le cnam
Ile-de-France

Rapport d'analyse

SEC102 année 2022 semestre 1
Date d'examen :30/01/2023
Nom :Bitan
Prénoms :Sarah
Nom second auditeur :Bitan
Prénoms second auditeur :Shmuel Nom troisieme auditeur :Assaban
Prénoms troisieme auditeur :Guil

Consignes

Note importante: ne pas modifier le format et la structure du fichier.
Les réponses peuvent être multiples et devront être séparées par une virgule

Réponse aux incidents

Veuillez décrire les étapes de la réponse aux incidents que vous suivriez dans un cas concrêt et la procédure de réponse à l'incident.

n° |Etape | Description |

01-001|* * 00 - Analyse et choix de la procédure a adopter * |Mise en place de la reponse a incident mon equipe et moi nous sommes basés sur le DFIR Conçu pour répondre aux missions opérationnelles de l'ANSSI en matière d'investigation et de réponse à incident car le DFIR fournit une compréhension approfondie des incidents de cybersécurité grâce à un processus forsenic 01-002|* 01 - Préparation * | • Mettre en place un plan pour l analyse doccumenter les différentes etapes , • Répartir les taches entre les differents membres du groupe , • Mettre en place de la documentation pour repondre a l incident et détailler nos avancées durant l analyse , • Mettre en place un outil de suivis de l'incident, • Préparer du matériel dédié à l'analyse ou la reprise d'activité(machine virtuelle,. . .), • Installer des outils pour la collecte, la conservation et l'analyse (Principalement volatility 3.0 , Differentes commades linux (via tsurugui) ghirda et plaso)

01-003|* Detection • tout d abord il faut eviter la propagation donc debrancher la machine du reseau dans notre cas cette etape a deja etait réalisé on peut donc passer a la suite ,

• Chercher des signe precurseur ou indicateur d un incident ,

• Consulter les systeme de detection et les antivirus pour voir si ils ont reprere une attaque ,

• Consulter les differents journaux du système d'exploitation, des services, des applications et des périphériques réseau,

• Collecter les détails de l'incident , • Mettre en place une timeline de l incidant quand la machine a été infécté ? comment? etc. . . 01-004|*Analyse • Les données sont ensuite examinées et analysées grace a nos differents outils et il nous faut ensuite tirer des conclusions sur les preuves trouvées.

01-005|* Mise en quarantaine,éradication et restauration

• Dans notre cas la mise en quarantaine a déja etait fait et etant donné que nous devions juste réaliser une analyse l'éradication et la réstauration n etaient pas necéssaire mais nous détaillerons quand meme ici les différentes etapes , • Supprimer les moyens mis en œuvre par l'attaquant pour accéder aux systèmes d'information ,

- Mettre en place les actions visant à bloquer ou contenir l'attaque ,
- Prévoir la réinstallation complète

01-06|* Post-incident

- Mettre en place des bonnes pratiques pour eviter que l incident se reproduise ,
- Analyser les différentes problematiques liées a cette attaque (par exemple fuite d information etc), • Collecter et conserver les données relatives à l'incident ,
- Evaluer chaque incident
- Entamer des poursuites judiciaires

Analyse mémoire RAM

Synthèse de l'analyse

n°	Question	Réponses
02-001	*Date de compromssion (eg. YYYYMMDD-HH:MM:SS)*	20140429-20:57:08
02-002	*Vecteur de compromssion*	Faible mot de pass de l utilisateur admin
02-003	*Vulnerabilités exploitées (eg. CVE-YYYY-XXXX)*	CVE-2009-4324,CVE-2007-4528
02-004	*Profile d'analyse*	WinXPSP2x86
02-005	*PID du processus vérolé*	852 (explorer.exe)
02-006	*IP du CC*	169.254.154.85
02-007	*Nom des fichiers illégitimes (sous la forme de name.exe ou name.dll)*	wuauctl.exe, explorer.exe
02-008	*Port utilisé par le malware*	local :1103
02-009	*PID du parent du malware*	660
02-010	*Nombre de page RWX du malware*	55 (nombre de page avec les droits d écriture lecture et d'éxécution trouvé grave a la commande vadinfo)

Méthodologie d'analyse

Veuillez décrire les étapes de vos analyses qui vous ont permis de trouver des preuves numériques.
Veuillez ne pas dépasser une page d'écriture.
1 On commence par le telechargement de la copie de la memoire vive, 2 l'installation de volatility , 3image info pour trouver le profile, 4conscan pour trouver le pid , 5 pstree pour trouver le pid parent , 6 analyse sur total virus qui detecte un virus poison ivy, 7 commande vad info pour trouver le nombre de pages générées , 8 utilisation des commandes comme pslist qui nous montre que explorer.exe n'a pas de ppid dans la liste et qu'il y'a de nombreux fichiers ou encore csrss.exe,pstree, psxview, dlllist, connscan, et cmdscan pour avoir plus d'informations sur le malware.

Analyse dump disque dur

Synthèse de l'analyse

n°	Question	Réponses
03-001	*Date de compromssion (eg. YYYYMMDD-HH:MM:SS)*	2013-06-30 14:56:02
03-002	*Vecteur de compromission*	faible mot de passe (IEUser cad le nom d'utilisateur)
03-003	*Nom du compte illégitime*	Hacker , Daily
03-004	*Type de partition*	vol2 (NTFS)
03-005	*Chemins du malware (eg: C:\Users\temp)*	C:\WINDOWS\system32\wuauctl.exe
03-006	*Clés de registre modifiées :*	HKEY_CLASSES_ROOT\CLSID\{C523F39F-9C83-11D3-9094-00104BD0D535}
03-007	*Adresse Ip de la Machine*	192.168.10.22
03-008	*Numéro du volume de stockage de la provenance du malware (de type* xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx	
03-009	*Nom du fichier source du malware*	Special Documentation.pdf
03-010	*Nom et numero de série des supports amovibles connectées*	CRMPXVOL_EN

Méthodologie d'analyse

Veuillez décrire les étapes de vos analyses qui vous ont permis de trouver des preuves numériques.
Veuillez ne pas dépasser une page d'écriture.

1 Téléchargement de la copie physique du disque dur vmdk , 2 Test du disque dur sur une machine virtuelle windows XP , 3 naviguation à travers les fichiers diiférents fichiers mais aucune piste concrètes a part l utilisateur hacker et le mot de passe de IEuser , 4 utilisation de avast ce qui n'a rien donné, 5 Conversion du fichier vmdk en raw avec qemu-utils , 6 installation de plaso pour analyser la

machine et son contenu et nous générer un fichier csv avec la timeline, 7 analyse de la timeline qui montre : 8 la création de 2 utilisateurs Daily et hacker , 9 L'ouverture du fichier Special Documentation.pdf , 10 l IP de la machine, 10 le chemin du malware

Analyse du malware

Synthèse de l'analyse

n°	Question	Réponses
04-001	*Nom du malware*	Poison Ivy
04-002	*Nom du fichier malveillant*	wuauctl.exe
04-003	*Classification*	Cheval de Troie famille RAT
04-004	*Système d'exploitation (eg. Windows 8, Windows 2000, ...)*	Windows XP
04-005	*Architecture (x86, x86_64, arm32, arm64)*	x86
04-006	*Méthode de persistence*	Il fait appel au malware a chaque connexion d un utilisateur , il utilise diverses techniques pour être exécutées par l'utilisateur ou par d'autres logiciels sur le système affecté (recherche sur internet sur le fonctionnement de poison ivy).
04-007	*Password de connexion*	admin
04-008	*MD5 hash*	69c5f02ada419c6d7927bc8b1e660f5f
04-009	*Date de compilation (format YYYYMMDD-HH:MM:SS)*	20080106-14:51:31
04-010	*Fonctionalités*	Selon la façon dont l'attaquant le configure, le code réseau lance un navigateur Web caché (le navigateur par

défaut du système) et s'injecte dans ce processus. Le code réseau télécharge alors à distance (depuis le PIVY de l'attaquant client en tant que shellcode) le reste du code et les données nécessaires pour le malware.Il possède à son actif de multiples attaques, telles la compromission des données de la société de sécurité américaine RSA, l'agression « Nitro » contre les fabricants de produits chimiques, l'intrusion dans des entreprises de la défense américaines, etc.

Méthodologie d'analyse

Veuillez décrire les étapes de vos analyses qui vous ont permis de comprendre le fonctionnement du malware.

Veuillez ne pas dépasser une page d'écriture.
Nous avons réalisé en premier lieu l'analyse de la mémoire vive de la machine Windows XP Service Pack 2 , lors de cette analyse nous avons constaté qu'elle était infecté par le malware Poison Ivy en utilisant les différentes commandes de volatility nous avos vu que ce malware s'était introduit sous forme de cheval de troie dans le fichier wuauctl.exe.Après ces constatations , nous sommes passé à l'analyse du disque dur de la deuxième machine Windows XP Service Pack 3.Nous avons tout d'abord créé une machine virtuelle Windows XP à laquelle nous avons attribué le disque dur , puis lors du démarrage de la machine , nous nous sommes rendus compte que l'utilisateur IEUser avait pour mot de passe son nom d'utilisateur donc une très faible sécurité (idem pour le compte Hacker qui ne nécessitait pas de mot de passe), nous avons fait tourner avast qui n'a détécté aucun malware.Pour obtenir plus d'informations sur cette machine , nous avons installé qemu-utils et convertit le fichier vmdk en raw après cela nous avons installé plaso pour connaitre les processus en cours ainsi que la timeline de la machine et d'autres informations.Pour finir , nous avons installé ghidra pour analyser le fichier raw et nous avons réalisé une analyse manuelle des fichiers via virustotal pour récupérer les informations complémentaires. .

TimeLine and conclusion

Timeline

n°	Question	Réponses
05-001	*Date de dépose du malware*	2013-06-30 14:56:02
05-002	*Date de la première execution du malware*	2013-06-30 14:58:44
05-003	*Date d'exécution du processus vérolé*	2013-06-30 14:58:54

Conclusion

n°	Question	Réponses
06-001	*Sévérité (faible, moyenne, élevée)*	élevée
06-002	*Nombre de machine(s) infectée(s)*	2
06-003	*Système d'exploitation affecté*	Windows XP SP2 et SP3
06-004	*Type de malware (eg:keylogger)*	Backdoor
06-005	*Type d'attaque (eg:phishing)*	Une évasion(attaque informatique qui va détourner les équipements de détection d'intrusion pour effectuer un exploit informatique ou installer un logiciel malveillant sur une machine ou un système du réseau sans se faire détecter)
06-006	*Nom de la souche du malware*	Poison Ivy
06-007	*IOC*	Des requetes DNS ont été produites par les 2 machines

Veuillez décrire les recommandations que vous proposeriez
Veuillez ne pas dépasser une page d'écriture.

avant tout il faudrait analyser tout le reseau car il est toujours possible que d autre machines soeint infecté . Il faudrait restaurer les information des 2 postes analysées (apres les avoir réinitialisé). Une fois l incident resolu il serait conseillé d'avoir des programmes antivirus ou anti-malware pour faire en sorte qu'il n'y ait pas de virus et les désinstaller , faire attention aux mails reçus et aux mises à jour , ne pas ouvrir n'importe quels fichiers , choisir des mots de passe complexes ou utiliser des génerateurs de mots de passe pour encore plus de compléxité et nettoyer la base de registre (cf copie d'écran).

Annexes

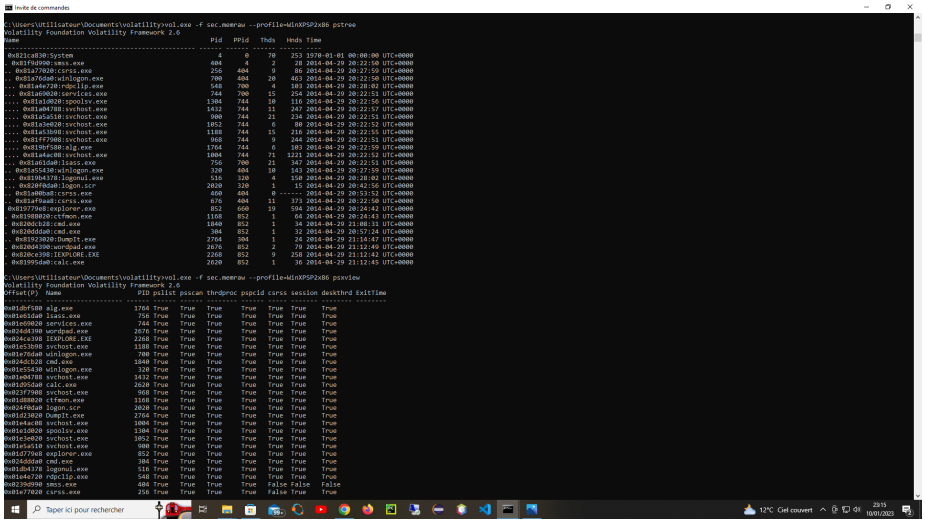

Figure 1: Utilisation des commandes pstree et psxview

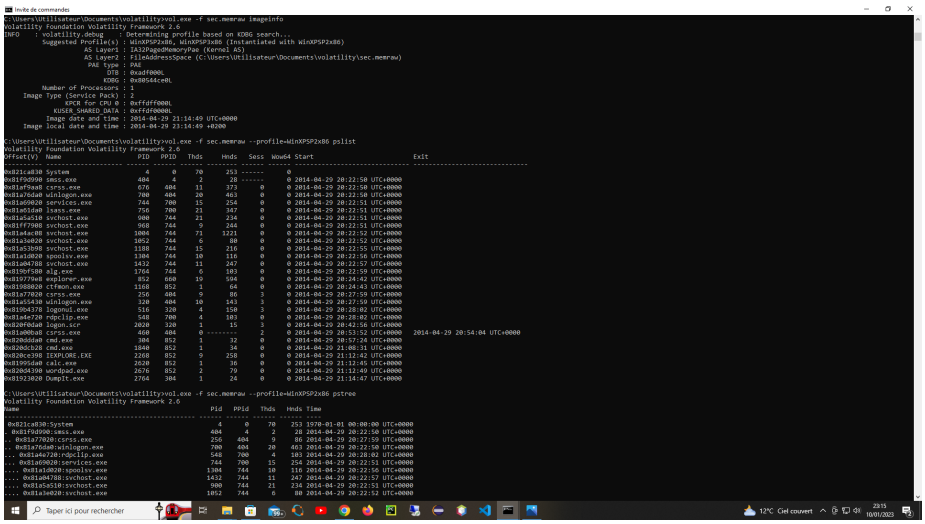

Figure 2: Utilisation de la commande pslist

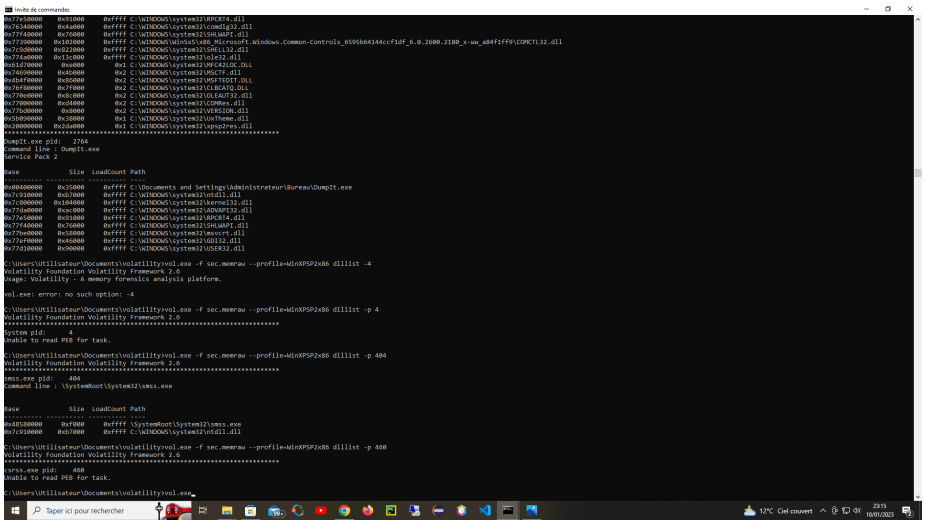

Figure 3: Utilisation de la commande dlllist

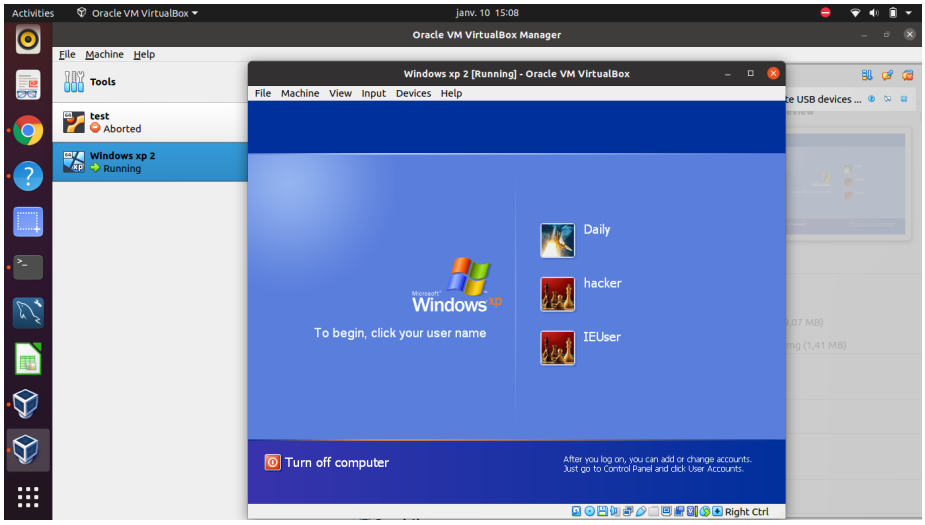

Figure 4: Création d'une machine virtuelle Windows XP pour analyser le disque dur

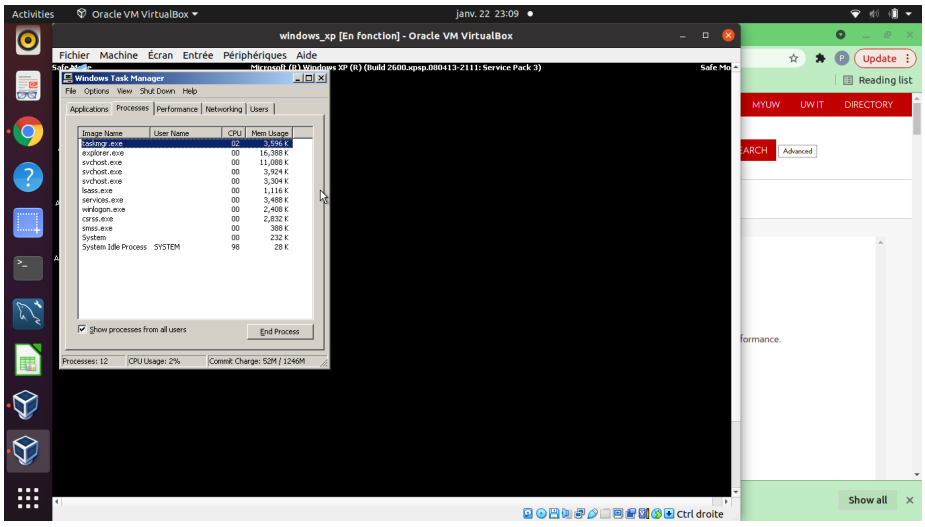

Figure 5: Utilisaon de Task Manager pour connaitre les processus en cours

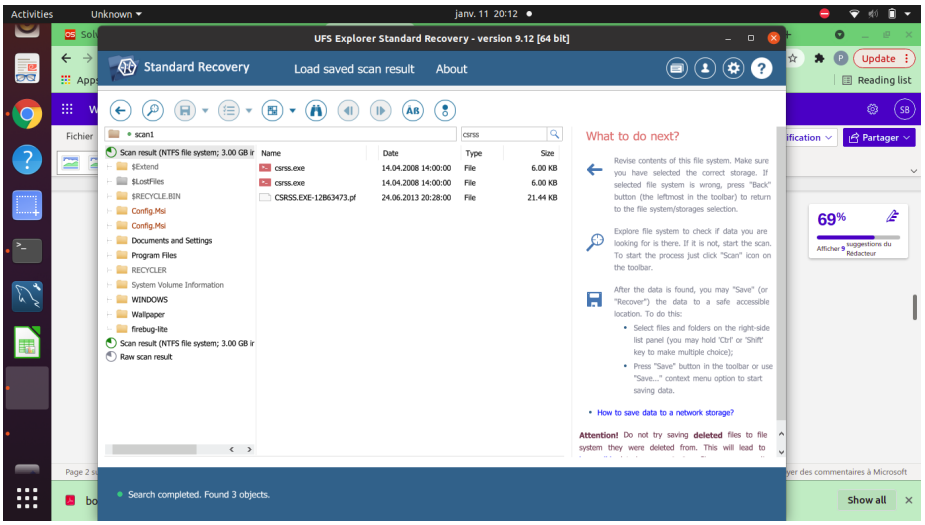

Figure 6: Utilisation d'UFS Explorer pour analyser csrss.exe

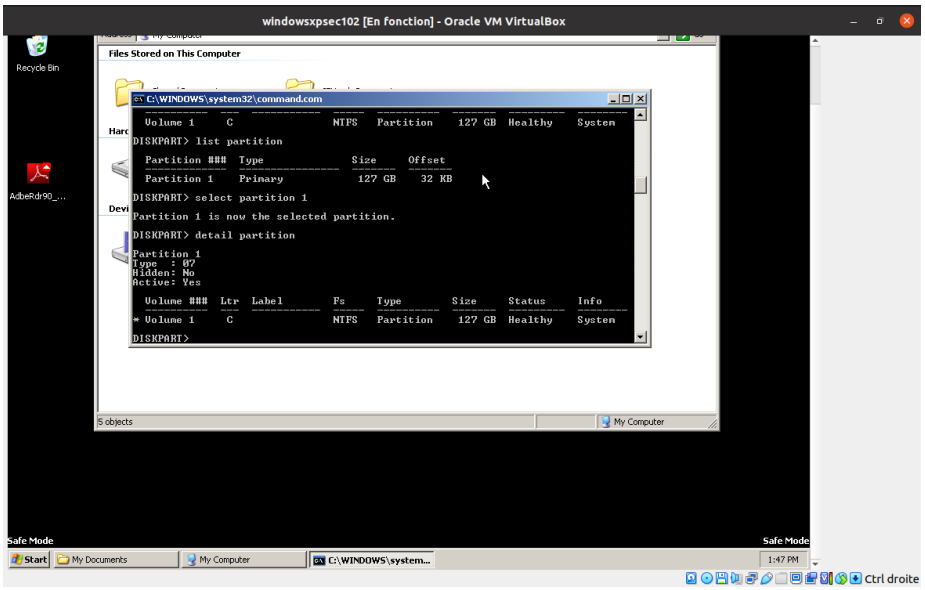

Figure 7: Recherche du numéro de volume de stockage de la provenance du malware

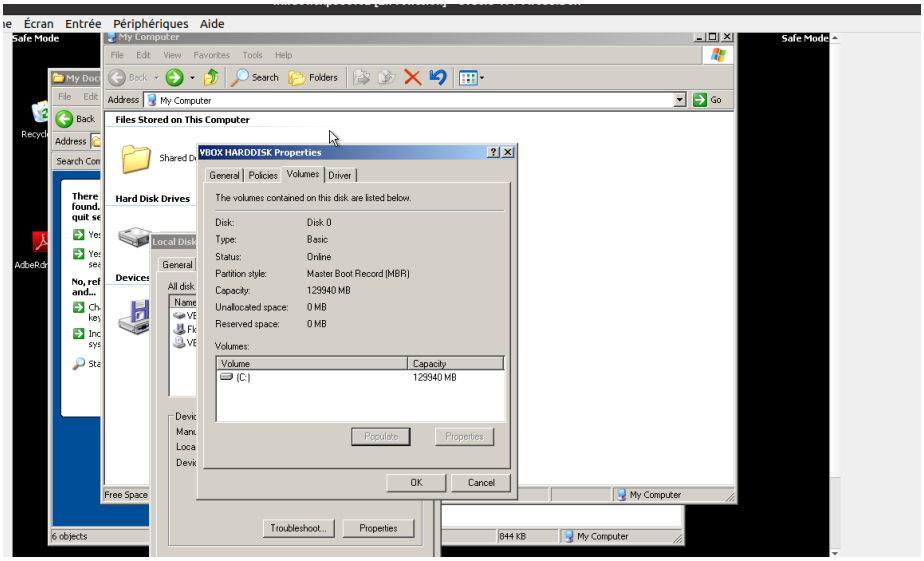

Figure 8: Informations sur le disque

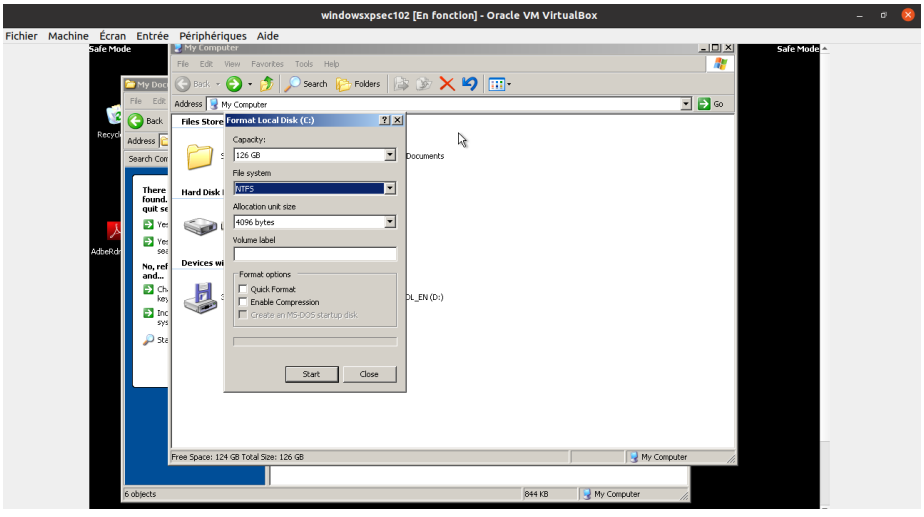

Figure 9: Type de partition

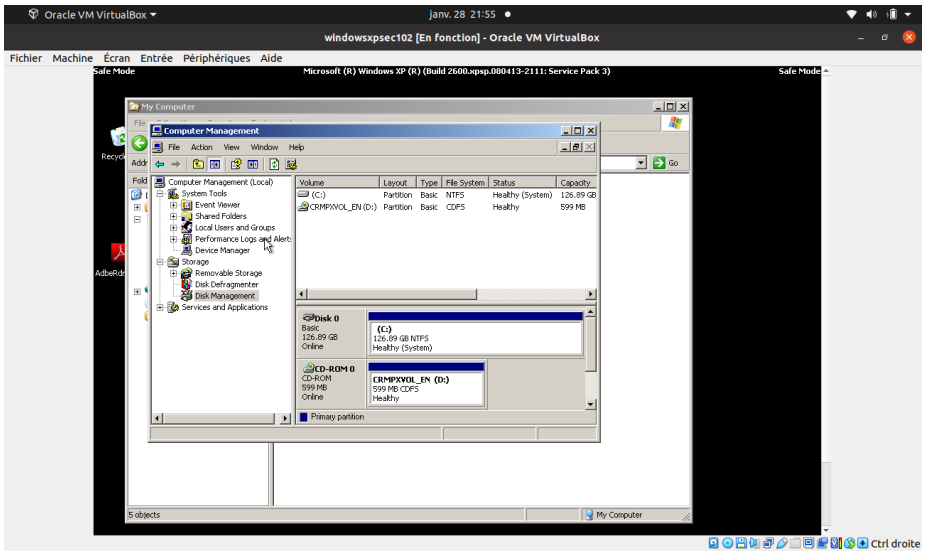

Figure 10: Supports amovble connectés

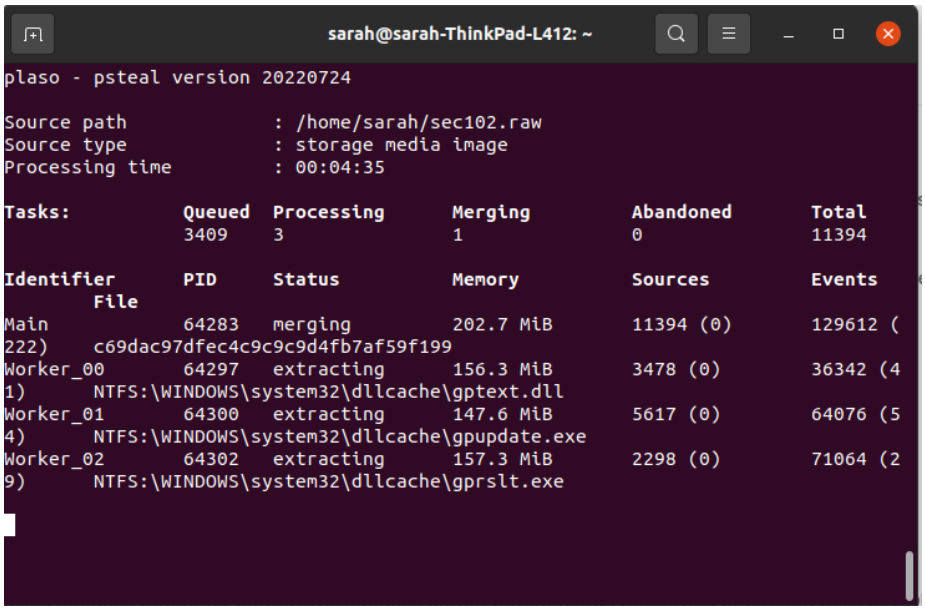

Figure 11: Installation de plaso

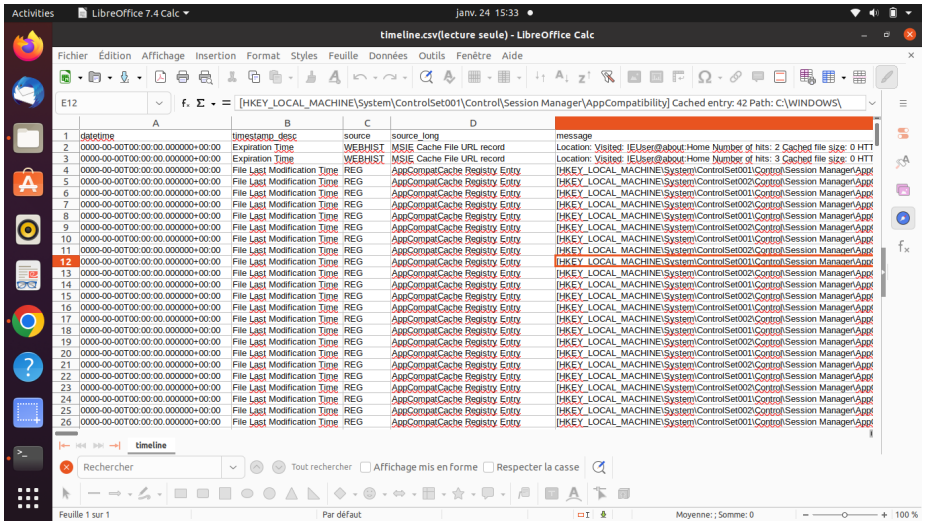

Figure 12: Création d'un fichier timeline.csv

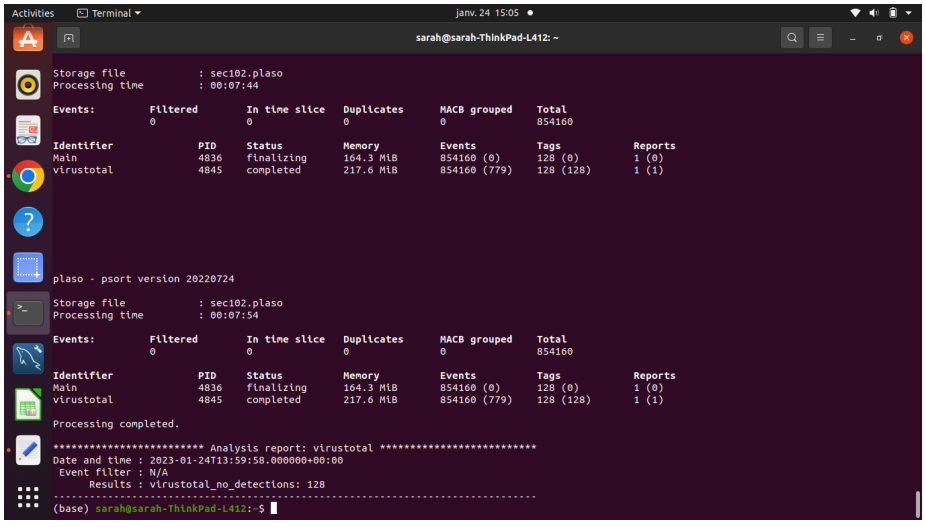

Figure 13: Détéction de virus avec virus total (ici il n'en trouve pas)

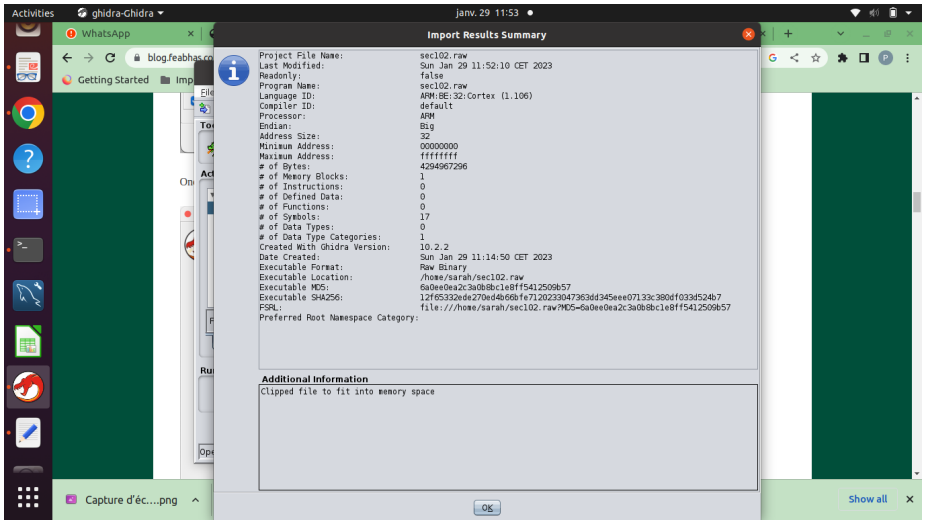

Figure 14: Installation de ghidra pour analyser le fichier vmdk convertie en raw

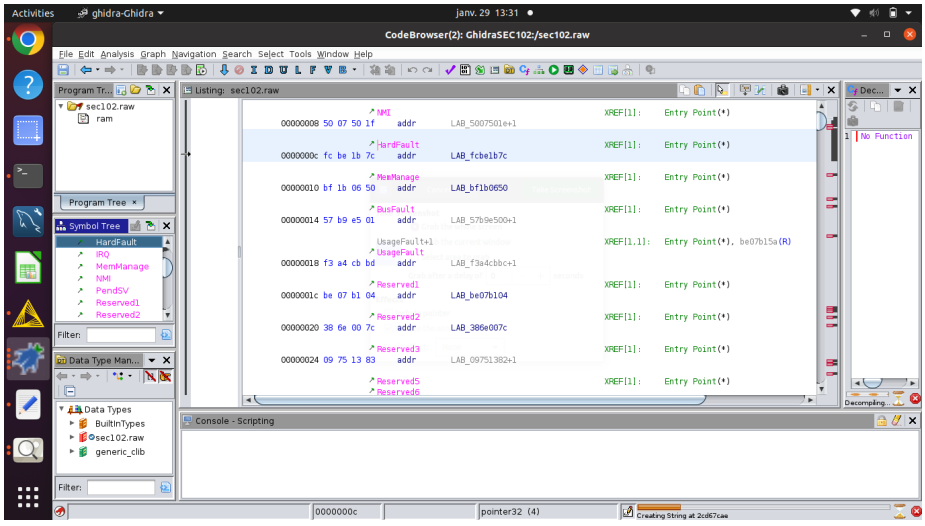

Figure 15: Analyse avec ghidra

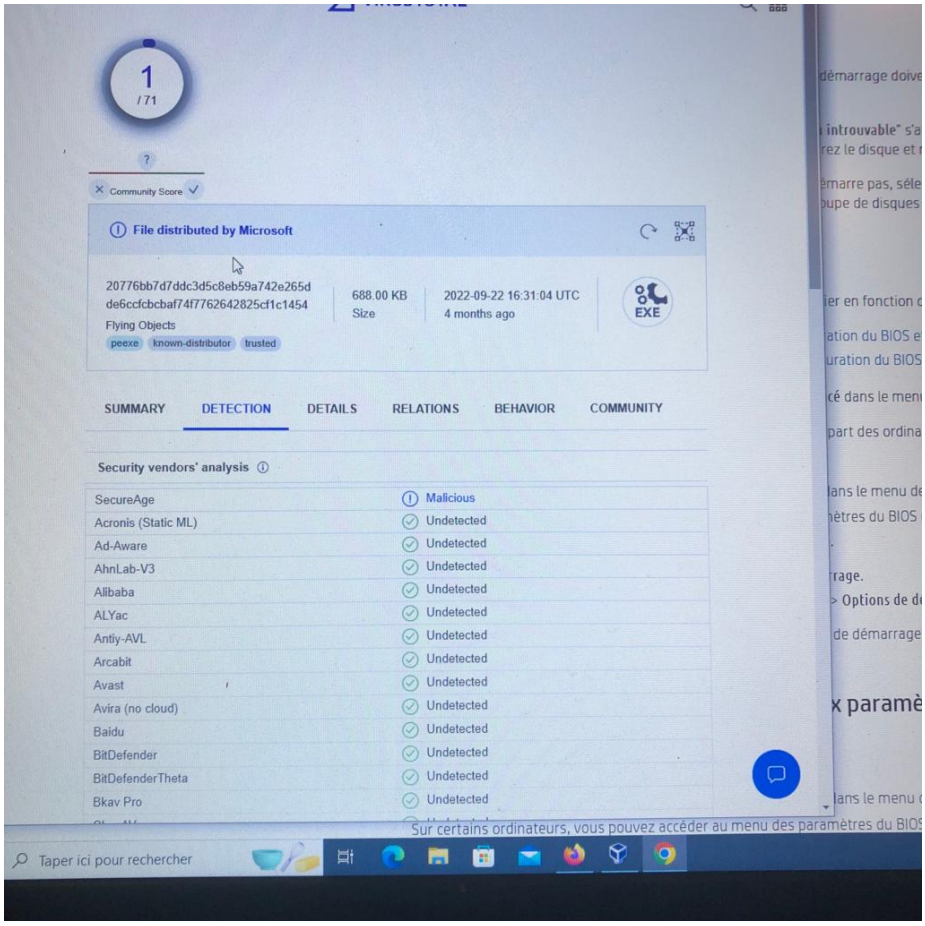

Figure 16: Analyse des fichiers de system32 avec virustotal

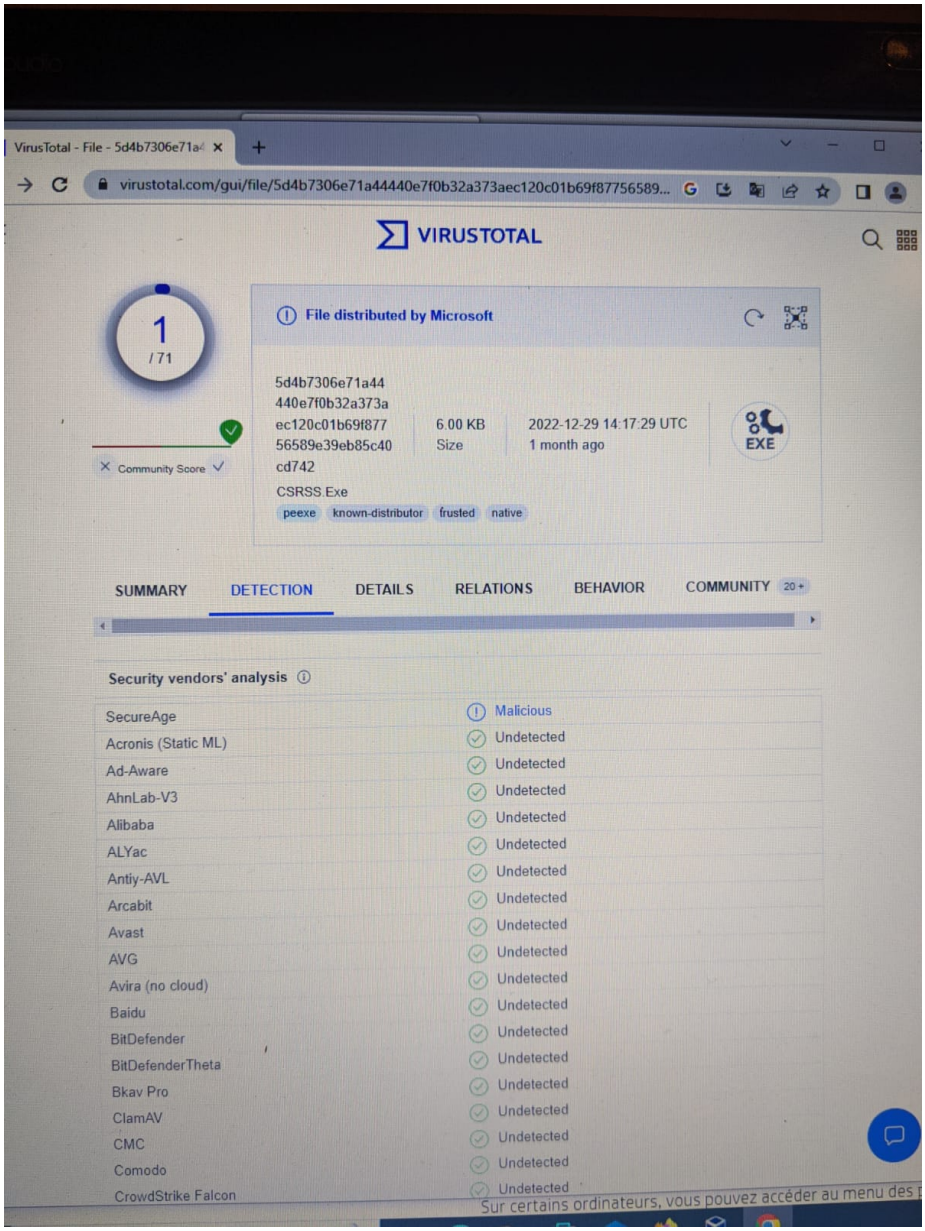

Figure 17: Analyse des fichiers de system32 avec virustotal

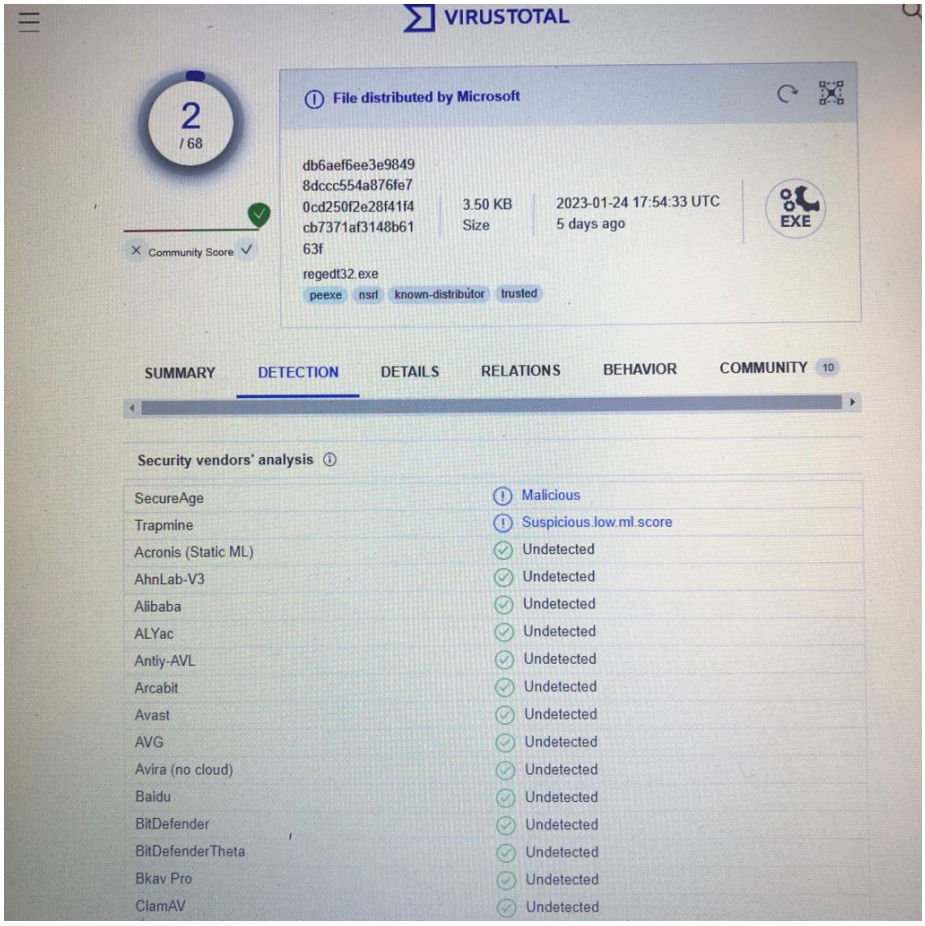

Figure 18: Analyse des fichiers de system32 avec virustotal

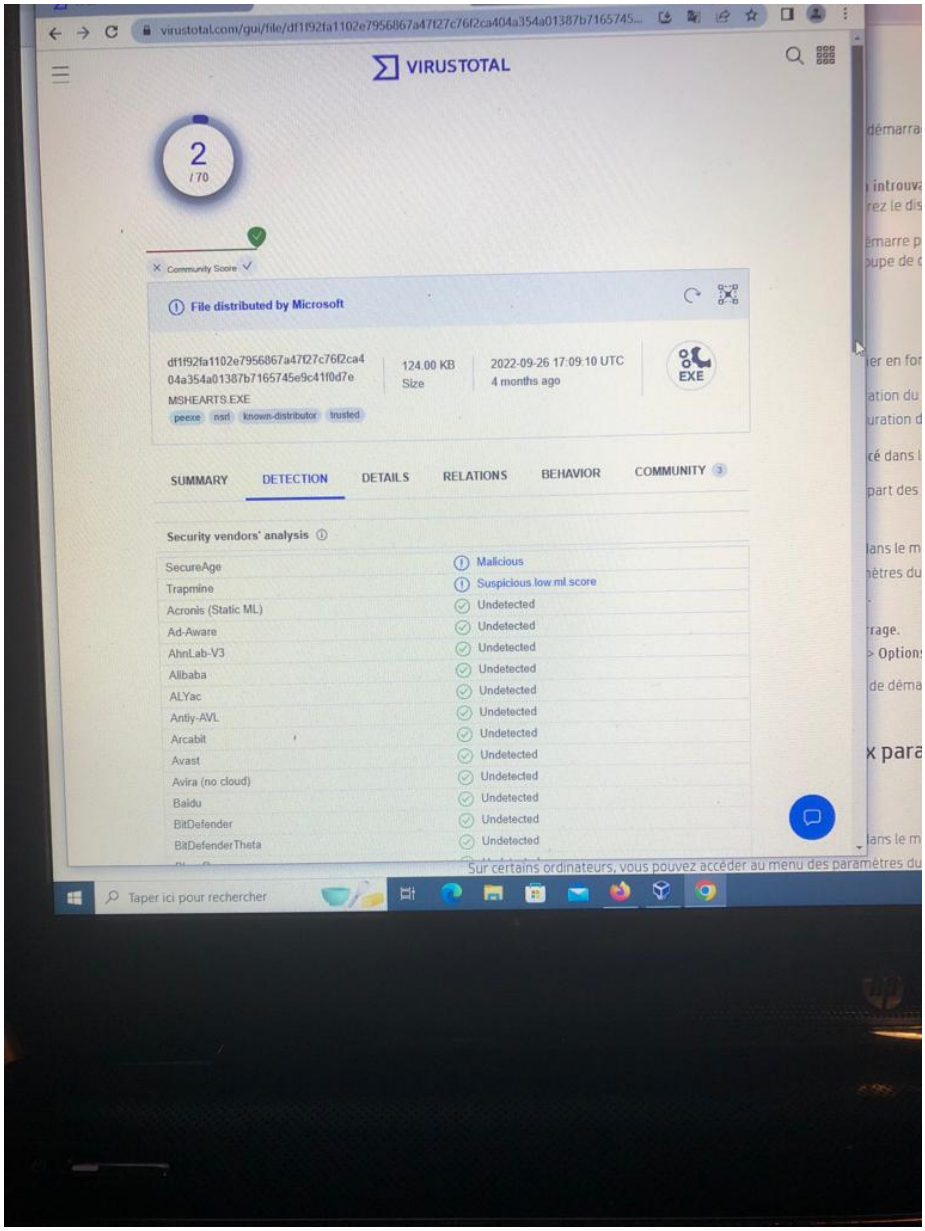

Figure 19: Analyse des fichiers de system32 avec virustotal

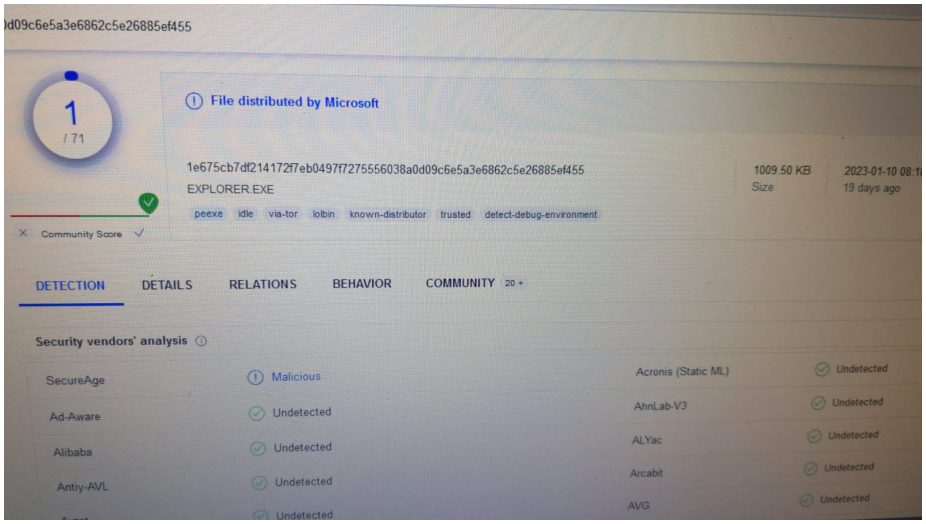

Figure 20: Analyse des fichiers de system32 avec virustotal

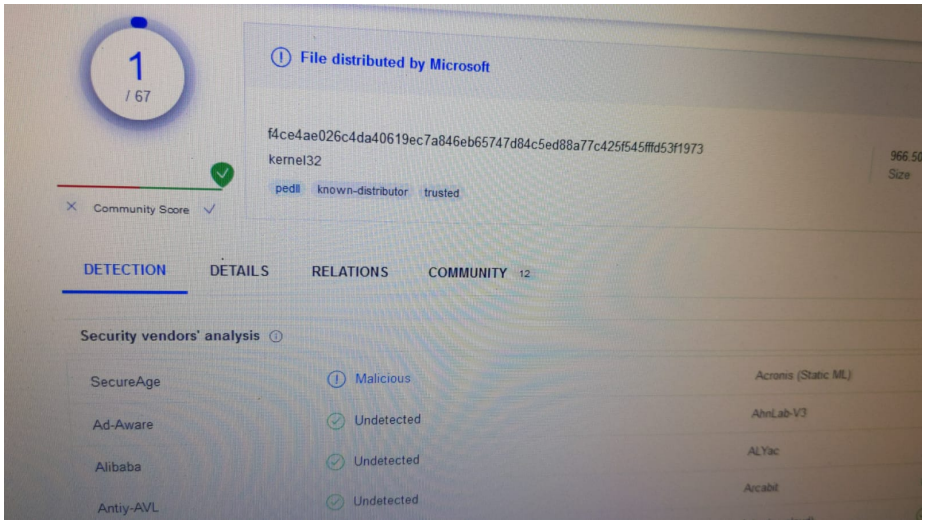

Figure 21: Analyse des fichiers de system32 avec virustotal

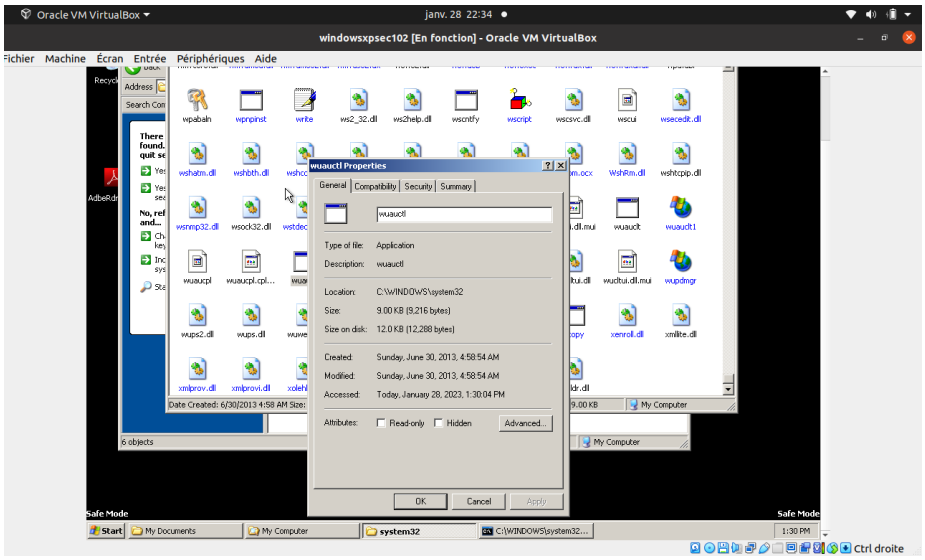

Figure 22: Chemin du malware

```
(base) sarah@sarah-ThinkPad-L412:~/Downloads$ md5sum SEC102.vmdk
69c5f02ada419c6d7927bc8b1e660f5f  SEC102.vmdk
(base) sarah@sarah-ThinkPad-L412:~/Downloads$
```

Figure 23: MD5 Hash