Analyse Morphologique : Comment détecter et caractériser les malwares grâce à Gorille ?

Cyber-Detect

CYBER-DETECT©
MORPHOLOGICAL ANALYSIS

Sylvain CECCHETTO

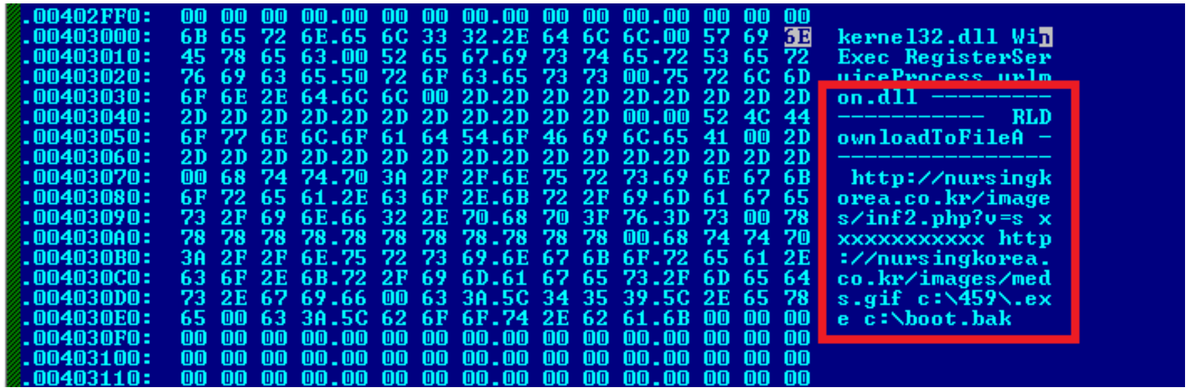
PLAN

- **Analyse morphologique : le moteur de Gorille**
- **Le problème des fichiers packés**
  - Détection de packers
  - Analyse dynamique
- **Les produits**
  - Gorille Expert
  - Gorille Cloud
  - Gorille Patrouille

CYBER-DETECT®
MORPHOLOGICAL ANALYSIS

Détection par signature : historique et problèmes

- De 1990 à 2000 : **le début de l'industrie des antivirus**
  - Création de Panda, Norton, AVG, F-Secure, Bitdefender, Kaspersky, …
- 1999 : **~98 000 malwares** uniques recensés*
- 2001 : création de ClamAV
- 2005 : **~330 000 malwares** uniques recensés*
- 2007 : **~5 500 000** nouveaux malwares **juste pour cette année***



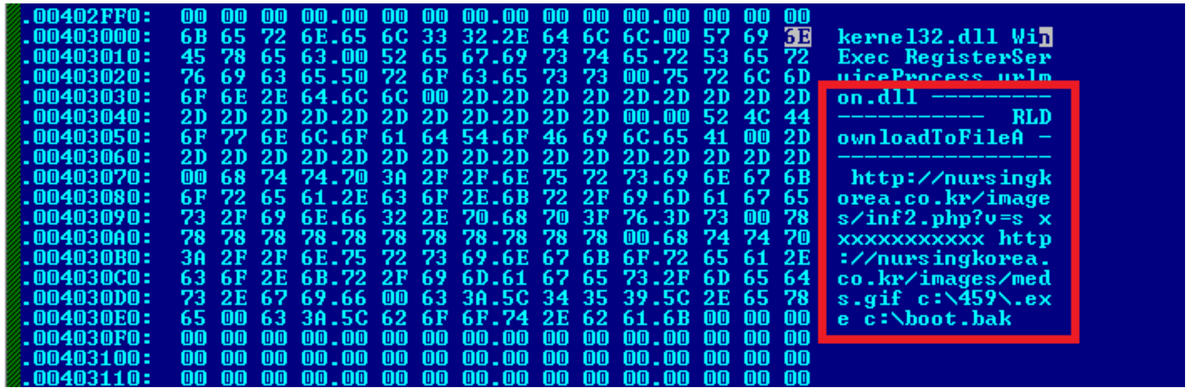
Détection par signature :

- **Fonctionnement :** reconnaitre dans un échantillons une suite continue d'octets commune à un ou plusieurs malwares connus.
- **Avantages :**
  - Simple à mettre en oeuvre
  - Analyse statique et rapide
- **Inconvénients et problèmes :**
  - Chaque jour de nouveaux malwares : les éditeurs doivent continuellement mettre à jour les bases
  - Les malwares polymorphes et packés

*Source : AV-TEST

Détection par signature : historique et problèmes

- De 1990 à 2000 : **le début de l'industrie des antivirus**
  - Création de Panda, Norton, AVG, F-Secure, Bitdefender, Kaspersky, …
- 1999 : **~98 000 malwares** uniques recensés*
- 2001 : création de ClamAV
- 2005 : **~330 000 malwares** uniques recensés*
- 2007 : **~5 500 000** nouveaux malwares **juste pour cette année***



Détection par signature :

- **Fonctionnement :** reconnaitre dans un échantillons une suite continue d'octets commune à un ou plusieurs malwares connus.
- **Avantages :**
  - Simple à mettre en oeuvre
  - Analyse statique et rapide
- **Inconvénients et problèmes :**
  - Chaque jour de nouveaux malwares : les éditeurs doivent continuellement mettre à jour les bases
  - Les malwares polymorphes et packés

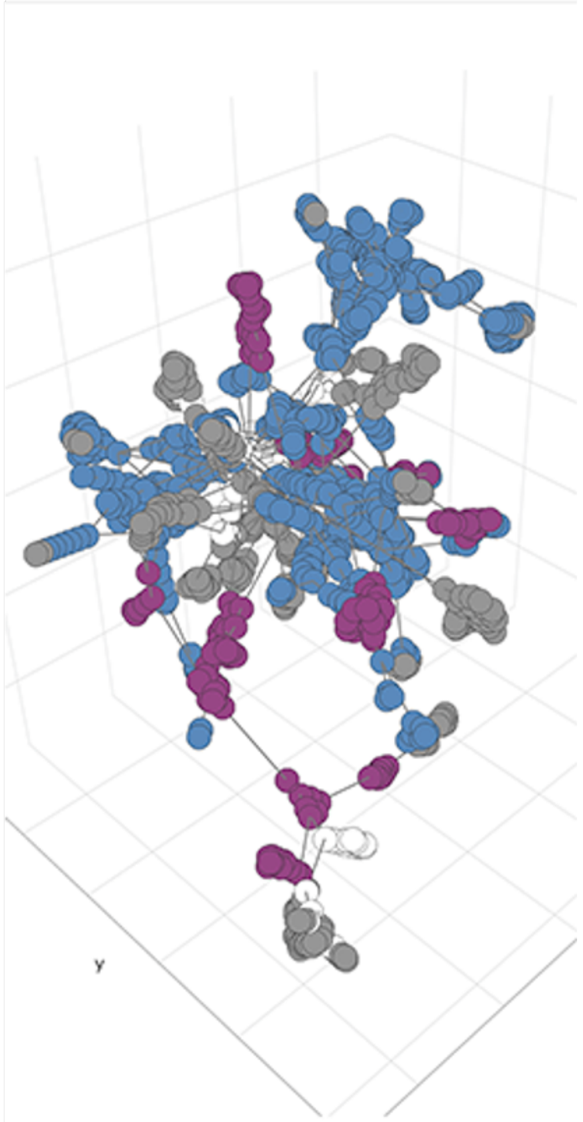
- Exemple : **Détection Emotet par les 68 AV de VirusTotal**
  - 7 septembre 2020 – Alerte de l'ANSSI – Détection 0/68
  - Octobre 2020 – Détection 7/68
  - 18 janvier 2021 – Détection 33/ 68
  - 21 mai 2021 – Détection 39/68

CYBER-DETECT® MORPHOLOGICAL ANALYSIS

*Source : AV-TEST

L’analyse morphologique : une signature 2.0

- **Idée :** conserver le concept de signatures tout en corrigeant les principaux défauts
- L’**analyse morphologique*** consiste à :
  1. **Caractériser les comportements** embarqués dans les fichiers exécutables
  2. **Comparer** ces comportements avec une base de données de comportements connus comme malveillants
- **Objectifs :**
  - ➡ Être résistant aux variants
  - ➡ Une fréquence de mise à jour de la base de données réduite



CYBER-DETECT® MORPHOLOGICAL ANALYSIS

*Guillaume Bonfante, Matthieu Kaczmarek, Jean-yves Marion. Morphological Detection of Malware. International Conference on Malicious and Unwanted Software, Fernando C. Colon Osorio, Oct 2008, Alexendria VA, United States. inria-00330021

*Guillaume Bonfante, Jean-yves Marion, Fabrice Sabatier, Aurélien Thierry. Code synchronization by morphological analysis. MALWARE 2012 - 7th International Conference on Malicious and Unwanted Software, Oct 2012, Fajardo, United States. hal-00764286

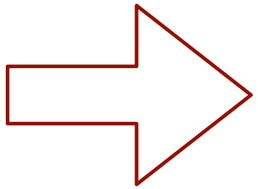
*Guillaume Bonfante, Jean-yves Marion, Fabrice Sabatier. Gorille sniffs code similarities, the case study of Qwerty versus Regin. Malware Conference, Oct 2015, Fajardo, Puerto Rico. pp.8. hal-01263123

Construction des bases

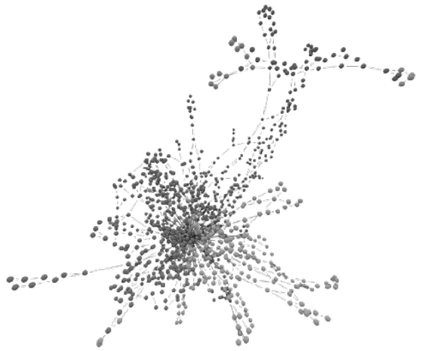
Pour chaque malwares de notre collection

Construction des bases

Pour chaque malwares de notre collection

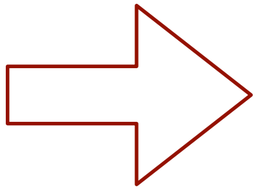


Étape 1 : Construction du graphe de flot de contrôle

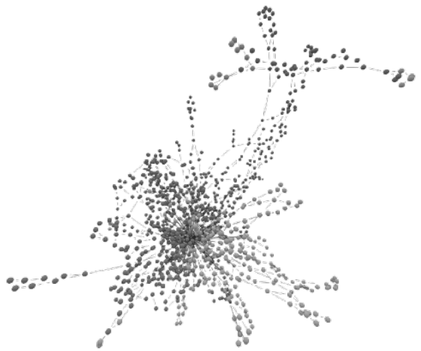


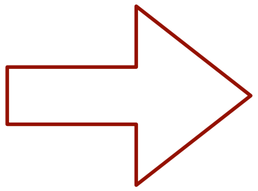
Construction des bases

Pour chaque malwares de notre collection

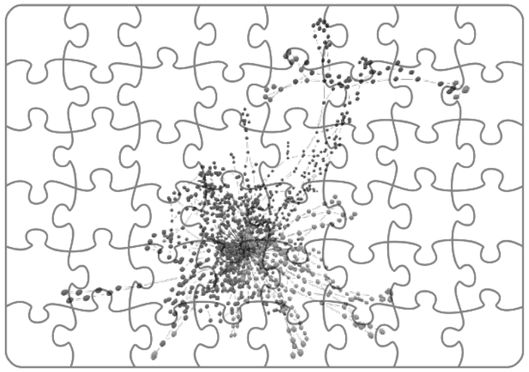


Étape 1 : Construction du graphe de flot de contrôle



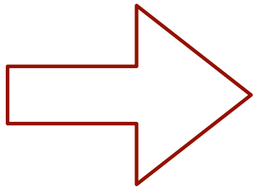


Étape 2 : Découpage en sous-graphes (sites)

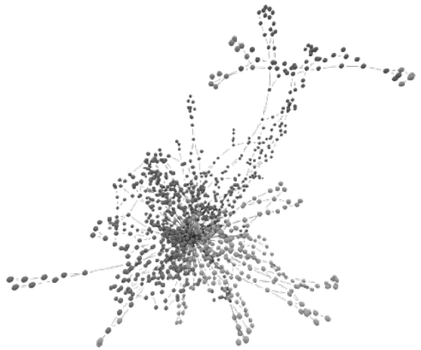


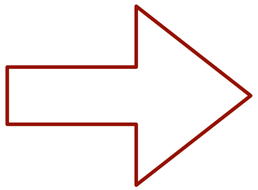
Construction des bases

Pour chaque malwares de notre collection

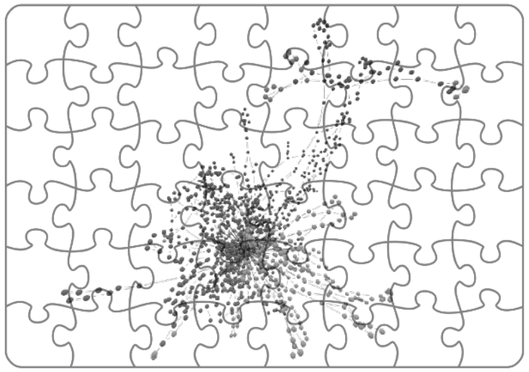


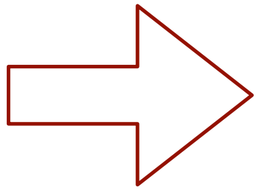
Étape 1 : Construction du graphe de flot de contrôle





Étape 2 : Découpage en sous-graphes (sites)





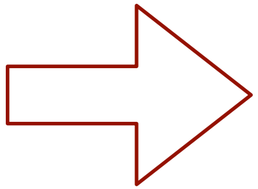
Étape 3 : Ajout des sites dans la base noire

Sites malveillants

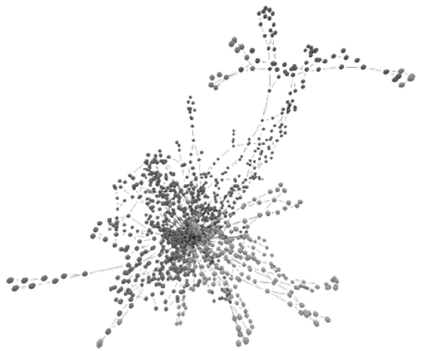
(base noire)

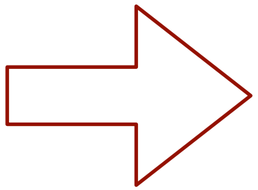
Construction des bases

Pour chaque malwares de notre collection

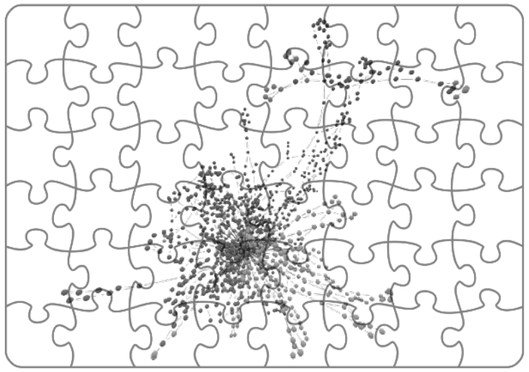


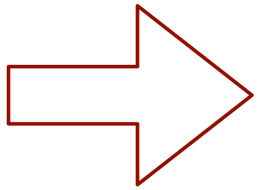
Étape 1 : Construction du graphe de flot de contrôle





Étape 2 : Découpage en sous-graphes (sites)





Étape 3 : Ajout des sites dans la base noire

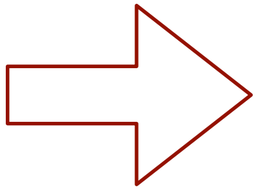
Sites malveillants

(base noire)

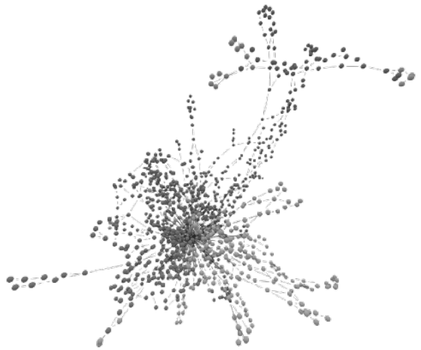
⚠ les malwares ne contiennent pas que du code malveillant

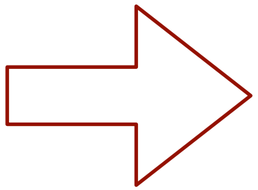
Construction des bases

Pour chaque malwares de notre collection

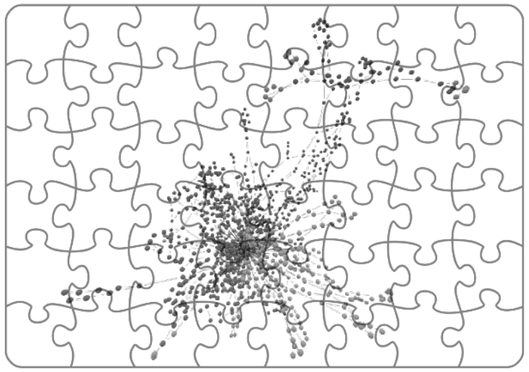


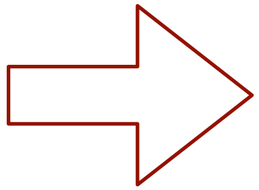
Étape 1 : Construction du graphe de flot de contrôle





Étape 2 : Découpage en sous-graphes (sites)





Étape 3 : Ajout des sites dans la base noire

Sites malveillants (base noire)

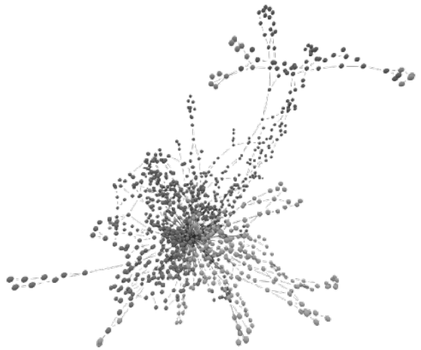
⚠ les malwares ne contiennent pas que du code malveillant

Pour chaque fichier bénin de notre collection

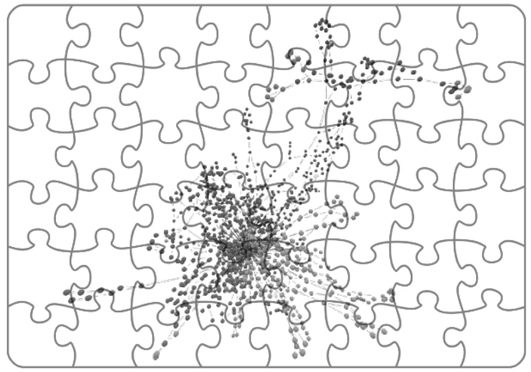
Construction des bases

Pour chaque malwares de notre collection

Étape 1 : Construction du graphe de flot de contrôle



Étape 2 : Découpage en sous-graphes (sites)



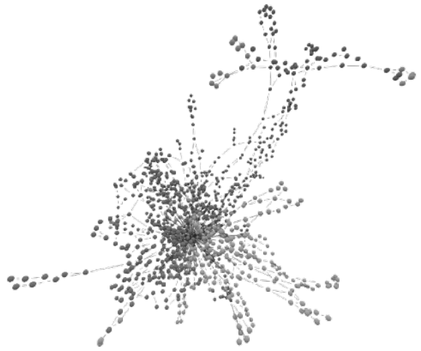
Étape 3 : Ajout des sites dans la base noire

Sites malveillants (base noire)

⚠ les malwares ne contiennent pas que du code malveillant

Pour chaque fichier bénin de notre collection

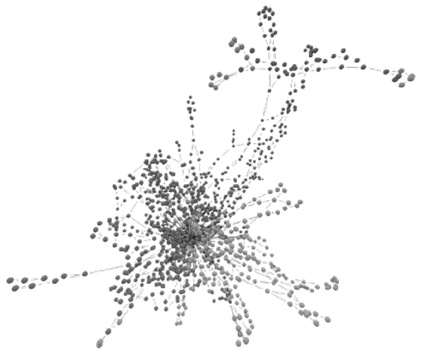
Étape 1 : Construction du graphe de flot de contrôle



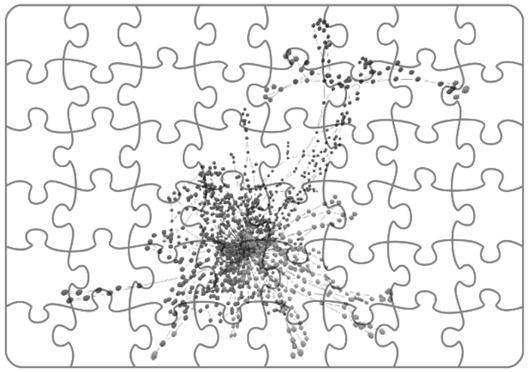
Construction des bases

Pour chaque malwares de notre collection

Étape 1 : Construction du graphe de flot de contrôle



Étape 2 : Découpage en sous-graphes (sites)



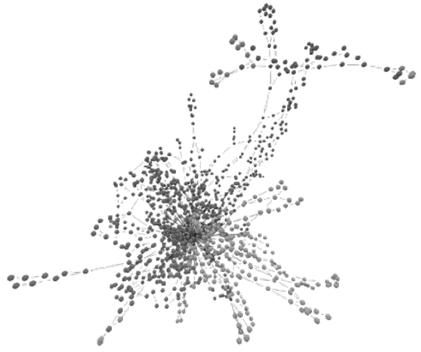
Étape 3 : Ajout des sites dans la base noire

Sites malveillants (base noire)

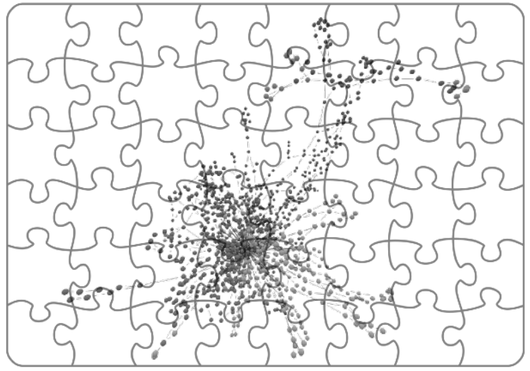
⚠ les malwares ne contiennent pas que du code malveillant

Pour chaque fichier bénin de notre collection

Étape 1 : Construction du graphe de flot de contrôle



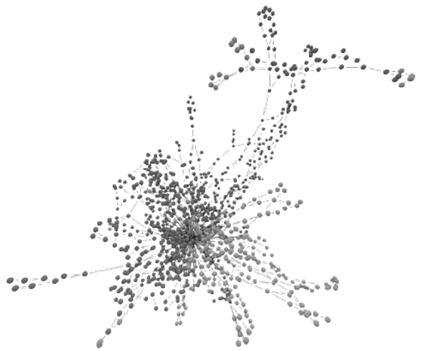
Étape 2 : Découpage en sous-graphes (sites)



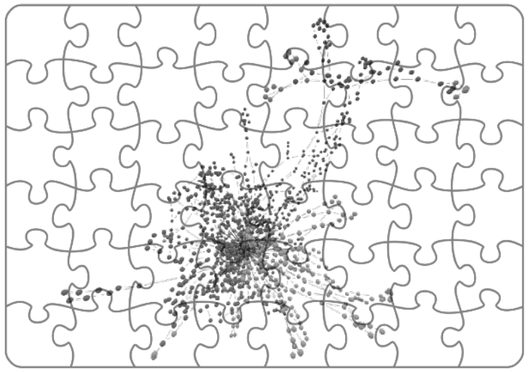
Construction des bases

Pour chaque malwares de notre collection

Étape 1 : Construction du graphe de flot de contrôle



Étape 2 : Découpage en sous-graphes (sites)



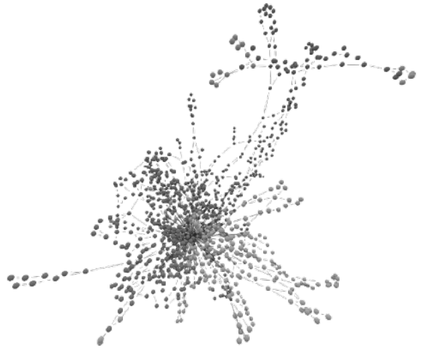
Étape 3 : Ajout des sites dans la base noire

Sites malveillants (base noire)

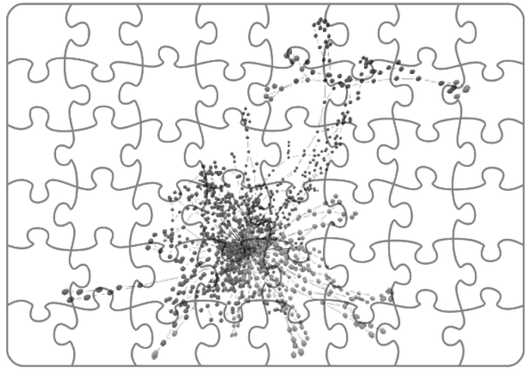
⚠ les malwares ne contiennent pas que du code malveillant

Pour chaque fichier bénin de notre collection

Étape 1 : Construction du graphe de flot de contrôle



Étape 2 : Découpage en sous-graphes (sites)

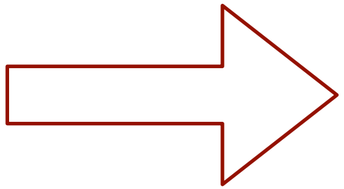


Étape 3 : Ajout des sites dans la base blanche

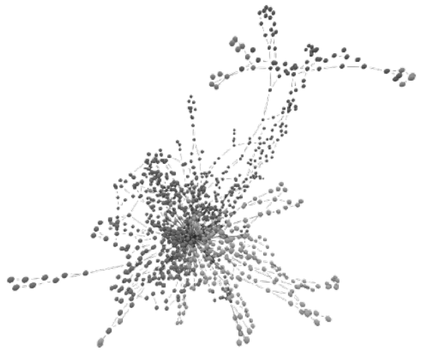
Sites bienveillants (base blanche)

Fichier binaire
à analyser

Fichier binaire
à analyser

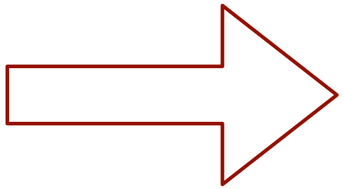


Étape 1 : Construction du graphe de flot de contrôle

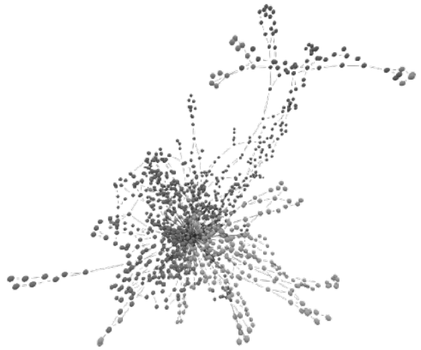


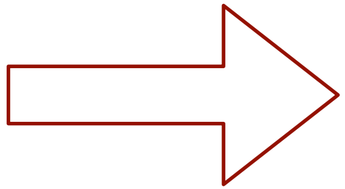
L’analyse morphologique en pratique

Fichier binaire
à analyser

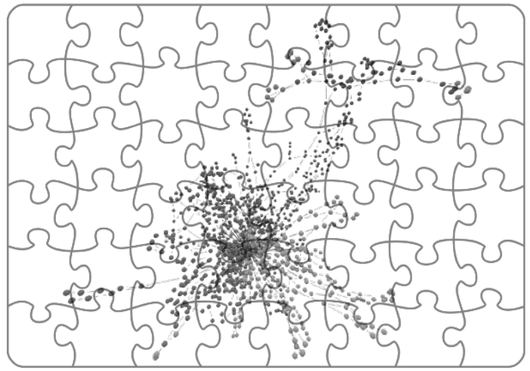


Étape 1 : Construction du graphe de flot de contrôle





Étape 2 : Découpage en sous-graphes (sites)

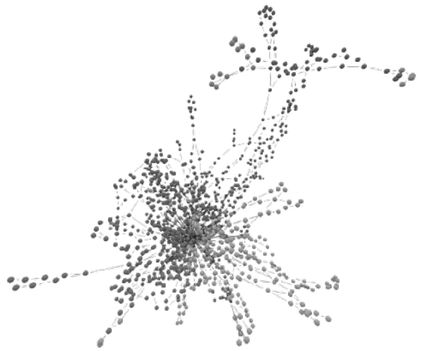


- Chaque site caractérise un comportement
- L’ensemble des sites détermine le comportement global du binaire

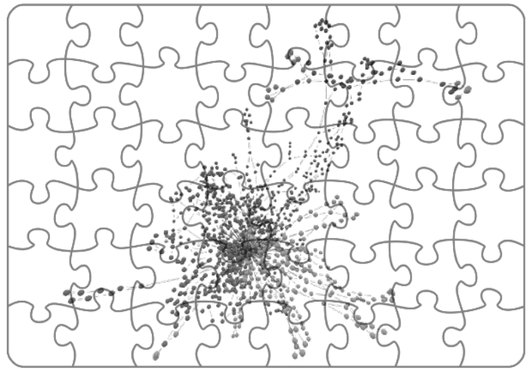
L'analyse morphologique en pratique

Fichier binaire
à analyser

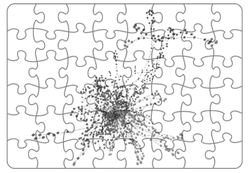
Étape 1 : Construction du graphe de flot de contrôle

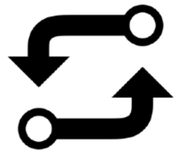


Étape 2 : Découpage en sous-graphes (sites)



- Chaque site caractérise un comportement
- L'ensemble des sites détermine le comportement global du binaire





Sites malveillants

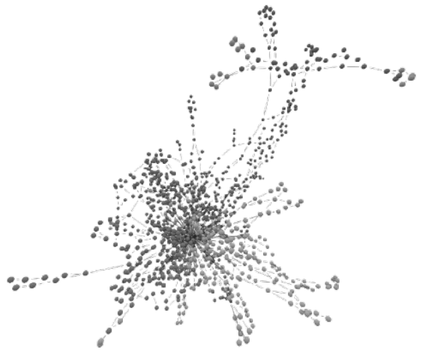
Sites bienveillants

Étape 3 : Comparaison des sites avec la base de données

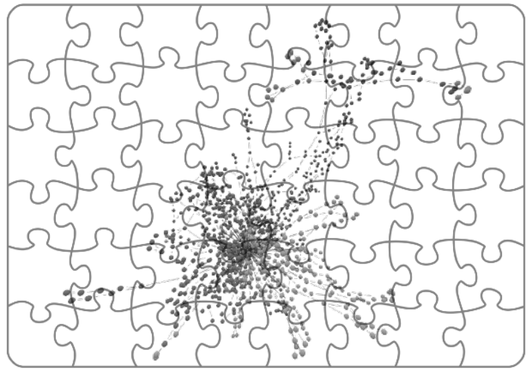
L'analyse morphologique en pratique

Fichier binaire
à analyser

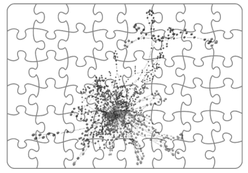
Étape 1 : Construction du graphe de flot de contrôle

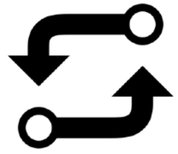


Étape 2 : Découpage en sous-graphes (sites)



- Chaque site caractérise un comportement
- L'ensemble des sites détermine le comportement global du binaire



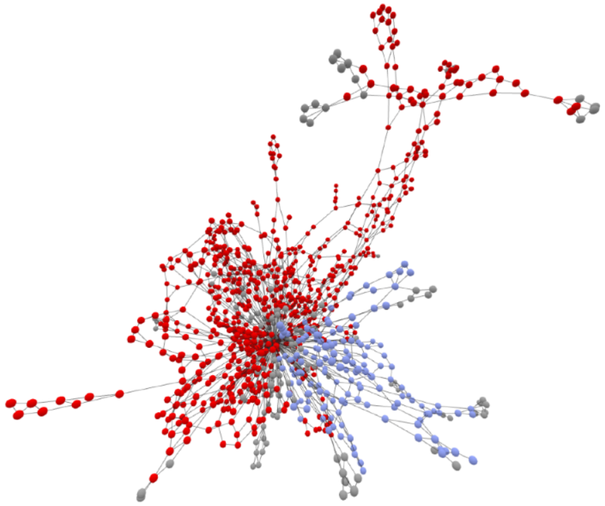


Sites malveillants

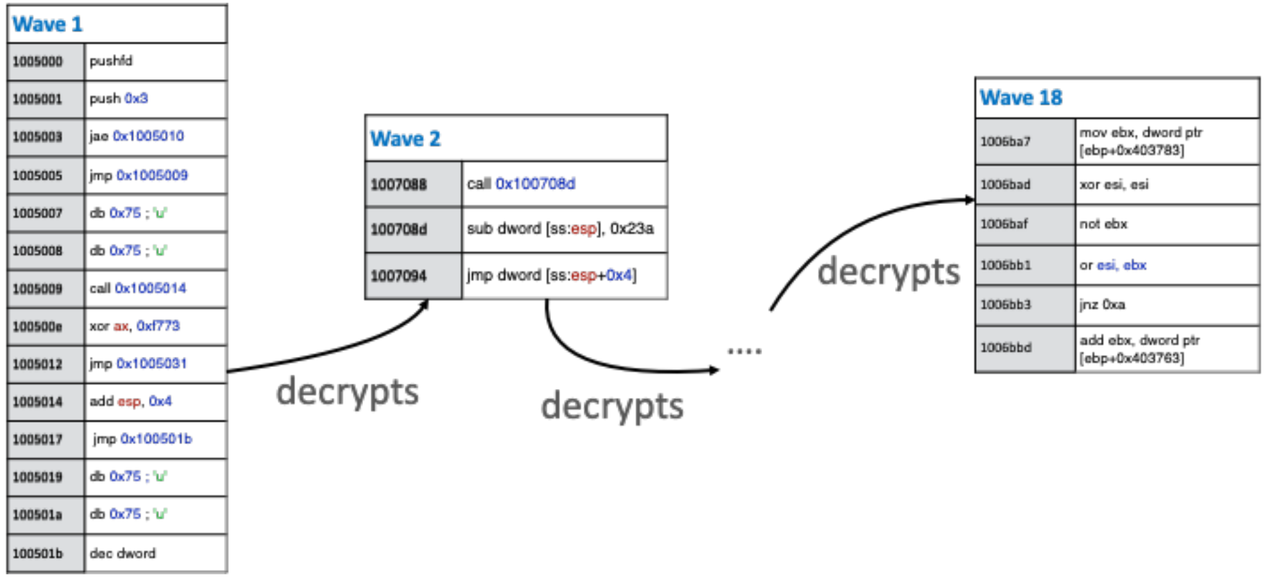
Sites bienveillants

Étape 3 : Comparaison des sites avec la base de données

Étape 4 : La corrélation des sites déclenche ou non une alerte



Le problème des fichiers protégés et packés



- **Problème :** certains malwares sont protégés :
  - Obfuscations
  - Packers (code auto-modifiant)
  - …

➡ **Objectif 1 :** Est-ce que le binaire est protégé ?

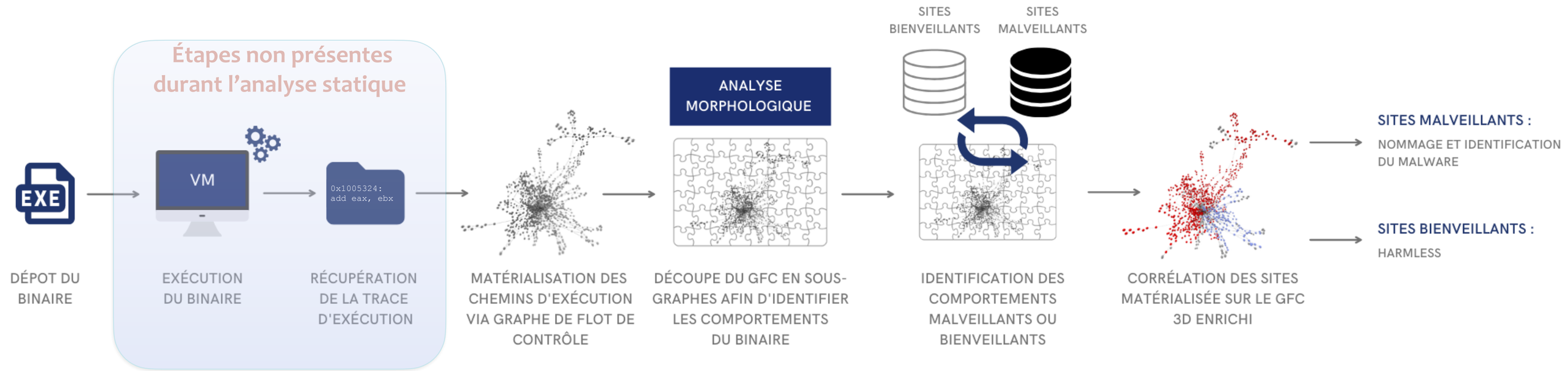
➡ **Objectif 2 :** Est-ce que je peux « dé-packer » le binaire ?

CYBER-DETECT®
MORPHOLOGICAL ANALYSIS

Gorille packer detection

- **Objectif :** détecter les samples packés
- **Solution 1 :** utilisation de Detect It Easy (règles YARA)
- **Solution 2 :** utiliser l'analyse morphologique
  - Génération d'une base contenant des sites de fichiers packés

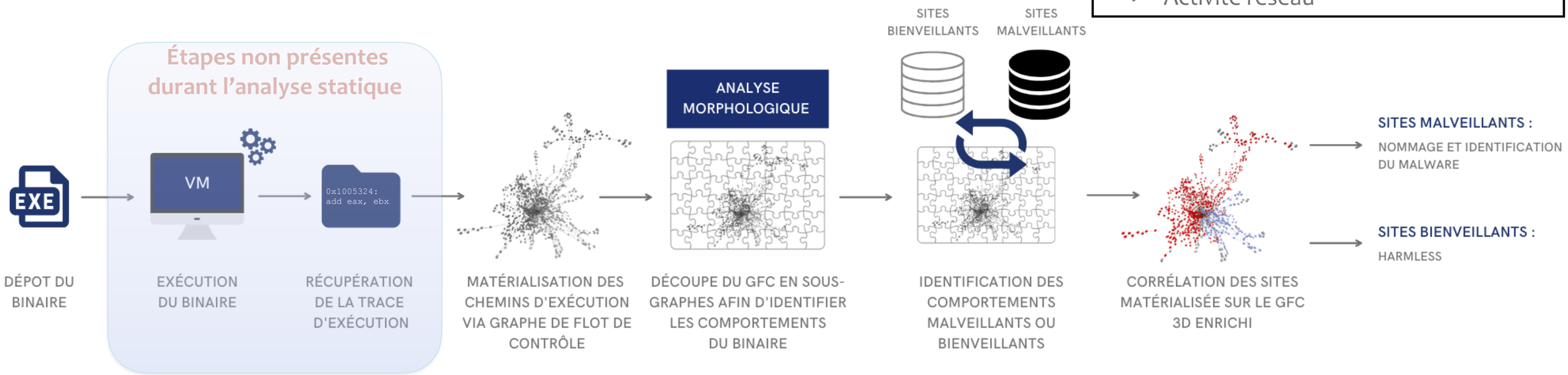
- Utilisation d'un moteur d'analyse dynamique
  - By-pass des techniques d'anti-analyse
  - Augmentation de la couverture de code désassemblé



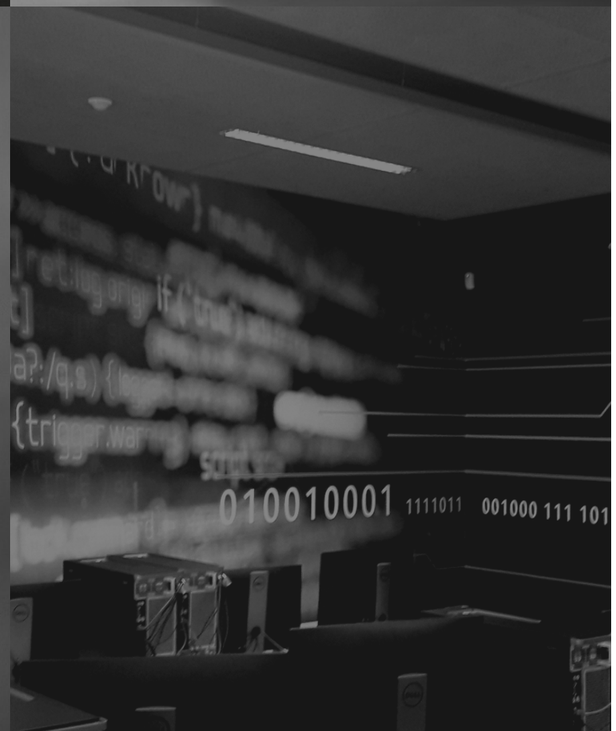
CYBER-DETECT® MORPHOLOGICAL ANALYSIS

- Utilisation d'un moteur d'analyse dynamique
  - By-pass des techniques d'anti-analyse
  - Augmentation de la couverture de code désassemblé

- Récupération d'informations supplémentaires
  - Dump des différentes vagues
  - Screenshots
  - Fichiers créés, exécutés, supprimés, …
  - Clés de registre Windows
  - Activité réseau



CYBER-DETECT® MORPHOLOGICAL ANALYSIS

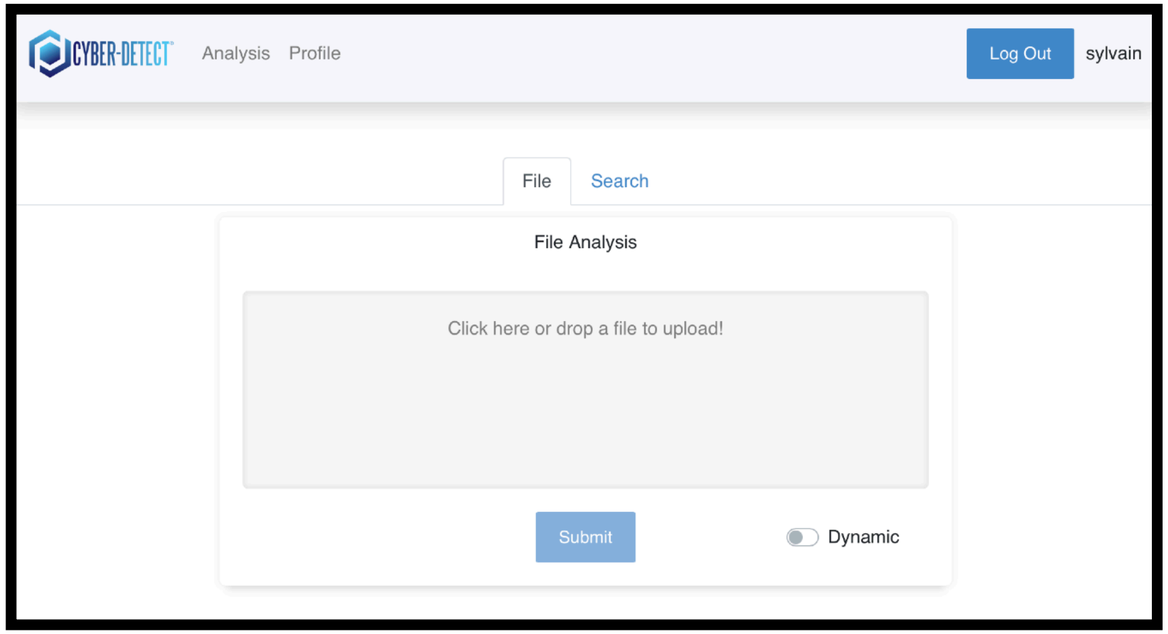



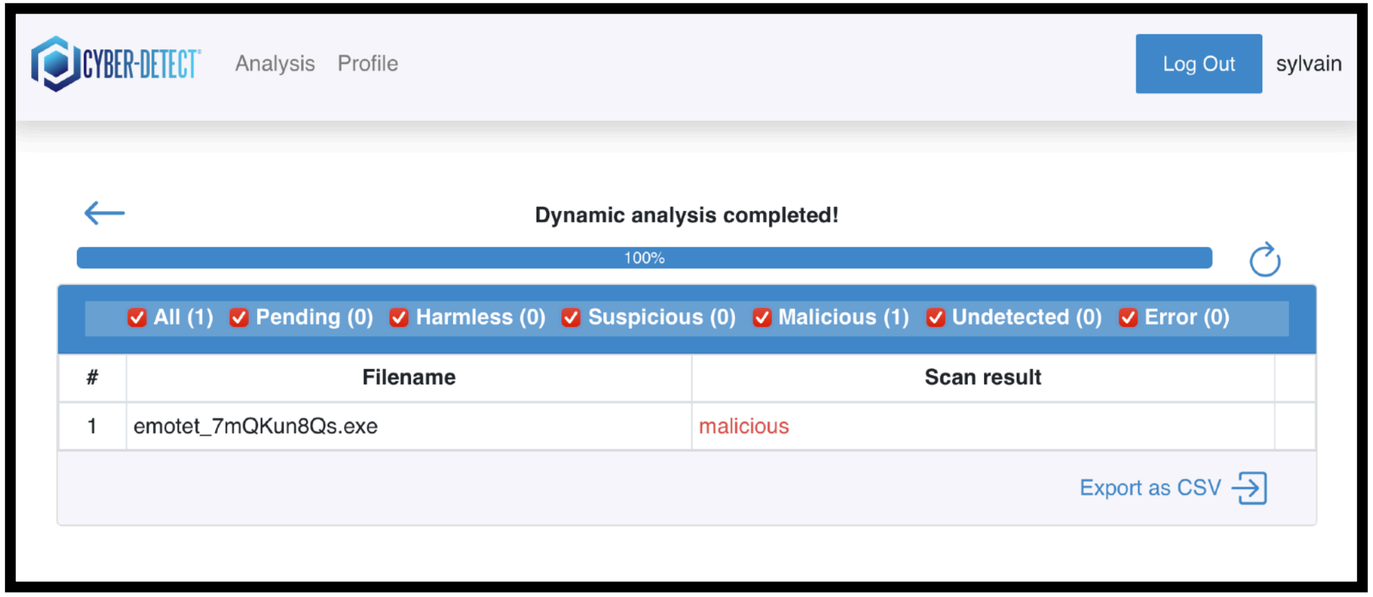
Gorille Expert

- Destiné aux analyses forensic
  - Rétro-ingénierie
  - Analyse post-incident
  - Comparaison de binaires
  - …
- Analyse statique et dynamique
- Outil en ligne de commande
  - Entièrement paramétrable
- Possibilité de créer ses propres bases de données
- Interfaçable avec IDA ou tout autre désassembleur

CYBER-DETECT®
MORPHOLOGICAL ANALYSIS

- **Application web** pour l'analyse et la détection des logiciels malveillants
  - 100% cloud ou *on premise*
  - API REST
  - Gestion des utilisateurs
  - Ne nécessite pas la gestion d'une base de données
  - Cache d'analyse





CYBER-DETECT® MORPHOLOGICAL ANALYSIS

e80bff855228e7b8e810ac5d10e25f61861b946cb90b1d714cd56dbe599c8015.exe

General | DIE | Gorille packer detection | Gorille static | 3D graph

Process: **e80bff855228e7b8e810ac5d10e25f61861b946cb90b1d714cd56dbe599c8015.exe**

MALICIOUS

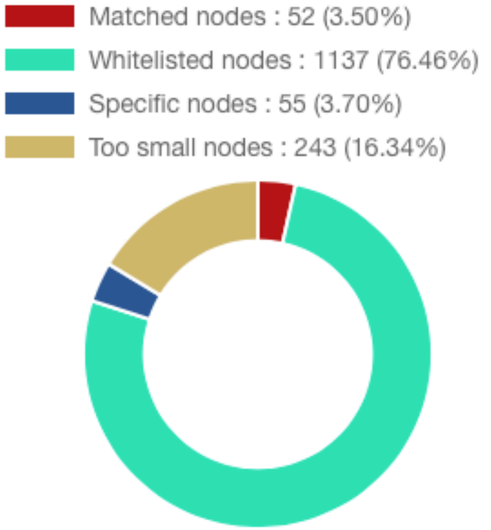
Process information

Export

Process name	e80bff855228e7b8e810ac5d10e25f61861b946cb90b1d714cd56dbe599c8015.exe
Status	0
Total sites	44
Waves	1
Protection	none

Program morphological analysis

Export



Malware database matches

Export

#	Matched sites	File name	Reputation
1	41% (18)	Generic malware	-34
2	32% (14)	Zbot	-18
3	32% (14)	Generic malware	-26
4	32% (14)	Zbot	-20
5	18% (8)	Generic malware	-9
6	16% (7)	Generic malware	-14

e80bff855228e7b8e810ac5d10e25f61861b946cb90b1d714cd56dbe599c8015.exe

General | DIE | Gorille packer detection | Gorille static | 3D graph

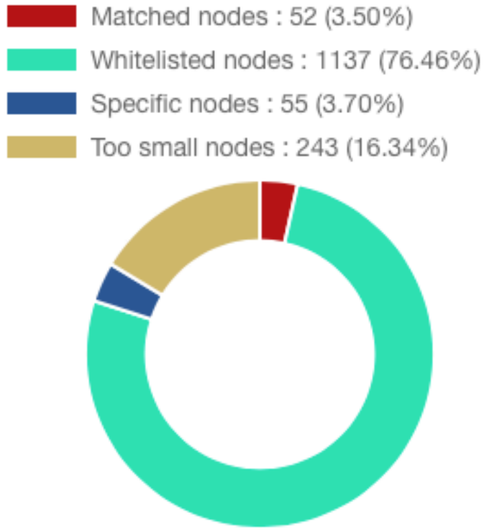
Process: **e80bff855228e7b8e810ac5d10e25f61861b946cb90b1d714cd56dbe599c8015.exe**

MALICIOUS

Process information Export

Process name	e80bff855228e7b8e810ac5d10e25f61861b946cb90b1d714cd56dbe599c8015.exe
Status	0
Total sites	44
Waves	1
Protection	none

Program morphological analysis Export



Malware database matches Export

#	Matched sites	File name	Reputation
1	41% (18)	Generic malware	-34
2	32% (14)	Zbot	-18
3	32% (14)	Generic malware	-26
4	32% (14)	Zbot	-20
5	18% (8)	Generic malware	-9
6	16% (7)	Generic malware	-14

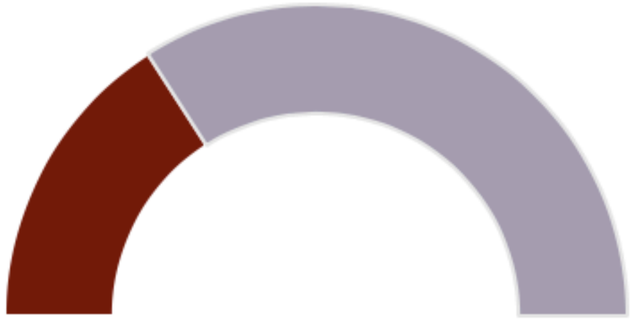
e80bff855228e7b8e810ac5d10e25f61861b946cb90b1d714cd56dbe599c8015.exe

General | DIE | Gorille packer detection | Gorille static | 3D graph

Match: **Zbot**

Matching malware information	Export
Malware name	Zbot
Total malicious sites	131
MD5	f1b0fafd5ba0e1cf7f52 0f3b341a2021
Reputation	-18

Submitted file sites Export



Zbot sites Export

- Mitre attack
- Malpedia
- Signature authenticode
- URL, strings, sections, …

hermeticWiper_2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf.exe

Result | File information | Mitre | Gorille packer detection | Gorille static | 3D graph

HermeticWiper

HermeticWiper is a data wiper that has been used since at least early 2022, primarily against Ukraine with additional activity observed in Latvia and Lithuania. Some sectors targeted include government, financial, defense, aviation, and IT services.

ID	S0697
Aliases	Trojan.Killdisk, DriveSlayer
Type	malware
Platforms	Windows

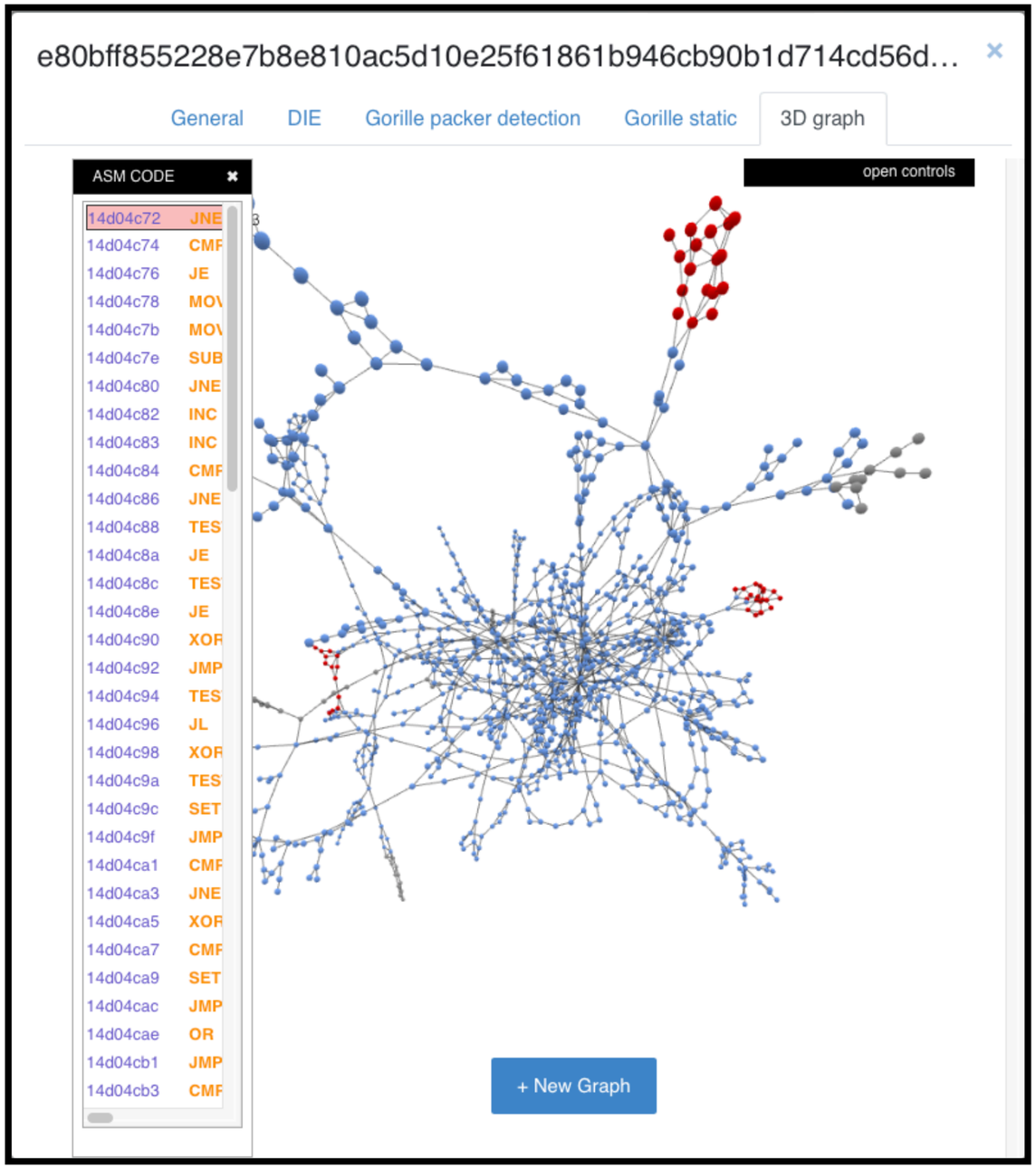
Techniques used

ID	Name	Use
T1561.001	Disk Content Wipe	HermeticWiper has the ability to corrupt disk partitions and obtain raw disk access to destroy data.
T1036.005	Match Legitimate Name or Location	HermeticWiper has used the name `postgressql.exe` to mask a malicious payload.
T1543.003	Windows Service	HermeticWiper can load drivers by creating a new service using the `CreateServiceW` API.
T1489	Service Stop	HermeticWiper has the ability to stop the Volume Shadow Copy service.
T1134	Access Token Manipulation	HermeticWiper can use `AdjustTokenPrivileges` to grant itself privileges for debugging with `SeDebugPrivilege`, creating backups with `SeBackupPrivilege`, loading drivers with `SeLoadDriverPrivilege`, and shutting down a local system with `SeShutdownPrivilege`.
T1070.001	Clear Windows Event Logs	HermeticWiper can overwrite the `C:\Windows\System32\winevt\Logs` file on a targeted system.
T1485	Data Destruction	HermeticWiper can recursively wipe folders and files in `Windows`, `Program Files`, `Program Files(x86)`, `PerfLogs`, `Boot, System`, `Volume Information`, and `AppData` folders using `FSCTL_MOVE_FILE`. HermeticWiper can also overwrite symbolic links and big files in `My Documents` and on the Desktop with random bytes.
T1484.001	Group Policy Modification	HermeticWiper has the ability to deploy through an infected system's default domain policy.
T1059.003	Windows Command Shell	HermeticWiper can use `cmd.exe /Q/c move CSIDL_SYSTEM_DRIVE\temp\sys.tmp1

Les modules de Gorille Cloud

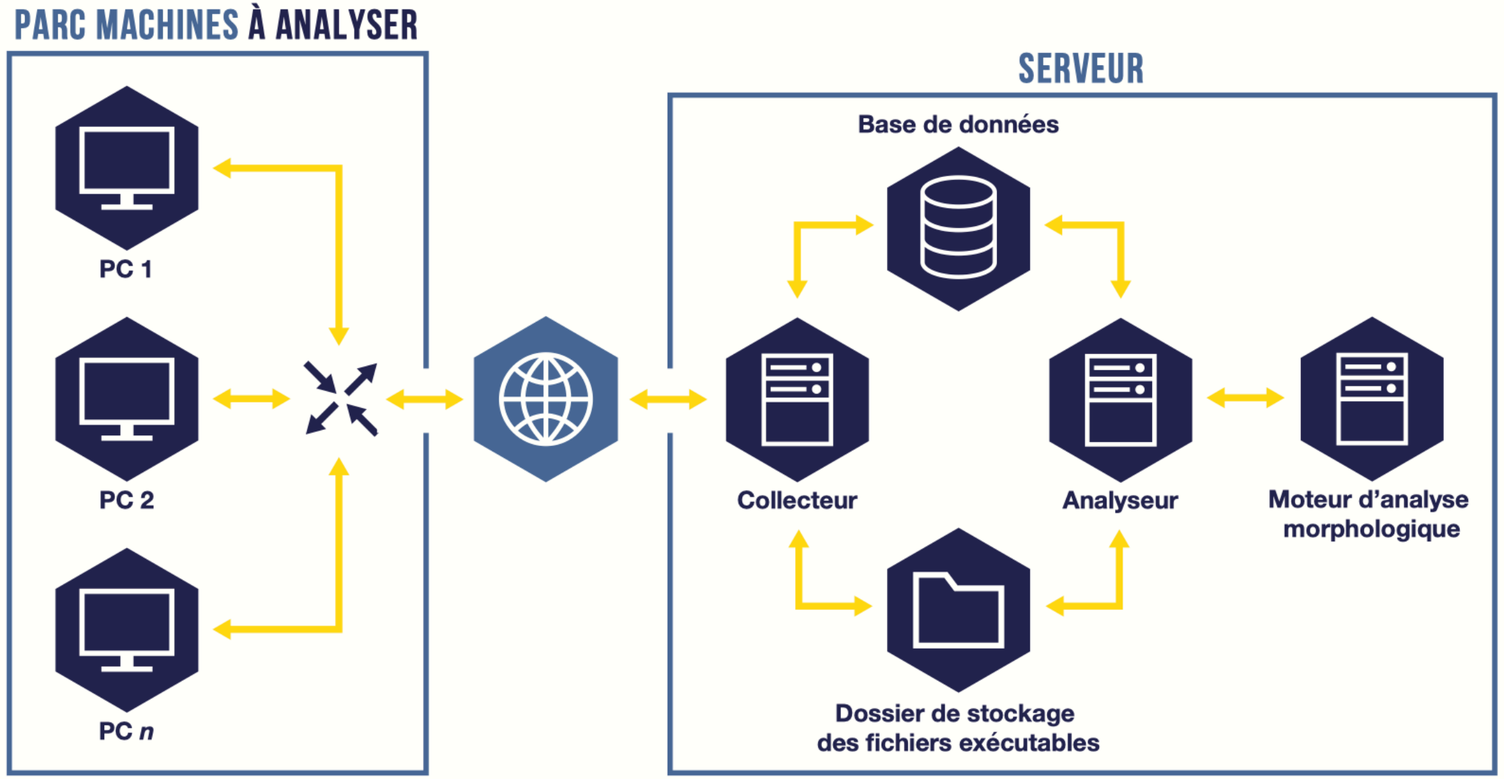
- **Détection et caractérisation des logiciels malveillants**
  - Whitelist (NSRL, logiciels couramment utilisés, distributions et mises à jour Windows, …)
  - Analyse morphologique Gorille statique
  - Analyse morphologique Gorille dynamique
  - Mitre Attack
- **Détection des installers, packers, archives, …**
  - Detect It easy (DIE)
  - Gorille Packer Detection (analyse morphologique Gorille packers)
- **Dé-package, dé-archivage, …**
  - Outils open source (upx, innoextract, unzip, …)
  - Exécution en sandbox
- **Visualisation du binaire sous la forme d'un graphe 3D**

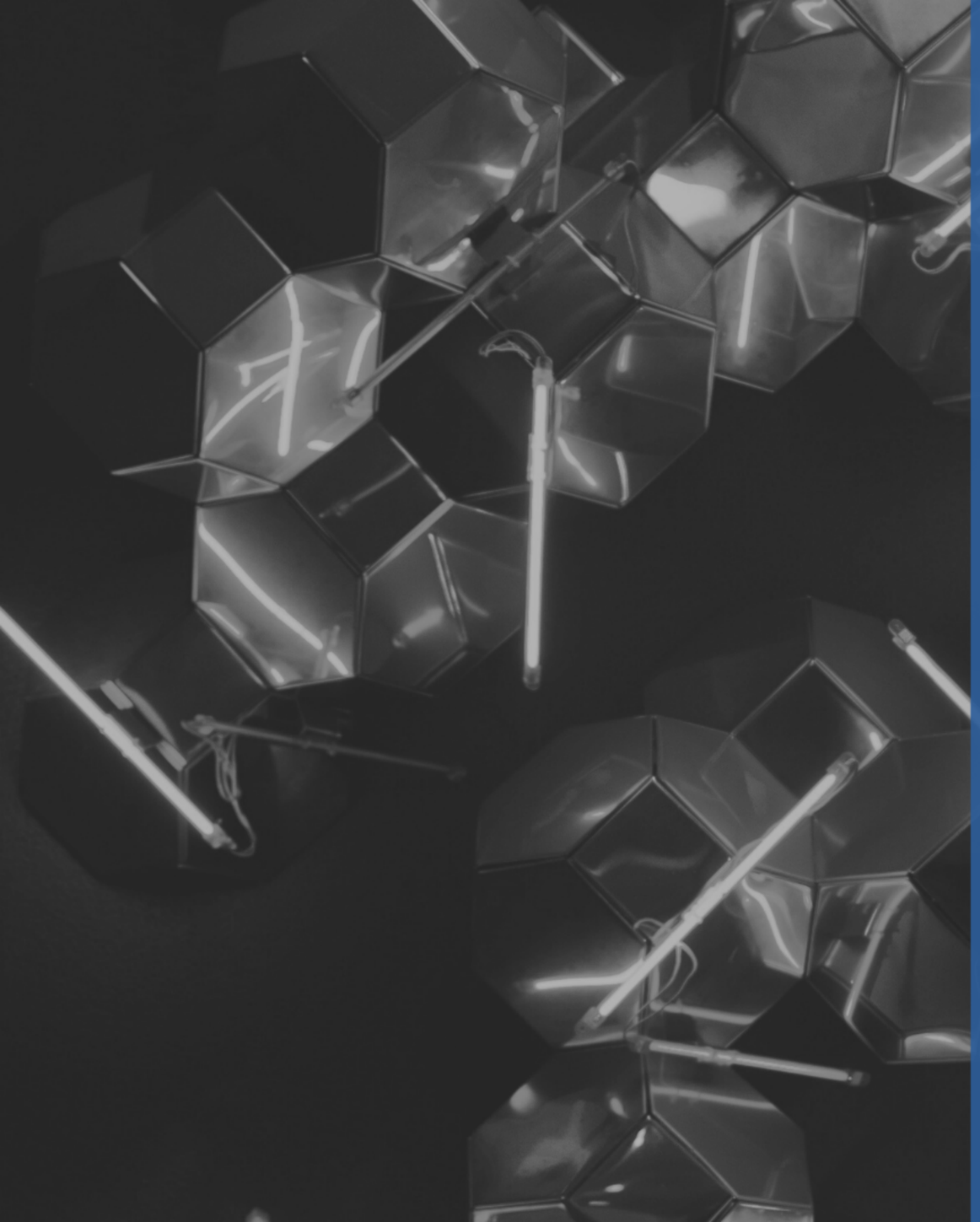
CYBER-DETECT®
MORPHOLOGICAL ANALYSIS



- **Analyse déportée d'un parc informatique pour la détection de logiciels malveillants**
  - 100% cloud ou *on premise*
  - Cohabitation aves les solutions antivirus existantes sur le parc
  - **Objectif :** débusquer la présence d'une menace dormante

1. **Récupération des fichiers exécutables** présents sur les postes à analyser
   - Utilisation d'une *whitelist*
2. **Analyse morphologique** asynchrone des fichiers récupérés
3. **Génération d'un rapport**
   - Liste des machines infectées
   - Liste des menaces découvertes
   - …





RESTONS EN CONTACT

CYBER-DETECT®
MORPHOLOGICAL ANALYSIS

Campus ARTEM
82, rue du Sergent Blandan
54000 NANCY

s.cecchetto@cyber-detect.eu