INTRODUCTION À LA SÉCURITÉ INFORMATIQUE SÉANCE 8

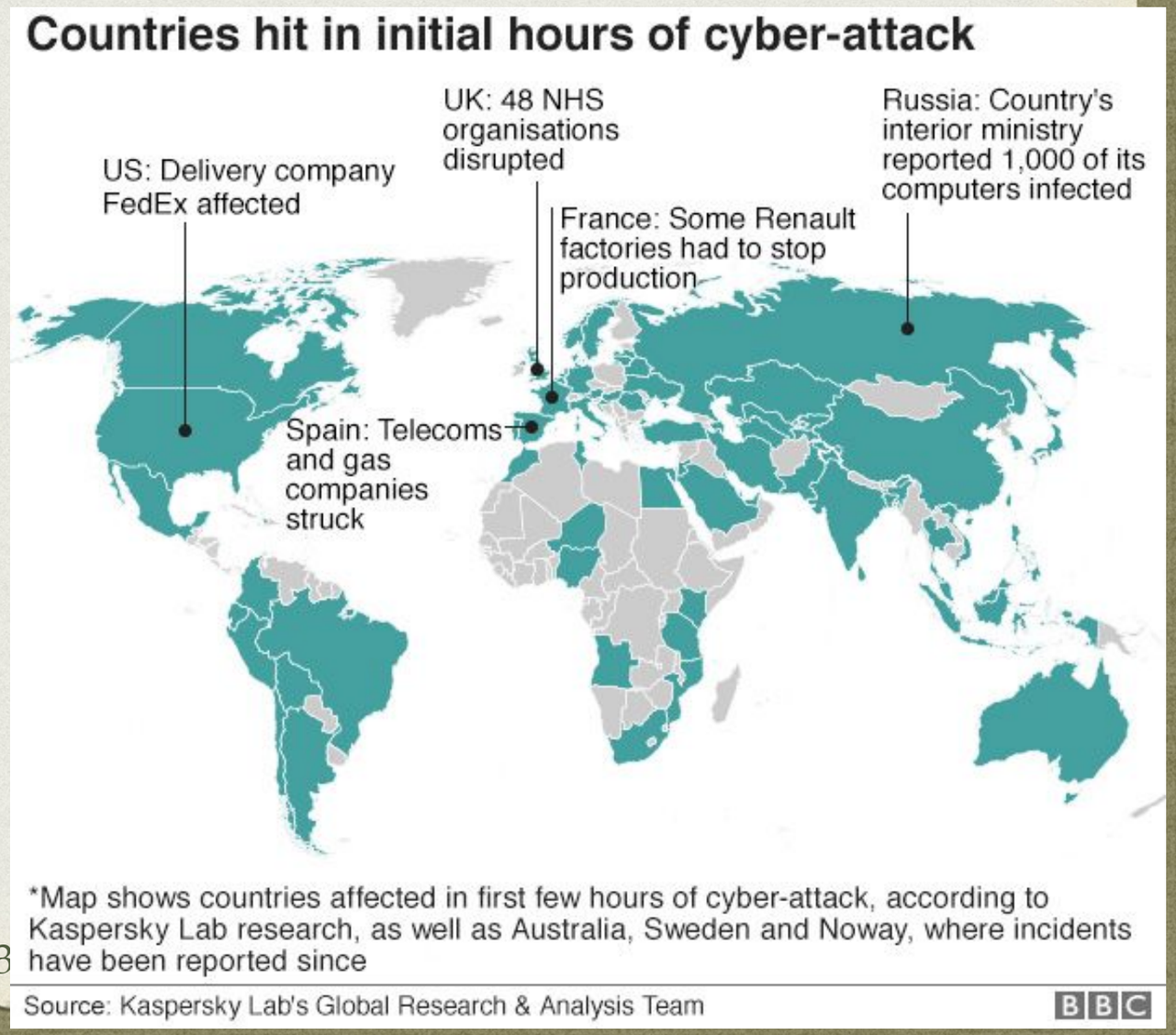
Marc-Olivier Killijian
UQAM, CNRS
INF4471 A21

MALICIELS

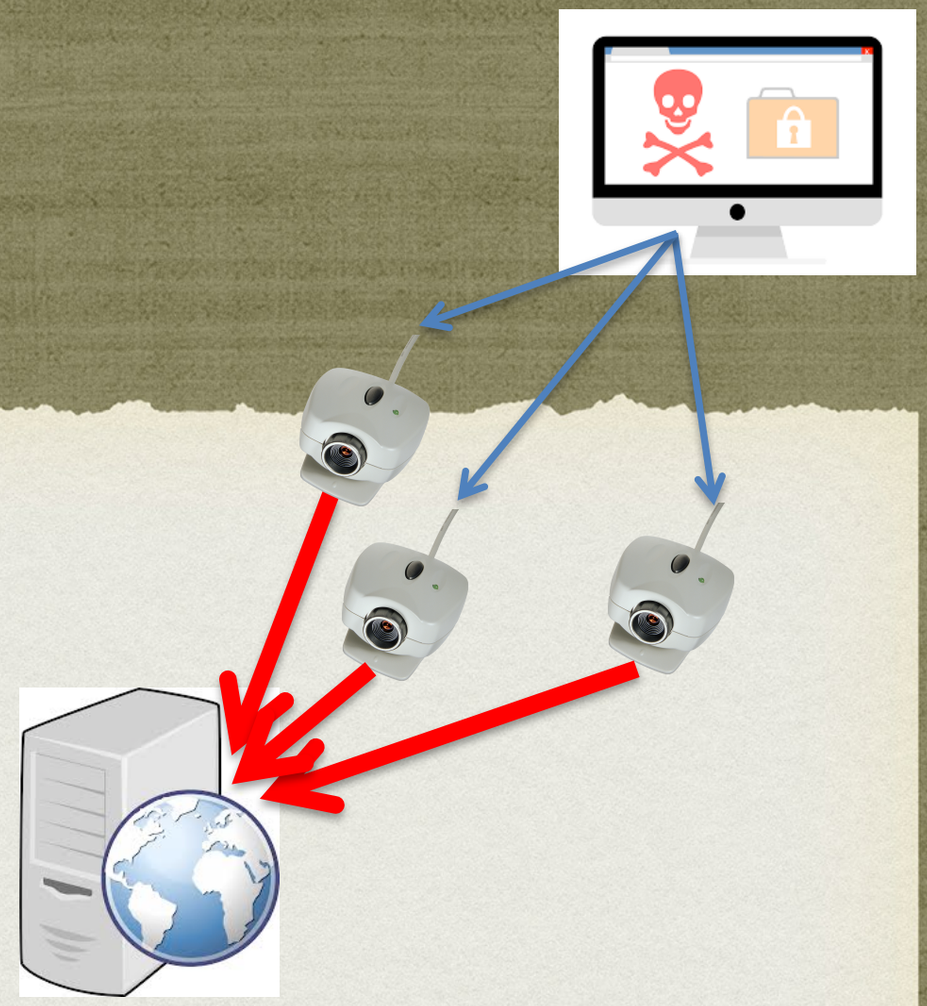
remerciements Jean-Yves Marion (LORIA-Nancy-France)

EX. WANNACRY

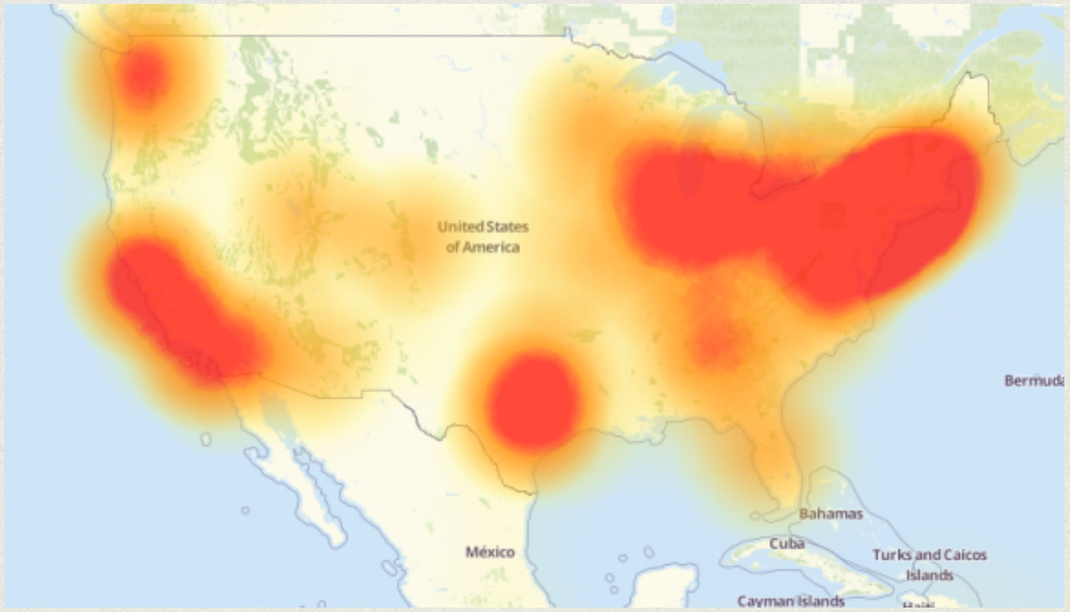
- Un ver qui se réplique et s'étend sur le réseau
- Vecteur d'infection : la vulnérabilité Eternal Blue
- Chiffre les HDD
- Rançon à payer en bitcoin



EX. IOT BOTNET MIRAI

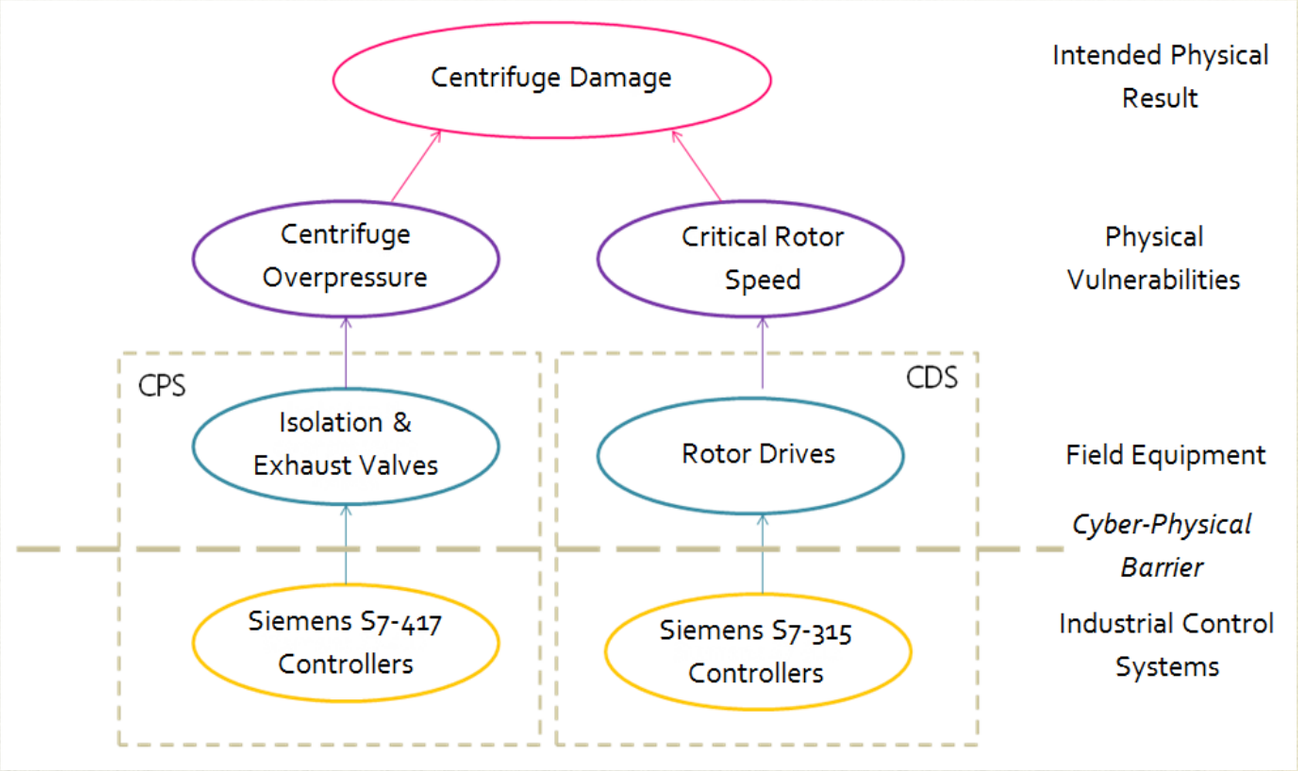


- un botnet de ~600k objets connectés 2016-2017
- qui lance des DDOS
  - OVH 1Tbps (record à l'époque)
  - serveur DNS DYN (Twitter, Amazon, Spotify, Netflix, etc.)
- cf. Understanding the Mirai Botnet



STUXNET

- Attaque des centrifugeuses iraniennes
- exploitation de 4 oday (Gvt USA + Israel)
- cf. épisode 282 NoLimitSecu



MOTIVATIONS DIVERSES

- **Extortion de fonds**
  Rançongiciel (WannaCry, etc.)
  Troyen bancaire (Emotet, Locky, Dridex)

- **Extraction d'information**
  APT28 - attaque contre Equifax (145M victimes)

- **Revenus et e-réputation**
  Pourriels, Cryptominers

- **Defacement (politique) et destruction**
  TV5 Monde, NotPetya, Stuxnet

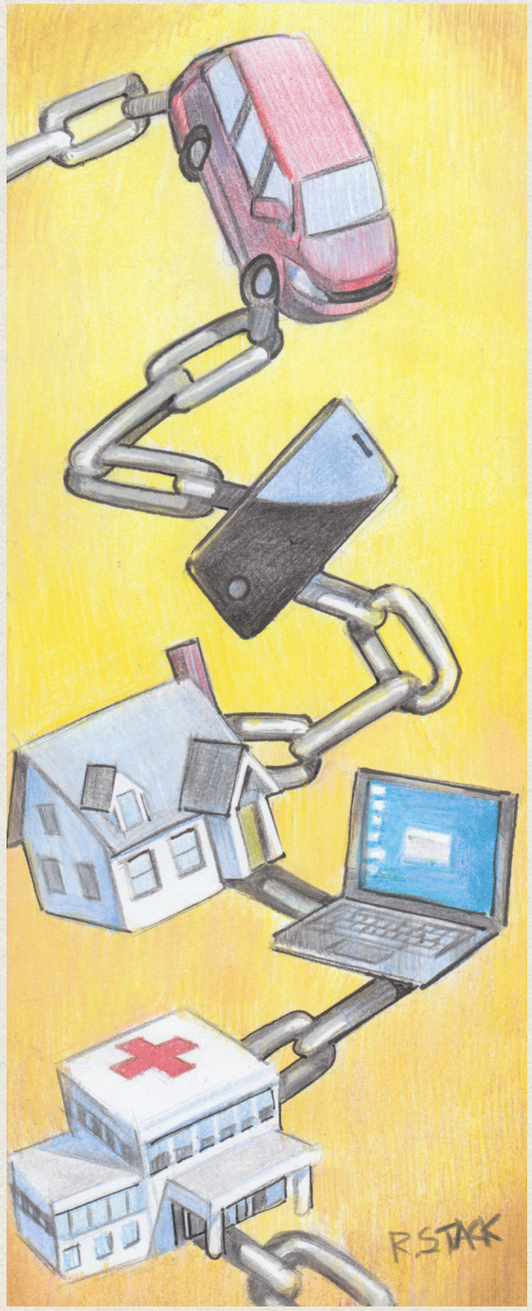
- **Malware-as-a-Service (MaaS)**
  Loaders (Emotet & other botnets)

RISQUES

- C - Confidentialité
  Perte de données (entreprise, personnelles)
  Perte de credentials

- I - Intégrité et modification de données
  Chiffrement des disques durs
  Modification de BDD

- A - Indisponibilité de services
  Infrastructures critiques
  Services publics
  Destruction ou extinction de dispositifs



MALICIELS ?

CLASSIFICATION GUIDE

How F-Secure classifies threats

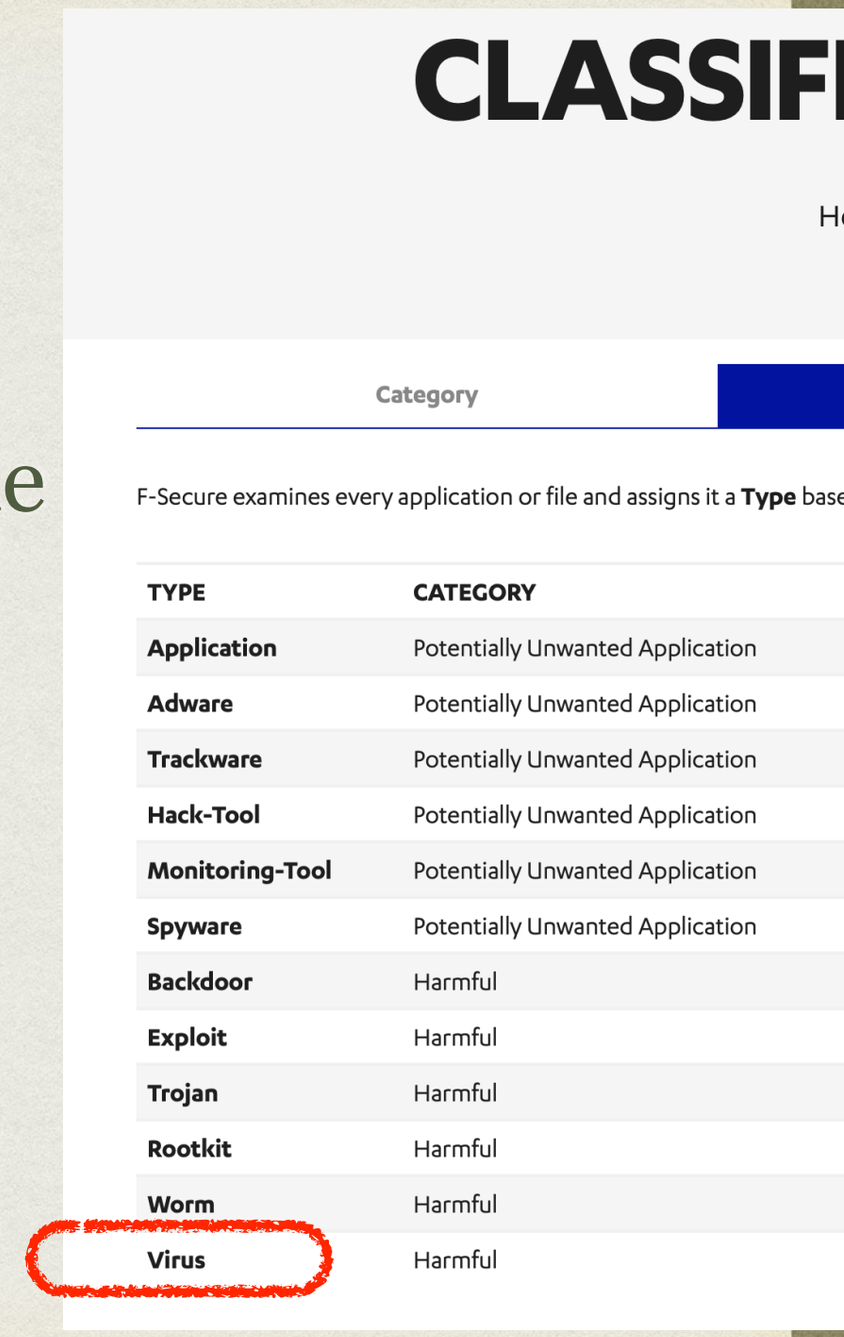
Category | **Type** | Platform

F-Secure examines every application or file and assigns it a **Type** based on the actions it can perform. The **Type** is used to determine the application or file's **Category**.

TYPE	CATEGORY	DESCRIPTION
Application	Potentially Unwanted Application	If misused, introduces a security risk. More >
Adware	Potentially Unwanted Application	Displays advertising material. More >
Trackware	Potentially Unwanted Application	Identifies a user or a device to a third party. More >
Hack-Tool	Potentially Unwanted Application	Bypasses safety or security mechanisms. More >
Monitoring-Tool	Potentially Unwanted Application	Monitors and records (some or all) user actions on the device. More >
Spyware	Potentially Unwanted Application	Collects information about user actions or a device, and sends it out. More >
Backdoor	Harmful	Provides unauthorized access to, and control of, a device. More >
Exploit	Harmful	Takes advantage of a vulnerability to create unexpected conditions. More >
Trojan	Harmful	Performs a harmful action without the user's knowledge or consent. More >
Rootkit	Harmful	Hides other applications or files on the device. More >
Worm	Harmful	Spreads copies of itself to other devices over a network. More >
Virus	Harmful	Directly tampers with an application or file's code. More >

VIRUS

- Un virus contamine son hôte (du code légitime)
- Ne peut exister (s'éxécuter) sans lui



CLASSIF

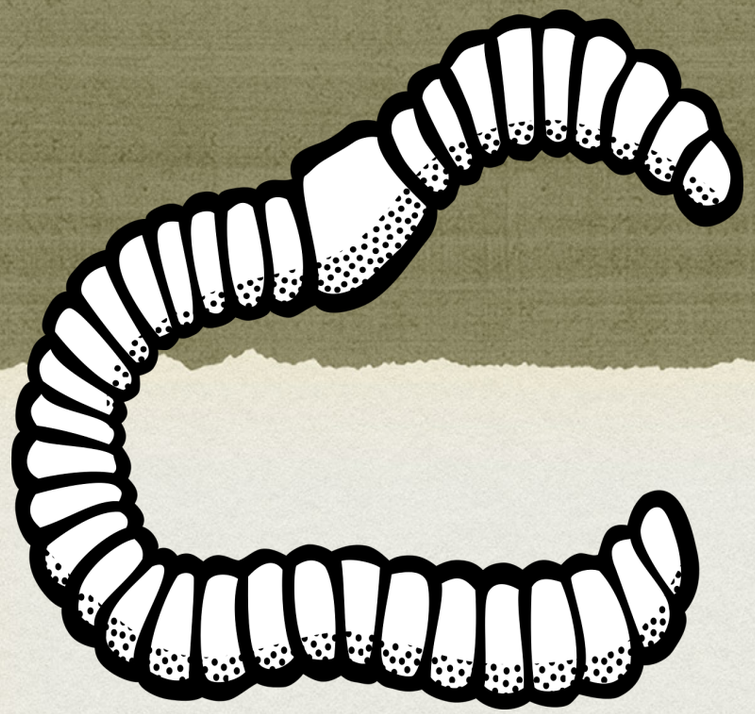
H

Category

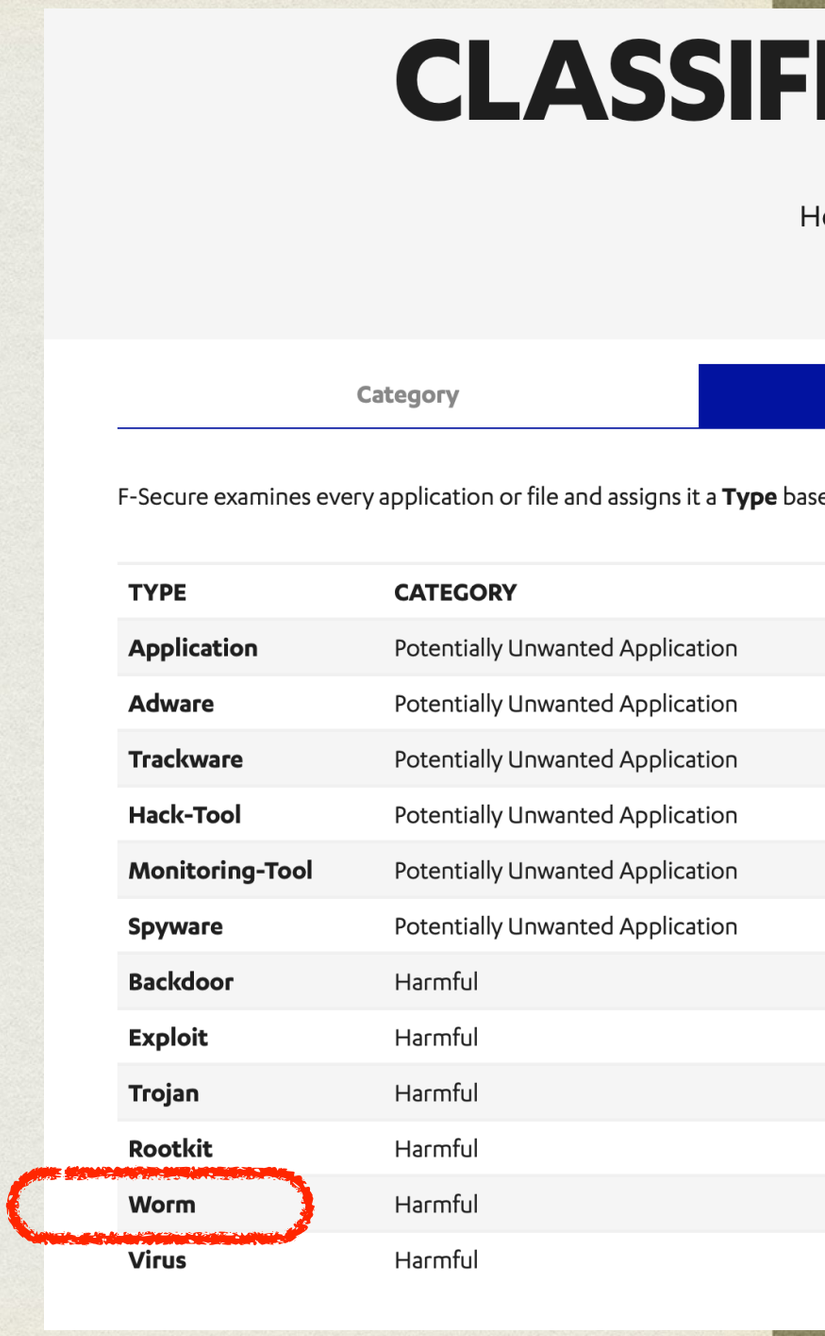
F-Secure examines every application or file and assigns it a **Type** base

TYPE	CATEGORY
Application	Potentially Unwanted Application
Adware	Potentially Unwanted Application
Trackware	Potentially Unwanted Application
Hack-Tool	Potentially Unwanted Application
Monitoring-Tool	Potentially Unwanted Application
Spyware	Potentially Unwanted Application
Backdoor	Harmful
Exploit	Harmful
Trojan	Harmful
Rootkit	Harmful
Worm	Harmful
Virus	Harmful

VER



- Un ver se répand à travers le réseau
  - Copie à d'autres dispositifs



CLASSIF

H

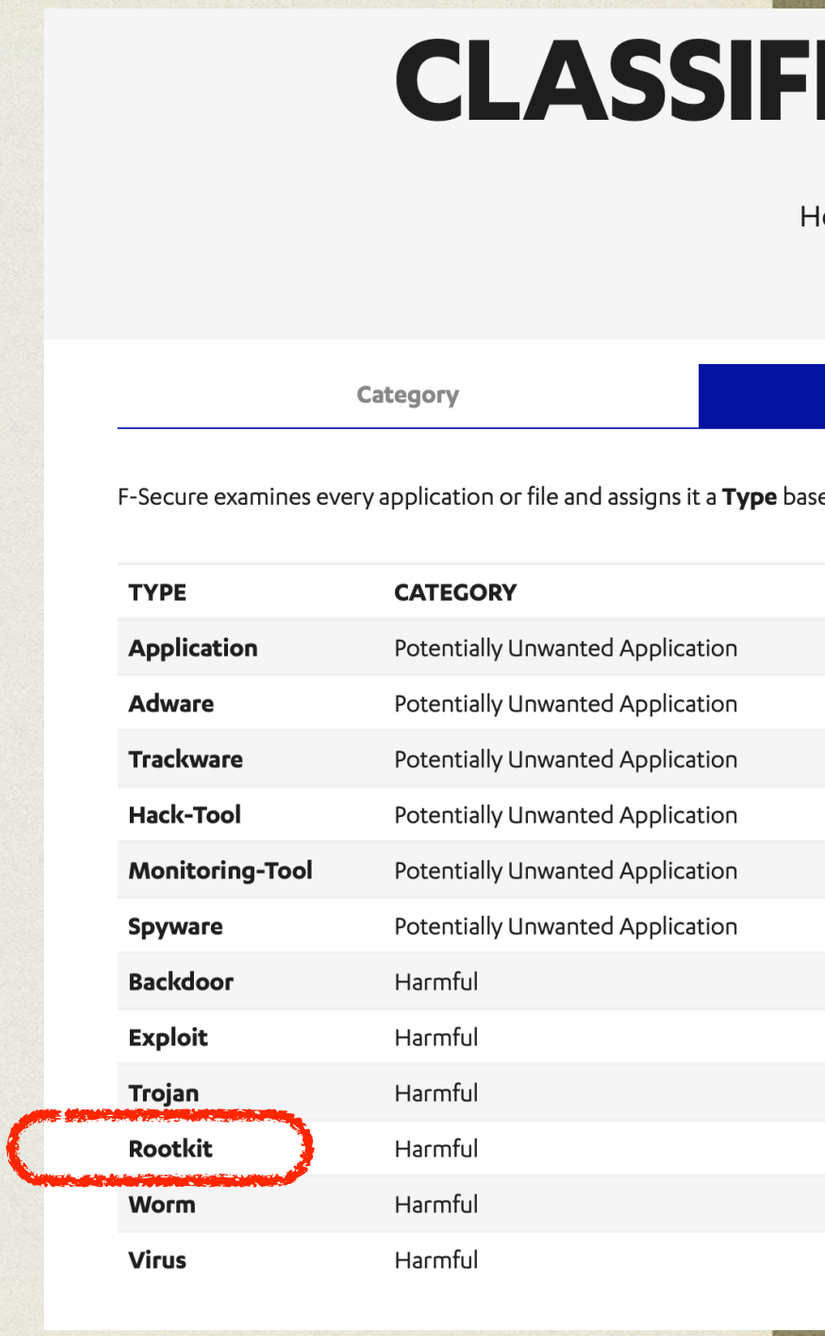
Category

F-Secure examines every application or file and assigns it a **Type** base

TYPE	CATEGORY
Application	Potentially Unwanted Application
Adware	Potentially Unwanted Application
Trackware	Potentially Unwanted Application
Hack-Tool	Potentially Unwanted Application
Monitoring-Tool	Potentially Unwanted Application
Spyware	Potentially Unwanted Application
Backdoor	Harmful
Exploit	Harmful
Trojan	Harmful
Rootkit	Harmful
Worm	Harmful
Virus	Harmful

ROOTKIT

- Un *rootkit* installe des outils/une librairie de hacks sur l'hôte



CLASSIFI

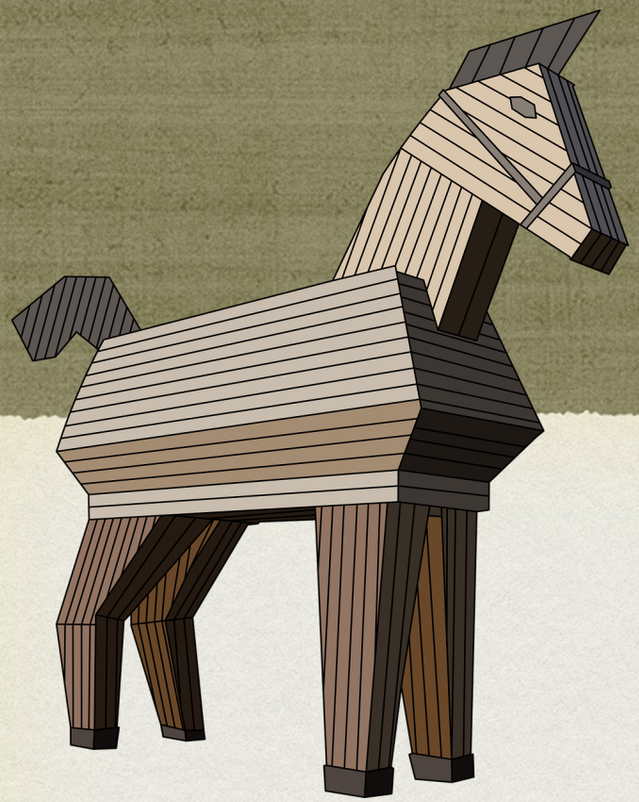
H

Category

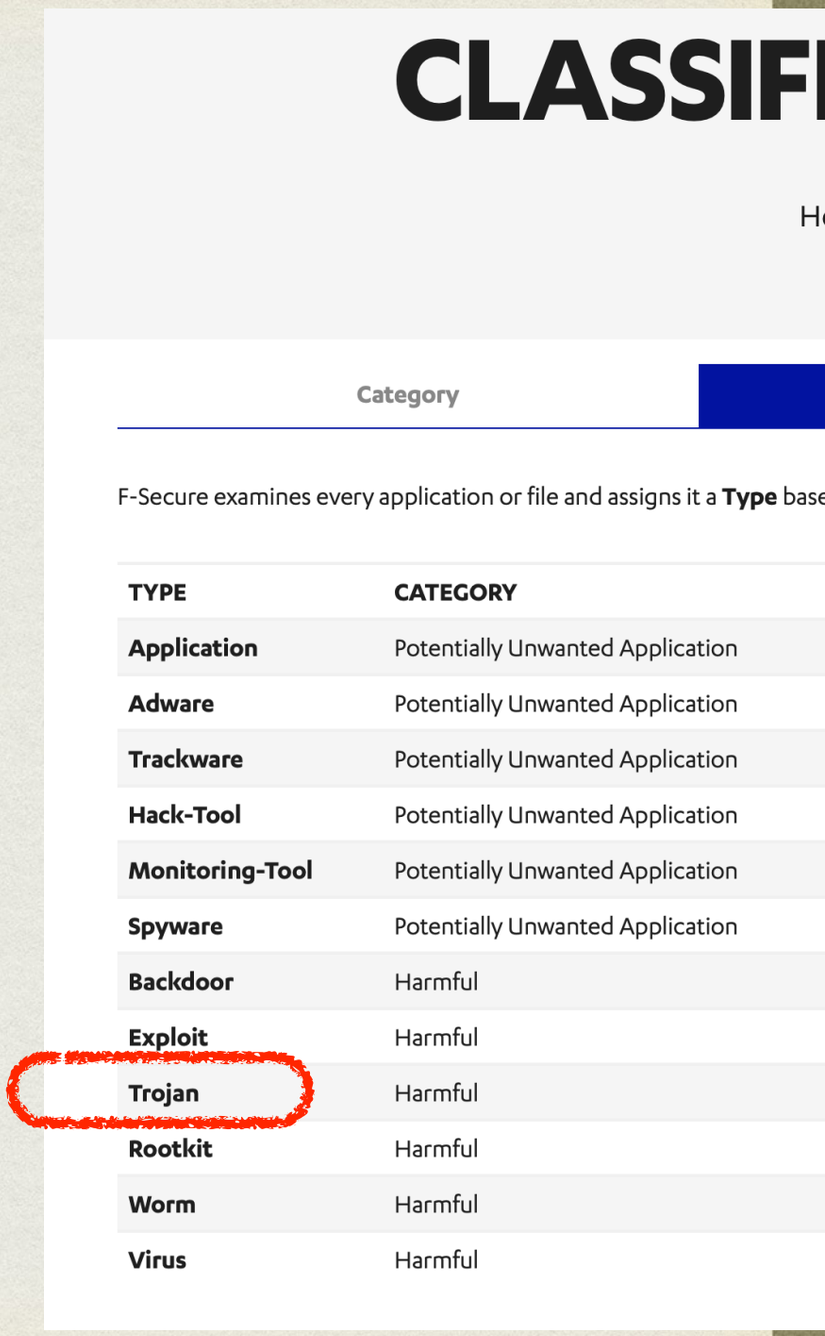
F-Secure examines every application or file and assigns it a **Type** base

TYPE	CATEGORY
Application	Potentially Unwanted Application
Adware	Potentially Unwanted Application
Trackware	Potentially Unwanted Application
Hack-Tool	Potentially Unwanted Application
Monitoring-Tool	Potentially Unwanted Application
Spyware	Potentially Unwanted Application
Backdoor	Harmful
Exploit	Harmful
Trojan	Harmful
Rootkit	Harmful
Worm	Harmful
Virus	Harmful

TROYEN



- Reste caché sous une apparence anodine
- Effectue des actions dangereuses contre l'hôte



CLASSIFI

H

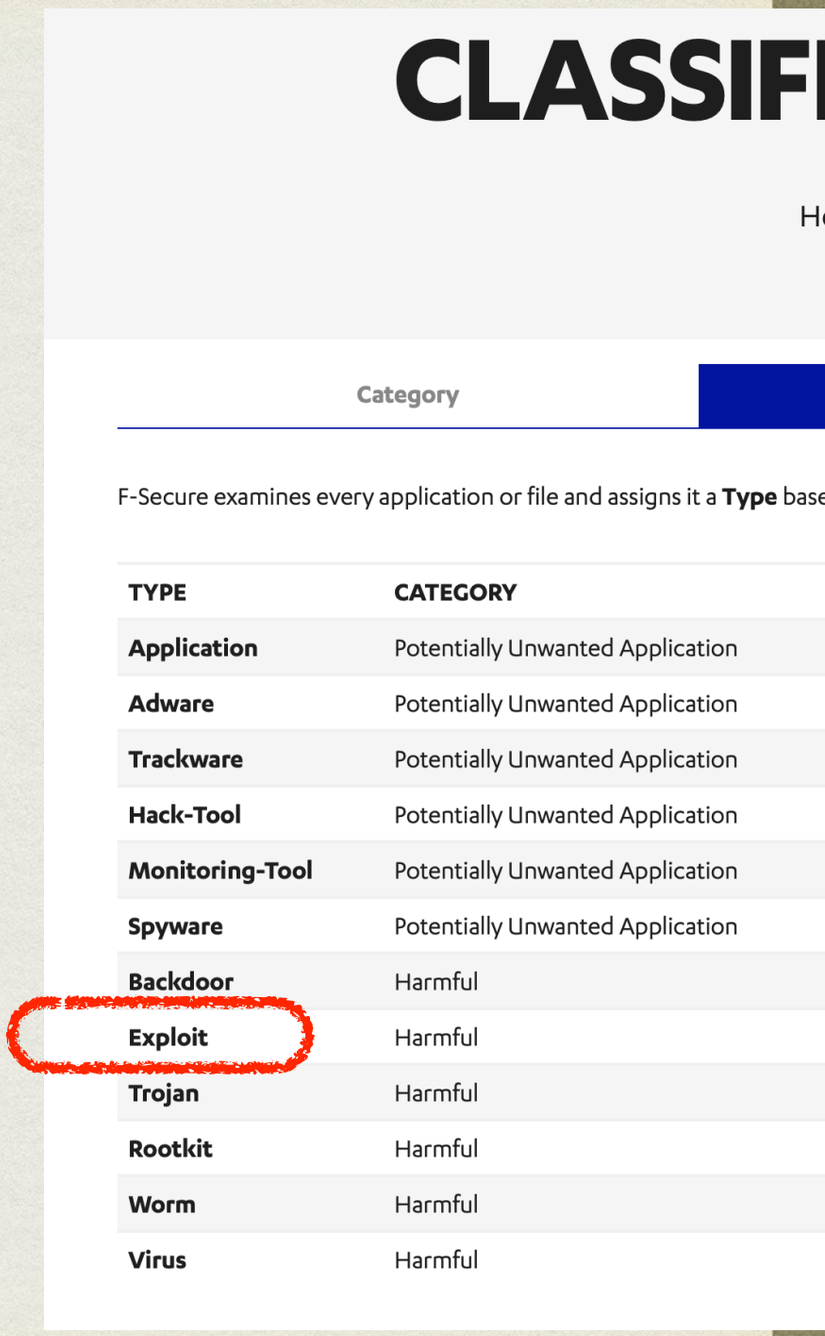
Category

F-Secure examines every application or file and assigns it a **Type** base

TYPE	CATEGORY
Application	Potentially Unwanted Application
Adware	Potentially Unwanted Application
Trackware	Potentially Unwanted Application
Hack-Tool	Potentially Unwanted Application
Monitoring-Tool	Potentially Unwanted Application
Spyware	Potentially Unwanted Application
Backdoor	Harmful
Exploit	Harmful
Trojan	Harmful
Rootkit	Harmful
Worm	Harmful
Virus	Harmful

EXPLOIT

- exploite une vulnérabilité



CLASSIFI

H

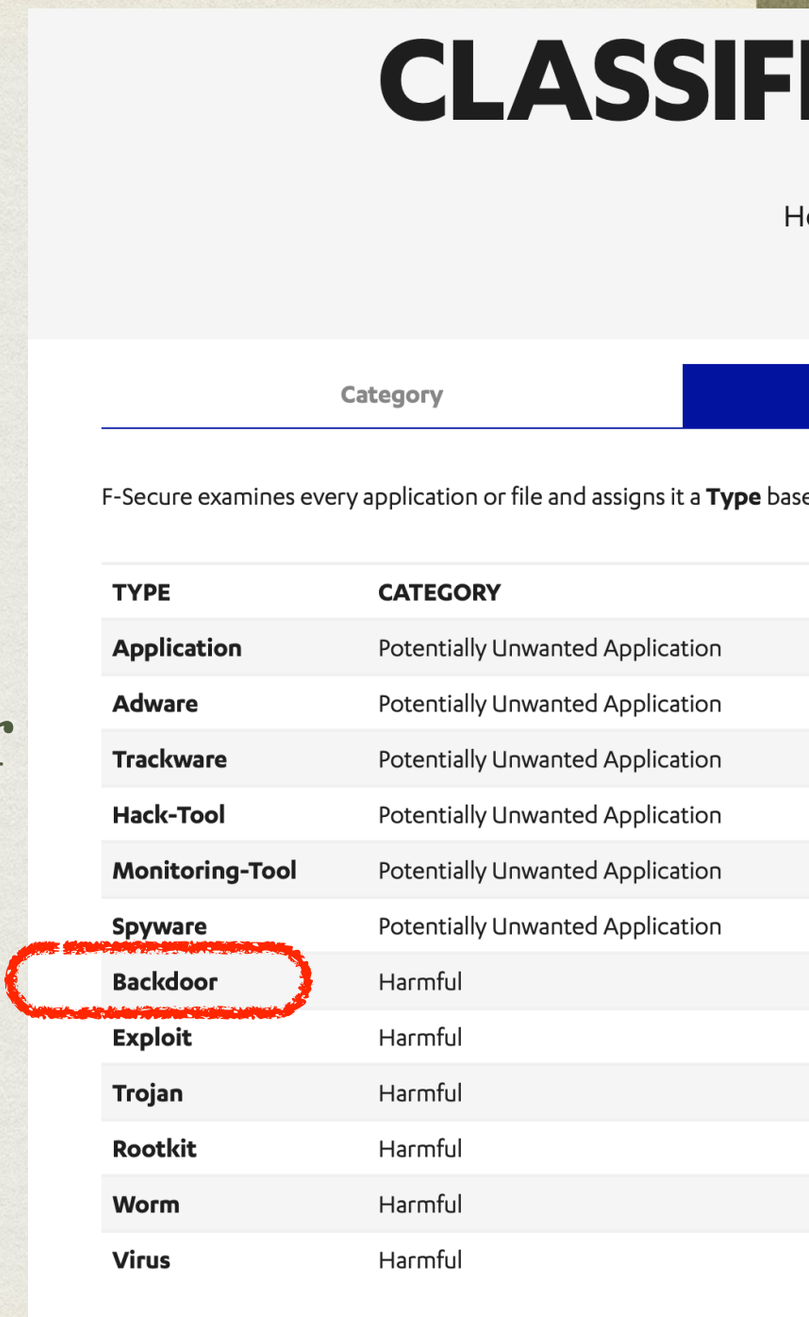
Category

F-Secure examines every application or file and assigns it a **Type** base

TYPE	CATEGORY
Application	Potentially Unwanted Application
Adware	Potentially Unwanted Application
Trackware	Potentially Unwanted Application
Hack-Tool	Potentially Unwanted Application
Monitoring-Tool	Potentially Unwanted Application
Spyware	Potentially Unwanted Application
Backdoor	Harmful
Exploit	Harmful
Trojan	Harmful
Rootkit	Harmful
Worm	Harmful
Virus	Harmful

BACKDOOR

- offre une porte dérobée sur son hôte
  - utilisée pour du contrôle distant par exemple



CLASSIFI

Ho

Category

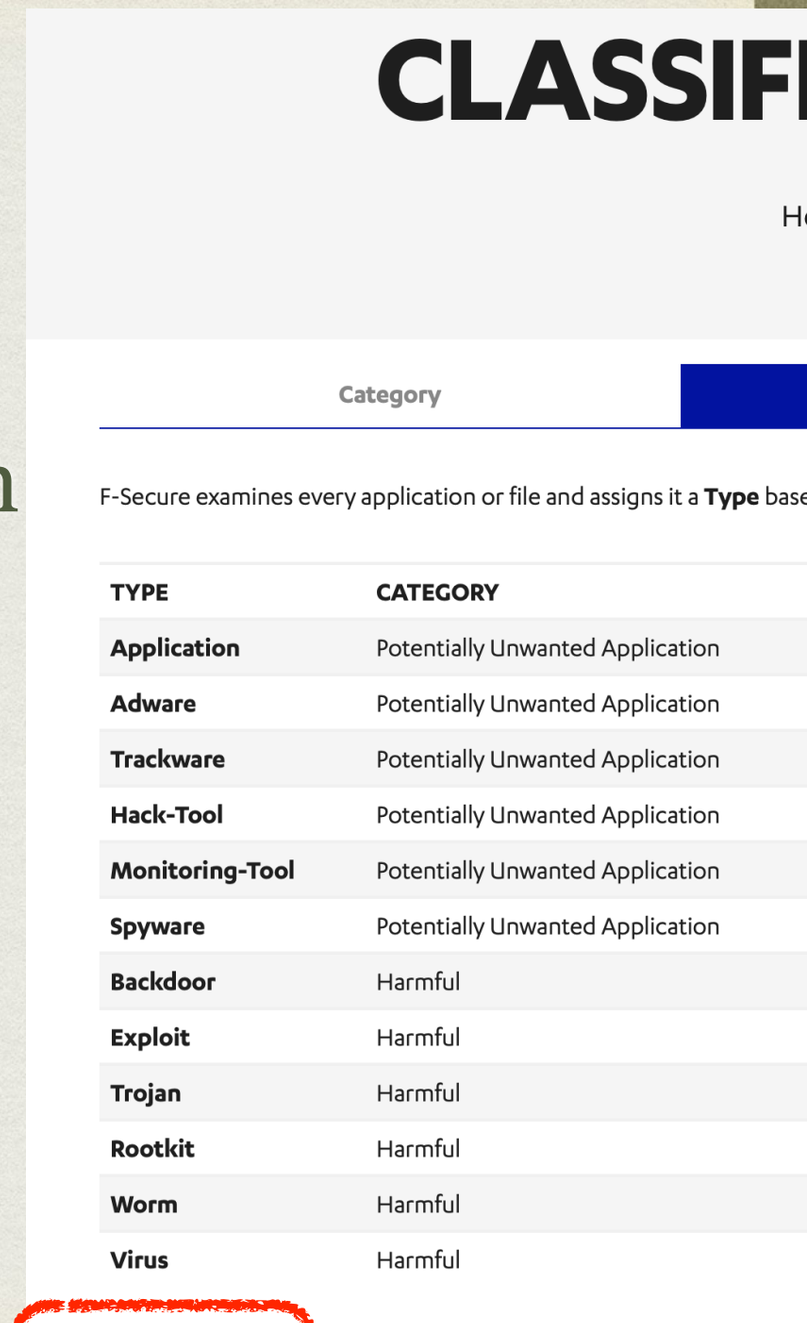
F-Secure examines every application or file and assigns it a **Type** base

TYPE	CATEGORY
Application	Potentially Unwanted Application
Adware	Potentially Unwanted Application
Trackware	Potentially Unwanted Application
Hack-Tool	Potentially Unwanted Application
Monitoring-Tool	Potentially Unwanted Application
Spyware	Potentially Unwanted Application
Backdoor	Harmful
Exploit	Harmful
Trojan	Harmful
Rootkit	Harmful
Worm	Harmful
Virus	Harmful

BOMBE LOGIQUE

- implantée dans un système
  - attend la réalisation d'une condition logique
  - avant de s'activer

(if MOK ∉ employés then `rm -fr /`)



CLASSIFI

H

Category

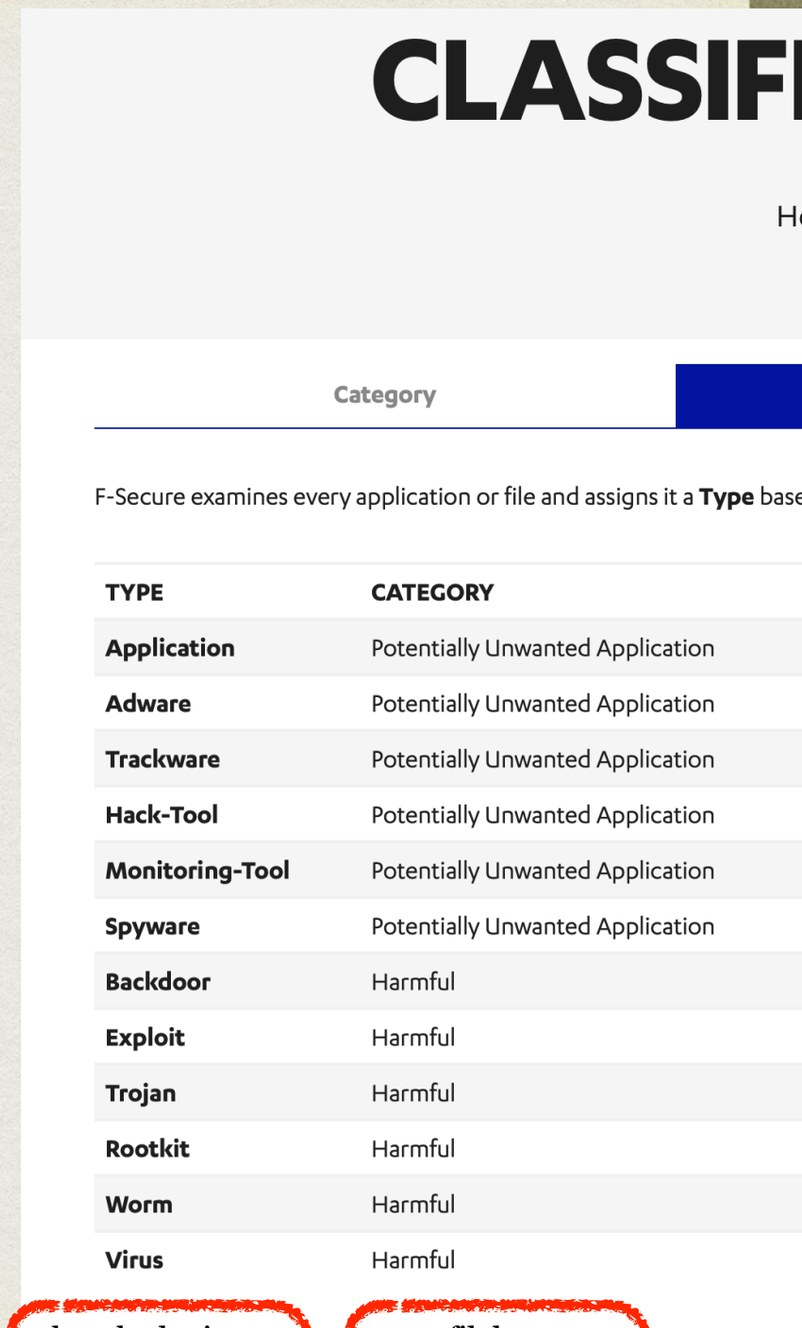
F-Secure examines every application or file and assigns it a **Type** base

TYPE	CATEGORY
Application	Potentially Unwanted Application
Adware	Potentially Unwanted Application
Trackware	Potentially Unwanted Application
Hack-Tool	Potentially Unwanted Application
Monitoring-Tool	Potentially Unwanted Application
Spyware	Potentially Unwanted Application
Backdoor	Harmful
Exploit	Harmful
Trojan	Harmful
Rootkit	Harmful
Worm	Harmful
Virus	Harmful

bombe logique

FILELESS

- Maliciel sans écriture dans un fichier
  - Tout est en mémoire
- Compromis persistance/discrétion
  - Extrêmement difficile à détecter
  - Ne résiste a priori pas aux reboot



CLASSIFI

H

Category

F-Secure examines every application or file and assigns it a **Type** base

TYPE	CATEGORY
Application	Potentially Unwanted Application
Adware	Potentially Unwanted Application
Trackware	Potentially Unwanted Application
Hack-Tool	Potentially Unwanted Application
Monitoring-Tool	Potentially Unwanted Application
Spyware	Potentially Unwanted Application
Backdoor	Harmful
Exploit	Harmful
Trojan	Harmful
Rootkit	Harmful
Worm	Harmful
Virus	Harmful

bombe logique

fileless

MALICIEL

- Tout cela n'est pas mutuellement exclusif
  - Ex. Stuxnet : ver + troyen + bombe logique
- Déf. Générale : *un maliciel est un programme informatique qui infiltre un système informatique à l'insu de l'utilisateur*

CLASSIF

H

Category

F-Secure examines every application or file and assigns it a **Type** base

TYPE	CATEGORY
Application	Potentially Unwanted Application
Adware	Potentially Unwanted Application
Trackware	Potentially Unwanted Application
Hack-Tool	Potentially Unwanted Application
Monitoring-Tool	Potentially Unwanted Application
Spyware	Potentially Unwanted Application
Backdoor	Harmful
Exploit	Harmful
Trojan	Harmful
Rootkit	Harmful
Worm	Harmful
Virus	Harmful

bombe logique

fileless

CYCLE DE VIE

1. **Intrusion** : comment pénétrer le système (bugs et vulnérabilités, mots de passes faibles, ingénierie sociale, etc.)

2. **Infection** : comment planter, protéger et répliquer le maliciel dans le système

3. **Exploitation** : quelle est la charge (vol de données, DDOS, etc.)

CYCLE DE VIE

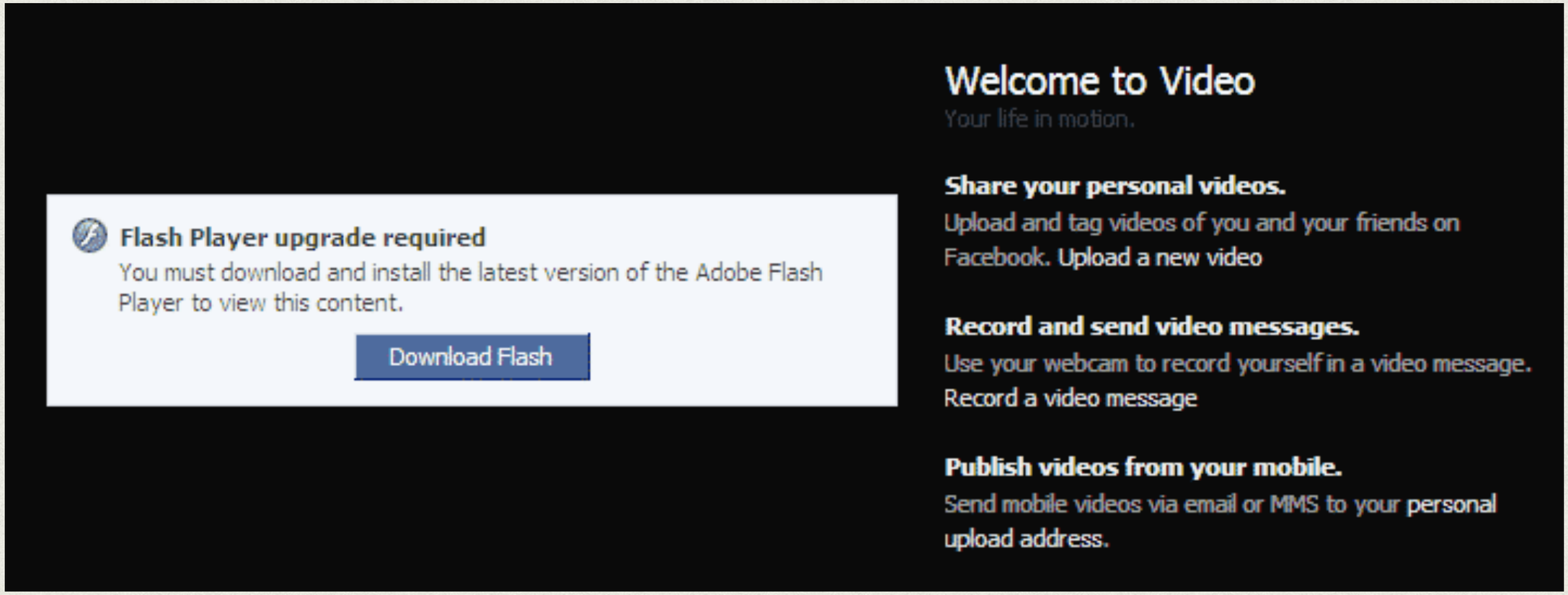
1. **Intrusion** : comment pénétrer le système (bugs et vulnérabilités, mots de passes faibles, ingénierie sociale, etc.)

2. **Infection** : comment planter, protéger et répliquer le maliciel dans le système

3. **Exploitation** : quelle est la charge (vol de données, DDOS, etc.)

INTRUSION

- Mots de passe : utiliser des credentials préalablement dérobés
- Ingénierie sociale : convaincre l'utilisateur d'installer notre soft



VULNÉRABILITÉS EXEMPLE D'INJECTION DE CODE (WEB)

```
$in = $_GET['exp'];
eval('$ans = ' . $in . ';');
```

Serveur web

```
http://site.com/calc.php?exp=" 10 ; system('rm *.*')"
```

Butineur de l'attaquant

VULNÉRABILITÉS EXEMPLE D'INJECTION DE CODE (WEB)

```
$in = $_GET['exp'];
eval('$ans = ' . $in . ';');
```

Serveur web

Eval va interpréter expr ...

```
http://site.com/calc.php?exp=" 10 ; system('rm *.*')"
```

Butineur de l'attaquant

VULNÉRABILITÉS EXEMPLE D'INJECTION DE CODE (WEB)

CVE List▾ CNAs▾ WGs▾ Board▾ About▾ News & Blog▾ NVD

Common Vulnerabilities and Exposures

Go to for:
CVSS Scores
CPE Info

Search CVE List | Download CVE | Data Feeds | Request CVE IDs | Update a CVE Entry

TOTAL CVE Entries: 142610

HOME > CVE > SEARCH RESULTS

Search Results

There are **7782** CVE entries that match your search.

Name	Description
CVE-2020-9688	Adobe Download Manager version 2.0.0.518 have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2020-9583	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2020-9582	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2020-9578	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2020-9576	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2020-9521	An SQL injection vulnerability was discovered in Micro Focus Service Manager Automation (SMA), affecting versions 2019.08, 2019.05, 2019.02, 2018.08, 2018.05, 2018.02. The vulnerability could allow for the improper neutralization of special elements in SQL commands and may lead to the product being vulnerable to SQL injection.
CVE-2020-9478	An issue was discovered in Rubrik 5.0.3-2296. An OS command injection vulnerability allows an authenticated attacker to remotely execute arbitrary code on Rubrik-managed systems.
CVE-2020-9436	PHOENIX CONTACT TC ROUTER 3002T-4G through 2.05.3, TC ROUTER 2002T-3G through 2.05.3, TC ROUTER 3002T-4G VZW through 2.05.3, TC ROUTER 3002T-4G ATT through 2.05.3, TC CLOUD CLIENT 1002-4G through 2.03.17, and TC CLOUD CLIENT 1002-TXTX through 1.03.17 devices allow authenticated users to inject system commands through a modified POST request to a specific URL.
CVE-2020-9435	PHOENIX CONTACT TC ROUTER 3002T-4G through 2.05.3, TC ROUTER 2002T-3G through 2.05.3, TC ROUTER 3002T-4G VZW through 2.05.3, TC ROUTER 3002T-4G ATT through 2.05.3, TC CLOUD CLIENT 1002-4G through 2.03.17, and TC CLOUD CLIENT 1002-TXTX through 1.03.17 devices contain a hardcoded certificate (and key) that is used by default for web-based services on the device. Impersonation, man-in-the-middle, or passive decryption attacks are possible if the generic certificate is not replaced by a device-specific certificate during installation.
CVE-2020-9269	SOPlanning 1.45 is vulnerable to authenticated SQL Injection that leads to command execution via the users parameter, as demonstrated by export_ical.php.
CVE-2020-9242	FusionCompute 8.0.0 have a command injection vulnerability. The software does not sufficiently validate certain parameters post from user, successful exploit could allow an authenticated attacker to launch a command injection attack.
CVE-2020-9199	B2368-22 V100R001C00;B2368-57 V100R001C00;B2368-66 V100R001C00 have a command injection vulnerability. An attacker with high privileges may exploit this vulnerability through some operations on the LAN. Due to insufficient input validation of some parameters, the attacker can exploit this vulnerability to inject commands to the target device.
CVE-2020-9054	Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by

VULNÉRABILITÉS EXEMPLE D'INJECTION SQL

Serveur SQL

```
var sql = "select * from users where username = '" + username +
"' and password = '" + password + '"";
```

```
Username: '; drop table users--;
```

Requête de l'attaquant

VULNÉRABILITÉS
EXEMPLE D'INJECTION SQL

Serveur SQL

```
var sql = "select * from users where username = '" + username +
"' and password = '" + password + "'";
```

le serveur va dropper users !

```
Username: '; drop table users--;
```

Requête de l'attaquant

VULNÉRABILITÉS
EXEMPLE D'INJECTION SQL

CVE List▾ CNAs▾ WGs▾ Board▾ About▾ News & Blog▾

Common Vulnerabilities and Exposures

NVD
Go to for:
CVSS Scores
CPE Info

Search CVE List | Download CVE | Data Feeds | Request CVE IDs | Update a CVE Entry

TOTAL CVE Entries: 142610

HOME > CVE > SEARCH RESULTS

Search Results

There are **8464** CVE entries that match your search.

Name	Description
CVE-2020-9521	An SQL injection vulnerability was discovered in Micro Focus Service Manager Automation (SMA), affecting versions 2019.08, 2019.05, 2019.02, 2018.08, 2018.05, 2018.02. The vulnerability could allow for the improper neutralization of special elements in SQL commands and may lead to the product being vulnerable to SQL injection.
CVE-2020-9483	**Resolved** When use H2/MySQL/TiDB as Apache SkyWalking storage, the metadata query through GraphQL protocol, there is a SQL injection vulnerability, which allows to access unpexcted data. Apache SkyWalking 6.0.0 to 6.6.0, 7.0.0 H2/MySQL/TiDB storage implementations don't use the appropriate way to set SQL parameters.
CVE-2020-9465	An issue was discovered in EyesOfNetwork eonweb 5.1 through 5.3 before 5.3-3. The eonweb web interface is prone to a SQL injection, allowing an unauthenticated attacker to perform various tasks such as authentication bypass via the user_id field in a cookie.
CVE-2020-9402	Django 1.11 before 1.11.29, 2.2 before 2.2.11, and 3.0 before 3.0.4 allows SQL Injection if untrusted data is used as a tolerance parameter in GIS functions and aggregates on Oracle. By passing a suitably crafted tolerance to GIS functions and aggregates on Oracle, it was possible to break escaping and inject malicious SQL.
CVE-2020-9398	ISPConfig before 3.1.15p3, when the undocumented reverse_proxy_panel_allowed=sites option is manually enabled, allows SQL Injection.
CVE-2020-9340	fauzantrif eLection 2.0 has SQL Injection via the admin/ajax/op_kandidat.php id parameter.
CVE-2020-9318	Red Gate SQL Monitor 9.0.13 through 9.2.14 allows an administrative user to perform a SQL injection attack by configuring the SNMP alert settings in the UI. This is fixed in 9.2.15.
CVE-2020-9269	SOPlanning 1.45 is vulnerable to authenticated SQL Injection that leads to command execution via the users parameter, as demonstrated by export_ical.php.
CVE-2020-9268	SoPlanning 1.45 is vulnerable to SQL Injection in the OrderBy clause, as demonstrated by the projets.php?order=nom_createur&by= substring.
CVE-2020-9006	The Popup Builder plugin 2.2.8 through 2.6.7.6 for WordPress is vulnerable to SQL injection (in the sgImportPopups function in sg_popup_ajax.php) via PHP Deserialization on attacker-controlled data with the attachmentUrl POST variable. This allows creation of an arbitrary WordPress Administrator account, leading to possible Remote Code Execution because Administrators can run PHP code on Wordpress instances. (This issue has been fixed in the 3.x branch of popup-builder.)
CVE-2020-8967	There is an improper Neutralization of Special Elements used in an SQL Command (SQL Injection) vulnerability in php files of GESIO ERP. GESIO ERP all versions prior to 11.2 allows malicious users to retrieve all database information.
CVE-2020-8887	Telestream Tektronix Medius before 10.7.5 and Sentry before 10.7.5 have a SQL injection vulnerability allowing an unauthenticated attacker to dump

EXPLOITATION DE BUGS

- Un bug est un comportement anormal
- Certains bugs peuvent être exploités pour modifier le flot de contrôle du programme - vulnérabilité
- Une vulnérabilité peut être utilisée pour lancer du code arbitraire
- Ex: simplification d'une *stack overflow*

COMPILATION 101

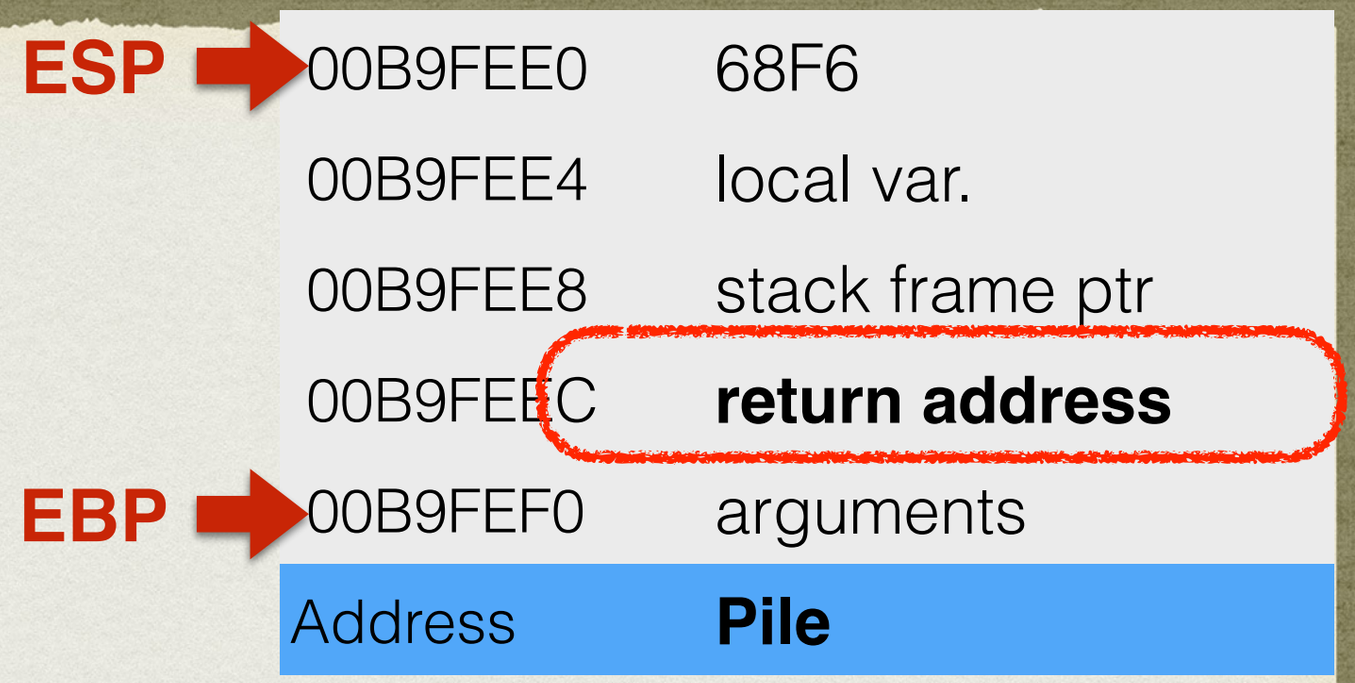
```
#include <stdio.h>
 int main()
   { puts("Hello!");
      return 0; }
```

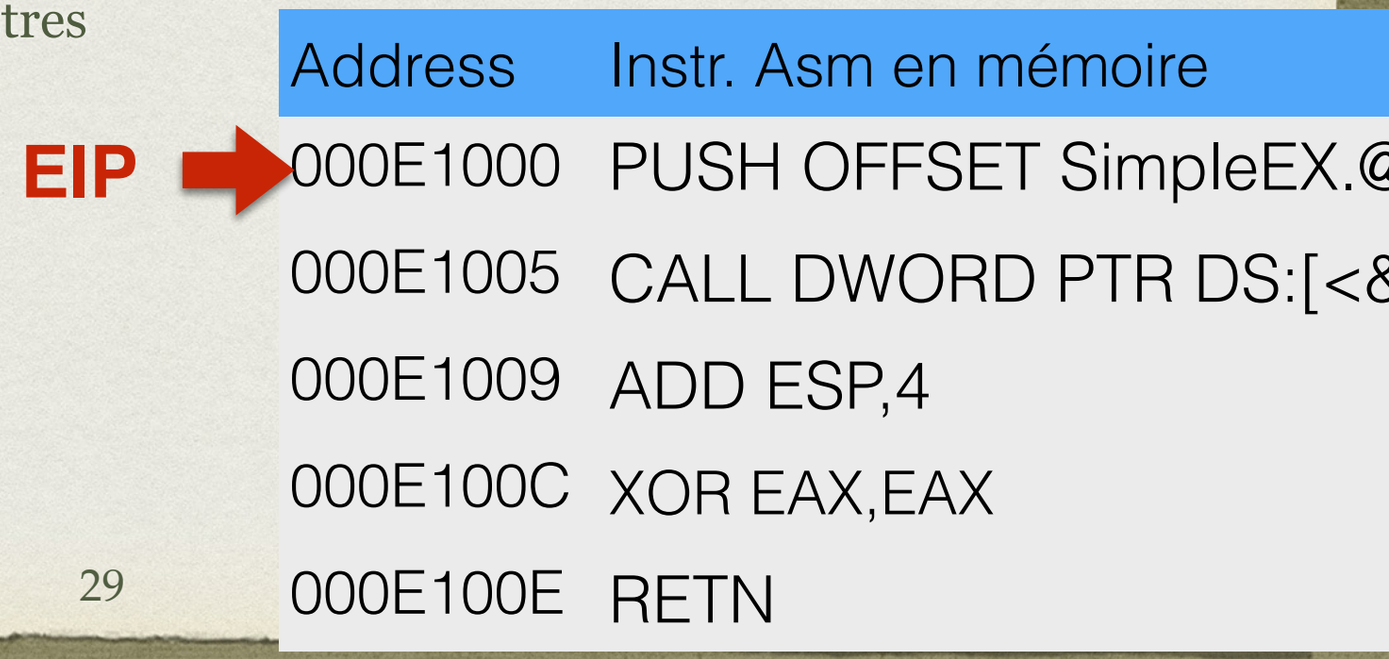
Address	Opcodes	Assembly instructions
000E1000 :	68 F4200300	PUSH OFFSET SimpleEX.@Hello!?
000E1005 :	A0 200300	CALL DWORD PTR DS:[<&MSVCR100.puts>]
000E1009 :	83C4 04	ADD ESP,4
000E100C :	33C0	XOR EAX,EAX
000E100E :	C3	RETN

X86-32 ASM 101

- Architecture 32 bits
  - Little endian
  - Registres généraux (EAX, EBX, ...)
  - Drapeaux (flags)
  - Pointeur d'instruction EIP
  - Pointeur de pile ESP
  - Base de la pile ESP

- Types d'instruction
  - mov : stocke valeurs en mémoire/registres
  - push/pop pile
  - sauts directs : jmp FEooh
    ou indirects : jmp EAX
  - sauts conditionnels : jnz, jne ...
  - call/ret
  - ...





STACK OVERFLOW

```
void copy(char *p)
 {
    char buffer[20];
    strcpy(buffer, p);
}

int main()
 {
     copy("111122223333");
 }
```

STACK OVERFLOW

```
void copy(char *p)
 {
    char buffer[20];
    strcpy(buffer, p);
}

int main()
 {
    copy("111122223333");
 }
```

Danger !

copie le contenu pointé par p
jusqu'au caractère nul (0x00)

STACK OVERFLOW

```
void copy(char *p)
 {
   char buffer[20];
   strcpy(buffer, p);
}

int main()
 {
    copy("111122223333");
 }
```

buffer est alloué sur la pile
(au dessus d'où est stockée
l'@ de retour après l'appel à copy)

STACK OVERFLOW

```
void copy(char *p)
 {
   char buffer[20];
   strcpy(buffer, p);
}

int main()
 {

copy(« 11112222333344445555
66667777");
 }
```

donc strcpy peut venir écraser
l'@ de retour de façon controlée

STACK OVERFLOW

```
void copy(char *p)
 {
   char buffer[20];
   strcpy(buffer, p);
}

int main()
 {

copy(« 111122223333444455556666777777");
 }
```

ainsi que stocker des valeurs controlées sur la pile !!!

STACK OVERFLOW

```
void copy(char *p)
 {
   char buffer[20];
   strcpy(buffer, p);
}

int main()
 {

copy(« 111122223333444
66667777");
 }
```

0xD0	1111
0xD4	2222
0xD8	3333
0xDC	4444
0xE0	5555
0xE4	6666 (EPP)
0xE8	**7777 (return address)**
0xEC	argument pointer to "111122223333"
0xF0	Previous EBP from main

STACK OVERFLOW

```
void copy(char *p)
 {
    char buffer[20];
    strcpy(buffer, p);
}

int main()
 {

copy(« 111122222333344445555
66667777");
 }
```

Execution de code arbitraire !

ANTI-STACK OVERFLOW

```
void copy(char *p)
 {
    char buffer[20];
    strncpy(buffer, p, 20);
}

int main()
 {

copy(« 111122222333344445555
66667777");
 }
```

ANTI-STACK OVERFLOW

- **DEP** : Data Execution Prevention
  - pourquoi exécuter des données ?
- **ASLR** : address Space Layout Randomization
  - impossible de connaitre une adresse à l'avance
- **Canaris** : valeurs aléatoires placées sur la pile, effacée par une attaque, dont la présence est vérifiée lors d'un *ret*

AUTRES VECTEURS DE PROPAGATION

- Concevoir une librairie véreuse et la mettre sur GitHub
- Concevoir une librairie véreuse et la cacher comme dépendance d'une librairie propre
- Infecter une librairie déjà établie si on a accès aux Pull requests sur GitHub
- Coder une app véreuse et la mettre sur un store pour téléphone rooté
- ...

CYCLE DE VIE

1. **Intrusion** : comment pénétrer le système (bugs et vulnérabilités, mots de passes faibles, ingénierie sociale, etc.)
2. **Infection** : comment planter, protéger et répliquer le maliciel dans le système
3. **Exploitation** : quelle est la charge (vol de données, DDOS, etc.)

INFECTION

- Réplication
  - Elevation de privilège : comment devenir super-utilisateur (*user/admin/root/kernel*) ? Vuln.
  - Latéralisation : comment contaminer d'autres dispositifs voisins ?
- Protection
  - Comment rester invisible, indétectable, etc.
- ...

CYCLE DE VIE

1. **Intrusion** : comment pénétrer le système (bugs et vulnérabilités, mots de passes faibles, ingénierie sociale, etc.)

2. **Infection** : comment planter, protéger et répliquer le maliciel dans le système

3. **Exploitation** : quelle est la charge (vol de données, DDOS, etc.)

EXPLOITATION - PAYLOADS

Backdoor

receive cmd
exec cmd
send result

Troyen/Spyware

capture int keyboard
if substring=bank => log
at night send log to C&C

Bombe logique

if grade(Alice) < A
rm -fr /Users/Prof

Ver

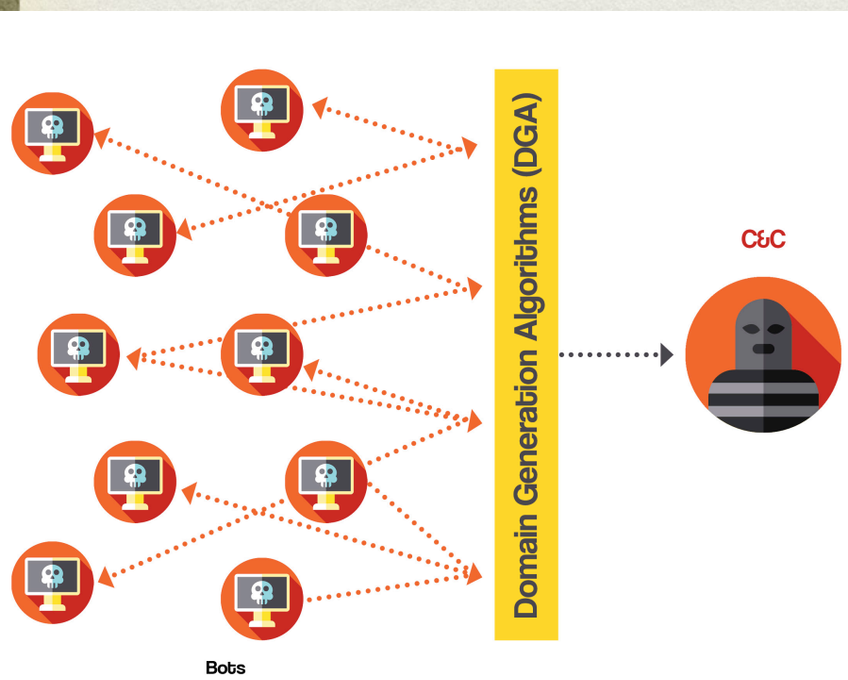
search vuln on network
exploit vuln to replicate

Rançongiciel

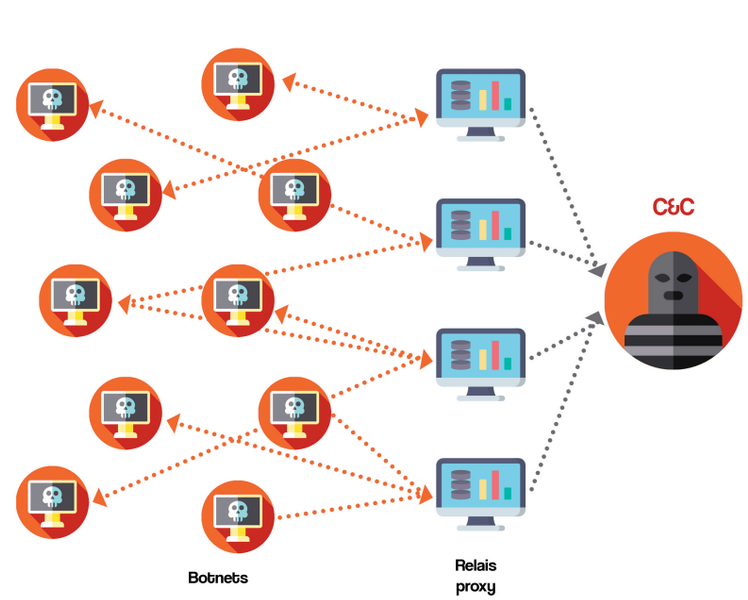
cipher(disk,$k_{publique}$)
sell $k_{private}$for bitcoins

EXPLOITATION - C&C

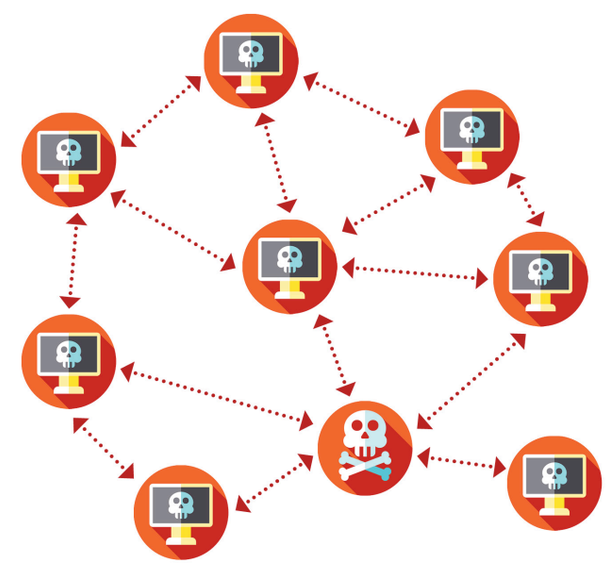
- Commande et Contrôle : mise-à-jour, commande, envoi/réception de données, etc.



Distribué centralisé avec
algo de génération de domaine (DGA)



centralisé
sur IRC ou HTTP



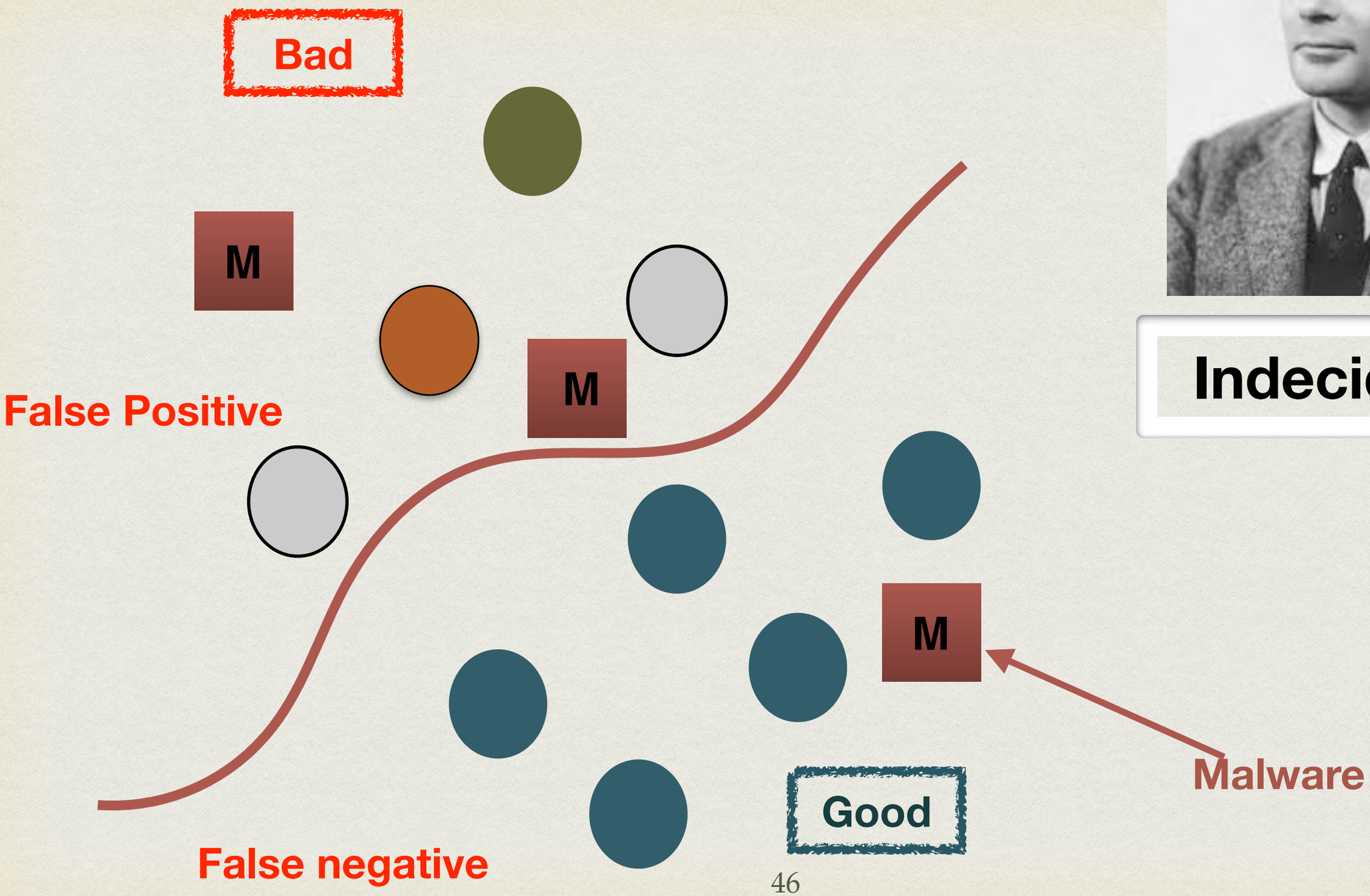
décentralisé (P2P)

ANTI-MALICIELS

remerciements Jean-Yves Marion (LORIA-Nancy-France)

DÉTECTION DE MALICIEL

Indecidable !



INDECIDABLE ?

IsVirus

```
if(P infects)
then return True
else return False
```

P

```
if(Antivirus returns OK)
then infect
else return 0
```

Impossible

INDECIDABLE ?

IsVirus

```
if(P infects)
then return True
else return False
```

P

```
if(Antivirus returns OK)
then infect
else return 0
```

Impossible

HEURISTIQUES DE DÉTECTION

Antivirus

if (*condition*)
then return True
else return False

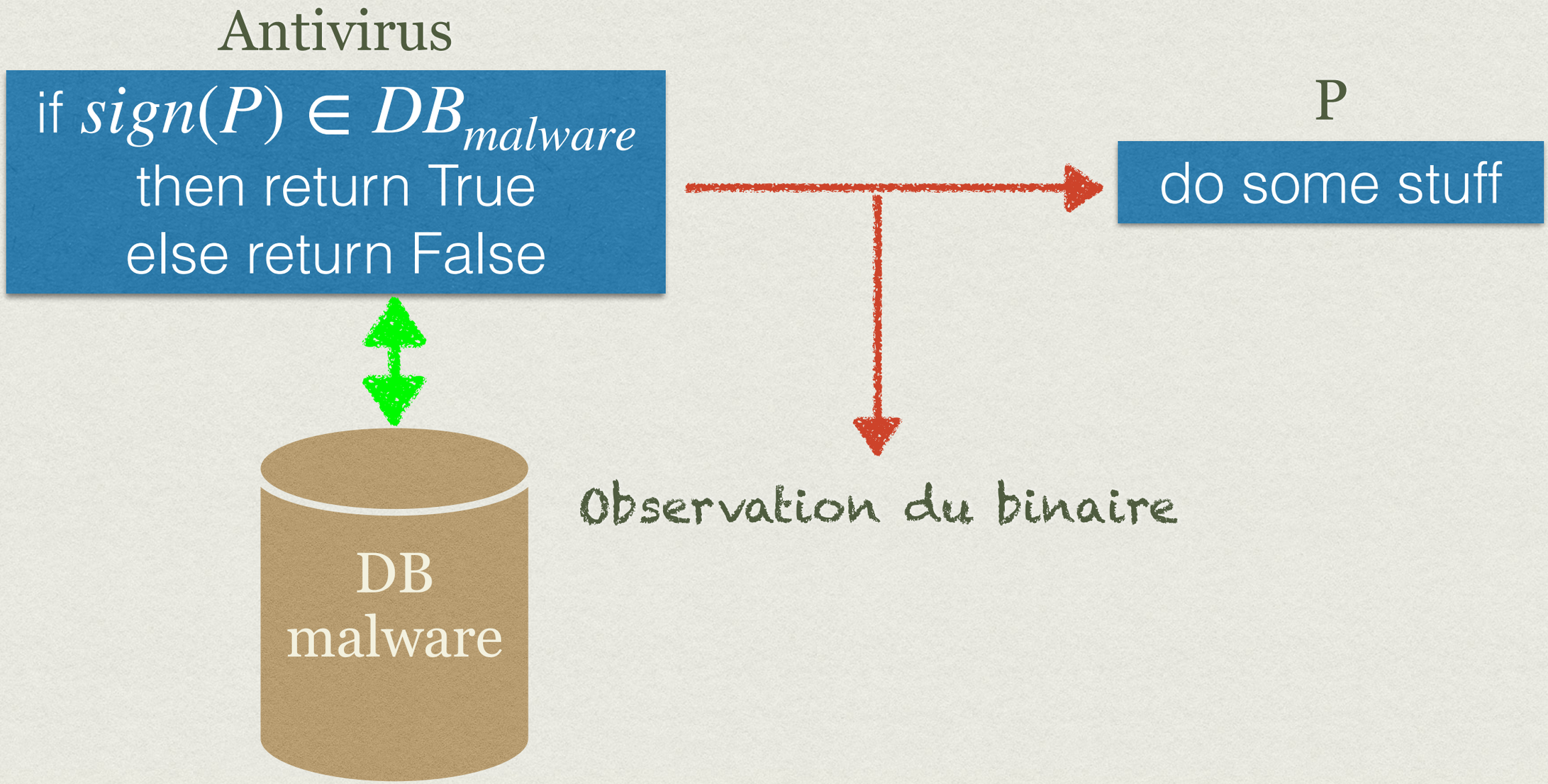
P

do some stuff

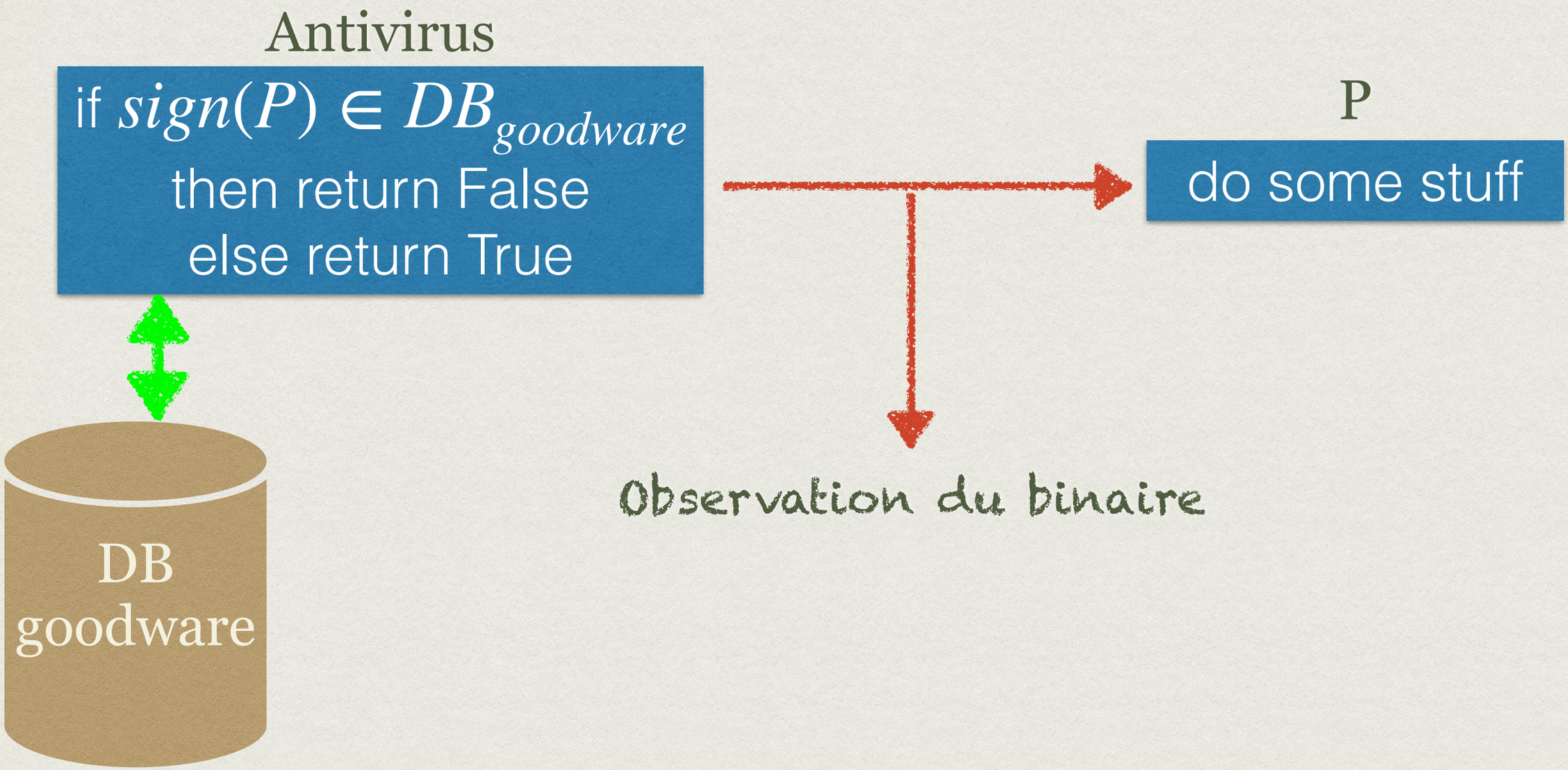
Observation du binaire

Observation du comportement

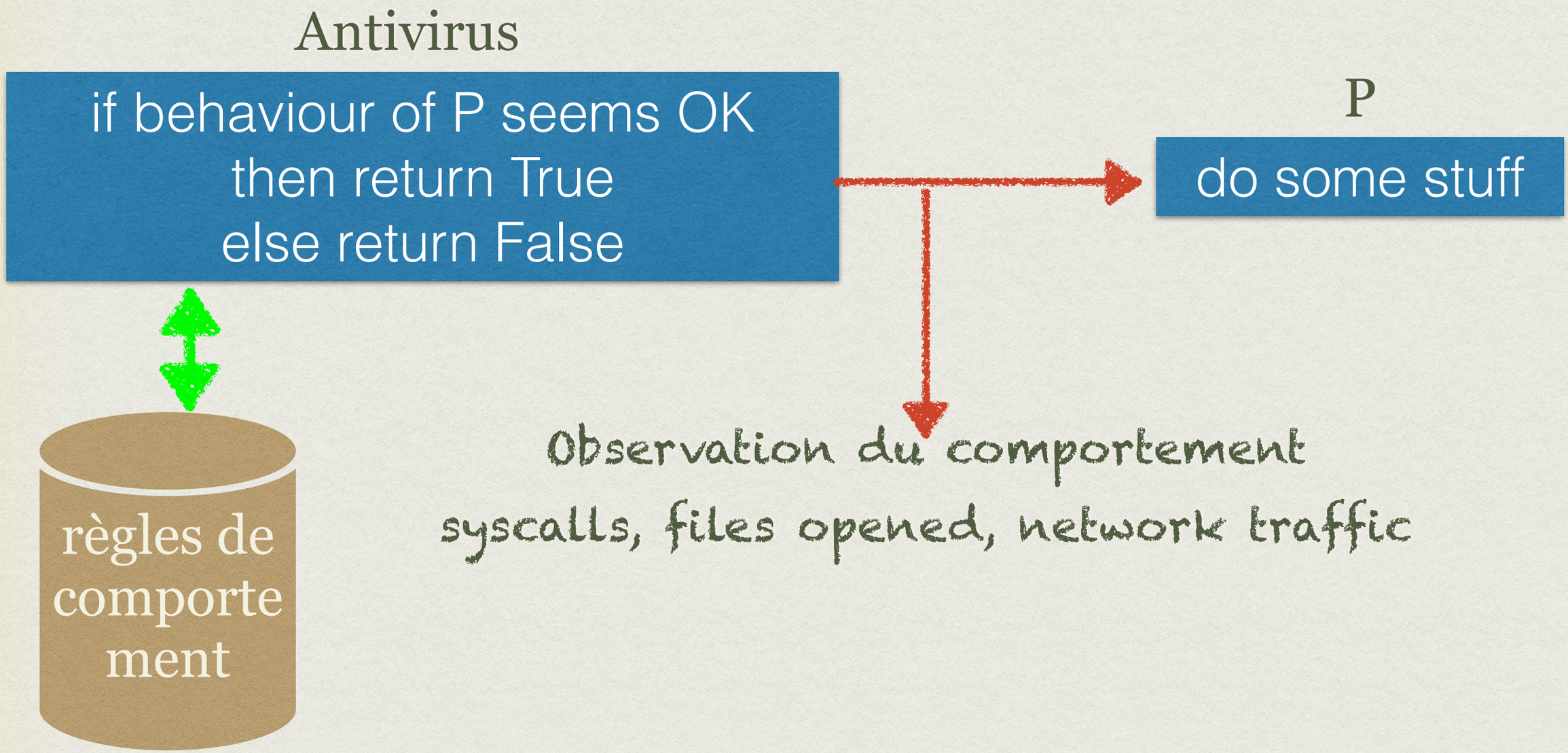
HEURISTIQUES 1
SIGNATURES



HEURISTIQUES 2
INTÉGRITÉ



HEURISTIQUES 3 ANALYSE DE COMPORTEMENT

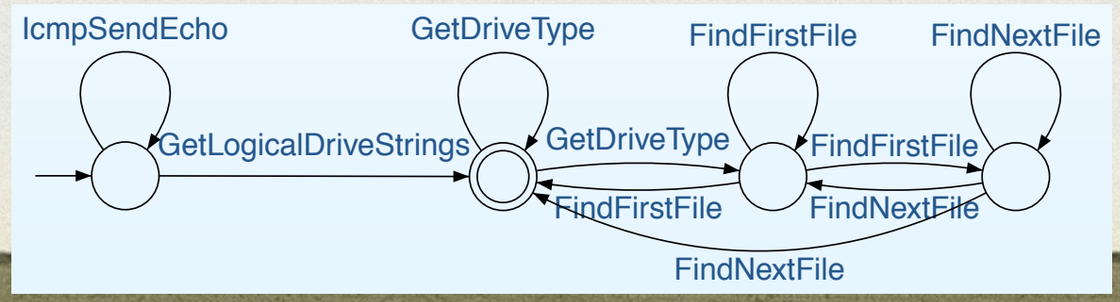


BILAN HEURISTIQUES

- Détection par signatures (*blacklist*)
  + efficace et facile à implémenter
  - incapable de détecter les mutations et nouvelles menaces

- Détection par test d'intégrité (*whitelist*)
  + facile à implémenter
  - inefficace, trop de mises-à-jour à suivre

- Détection par analyse comportementale
  + détection de nouvelles menaces
  - qu'est-ce qu'un comportement malveillant ?

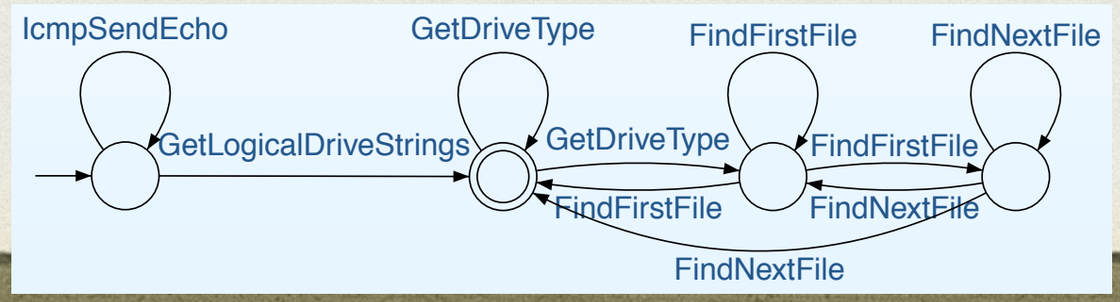


BILAN HEURISTIQUES

- Détection par signatures (*blacklist*)
  + efficace et facile à implémenter
  - incapable de détecter les mutations et nouvelles menaces

- Détection par test d'intégrité (*whitelist*) la plupart des antivirus
  + facile à implémenter
  - inefficace, trop de mises-à-jour à suivre

- Détection par analyse comportementale
  + détection de nouvelles menaces
  - qu'est-ce qu'un comportement malveillant ?



SIGNATURES BINAIRES

- règles YARA : expressions régulières du bytecode

```
rule cerber3{
meta:
  author = "pekeinfo"
  date = "2016-09-09"
  description = "Cerber3 "
strings:
  $a = {00 6A 00 68 80 00 00 00 6A 03 6A 00 6A 03 6A 01 8B 85}
  $b = {68 3B DB 00 00 ?? ?? ?? ?? 00 ?? FF 15}

condition:
  1 of them
}
```

SIGNATURES BINAIRES

- règles YARA : expressions régulières du bytecode

```
rule Mirai_5 : MALW
{
    meta:
        description = "Mirai Variant 5"
        author = "Joan Soriano / @joanbtl"
        date = "2017-04-16"
        version = "1.0"
        MD5 = "7e17c34cddcaeb6755c457b99a8dfe32"
        SHA1 = "b63271672d6a044704836d542d92b98e2316ad24"
    strings:
            $dir1 = "/dev/watchdog"
            $dir2 = "/dev/misc/watchdog"
            $s1 = "PMMV"
            $s2 = "ZOJFKRA"
            $s3 = "FGDCWNV"
            $s4 = "OMVJGP"
            $ssl = "ssl3_ctrl"
    condition:
            $dir1 and $dir2 and $s1 and $s2 and $s3 and $s4 and $ssl
}
```

SIGNATURES BINAIRES

- règles YARA : expressions régulières du bytecode

```
rule Emotets{
meta:
  author = "pekeinfo"
  date = "2017-10-18"
  description = "Emotets"
strings:
  $mz = { 4d 5a }
  $cmovnz={ 0f 45 fb 0f 45 de }
  $mov_esp_0={ C7 04 24 00 00 00 00 89 44 24 0? }
  $_eax={ 89 E? 8D ?? 24 ?? 89 ?? FF D0 83 EC 04 }
condition:
  ($mz at 0 and $_eax in( 0x2854..0x4000)) and ($cmovnz or $mov_esp_0)
}
```

SIGNATURES BINAIRES

- Faux positifs
  programmes corrects sont détectés malveillants

- Faux négatifs
  programmes malveillants non-détectés

+ Précision : peu de faux positifs

+ Efficacité : algorithmes de recherche de sous-chaines rapides
  (Karp & Rabin, Knuth, etc.)

- Signatures construites quasi-manuellement

- Vulnérable aux protections du maliciel

OBFUSCATION DU CODE

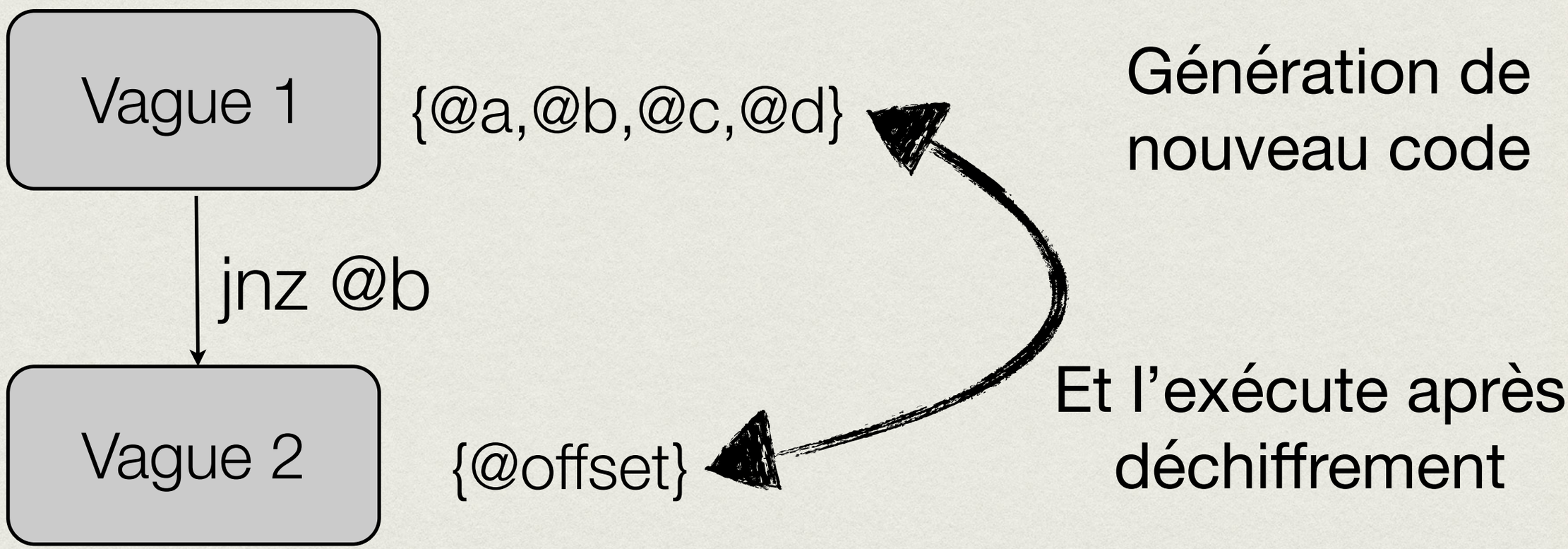
OBFUSCATION DU CODE

multiples méthodes pour rendre plus difficile l'analyse humaine ou automatique du code

- Chiffrement
- Auto-modification, packers
- Recouvrement code (multi-interprétation)
- Anti-debug
- Modification de la pile
- Interpréteurs virtuels
- Sauts indirects
- Modification des gestionnaires d'interruptions
- Prédicats opaques
- Tressage de code

EXEMPLE DES PACKERS

```
@a: mov esi , $index
@b: xor [@offset + esi], $key
@c: sub esi , 4
@d: jnz @b
@offset: [encrypted data]
```



PROTECTION CLASSIQUE DES MALICIELS

Déchiffrement

Déchiffrement

Déchiffrement

Vague 1

01005000	pushfd	
01005001	push	0x3
01005003	jae	0x1005010
01005005	jmp	0x1005009
01005007	db	0x75 ; 'u'
01005008	db	0x75 ; 'u'
01005009	call	0x1005014
0100500e	xor	ax, 0xf773
01005012	jmp	0x1005031
01005014	add	esp, 0x4
01005017	jmp	0x100501b
01005019	db	0x75 ; 'u'
0100501a	db	0x75 ; 'u'
0100501b	dec	dword

Vague 2

01007088	call	0x100708d
0100708d	sub	dword [ss:esp], 0x23a
01007094	jmp	dword [ss:esp+0x4]

.....

Vague 18

1006ba7 mov ebx, dword ptr [ebp+0x403783]
1006bad xor esi, esi
1006baf not ebx
1006bb1 or esi, ebx
1006bb3 jnz 0xa
1006bbd add ebx, dw[illegible]p+0x403763]

payload

Un run du **packer** Telock
avec 18 vagues

Un run est une séquence de vagues

Schéma de code auto-modifiant

QUI PROTÈGE PLUTÔT BIEN !

- L’analyse statique ne détecte pas des variations
  - de l’enveloppe (d’un packer)
  - la signature change avec un packer différent et/ou une clé différente
- Analyse dynamique du code ...
  - Executer tous les chemins d’exécution ...
  - Dans un environnement sûr : bac-à-sable ou une VM
  - En instrumentant le programme (un peu comme en debug)
  - Mais très complexe, couteux, etc. pas automatique
  - Pas vraiment possible dans un antivirus, réservé aux labos qui essaye de trouver des signatures de packers génériques

QUI PROTÈGE PLUTÔT BIEN !

- L'analyse statique ne détecte pas des variations
  - de l'enveloppe (d'un packer)
  - la signature change avec un packer différent et/ou une clé différente
- Analyse dynamique du code ...
  - Executer tous les chemins d'exécution ...
  - Dans un environnement sûr : bac-à-sable ou une VM
  - En instrumentant le programme (un peu comme en debug)
  - Mais très complexe, couteux, etc. pas automatique
  - Pas vraiment possible dans un antivirus, réservé aux labos qui essaye de trouver des signatures de packers génériques

!!! mettre à jour son antivirus !!!