Introduction à l'analyse de Malwares

Mickaël OHLEN – IR3

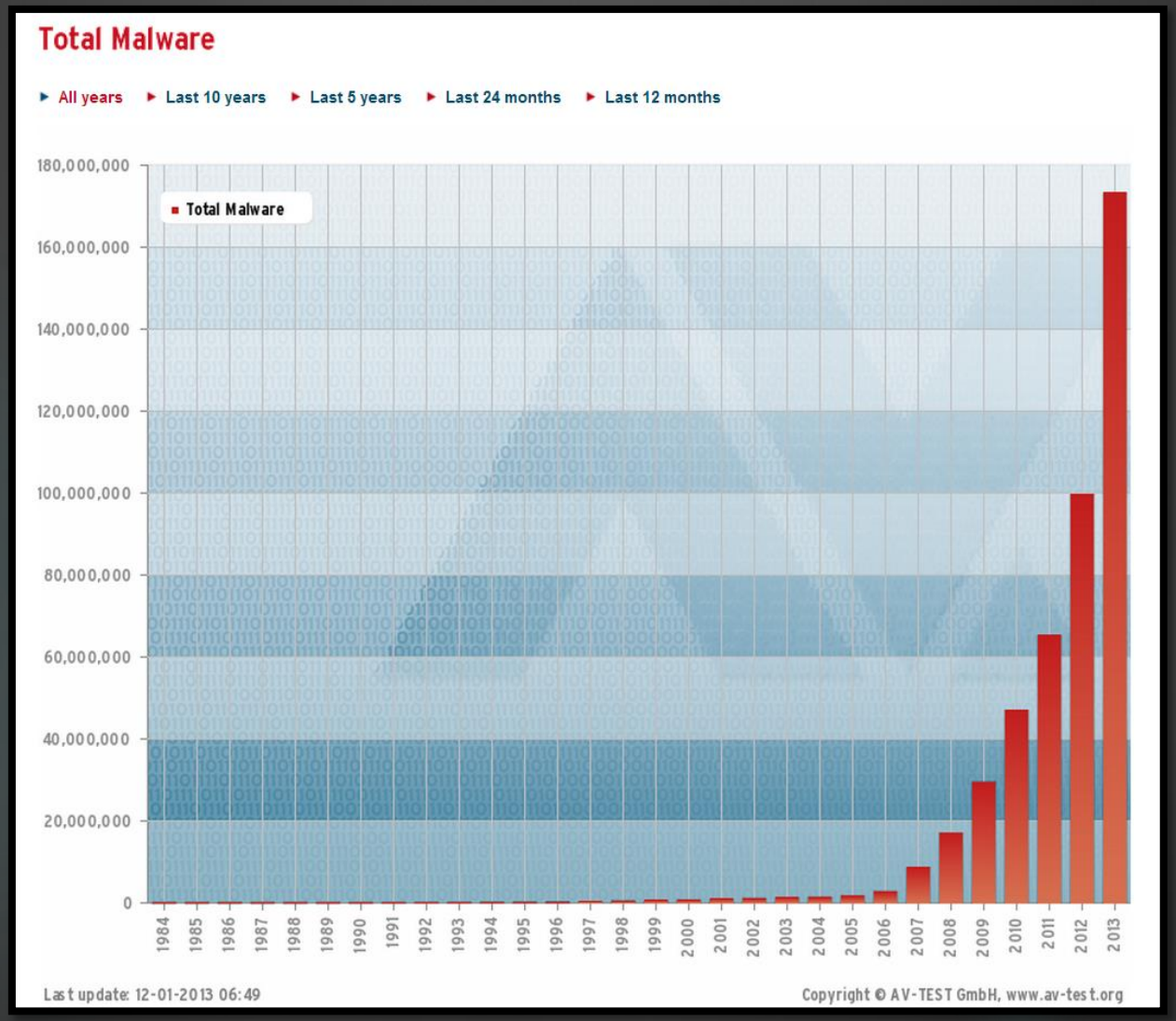
Plan

- 1. Qu'est ce qu'un malware ?
- 2. Analyse
- 3. Techniques d'obfuscation
- 4. Démonstration (Analyse de CLogger)

- 1. Qu'est ce qu'un malware ?
- 2. Analyse
- 3. Techniques d'obfuscation
- 4. Démonstration (Analyse de CLogger)

« Un *malware* est un logiciel créé dans le but de compromettre un système informatique sans l'accord du propriétaire de ce système. »

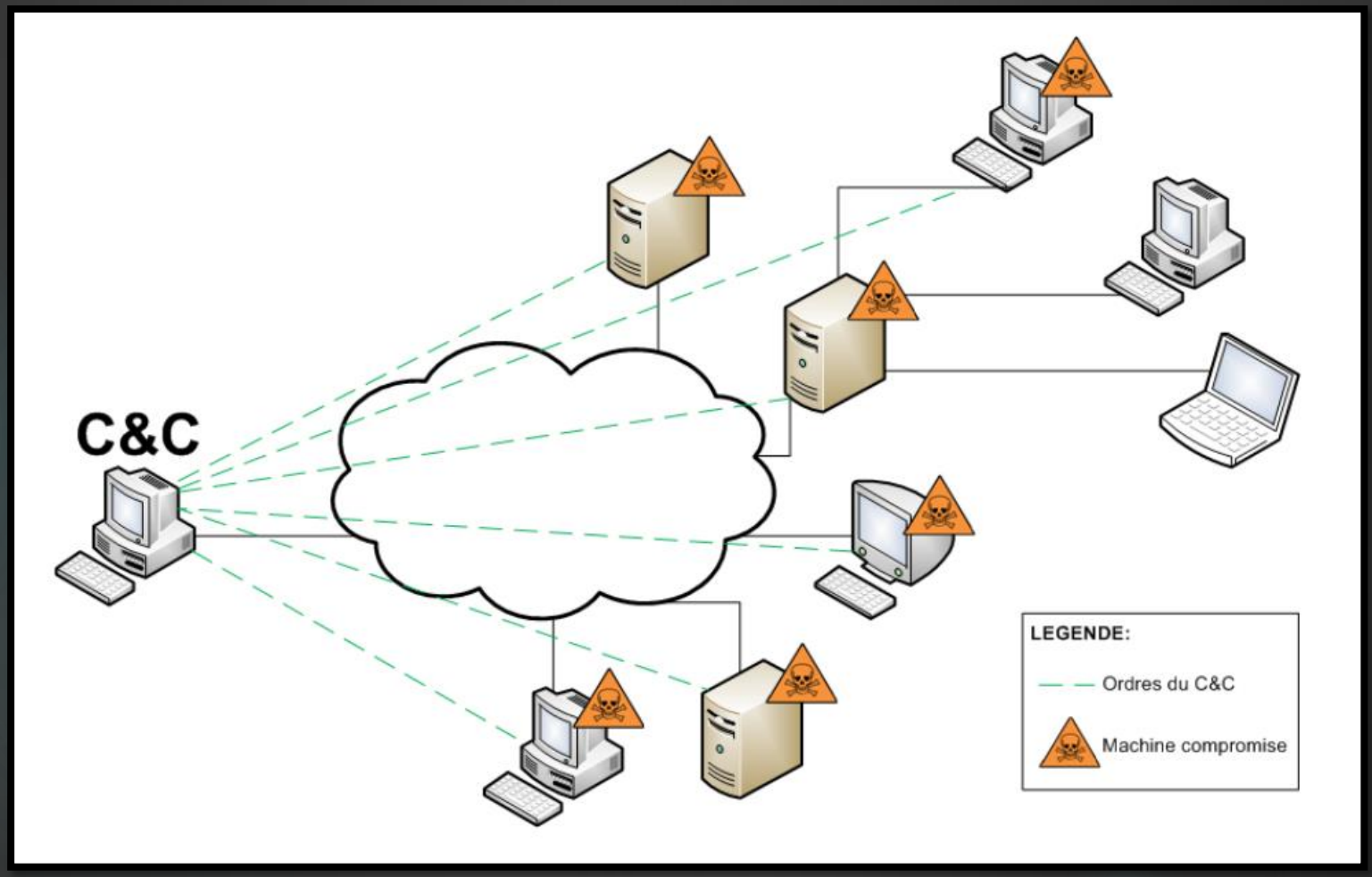
Ils nous envahissent !



Les familles de Malwares

- Backdoor
- Ransomware
- Stealer
- Rootkit

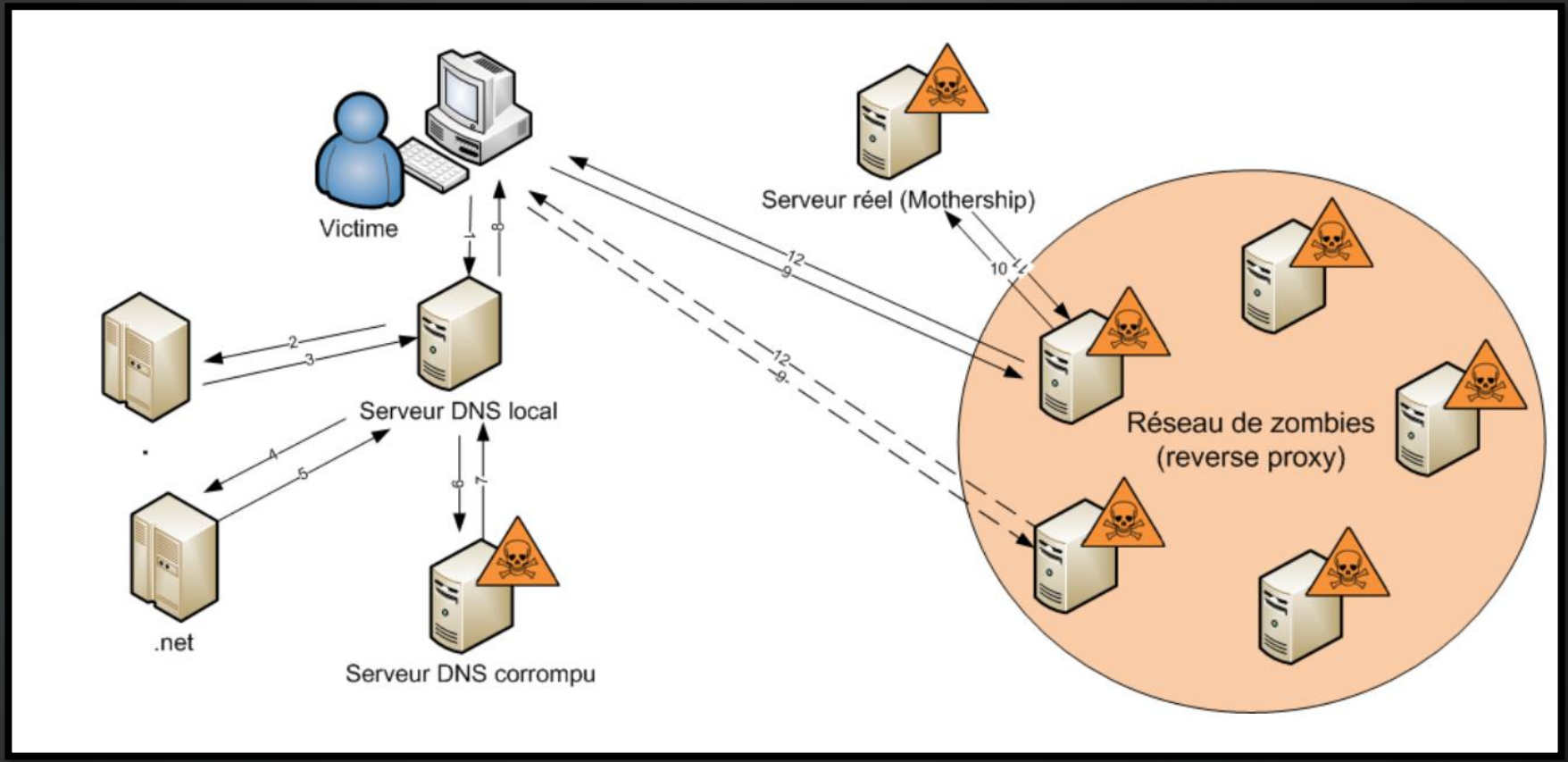
Command and Control (C&C)



Communication avec le C&C

- MAJ des noms de domaines
  - Le C&C transmet une nouvelle liste de noms de domaines.
- Fast flux
  - 1 nom de domaine = plusieurs adresses IP
- DGA (Domain Generation Algorithms)
  - Génération d'un très grand nombre d'adresses DNS pour contacter un C&C.
    - Exemple : Conficker > 50000 domaines par jour

Fast flux simple



Techniques de persistance

- Base de registre
  - [HKLM]\Software\Microsoft\Windows\CurrentVersion\Run]
- Fichier
  - C:\boot.ini
- Service
  - [HKLM]/SYSTEM/CurrentControlSet/Service
- Driver

Techniques de dissimulation

- Injection de code
  - Se cacher dans un processus existant
- Hook
  - Remplacer un appel système

- 1. Qu'est ce qu'un malware ?
- 2. Analyse
- 3. Techniques d'obfuscation
- 4. Démonstration (Analyse de CLogger)

Pourquoi analyser un malware ?

- Comprendre son fonctionnement
  - Quel est l'**objectif** du malware ?
  - Quelles sont ses **actions** ?
  - Comment se **propage** t-il ?
  - Quelle est son **origine** ?
- Définir des méthodes d'éradication
  - Comment **s'en débarrasser** ?
  - Comment **retrouver** les machines infectées ?
  - Comment **prévenir** une infection future ?

De quoi a t-on besoin ?

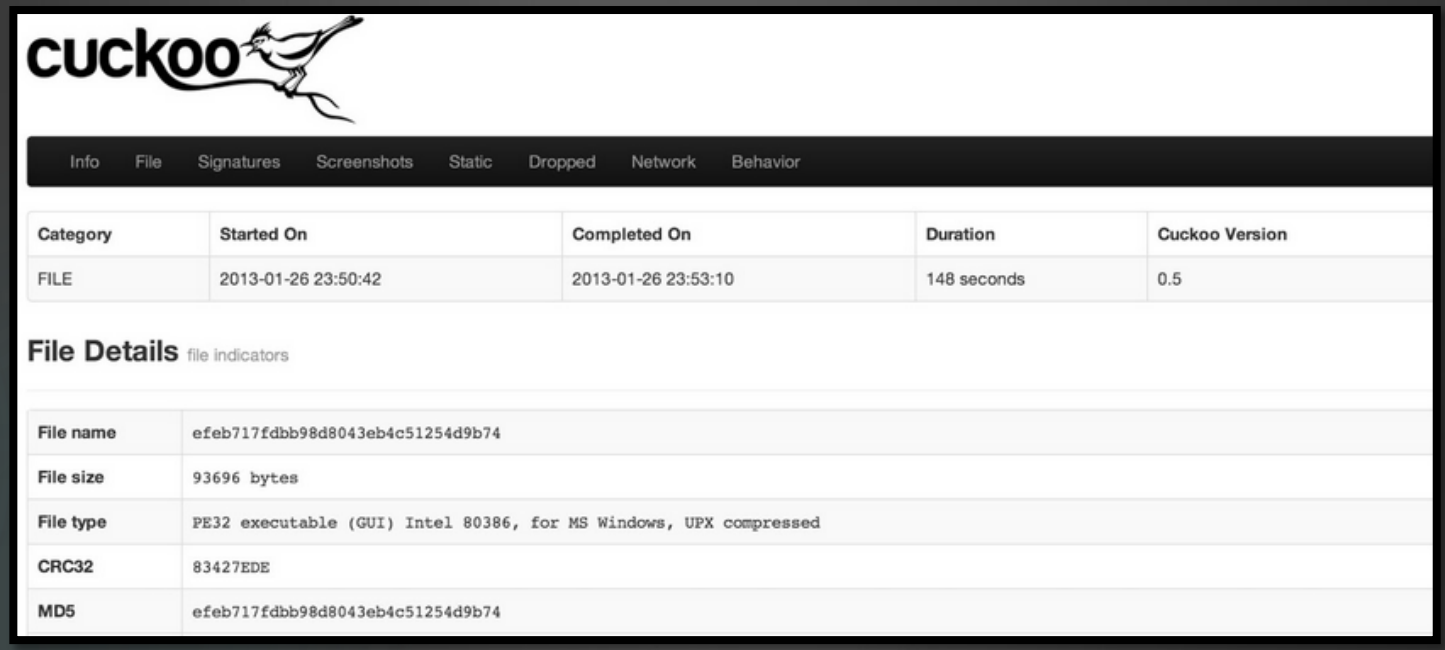
- Un échantillon (sample)
- Un environnement sécurisé et isolé
- Des connaissances en programmation, système, sécurité et réseau
- Du courage et de la patience ☺

Pourquoi un environnement sécurisé et isolé ?

- Besoin d'**exécuter** le malware pour l'analyser dynamiquement
- **Interagir** avec le malware pour comprendre son fonctionnement
- **Observer** les interactions du malware avec le système
  - Quels fichiers sont infectés ?
  - Quelles sont les informations échangées sur le réseau ?
  - Quels sont ses impacts au niveau du système ?

Environnements d'analyse

- Sandbox



- Machine virtuelle
  - Isoler le réseau (Host-only Adapter, FakeNet…)
  - Simuler une machine physique

Processus d'analyse

Analyse statique

- Format de fichier
- Chaines de caractères
- Format PE
- Désassemblage

Analyse dynamique

- Base de registre
- Système de fichiers
- Activité réseau
- Débogage

Analyse statique

- Déterminer le format de fichier
  - Commande file

```
mohlen@mohlen-VirtualBox:~/Téléchargements$ file f0001101001
f0001101001: PDF document, version 1.5
```

    - Magic numbers
      - MZ : fichier au format executable Windows.
      - %PDF : fichier au format PDF.
      - GIF : fichier au format GIF.
      - CAFEBABE (en héxadecimal) : fichier contenant une classe Java.
      - PK : fichier au format ZIP.

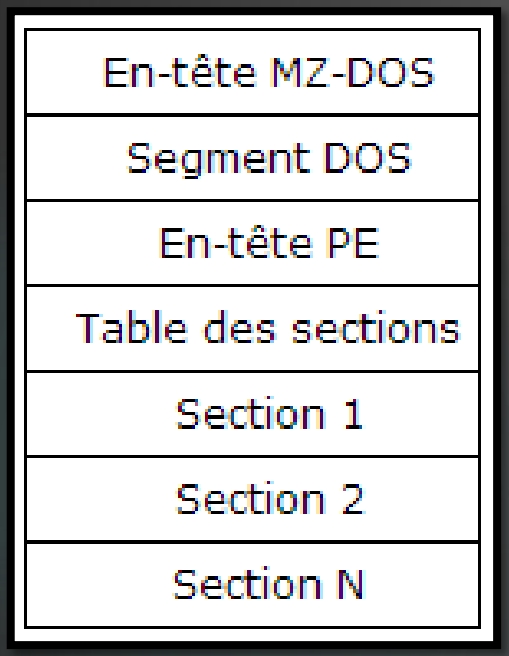
Analyse statique

- Identifier les chaines de caractères
  - Commande strings

```
mohlen@mohlen-VirtualBox:~$ strings malware
Ph(3@
h(3@
Ph(3@
h(3@
\*.*
\*.*
XPhFM@
[...]
.db.mp3.waw.jpgjpeg.txt.rtf.pdf.rar.zipeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeVery bad news...
[...]
```

Analyse statique

- Analyser le format PE

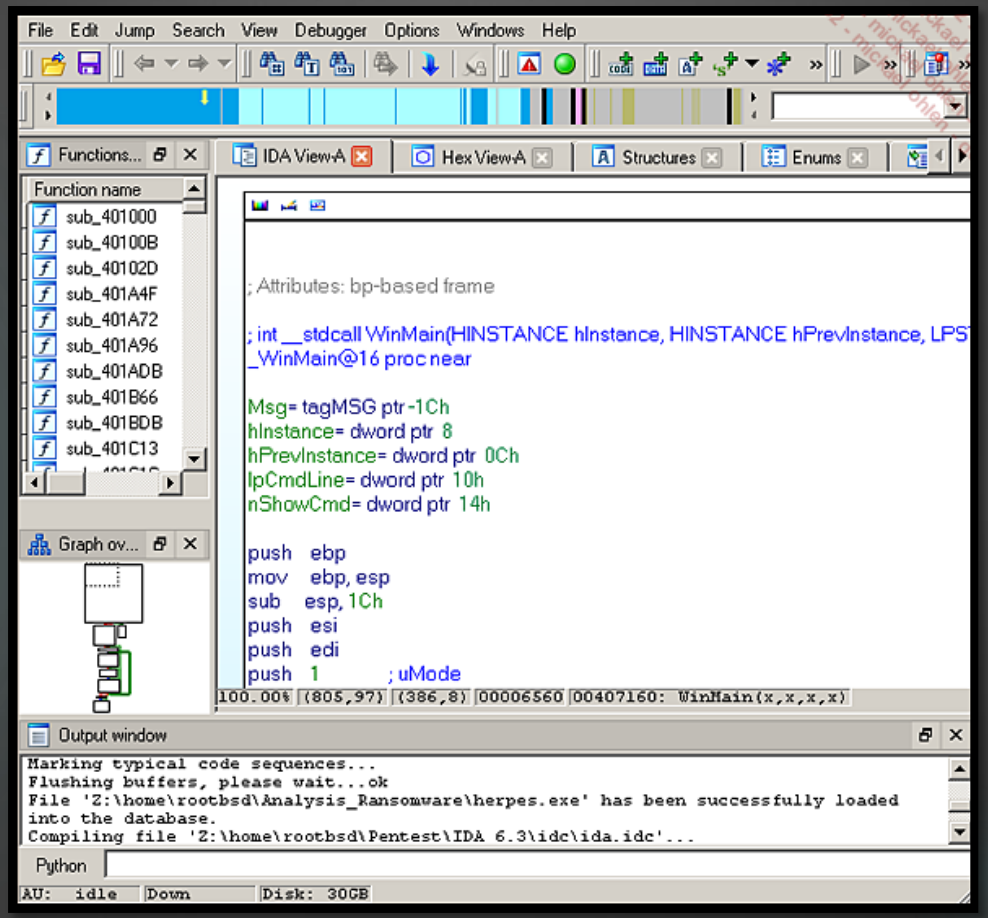


Champ	Informations utiles
Imports	Fonctions d'autres librairies utilisées par le malware
Exports	Fonctions du malware appelables par d'autres programmes
Time Date Stamp	Date de compilation
Ressources	Strings, icon …

- PE Explorer, PEview

Analyse statique

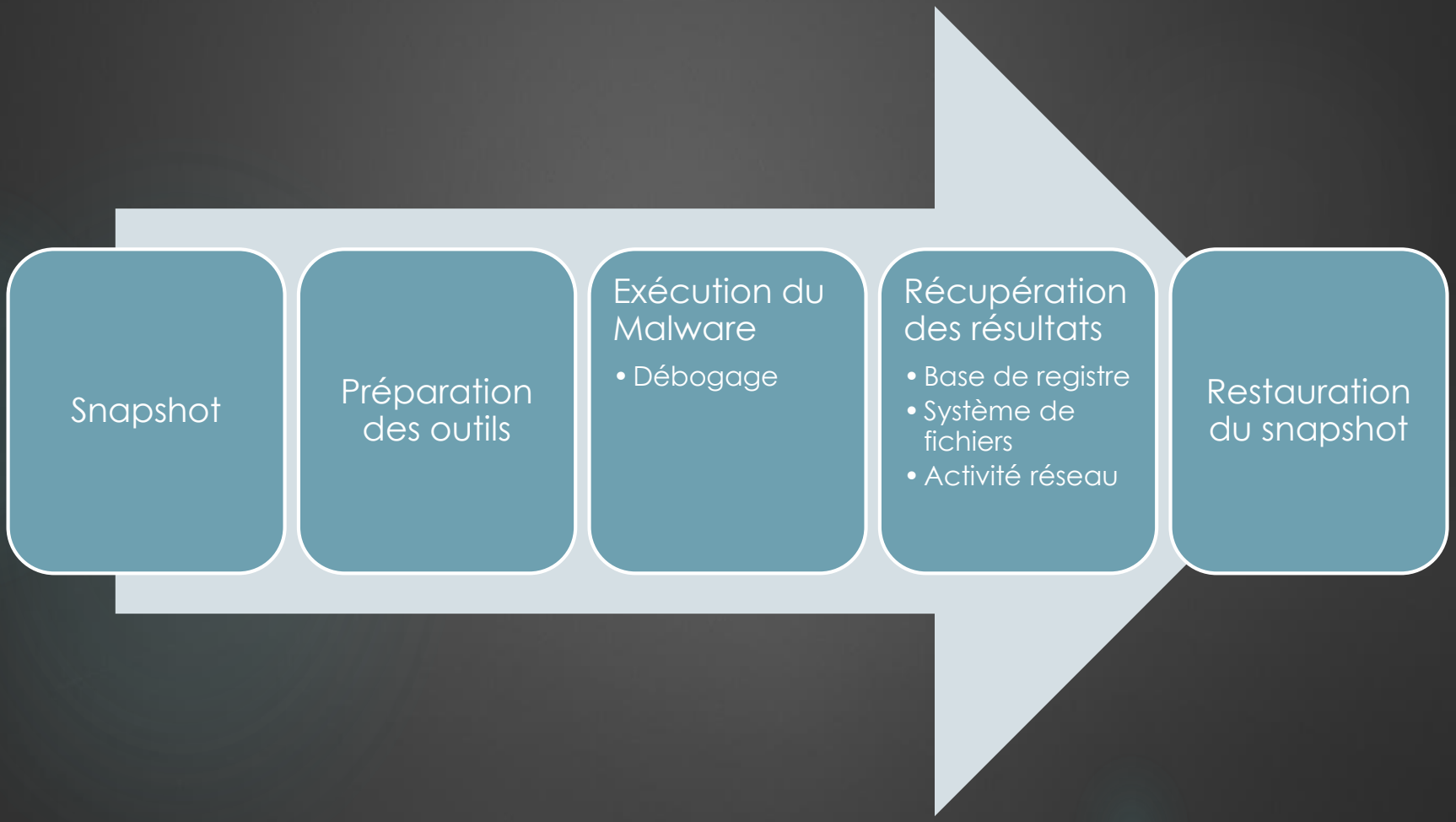
- Désassemblage
  - IDA PRO



Analyse statique

- Avantages
  - Large couverture
  - Indépendant de l'architecture
  - Pas de risque d'infection
- Limites
  - Assembleur ☹
  - Obfuscation

Analyse dynamique



Analyse dynamique

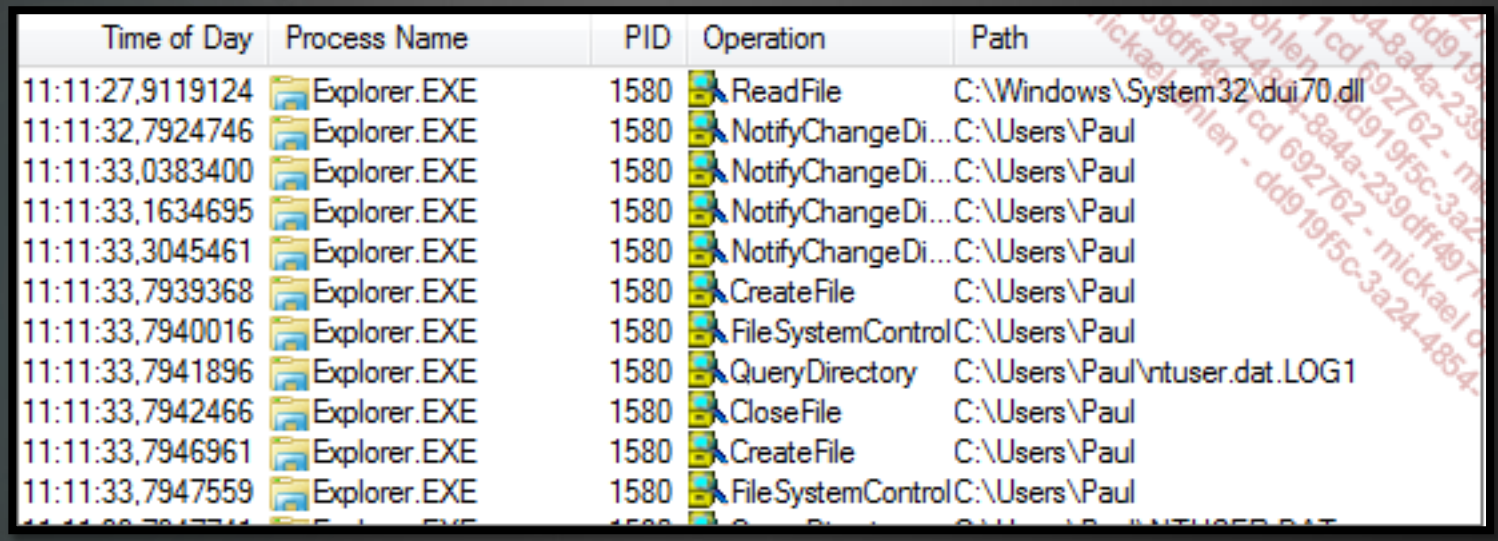
- Activité au niveau de la base de registre
  - Process Monitor

Time of Day	Process Name	PID	Operation	Path
11:11:27,4260046	Explorer.EXE	1580	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes
11:11:27,4261323	Explorer.EXE	1580	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Segoe UI
11:11:27,4262149	Explorer.EXE	1580	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes
11:11:27,4381410	Explorer.EXE	1580	RegOpenKey	HKLM\SOFTWARE\Microsoft\CTF\KnownClasses
11:11:27,4389233	Explorer.EXE	1580	RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-A
11:11:27,4389599	Explorer.EXE	1580	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-A
11:11:27,4391009	Explorer.EXE	1580	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-A
11:11:27,4399759	Explorer.EXE	1580	RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-A
11:11:27,4400122	Explorer.EXE	1580	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-A
11:11:27,4401433	Explorer.EXE	1580	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-A
11:11:27,9466043	Explorer.EXE	1580	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
11:11:27,9467395	Explorer.EXE	1580	RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\AlwaysShowM
11:11:27,9468264	Explorer.EXE	1580	RegOpenKey	HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
11:11:27,9469200	Explorer.EXE	1580	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\AlwaysSho
11:11:27,9470029	Explorer.EXE	1580	RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
11:11:27,9470468	Explorer.EXE	1580	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced
11:11:27,9471119	Explorer.EXE	1580	RegOpenKey	HKCU\Software\Microsoft\Internet Explorer\Toolbar

  - Regshot

Analyse dynamique

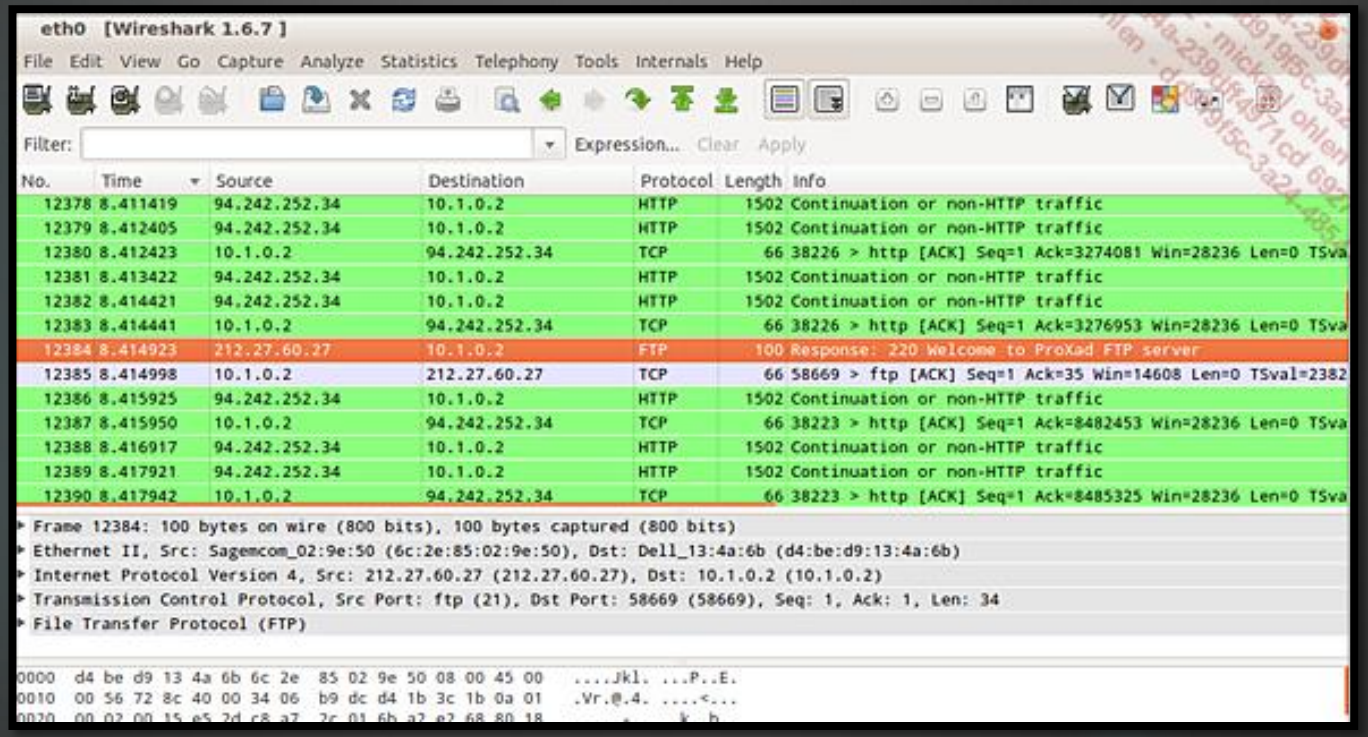
- Activité au niveau du système de fichiers
  - Process Monitor



Time of Day	Process Name	PID	Operation	Path
11:11:27,9119124	Explorer.EXE	1580	ReadFile	C:\Windows\System32\dui70.dll
11:11:32,7924746	Explorer.EXE	1580	NotifyChangeDi...	C:\Users\Paul
11:11:33,0383400	Explorer.EXE	1580	NotifyChangeDi...	C:\Users\Paul
11:11:33,1634695	Explorer.EXE	1580	NotifyChangeDi...	C:\Users\Paul
11:11:33,3045461	Explorer.EXE	1580	NotifyChangeDi...	C:\Users\Paul
11:11:33,7939368	Explorer.EXE	1580	CreateFile	C:\Users\Paul
11:11:33,7940016	Explorer.EXE	1580	FileSystemControl	C:\Users\Paul
11:11:33,7941896	Explorer.EXE	1580	QueryDirectory	C:\Users\Paul\ntuser.dat.LOG1
11:11:33,7942466	Explorer.EXE	1580	CloseFile	C:\Users\Paul
11:11:33,7946961	Explorer.EXE	1580	CreateFile	C:\Users\Paul
11:11:33,7947559	Explorer.EXE	1580	FileSystemControl	C:\Users\Paul

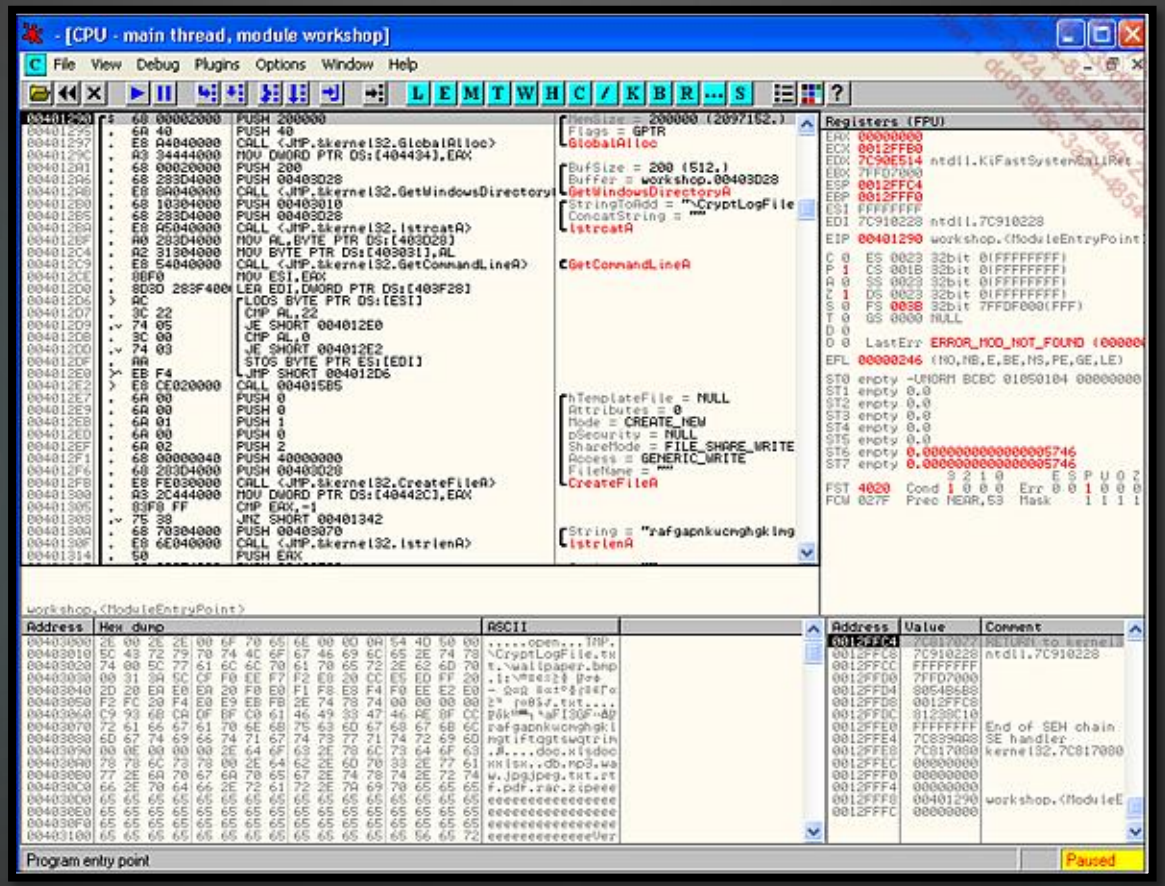
Analyse dynamique

- Activité réseau
  - WireShark



Analyse dynamique

- Débogage
  - OllyDbg



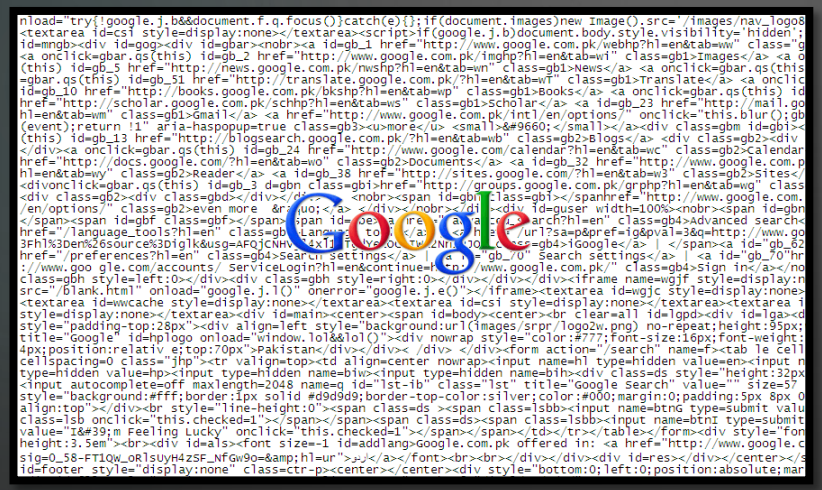
Analyse dynamique

- Avantages
  - Comportement réel du malware
  - Interaction
- Limites
  - Un seul flux d'exécution
  - Problème de sécurité
  - Obfuscation

- 1. Qu'est ce qu'un malware ?
- 2. Analyse
- 3. Techniques d'obfuscation
- 4. Démonstration (Analyse de CLogger)

«

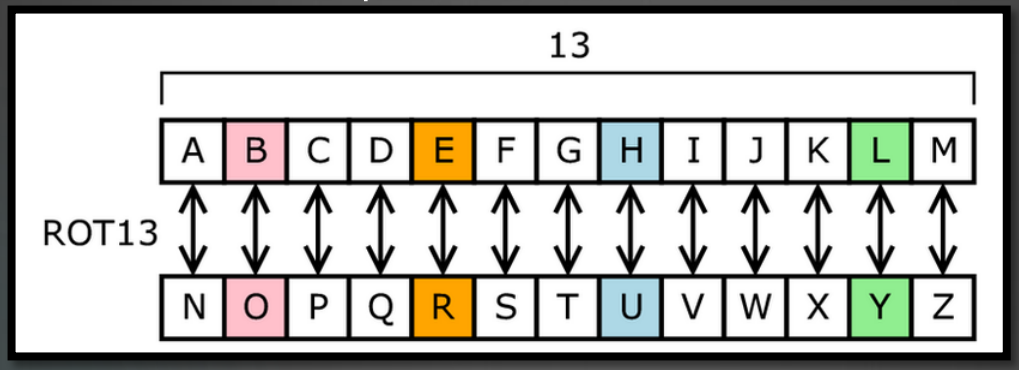
L'*Obfuscation* est une technique rendant un binaire ou un texte illisible et/ou difficile à comprendre.



»

Chaines de caractères

- ROT13
  - Décaler chaque lettre de 13 caractères

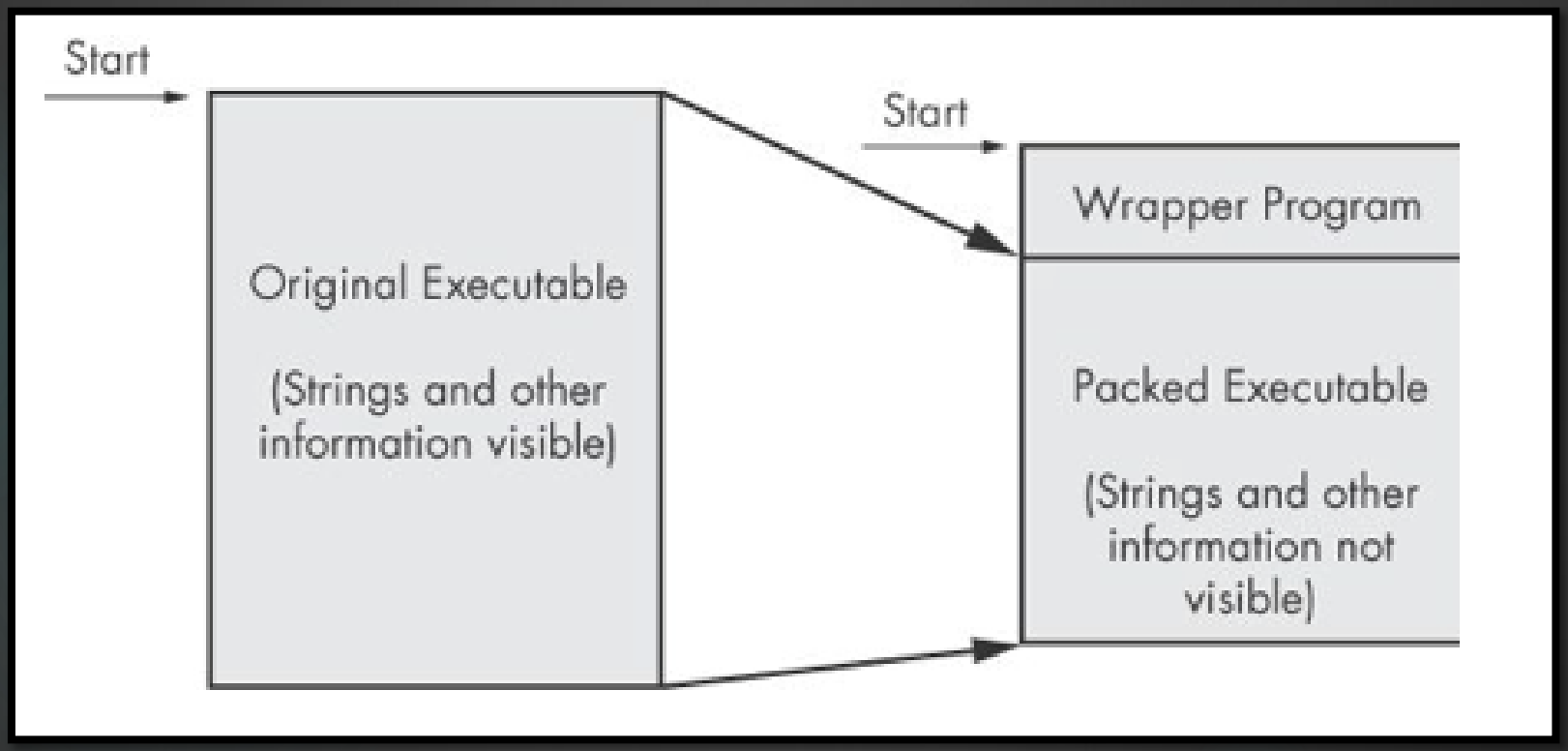


  - Ex : Herpesnet

```
mohlen@mohlen-VirtualBox:~$ strings herpesnet
[...]
tcerfhygy
uggc://qq.mrebkpbqr.arg/urecarg/
74978o6rpp6p19836n17n3p2pq0840o0
uggc://jjj.mrebkpbqr.arg/urecarg/
sgc.mrebkpbqr.arg
uggc://sex7.zvar.ah/urecarg/
hcybnq@mrebkpbqr.arg
hccvg
ujsdsdbbngfgjhhuugfgfujd
rffggghooo
Ashfurncsmx
[...]
```

```
mohlen@mohlen-VirtualBox:~$ strings herpesnet | rot13
[...]
gpresultl
http://dd.zeroxcode.net/herpnet/
74978b6ecc6c19836a17a3c2cd0840b0
http://www.zeroxcode.net/herpnet/
ftp.zeroxcode.net
http://frk7.mine.nu/herpnet/
upload@zeroxcode.net
uppit
hwfqfqooatstwuuhhtstshwq
esstttubbb
Nfusheapfzk
[...]
```

Packers


Start
Original Executable
(Strings and other information visible)
Start
Wrapper Program
Packed Executable
(Strings and other information not visible)

Anti VM

- Détection de caractéristiques types
  - Port « VM » ouvert sous VMWare
- Détection de processus
  - « VBoxService.exe » sous VirtualBox
- Exploitation de vulnérabilité
  - VirtualBox (CVE-2012-3221)

```
int crash() {
  asm (
    "int $0x8;"
    : // output: none
    : // input: none
    :"%eax", "%ebx", "%ecx", "%edx"    // clobbered register
  );
  return(0);
```

Anti debug

- Gestion du temps
- Détection de points d'arrêt

```
bool CheckForCCBreakpoint(void* pMemory,  size_t SizeToCheck)
{
     unsigned char *pTmp = (unsigned char*)pMemory;
    for (size_t i = 0; i < SizeToCheck; i++)
     {
         if(pTmp[i] == 0xCC)
             return true;
     }

    return false;
}
```

- Détection de processus

```
HANDLE hOlly = FindWindow(TEXT("OLLYDBG"), NULL);

if(hOlly)
    ExitProcess(0);
```

- 1. Qu'est ce qu'un malware ?
- 2. Analyse
- 3. Techniques d'obfuscation
- 4. Démonstration (Analyse de CLogger)

Résultats d'analyse

- Persistance dans la base de registre
- Capture *SSC.jpg* dans dossier temp
- C&C = decyphersoftware@gmail.com
- Obfuscation basique
- Fonctionnalités
  - Upload FTP
  - Désactivation pare feu et TM
- Stealer

Conclusion

- Domaine porteur
- Malwares de plus en plus sophistiqués
  - Analyse difficile
- Règles d'or
  - Ne pas chercher à comprendre tout à 100%
  - Si un outil ne fonctionne pas, en prendre un autre
  - Maintenir ses outils à jour

Pour aller plus loin

- Trouver des samples
  - http://openmalware.org/
  - http://malwaredb.malekal.com
  - http://virusshare.com/
- Outils
  - Sandbox en ligne : http://www.malwr.com
  - Détecteur de packers : PEiD
  - Désassembleur : IDA
  - Debugeur : OllyDbg
- Documentation
  - http://www.malware.lu/
  - Practical Malware Analysis

Merci de votre attention

- Questions ?