CARTOGRAPHIE DE LA MENACE

Potentiels schéma d’attaque

Société X

Analyse du DD/MM/YYY

Table des matières

[OBJET 2](#_Toc183607403)

[DEFINITION DES PRIORITES 3](#_Toc183607404)

[LISTE DES GROUPES D’ATTAQUANTS 4](#_Toc183607405)

[TECHNIQUES UTILISEES PAR LES ATTAQUANTS 5](#_Toc183607406)

[LOGICIELS UTILISEES PAR LES ATTAQUANTS 6](#_Toc183607407)

[CARTOGRAPHIE DES TECHNIQUES (G0073) 7](#_Toc183607408)

[MESURES DE PROTECTIONS 8](#_Toc183607409)

[MITIGATION 8](#_Toc183607410)

[DETECTION 8](#_Toc183607411)

[CVE A CORRIGER URGEMMENT 9](#_Toc183607412)

# OBJET

Le présent document a pour but de lister les attaquants et schémas d’attaques possibles au sein de notre organisation.

*Il s’agit ici d’un document d’exemple, incomplet.*

# DEFINITION DES PRIORITES

[Présenter ici le modèle de priorisation retenue et le justifier]

|  |  |
| --- | --- |
| Cible | Priorité |
| Notre secteur d’activité et pays | 1 |
| Notre secteur d’activité | 2 |
| Les domaines de nos clients | 3 |

Explication : si le groupe d'attaquant cible notre secteur d'activité dans votre pays, alors il y a plus de probabilité de le voir s'en prendre à vous que s'il ne cible uniquement le domaine d'un de vos clients.

# LISTE DES GROUPES D’ATTAQUANTS

[Ajouter ou supprimer des colonnes suivants vos besoins.  
Par exemple, dans certains cas il peut être intéressant de lister le pays rattaché au groupe d’attaquants.]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Name | Associated group | Cible notre domaine ? | Cible notre pays ? | Priorité |
| [G1007](https://attack.mitre.org/groups/G1007) | [Aoqin Dragon](https://attack.mitre.org/groups/G1007) | N/A | Oui | Non | 2 |
| [G0073](https://attack.mitre.org/groups/G0073) | [APT19](https://attack.mitre.org/groups/G0073) | Codoso, C0d0so0, Codoso Team, Sunshop Group | Oui | N/A | 2 |
| [G0087](https://attack.mitre.org/groups/G0087) | [APT39](https://attack.mitre.org/groups/G0087) | ITG07, Chafer, Remix Kitten | Oui | Oui (Europe) | 1 |

# TECHNIQUES UTILISEES PAR LES ATTAQUANTS

*Dans le cadre du document d’exemple, nous utiliserons G1007 et G0073, quand bien même ils ne sont pas en P1 d'après notre échelle. Les données du tableau suivant seront incomplètes et ont pour unique but de fournir un exemple de présentation.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Domain | Technique ID | Name | Utilisé par | Nombre groupe attaquants |
| Enterprise | [T1587](https://attack.mitre.org/techniques/T1587) | [Develop Capabilities](https://attack.mitre.org/techniques/T1587): [Malware](https://attack.mitre.org/techniques/T1587/001) | G1007 | 1 |
| Enterprise | [T1027](https://attack.mitre.org/techniques/T1027) | Obfuscated Files or Information | G1007 G0073 | 2 |

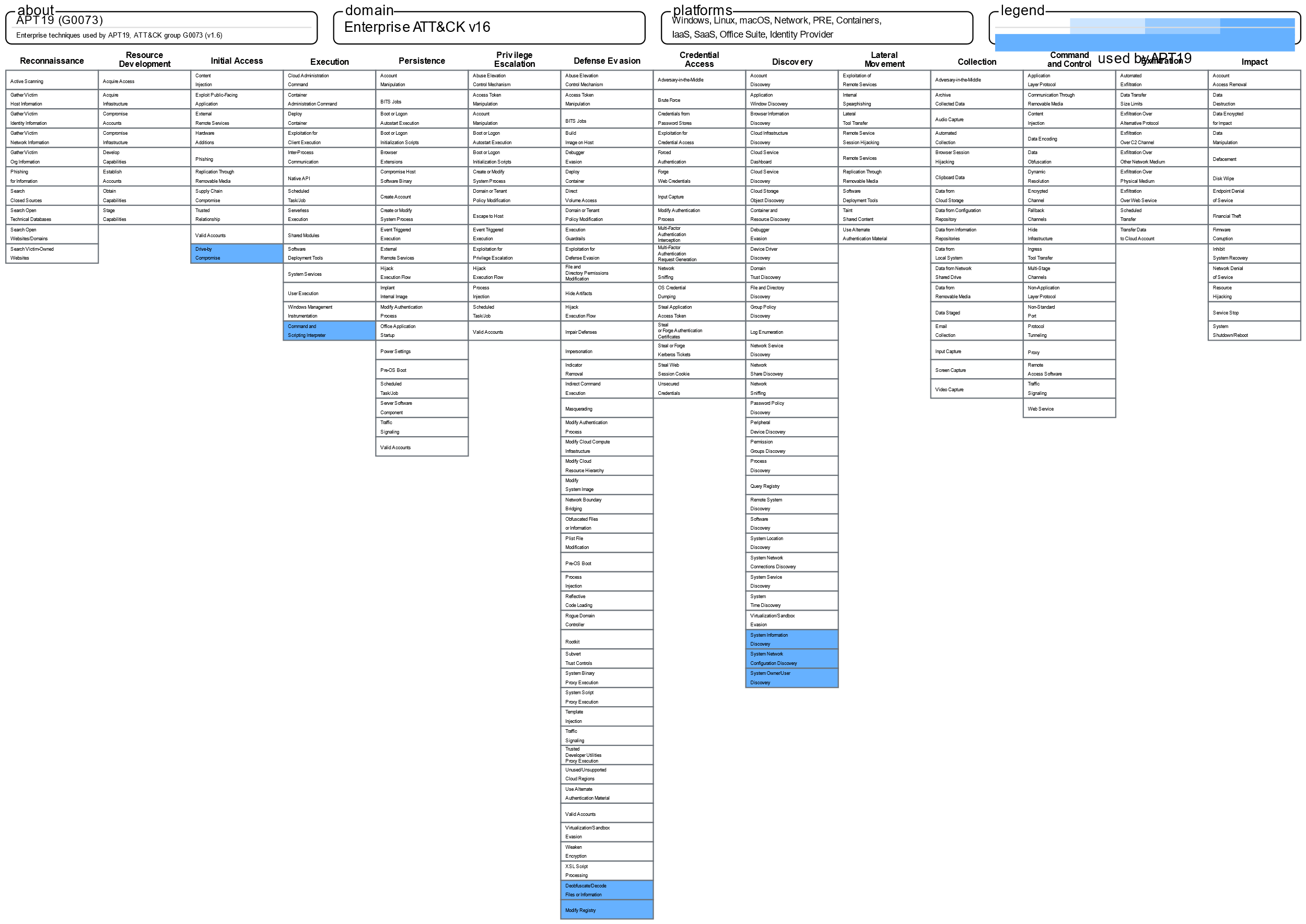
Objectif : si une technique est utilisée par plusieurs attaquants potentiels, il peut être judicieux de mettre en place les contre-mesures en priorité.

Pourquoi le champ « domain » est intéressant ? Dans certains cas, il est plus judicieux de séparer les domaines car les acteurs en charge de la mise en place des contre-mesures et les enjeux ne sont pas forcément les mêmes. De plus, en fonction de votre domaine et pays vous aurez potentiellement de très nombreuses techniques listées ici.

# LOGICIELS UTILISEES PAR LES ATTAQUANTS

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Name | Utilisé par | Nombre groupe attaquants |
| [S1027](https://attack.mitre.org/software/S1027) | [Heyoka Backdoor](https://attack.mitre.org/software/S1027) | G1007 | 1 |
| [S1026](https://attack.mitre.org/software/S1026) | [Mongall](https://attack.mitre.org/software/S1026) | G1007 | 1 |
| [S0154](https://attack.mitre.org/software/S0154) | [Cobalt Strike](https://attack.mitre.org/software/S0154) | G0073 | 1 |
| [S0363](https://attack.mitre.org/software/S0363) | [Empire](https://attack.mitre.org/software/S0363) | G0073 | 1 |

# CARTOGRAPHIE DES TECHNIQUES (G0073)



# MESURES DE PROTECTIONS

[*A personnalité suivant votre environnement et analyses précédentes]*

## MITIGATION

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Name | Technique ciblée | Nombre de techniques ciblées |
| [M1048](https://attack.mitre.org/mitigations/M1048) | [Application Isolation and Sandboxing](https://attack.mitre.org/mitigations/M1048) | T1203 |  |
| [M1050](https://attack.mitre.org/mitigations/M1050) | [Exploit Protection](https://attack.mitre.org/mitigations/M1050) | T1203 |  |
| [M1051](https://attack.mitre.org/mitigations/M1051) | [Update Software](https://attack.mitre.org/mitigations/M1051) | T1203 |  |

## DETECTION

|  |  |  |
| --- | --- | --- |
| ID | Name | Exemple de mesures |
| [DS0015](https://attack.mitre.org/datasources/DS0015) | [Application Log](https://attack.mitre.org/datasources/DS0015) | sourcetype=WinEventLog:Application EventCode=1000| search application IN ("chrome.exe", "firefox.exe", "winword.exe", "excel.exe", "acrord32.exe", "flashplayer.exe")| stats count by application event\_description| where event\_description IN ("crash", "instability", "unexpected termination") |
| [DS0022](https://attack.mitre.org/datasources/DS0022) | [File](https://attack.mitre.org/datasources/DS0022) | sourcetype=linux\_auditd| search file\_path IN ("/Users/*/Library/", "C:\Users\*\AppData\Roaming\", "/home/\*/.config/", "/var/tmp/")| stats count by file\_path process\_name user| where process\_name IN ("chrome.exe", "firefox.exe", "winword.exe", "excel.exe", "acrord32.exe", "flashplayer.exe") |
| [DS0029](https://attack.mitre.org/datasources/DS0029) | [Network Traffic](https://attack.mitre.org/datasources/DS0029) | sourcetype=network\_flow OR (sourcetype=Sysmon AND EventCode=3)| search process\_name IN ("chrome.exe", "firefox.exe", "winword.exe", "excel.exe", "acrord32.exe", "flashplayer.exe")| stats count by src\_ip dest\_ip dest\_port process\_name| where dest\_ip NOT IN ("") |
| [DS0009](https://attack.mitre.org/datasources/DS0009) | [Process](https://attack.mitre.org/datasources/DS0009) | Analytic 1 - Office Application Process Execution  (source="*WinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode="1") OR (source="*WinEventLog:Security" EventCode="4688") AND (Image= "\winword.exe" OR Image= "\excel.exe" OR Image= "*\powerpnt.exe") AND (CommandLine= "*macro*" OR CommandLine= "*automation*" OR CommandLine= "*shellcode*") AND ParentCommandLine= "*open\*"  Analytic 2 - Unusual Child Process Creation  (source="*WinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode="1") OR (source="*WinEventLog:Security" EventCode="4688") AND (ParentImage= "\winword.exe" OR ParentImage= "\excel.exe" OR ParentImage= "\powerpnt.exe") AND (Image != "\system32\" OR Image != "\*\program files") |

# CVE A CORRIGER URGEMMENT

|  |  |  |  |
| --- | --- | --- | --- |
| CVE ID | CVSS | EPSS | GROUPE ATTAQUANTS |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |