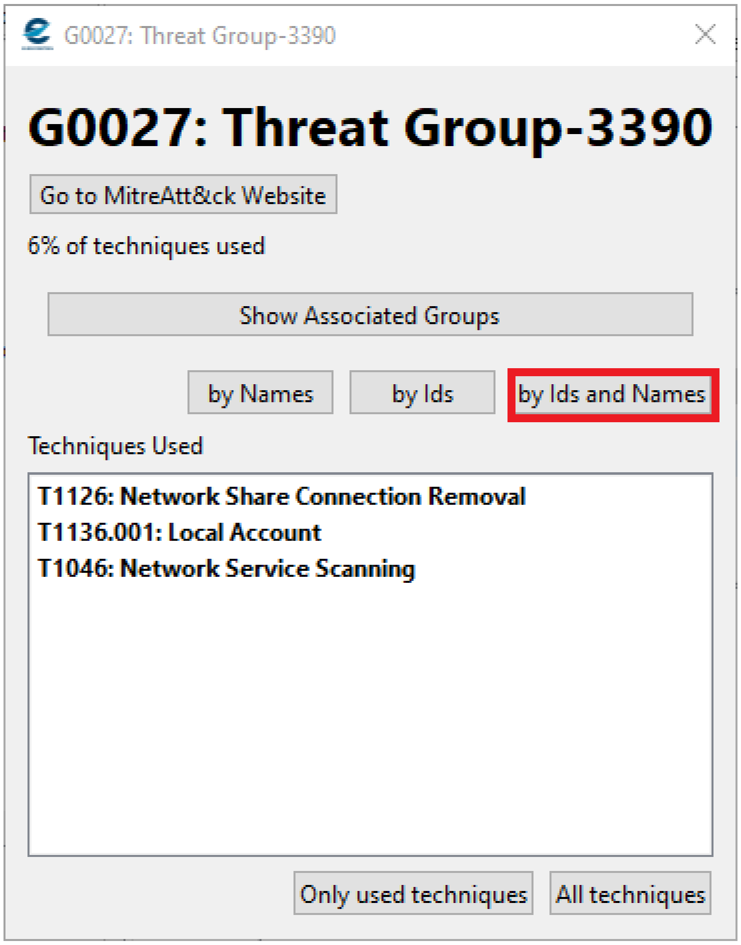


6% of techniques used

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

Fig. 29: This button allows to display techniques by their ids

To see the techniques by their ids and names, click the button `by Ids and Names`.

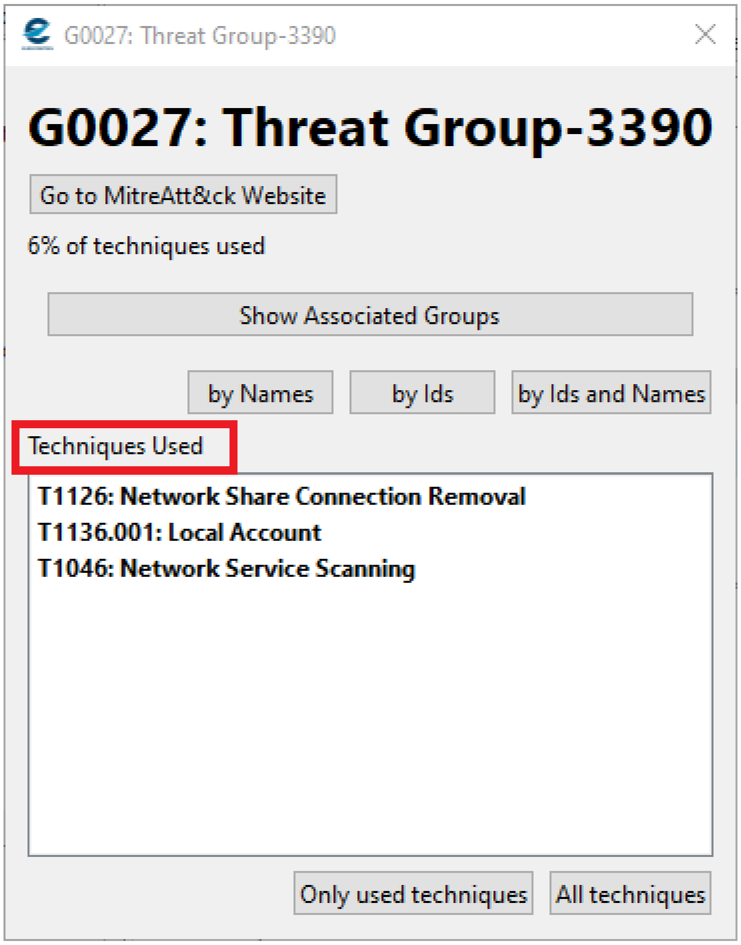


T1126: Network Share Connection Removal
T1136.001: Local Account
T1046: Network Service Scanning

Fig. 30: This button allows to display techniques by their ids and names

Label

The label point out which techniques are displayed in the list view.
There can be two labels.



G0027: Threat Group-3390

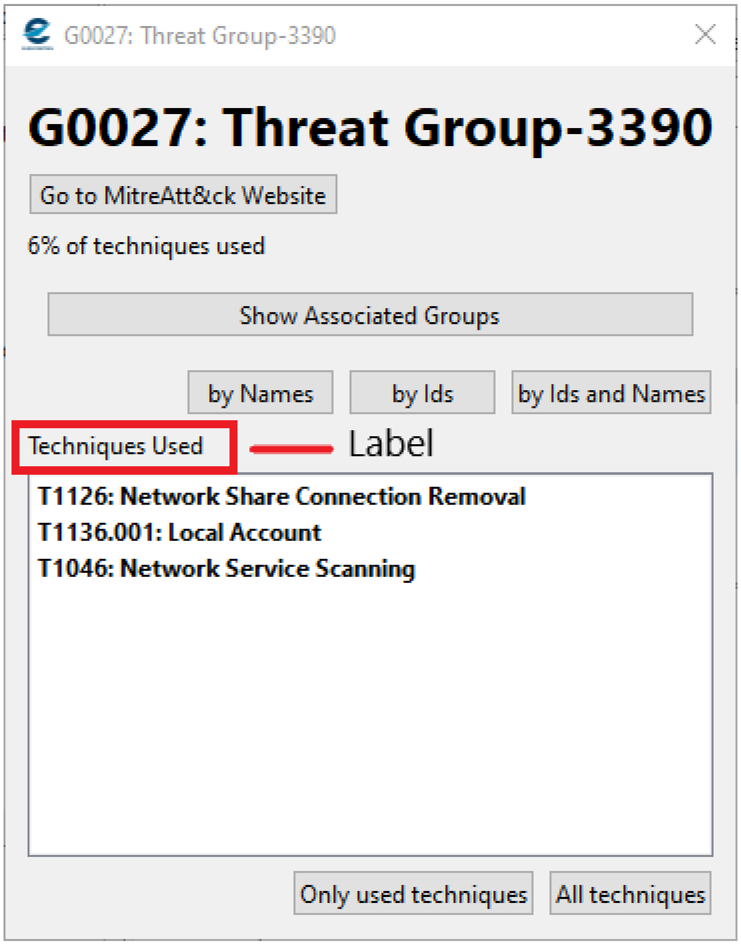
6% of techniques used

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

Fig. 31: Show Details Label

· Techniques Used

This label means that the techniques contained in the list view are only the techniques that this specific group have in common with the techniques in the Techniques Section.



G0027: Threat Group-3390

6% of techniques used

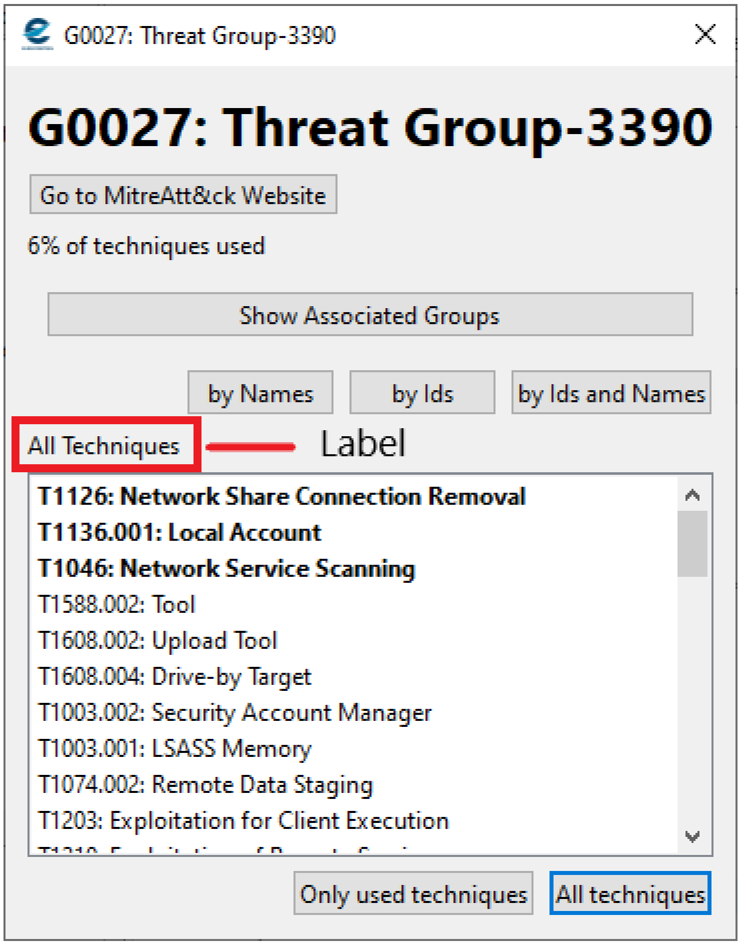
Techniques Used

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

Fig. 32: Show Details when *Techniques Used* label is displayed

· All techniques

This label means that the techniques displayed in the list view are all techniques used by this specific group. The techniques that this group have in common with the techniques in the Techniques Section are displayed in bold.



G0027: Threat Group-3390

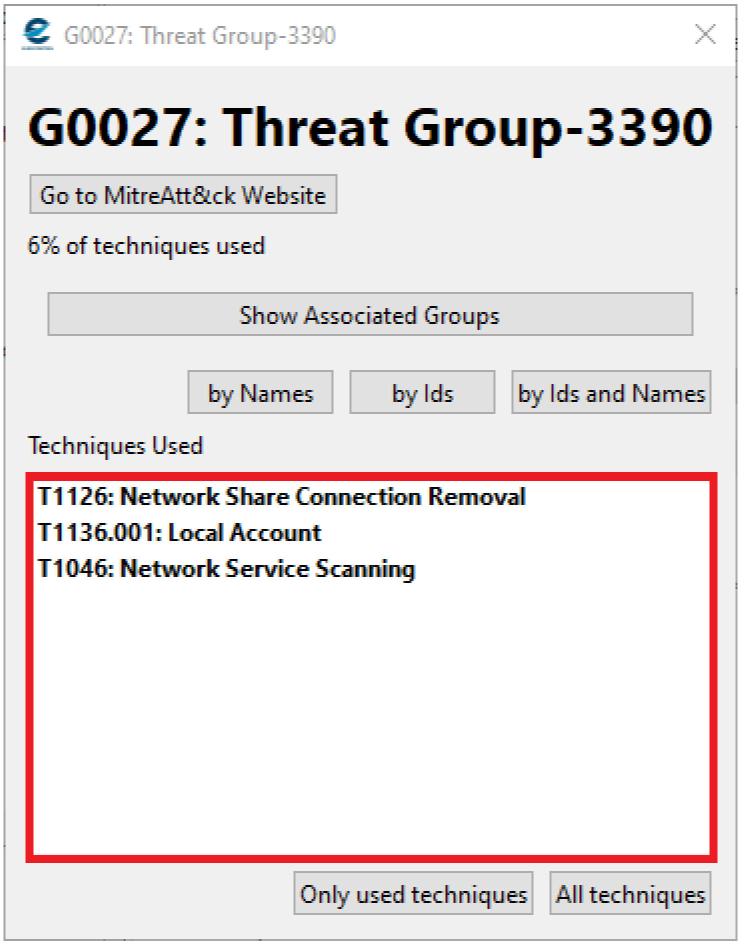
6% of techniques used

T1126: Network Share Connection Removal
T1136.001: Local Account
T1046: Network Service Scanning
T1588.002: Tool
T1608.002: Upload Tool
T1608.004: Drive-by Target
T1003.002: Security Account Manager
T1003.001: LSASS Memory
T1074.002: Remote Data Staging
T1203: Exploitation for Client Execution

Fig. 33: Show Details when *All Techniques* label is displayed. *Local Account*, displayed in bold, is a technique contained in the Techniques Section and used by Threat Group-3390.

List view

The list view contains a list of techniques. Refer to *Label* to see which techniques are displayed.



G0027: Threat Group-3390

6% of techniques used

Techniques Used

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

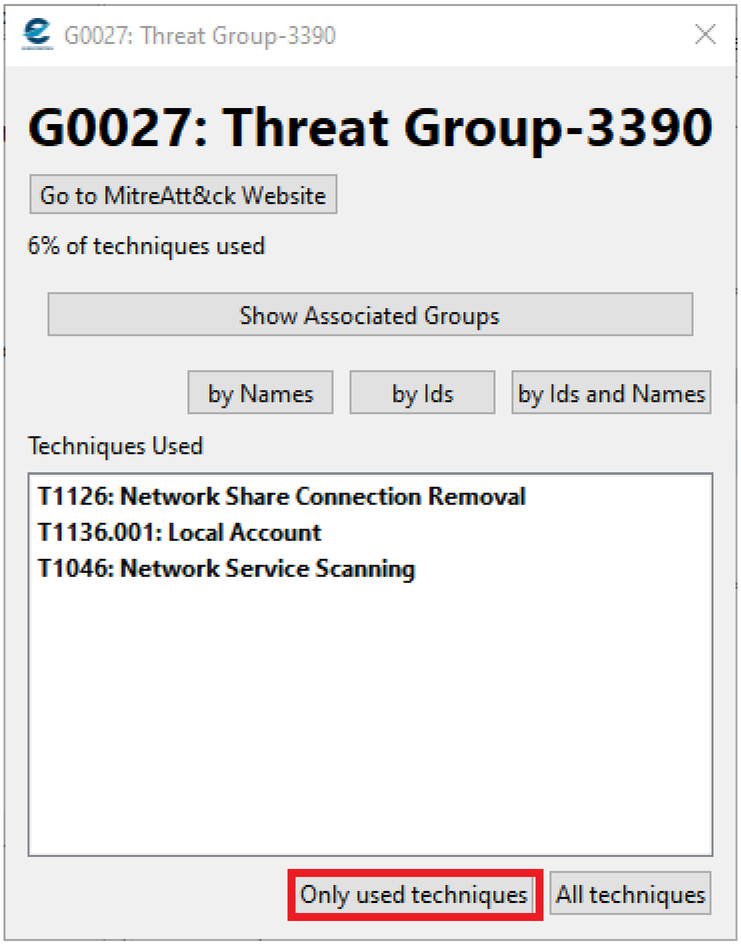
Fig. 34: Show Details List View

Note: See *Techniques Options* for the options of the listview.

Techniques Buttons

· *Show less Techniques* button

This button will change the label to *Techniques Used* and update the list view to contain only the techniques that this specific group have in common with the techniques in the Techniques Section.



G0027: Threat Group-3390

6% of techniques used

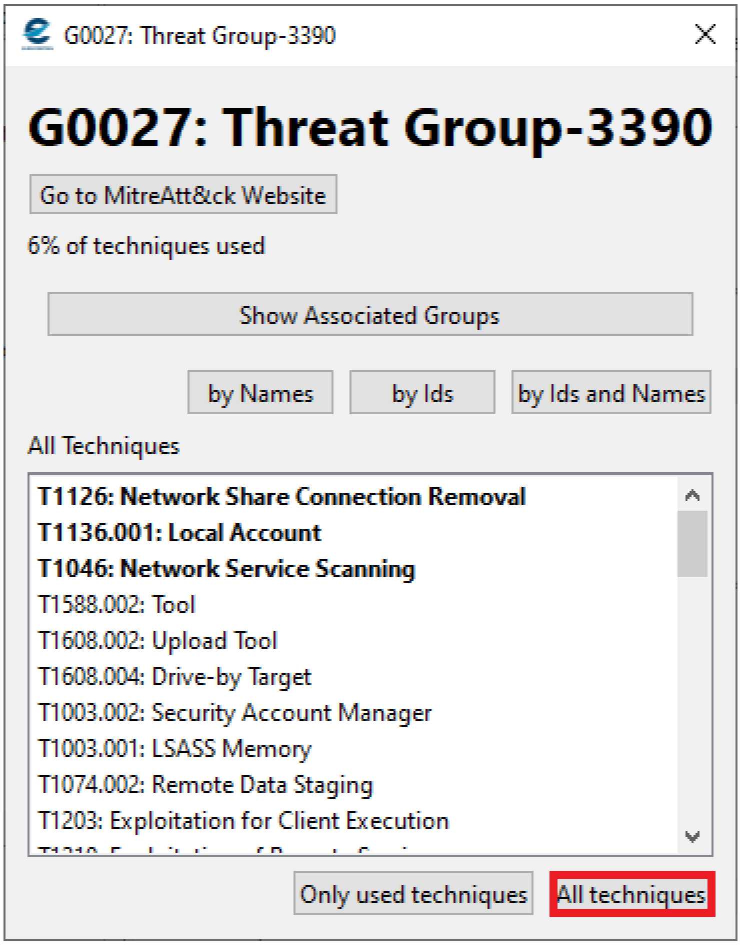
Techniques Used

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

Fig. 35: *Only used techniques* Button

· *All Techniques* button

This button will change the label to *All techniques* and update the list view to contain all techniques used by this specific group. The techniques that this groups have in common with the techniques in the Techniques Section will be displayed in bold.



G0027: Threat Group-3390

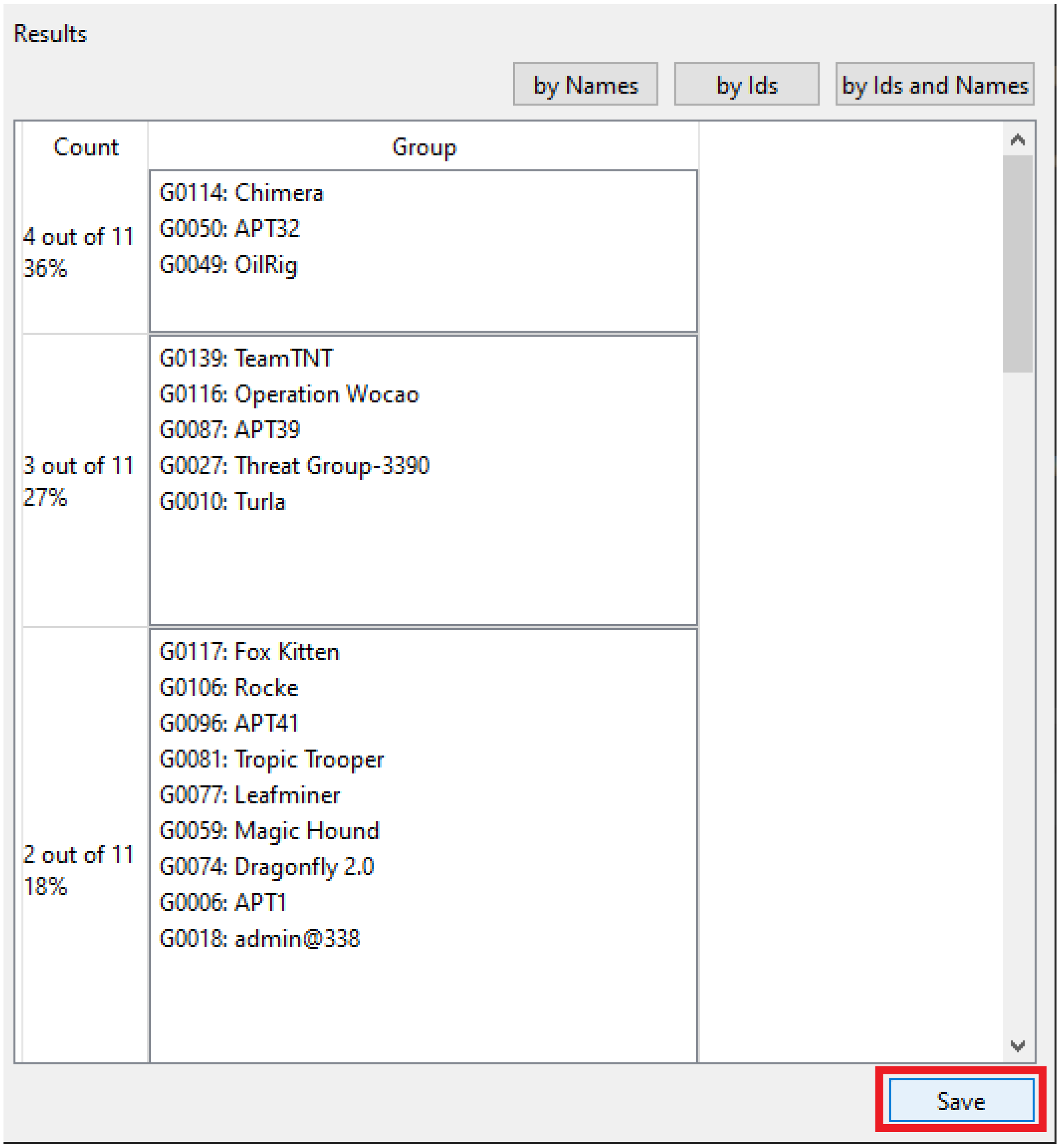
6% of techniques used

T1126: Network Share Connection Removal
T1136.001: Local Account
T1046: Network Service Scanning
T1588.002: Tool
T1608.002: Upload Tool
T1608.004: Drive-by Target
T1003.002: Security Account Manager
T1003.001: LSASS Memory
T1074.002: Remote Data Staging
T1203: Exploitation for Client Execution

Fig. 36: *All techniques* Button

4.6 Save

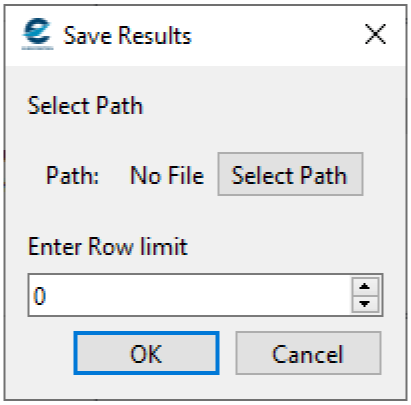
This option opens a new window to export the result table.



Results

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

Fig. 37: Save option



Save Results

Select Path

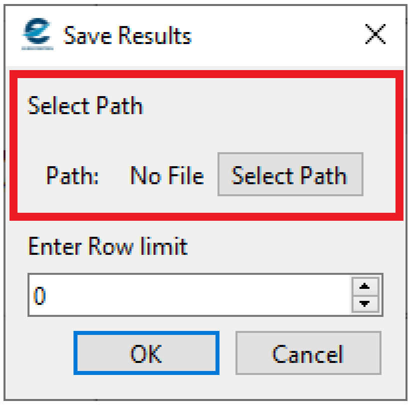
Path: No File

Enter Row limit

0

Fig. 38: Save Window

1. Select path to save the result



Save Results

Select Path

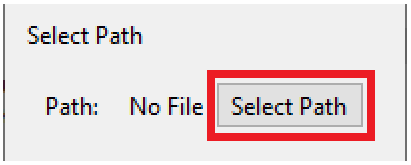
Path: No File

Enter Row limit

0

Fig. 39: Select path area

The button Select path will open a file dialog.

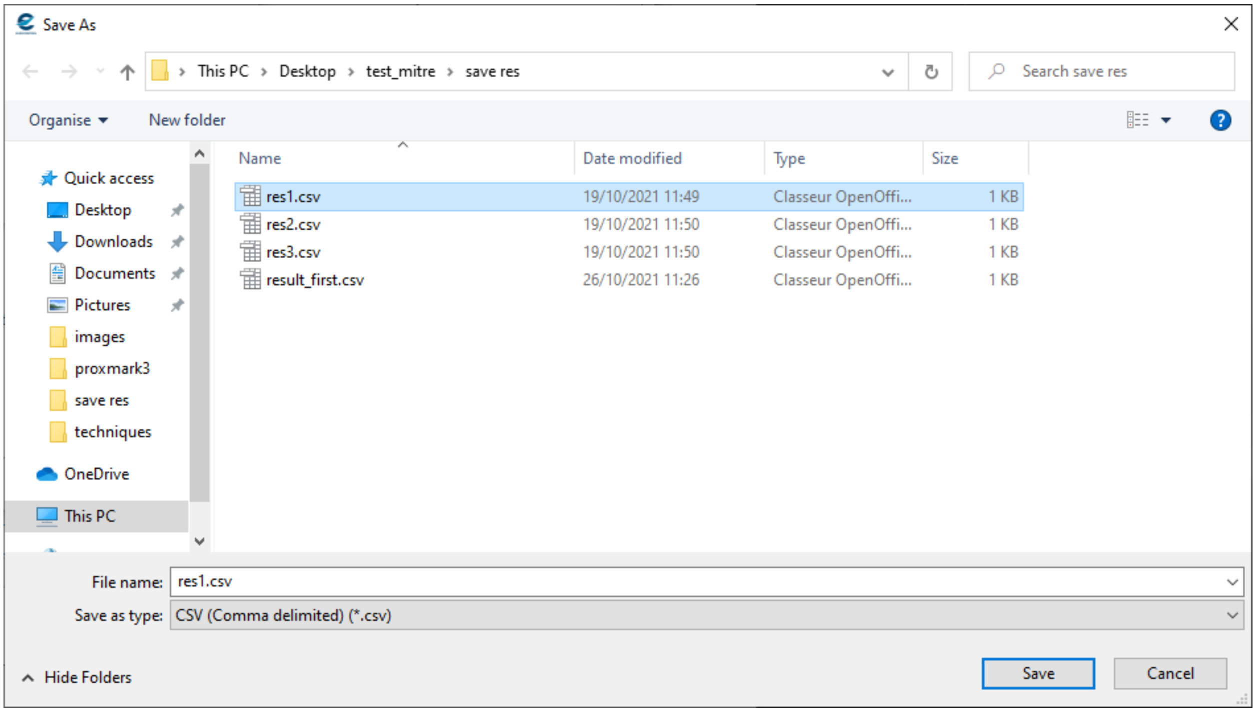


Select Path

Path: No File

Fig. 40: Select path button

Select the path to save the result. The file must have a Csv extension.



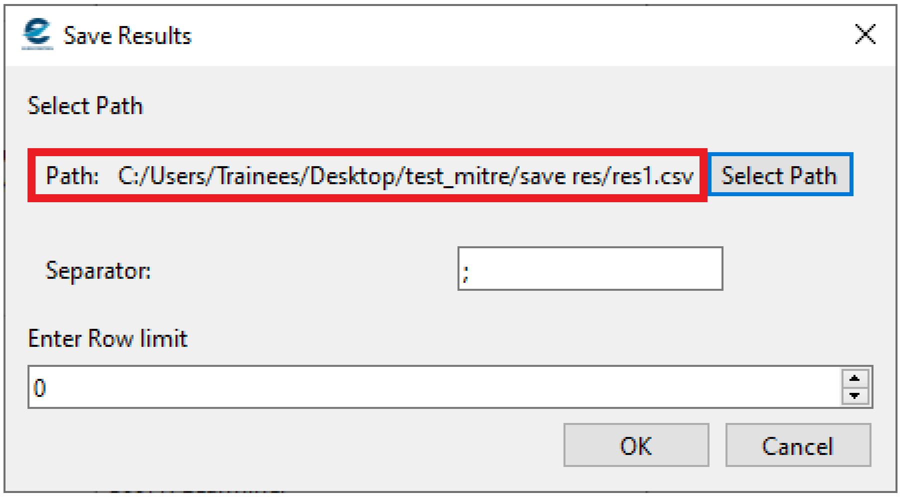
Name	Date modified	Type	Size
res1.csv	19/10/2021 11:49	Classeur OpenOffi...	1 KB
res2.csv	19/10/2021 11:50	Classeur OpenOffi...	1 KB
res3.csv	19/10/2021 11:50	Classeur OpenOffi...	1 KB
result_first.csv	26/10/2021 11:26	Classeur OpenOffi...	1 KB

File name: res1.csv

Save as type: CSV (Comma delimited) (*.csv)

Fig. 41: Select path

The path will be displayed in the save window.



Path: C:/Users/Trainees/Desktop/test_mitre/save res/res1.csv

Separator: ;

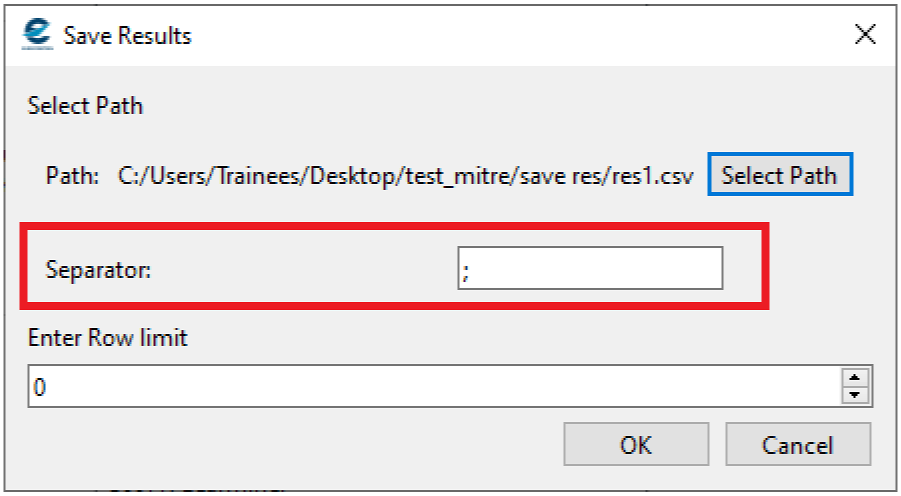
Enter Row limit

0

Fig. 42: The path where the results will be save is ``

2. Choose delimiter

The delimiter area will be displayed after selecting a cvs file location. By default, the delimiter is ;


Save Results

Select Path

Path: C:/Users/Trainees/Desktop/test_mitre/save res/res1.csv

Separator: ;

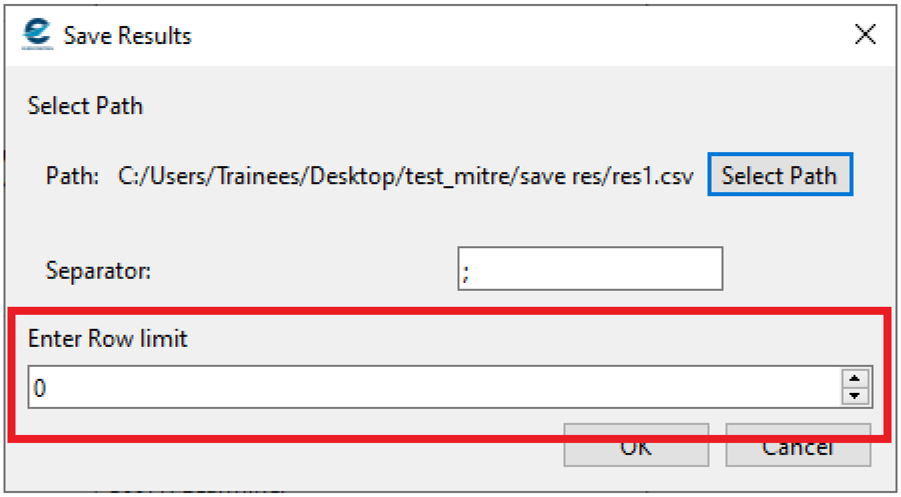
Enter Row limit

0

Fig. 43: Delimiter (Csv files)

3. Choose row limit

   If the row limit is set to 0, all the table will be saved. Otherwise, only the first rows will be saved limited by the number of rows chosen. By default, the row limit is set to 0.


Save Results

Select Path

Path: C:/Users/Trainees/Desktop/test_mitre/save res/res1.csv

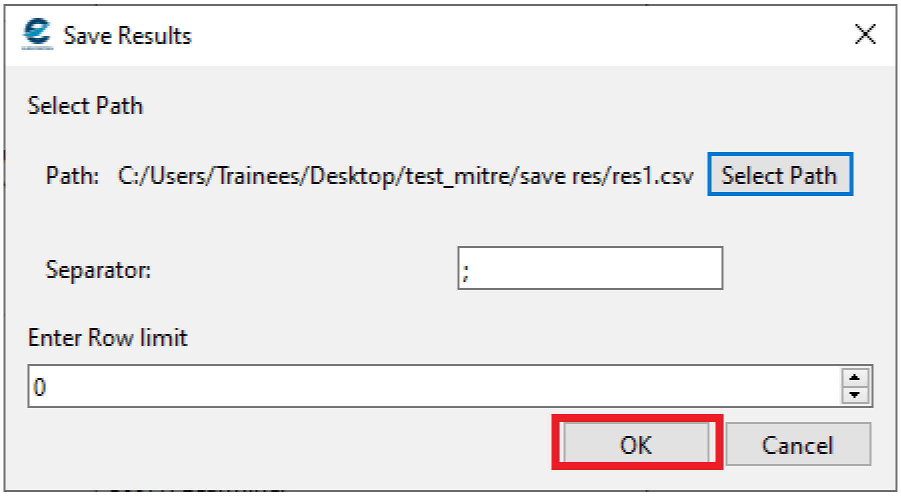
Separator: ;

Enter Row limit

0

Fig. 44: Limit rows

4. Click Ok



Save Results

Select Path

Path: C:/Users/Trainees/Desktop/test_mitre/save res/res1.csv

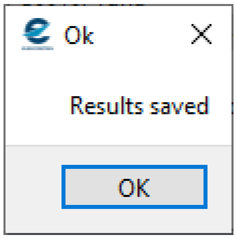
Separator: ;

Enter Row limit

0

Fig. 45: Save the results

A pop up window will confirm that the results have been saved.

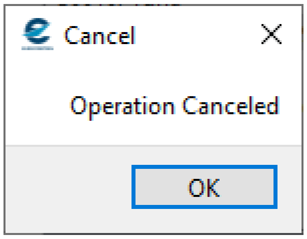


Ok

Results saved

Fig. 46: Confirm Window

In case of canceling, an other window will be displayed.



Cancel

Operation Canceled

Fig. 47: Save canceled