THREAT MAPPING

Potential attack patterns

Company X

Analysis performed on DD/MM/YYYY

Table des matières

[OBJECT 2](#_Toc183607860)

[LIST OF ATTACKER GROUPS 4](#_Toc183607861)

[SOFTWARES USED BY ATTACKERS 6](#_Toc183607862)

[MAPPING TECHNIQUES (G0073) 7](#_Toc183607863)

[[To be adapted to your environment and previous analyses]. 8](#_Toc183607864)

[MITIGATION 8](#_Toc183607865)

[DETECTION 8](#_Toc183607866)

[CVE TO BE CORRECTED URGENTLY 9](#_Toc183607867)

# OBJECT

The purpose of this document is to list possible attackers and attack patterns within our organisation.

This is an incomplete example document.

DEFINITION OF PRIORITIES

[Present here the prioritisation model chosen and justify it].

|  |  |
| --- | --- |
| Target | Priority |
| Our business sector and country | 1 |
| Our business sector | 2 |
| Our customers' domains | 3 |

Explanation: if the attacking group targets our sector of activity in your country, then they are more likely to attack you than if they only target the domain of one of your customers.

# LIST OF ATTACKER GROUPS

[Add or remove columns as required. For example, in some cases it may be useful to list the country associated with the group of attackers].

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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 USED BY ATTACKERS

*For the purposes of this example document, we will use G1007 and G0073, even though they are not in P1 according to our scale. The data in the following table will be incomplete and is intended solely to provide an example of presentation.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 |

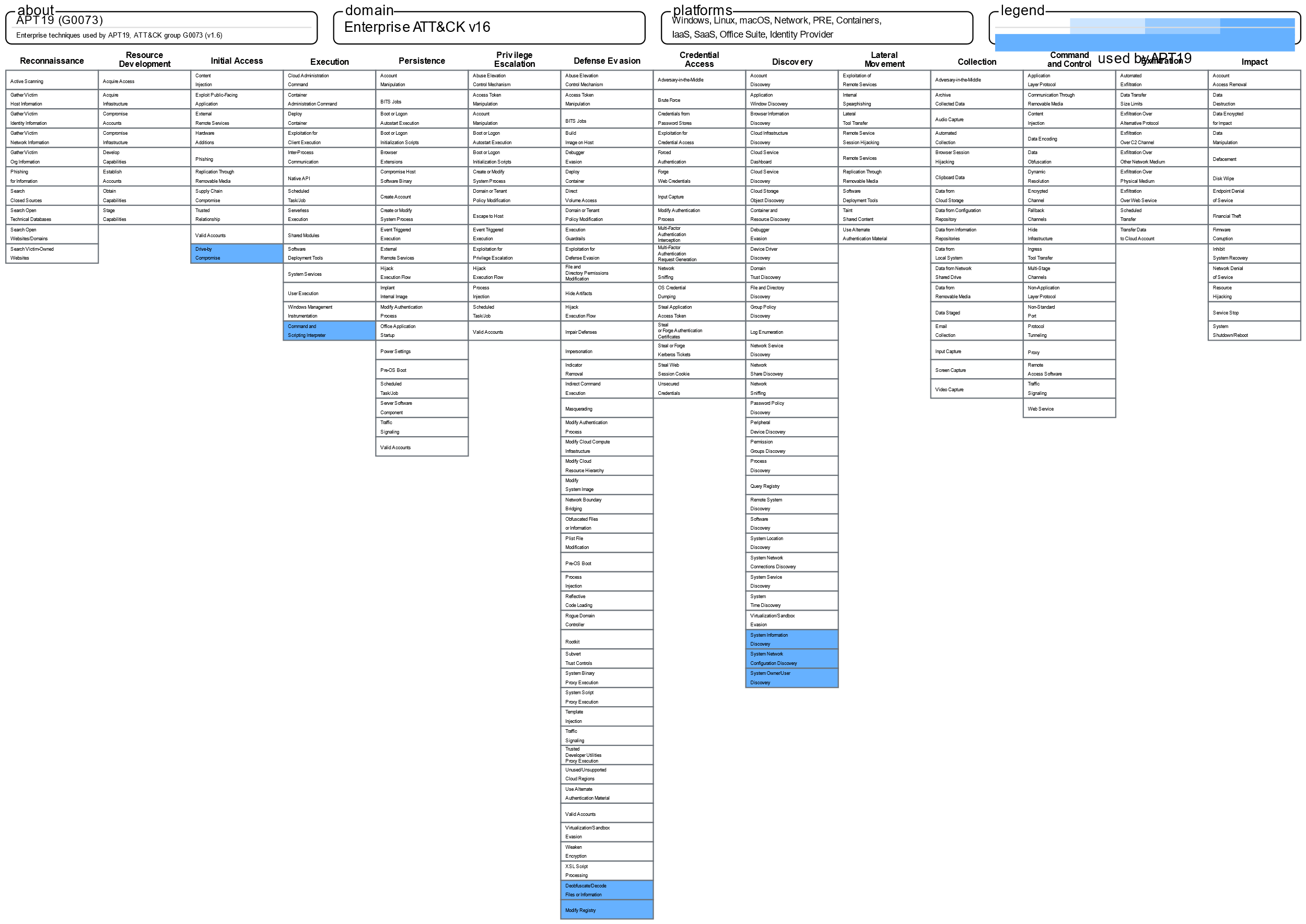
Objective: if a technique is used by several potential attackers, it may make sense to implement countermeasures first.

Why is the ‘domain’ field useful? In some cases, it makes more sense to separate the domains because the people responsible for implementing countermeasures and the issues at stake are not necessarily the same. What's more, depending on your domain and country, you'll potentially have many of the techniques listed here.

# SOFTWARES USED BY ATTACKERS

|  |  |  |  |
| --- | --- | --- | --- |
| 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 |

# MAPPING TECHNIQUES (G0073)



PROTECTION MEASURES

## [To be adapted to your environment and previous analyses].

## 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 TO BE CORRECTED URGENTLY

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