Sécurité des téléphones et analyse de programmes malveillants

Pierre Graux
Université de Lille

Journée de l'Enseignement de l'Informatique et de l'Algorithmique
8 février 2023

20 juillet 2021

Juillet 20, 2021

Projet Pegasus. Emmanuel Macron est un des dirigeants mondiaux sélectionnés comme cibles potentielles du logiciel espion de NSO

Court historique des logiciels de renseignement

- 2013 : FinFisher

Court historique des logiciels de renseignement

- 2013 : FinFisher
- 2015 : Twitter Hacking Team compromis

Court historique des logiciels de renseignement

- 2013 : FinFisher
- 2015 : Twitter Hacking Team compromis
- 2016 : Pegasus, Infection par un lien dans un SMS (vulnérabilité safari et iOS)

Court historique des logiciels de renseignement

- 2013 : FinFisher
- 2015 : Twitter Hacking Team compromis
- 2016 : Pegasus, Infection par un lien dans un SMS (vulnérabilité safari et iOS)
- 2017 : Shadow Broker, fuite de logiciel espion (vulnérabilité EternalBlue)

Court historique des logiciels de renseignement

- 2013 : FinFisher
- 2015 : Twitter Hacking Team compromis
- 2016 : Pegasus, Infection par un lien dans un SMS (vulnérabilité safari et iOS)
- 2017 : Shadow Broker, fuite de logiciel espion (vulnérabilité EternalBlue)
- 2019 : Pegasus, Infection zero-click (injections réseaux, vulnérabilité whatsapp)

Court historique des logiciels de renseignement

- 2013 : FinFisher
- 2015 : Twitter Hacking Team compromis
- 2016 : Pegasus, Infection par un lien dans un SMS (vulnérabilité safari et iOS)
- 2017 : Shadow Broker, fuite de logiciel espion (vulnérabilité EternalBlue)
- 2019 : Pegasus, Infection zero-click (injections réseaux, vulnérabilité whatsapp)
- 2021 : Pegasus, Révélations “grand public” par 17 médias
  180 journalistes dans 20 pays ciblés par 10 pays

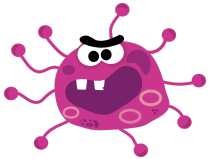
Vulnérabilité ≠ malware

Vulnérabilité
Cause

Faiblesse permettant à un attaquant de porter atteinte au bon fonctionnement d'un système

Malware
Conséquence

Logiciel malveillant



Vulnérabilité

Capacité offerte :

- RCE : exécution d'un programme à distance
- LPE : élévation de privilège
- Signing Bypass : installation de logiciel arbitraire
- Sandbox escape : évasion de mesure de sécurité

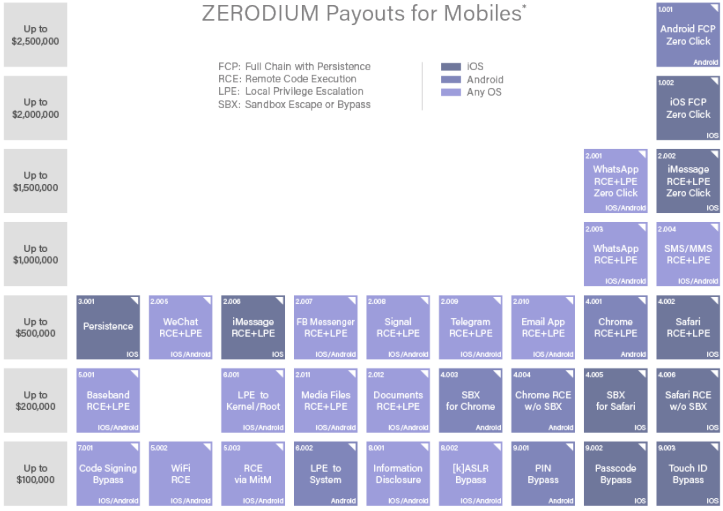
Condition de mise en place :

- Zero Click : aucune interaction avec l'utilisateur
- Persistance : persistant après le redémarrage de l'appareil

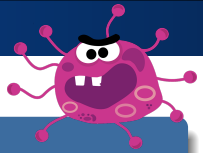
Nec plus ultra

- FCP : Chaîne d'exploitation complète

Prix d'une vulnérabilité



Malware



Différents types pour des objectifs différents

- Ransomware : réclame un paiement pour obtenir le déchiffrement du SI
- Spyware : logiciel espion
- Botnet : ensemble de machines contrôlées par un attaquant
- Premium service : utilisation de service payant

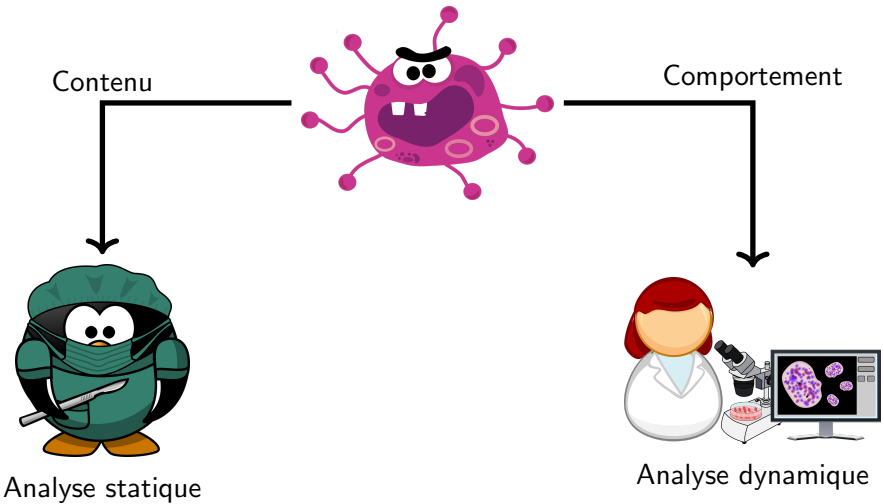
Différents formats pour des plateformes différentes

- Programme pour ordinateur
- Application pour téléphone

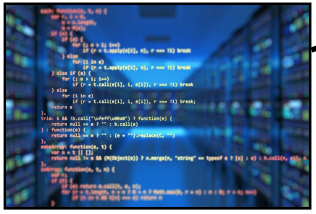
Comprendre le fonctionnement d'un malware

Technical Analysis of Pegasus Spyware, Lookout, 2016

Analyse de malware



Analyse statique



Compilation

Code source

Programme

Analyse statique

Compilation

Rétro-ingénierie

Code source **Programme**

Quelles informations contient un programme ?

Le jeu du chat et de la souris

Obscurcissement (*obfuscation*) :

technique visant à rendre plus complexe la rétro-ingénierie d'un programme.

Une bataille sans fin :

Il est impossible d'obscurcir parfaitement un programme [1].
Il est impossible d'automatiser l'analyse de programme [2].

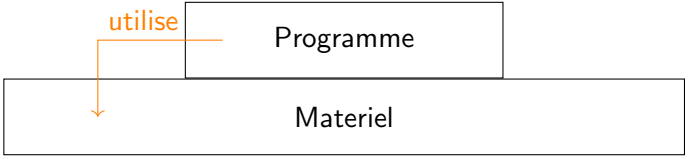
[1]: *"On the (im)possibility of obfuscating programs"*, Boaz Barak et al., CRYPTO 2001
[2]: *"Classes of recursively enumerable sets and their decision problems"*, H. G. Rice, TRAN 1953

Analyse dynamique

Comment exécuter un malware sans impacter le système d'analyse ?

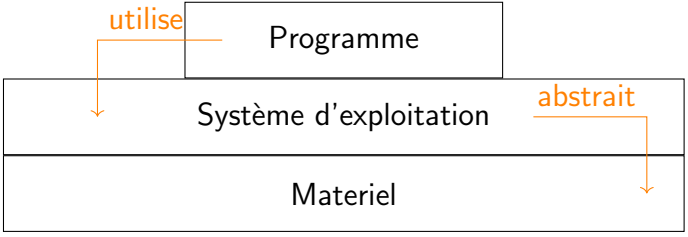
"All problems in computer science can be solved by another level of indirection, except for the problem of too many layers of indirection.", David Wheeler.

Virtualisation



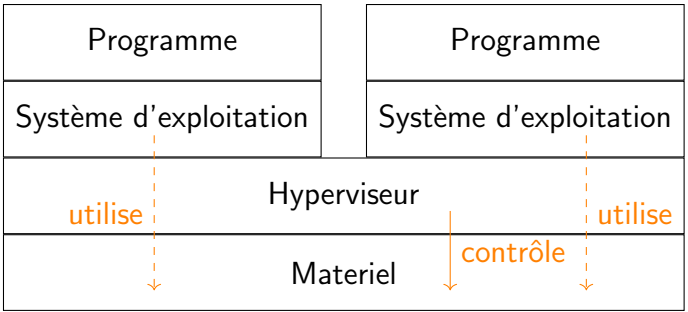
Virtualisation

Abstraction n°1 : système d'exploitation



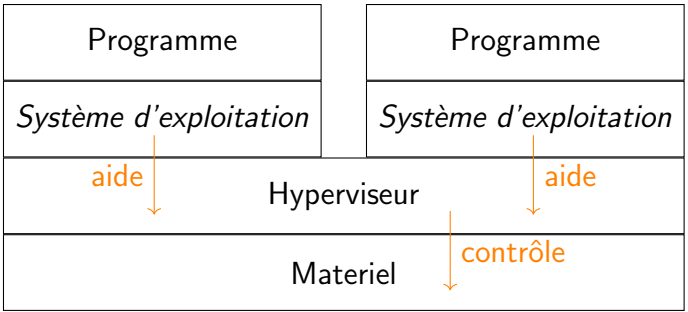
Virtualisation

Abstraction n°2 : hyperviseur type 1



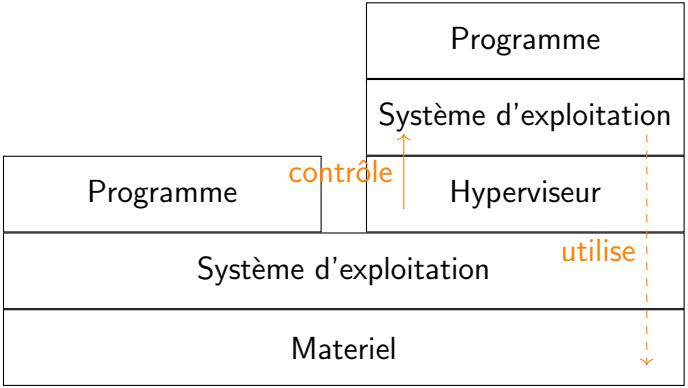
Virtualisation

Abstraction n°3 : paravirtualisation

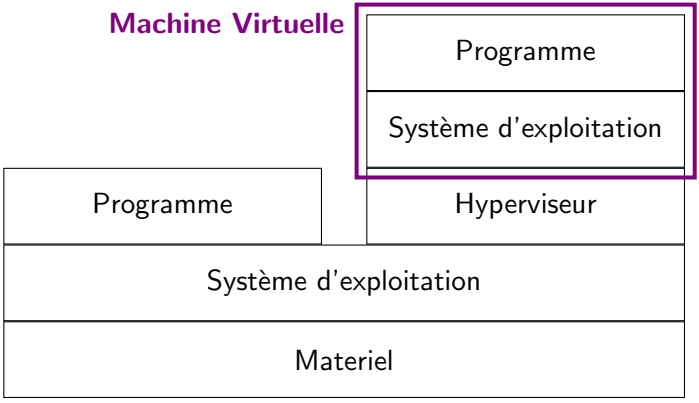


Virtualisation

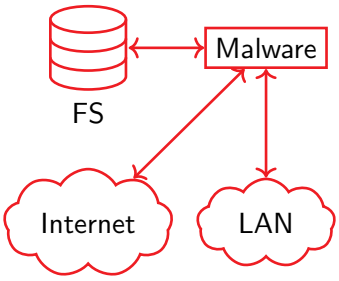
Abstraction n°4 : hyperviseur type 2



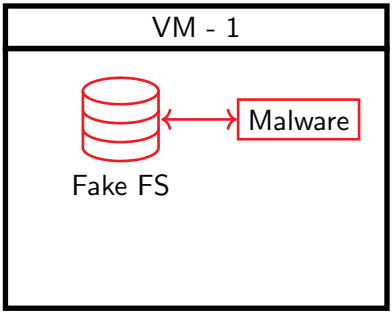
Virtualisation



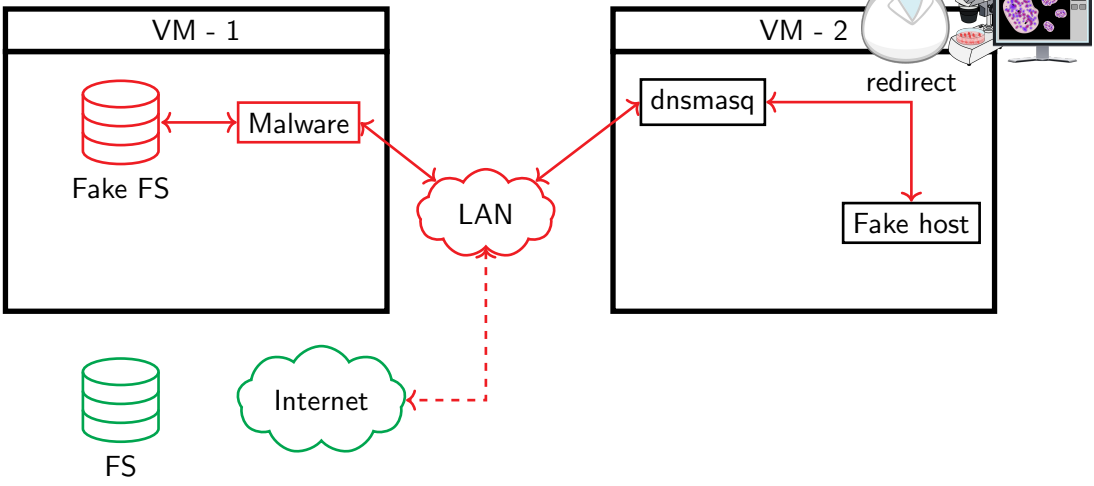
Environnement d'analyse



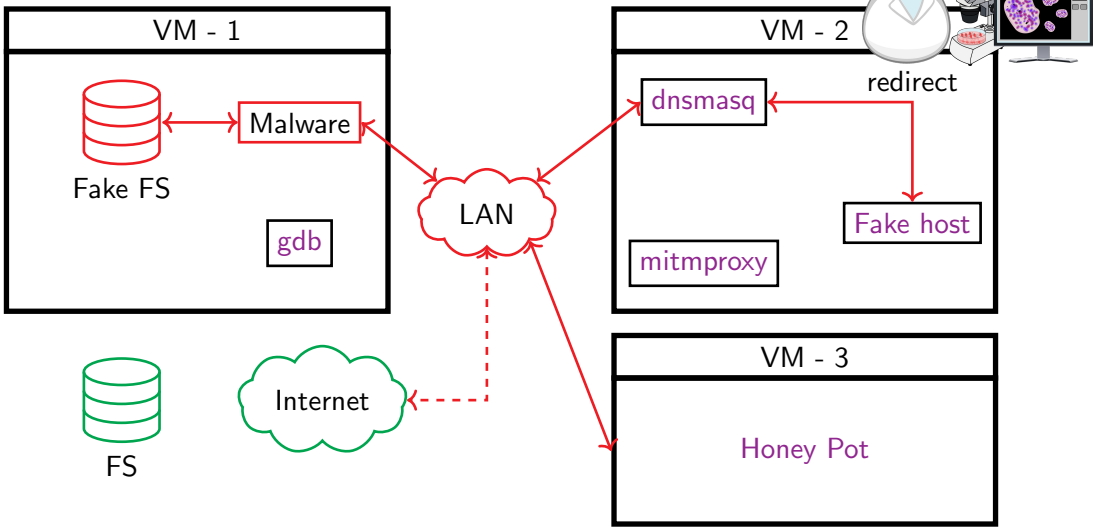
Environnement d'analyse



Environnement d'analyse



Environnement d'analyse



Suivre les traces d'un malware

Smartphone et forensique : comment attraper Pégasus for fun and non-profit, E. Maynier, SSTIC, 2022
Forensic Methodology Report: How to catch NSO Group's Pegasus, Amnesty International, 2021

Indice de compromission

IOA / IOC
Outil

Indicator Of Attack
Indicator Of Compromise

Cyber Threat Hunting
Action

Recherche pro-active de menace

Exemples d'indicateurs pour téléphone

Indicateur d'attaque (IOA)

- SMS contenant un lien vers une page identifiée

Indicateur de compromission (IOC)

- Logs réseaux
- Processus spécifiques
- Historique de navigation

Exemples d'utilisation des indicateurs

Méthode de *hunting*

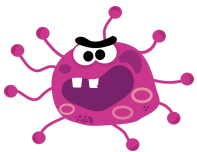
- Signature de la suite cryptographie des serveurs web
- Recherche dans les caches DNS

Traitement des vulnérabilités

Full/Responsible disclosure

Merci de votre attention

Menaces



Moyens de défense