Rapport d'Analyse de Malware

Projet : Constructing Defense

Sujet : Déploiement d'un laboratoire d'analyse et étude d'un malware

Étudiant : Mohamed Rayen AKAICHI
Infrastructure : DetectionLab (Windows 10) & Kali Linux

25 février 2026

Table des matières

1 Résumé Exécutif

Ce rapport détaille la mise en place d'une infrastructure d'analyse de malwares (DetectionLab) et son utilisation pour étudier un échantillon de la famille **Socks5Systemz**.

L'analyse démontre comment ce malware utilise l'ingénierie sociale (faux installateur de convertisseur audio) et des techniques de "packing" (Inno Setup) pour infiltrer un système. Une fois exécuté, il enrôle la machine dans un botnet en communiquant avec un serveur de commande (C2) via HTTP. Le rapport fournit les indicateurs de compromission (IOCs) et une règle YARA pour la détection.

2 Mise en Place de l'Environnement (Lab Setup)

L'analyse dynamique nécessite un environnement isolé et instrumenté. j'ai choisi de déployer **DetectionLab** sur une machine hôte Windows.

2.1 Déploiement de DetectionLab

DetectionLab automatise la création d'un domaine Windows surveillé (Active Directory, Splunk, Sysmon).

Pré-requis et Installation :

1. Installation de **VirtualBox** et **Vagrant** sur l'hôte Windows.
2. Désactivation des conflits de virtualisation (Hyper-V, Isolation du noyau) pour assurer la stabilité des VMs.
3. Déploiement via PowerShell :

```
git clone https://github.com/clong/DetectionLab.git
cd DetectionLab/Vagrant
./prepare.ps1
vagrant up
```

Listing 1 – Commandes de déploiement

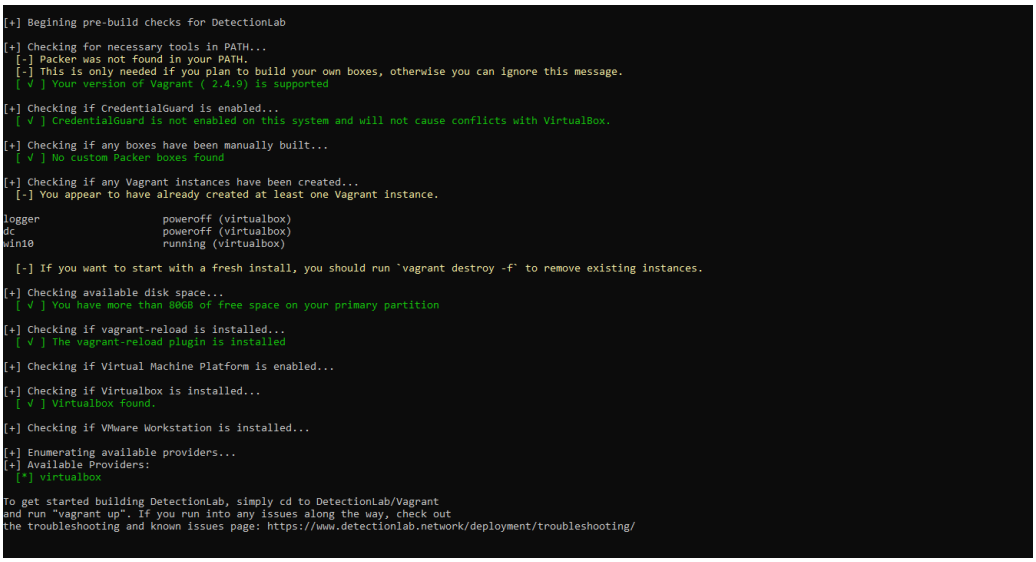

FIGURE 1 – Déploiement automatisé des VMs via Vagrant

2.2 Transfert du Malware (Kali vers Windows)

Pour transférer l'échantillon de la machine d'attaque (Kali Linux) vers la victime (Win10) sans exposer l'hôte, j'ai mis en place un serveur HTTP temporaire sur un réseau Host-Only isolé.

Configuration Réseau :

— Kali Linux IP (Host-Only) : `192.168.56.108`

— Win10 Victime IP : `192.168.56.104`

Exécution du transfert : Sur Kali, un serveur Python a été lancé dans le répertoire du malware :

```
sudo python3 -m http.server 80
```

Listing 2 – Lancement du serveur Python sur Kali

Sur la machine victime Windows 10, le fichier a été récupéré via le navigateur à l'adresse `http://192.168.56.108/malware.exe`.

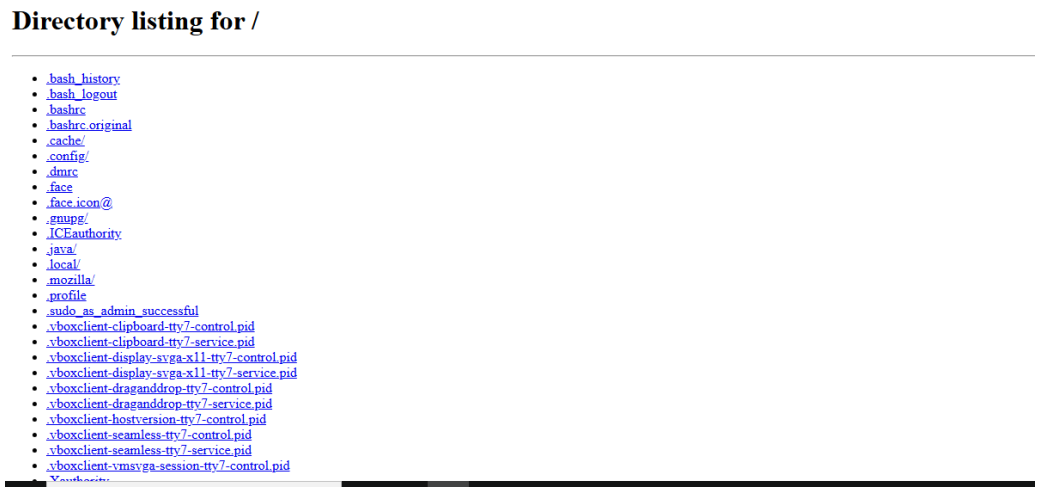

FIGURE 2 – Méthode de transfert du malware via HTTP

3 Identification de l'Échantillon

Nom du fichier	f027ab54...2b.exe (Renommé SystemUpdate.exe)
Type de fichier	PE32 Executable (GUI) Intel 80386
Taille	546 KB
Hash SHA256	f027ab542dc3fa47097d26472933cdb50c9960f00aab2e7a32443db5ae89ed2b
Classification	Dropper / Botnet Client (Socks5Systemz)

TABLE 1 – Carte d'identité du malware

4 Analyse Statique (Kali Linux)

L'analyse des chaînes de caractères (`strings`) a révélé que le malware est encapsulé ("packed") dans un installateur **Inno Setup**.

```
This installation was built with Inno Setup.
FileDescription: Audio Book Conversion Setup
```

```
3 ProductName: Audio Book Conversion
```

Listing 3 – Indicateurs Inno Setup

Cette technique de "Trojan" vise à tromper l'utilisateur en se faisant passer pour un logiciel légitime de conversion audio.

5 Analyse Dynamique (Windows 10)

L'échantillon a été exécuté sur la VM Windows 10 instrumentée.

5.1 Chaîne d'Exécution (Process Monitor)

L'outil **Process Monitor** a permis de tracer l'infection :

1. **Dropper :** Le faux installateur s'exécute.
2. **Installation :** Il déploie la charge utile dans `%LOCALAPPDATA%`.
3. **Persistance :** L'exécutable `audiobookconversion14230.exe` est lancé.

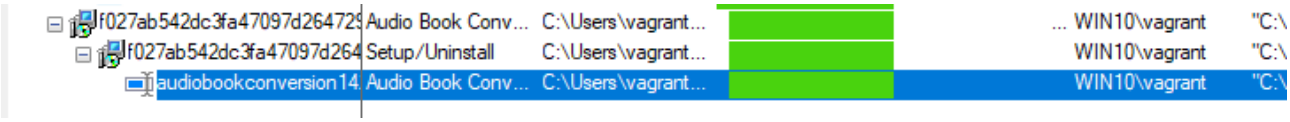

FIGURE 3 – Visualisation de l'arbre des processus infectieux

5.2 Activité Botnet (Relais Proxy)

L'analyse prolongée du trafic réseau (fichier CSV exporté depuis Wireshark) a révélé que la machine compromise est activement utilisée comme nœud de sortie (Proxy) pour le botnet.

Nous avons observé la séquence suivante :

1. Une IP externe (`94.26.38.3`) envoie une requête HTTP `GET /rand` à notre machine victime.
2. Immédiatement après, notre machine relaie cette même requête vers une cible tierce (`45.11.182.186`).
3. La réponse de la cible est ensuite renvoyée à l'IP initiale.

Cette activité confirme que le malware **Socks5Systemz** transforme l'hôte en relais pour masquer les activités illicites des attaquants.

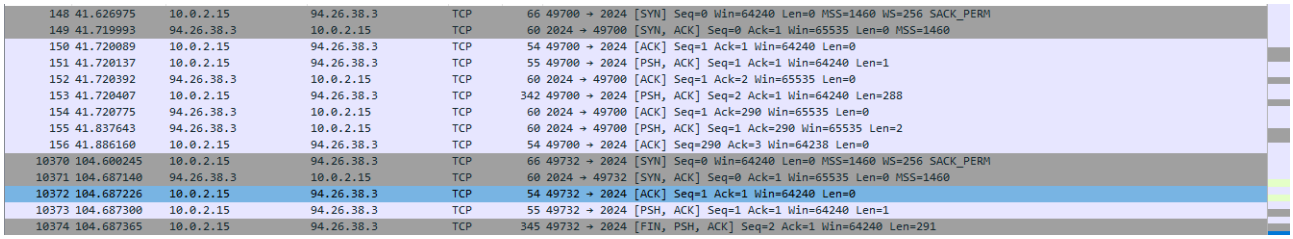

FIGURE 4 – Preuve du comportement de "Man-in-the-Middle" du botnet

6 Conclusion

L'analyse a confirmé la nature malveillante du fichier. Il s'agit d'un botnet Socks5Systemz utilisant un installateur légitime (Inno Setup) pour l'évasion. L'analyse dynamique a non seulement révélé l'exfiltration de données vers un C2, mais a également prouvé l'utilisation active de la machine compromise comme proxy SOCKS, transformant la victime en bouclier pour les activités des cybercriminels.