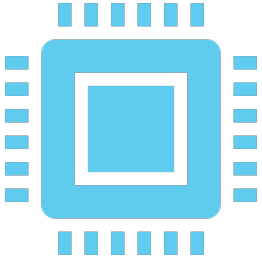
Scan email

Auteur : KOLAWOLE ABDOULAYE

INTRODUCTION



Attaque système informatique

Avant : Disquettes infectées, applications serveur

Aujourd'hui : Par email (pièce jointe)

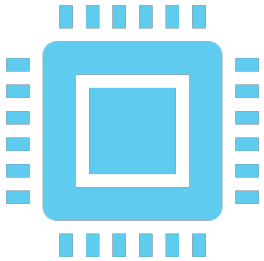
Problème ?

Solution : le sandboxing

LE SANDBOXING

- Définition : environnement test
  - mécanisme de sécurité informatique
    - moins de risques pour la machine hôte ou le système d'exploitation
  - Exécute du code non testé ou de provenance douteuse

LE SANDBOXING



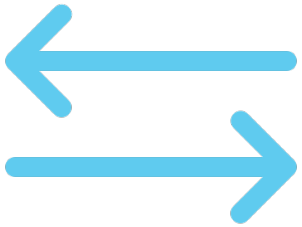
Caractéristiques

Offre un ensemble de ressources contrôlé

- Espace de stockage temporaire sur le disque dur

Désactiver ou restreint

- Accès aux réseaux
- La possibilité d'inspecter le système hôte
- Utiliser des périphériques



➔ Exemple particulier de virtualisation

LE SANDBOXING

- Sandbox :
  - Une couche supplémentaire de protection
    - Menaces jour zéro (auparavant non détectées)
    - Attaques furtives
- Méthode traditionnelle (avant sandbox):
  - Basées sur la détection de signatures

LE SANDBOXING : Outils

En local

Cuckoo

Joe Sandbox Deskop

Dans le cloud

Joe Sandbox Cloud

HOSTED EMAIL SECURITY

G suite

Outils en local : Fonctionnement

Création d'environnement virtuel

Exécution des fichiers : pièces jointes, etc…

Analyse du comportement

Regarder et écouter pour déterminer ce que fait le code et avec qui il communique

Générer un rapport détailler sur les fichiers/clé du registre Windows créé/ modifié/ supprimé, les requêtes réseaux

➔ **Fichier malicieux ou pas**

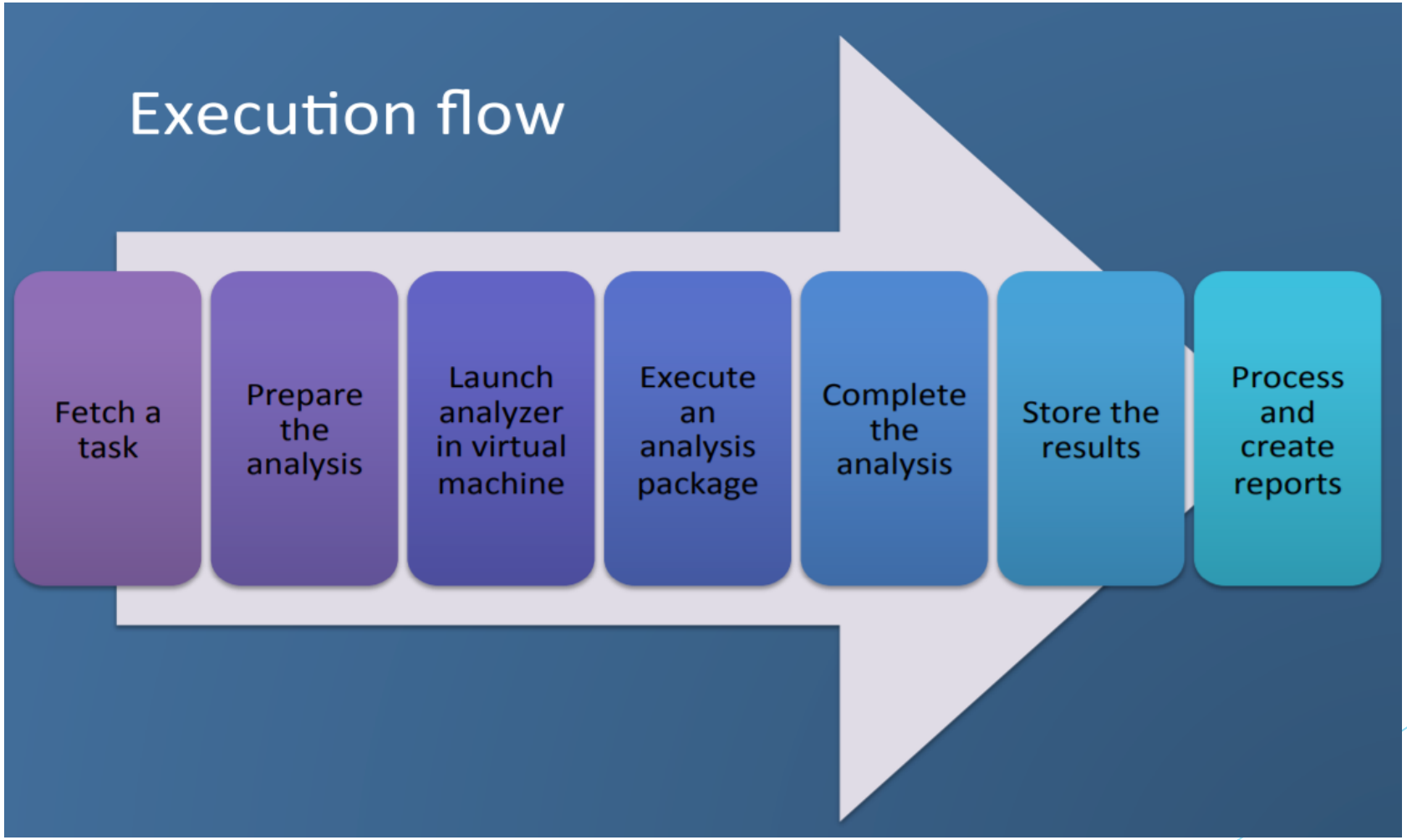
Outils en local : Cuckoo

100% pyhton

3 composants

- Scheluder
  - Distribue les tâches en attente au pool de machines disponibles
- Analyser
  - Exécute et analyse les fichiers
- Cmonitor & chook
  - Personnalise Microsoft Detours grâce à des hooks

Outils en local : Cuckoo



Outils en local : Cuckoo

- Traces d'appels effectuées par tous les processus générés par le malware.
- Fichiers créés, supprimés et téléchargés par le malware lors de son exécution.
- Vidages de mémoire des processus malveillants.
- Trace de trafic réseau au format PCAP.
- Captures d'écran pris lors de l'exécution du malware.
- Vidages mémoire complets des machines.

Outils en cloud : Fonctionnement

Interception du mail

Exécution des fichiers : pièces jointes, etc…

Analyse du comportement

Regarder et écouter pour déterminer ce que fait le code et avec qui il communique

Générer un rapport

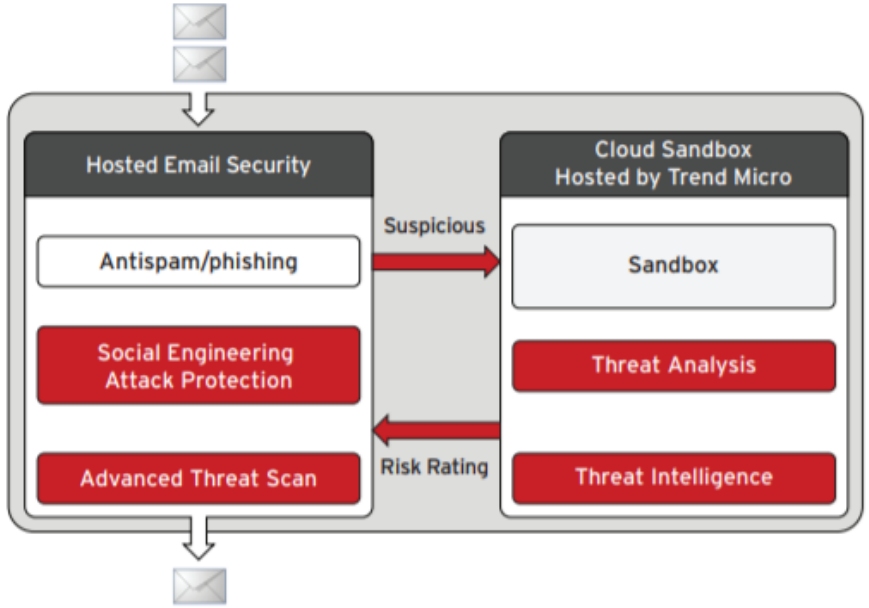
Fichier malicieux ou pas ?

Malicieux ➔ Mise en quarantaine et envoie mail au client

Pas malicieux ➔ remet fichier dans le flux et envoie de mail au client

Outils en cloud : Exemples

- Hosted email



- Joe Sandbox Cloud, Gsuite etc…

MERCI DE VOTRE ATTENTION