الجامعـــــة الدوليـــــة للربـــــاط
ⵜⴰⵙⴷⴰⵡⵉⵜ ⵜⴰⵅⴰⵡⴰⵢⵜ ⵏ ⵔⵕⴱⴰⵟ
Université Internationale de Rabat

Rapport de projet de recherche

Analyse et reverse engineering d'outils de hacking du dark web

Réalisé par : Ilias Belharda

Chihab Medagheri Alaoui

Salma Faris

Aya Fdail

Supervisé par : Othmane Cherqi

Academic Year : 2024 /2025

Table des matières

1. Introduction

a) Contexte du projet

C'est quoi le Dark Web ?

Le dark web, une partie d'internet intentionnellement cachée aux navigateurs et moteurs de recherche standard, sert de terrain de jeu dissimulé pour un éventail d'activités, dont beaucoup sont de nature illégale. Dans ses recoins cryptés, il abrite des places de marché pour des biens illicites, notamment des drogues, des armes à feu et, de manière notable pour notre discussion, des outils et services liés à la cybercriminalité. Accéder au dark web nécessite des logiciels spécifiques comme Tor, qui permettent aux utilisateurs et aux opérateurs de sites web de rester anonymes et en grande partie intraçables.

L'un des principaux impacts du dark web sur la cybersécurité est la facilitation d'un marché noir numérique pour les outils et services de cybercriminalité. Les cybercriminels peuvent y acheter et vendre des malwares, des outils de piratage, des données volées, et même engager les services d'autres criminels pour des tâches spécifiques. Ces environnements transactionnels anonymes contribuent de manière significative à l'escalade et à la généralisation des menaces cybernétiques

Définition de la problématique

Le dark web facilite un marché noir numérique où des outils de cybercriminalité, tels que malwares et données volées, sont échangés. Cette recherche vise à analyser ces forums pour mieux comprendre les outils disponibles et leurs impacts sur la cybersécurité.

Objectifs du projet

L'objectif principal est de télécharger et analyser des forums d'exploit trouvés sur le Web Selfless, d'utiliser des techniques de reverse engineering pour comprendre leur fonctionnement, et d'utiliser des environnements sandbox pour analyser leur comportement en toute sécurité.

Questions de recherche

- Quels types d'outils et de services sont partagés sur ces forums ?
- Quels comportements malveillants peut-on identifier via le sandboxing ?
- Quelles contre-mesures peuvent être développées à partir de ces analyses ?

b) Méthodologie adoptée

Ce projet repose sur trois étapes principales :

Navigation et identification des forums d'exploit.

Analyse des outils via le reverse engineering.

Utilisation de « sandboxing » pour étudier leur comportement en environnement contrôlé.

---

2. Exploration du Web Selfless et des Forums d'Exploit

a) Définition et caractéristiques du Web Selfless

Le Web Selfless représente des réseaux non conventionnels d'échange d'informations sur Internet, accessibles principalement via des outils spécialisés comme Tor. Contrairement au Web classique, il favorise l'anonymat et l'absence de censure, le rendant attrayant pour les activités illicites.

b) Navigation et identification des forums d'exploit

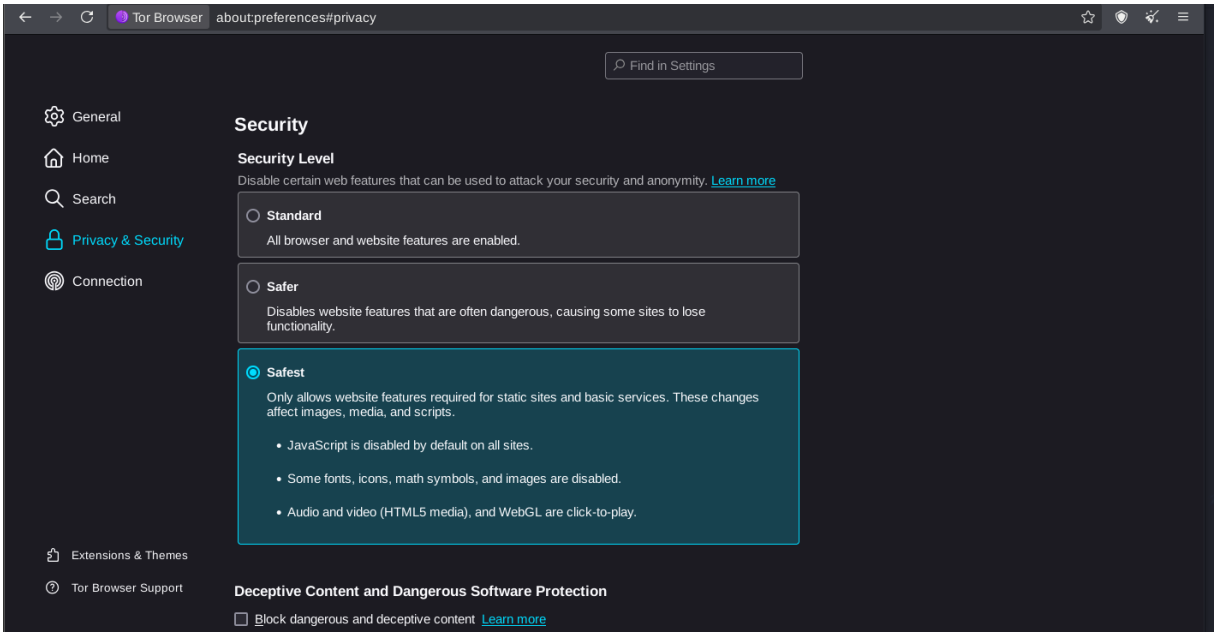
La navigation dans ces réseaux exige une configuration sécurisée pour éviter toute compromission. Les forums ciblés ont été identifiés selon leur activité et la qualité des outils proposés.

c) Sélection des trois forums d'exploit

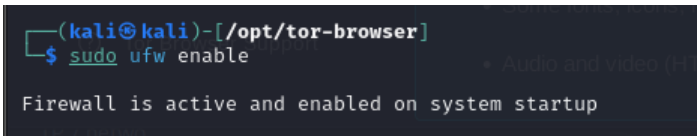
Les forums choisis sont basés sur leur réputation dans la communauté et leur activité récente. Un processus de vérification rigoureux a permis d'éviter les forums inactifs ou frauduleux.

d) Préparation d'un environnement sécurisé :

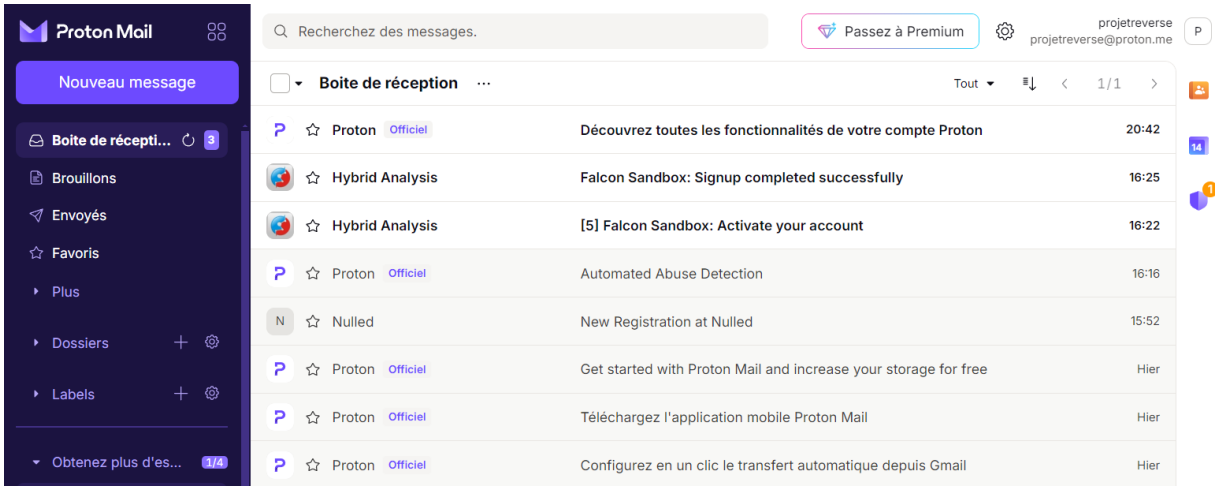
Après avoir téléchargé Tor Browser, nous avons désactivé toutes les extensions afin qu'il n'exécute ni PHP, ni JavaScript, ni aucune autre fonctionnalité en mettant le niveau de sécurité dans « Safest » :



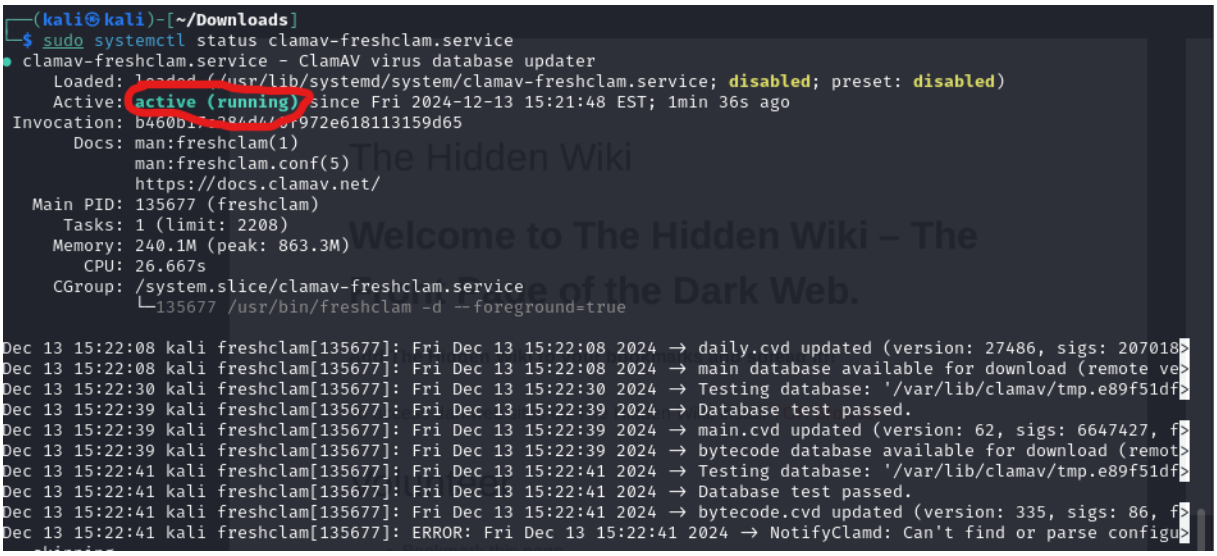
Et pour être plus prudent on a téléchargé et activé un firewall :



Et aussi créer un mail temporaire :



Utilisation de **ClamAV** comme antivirus :

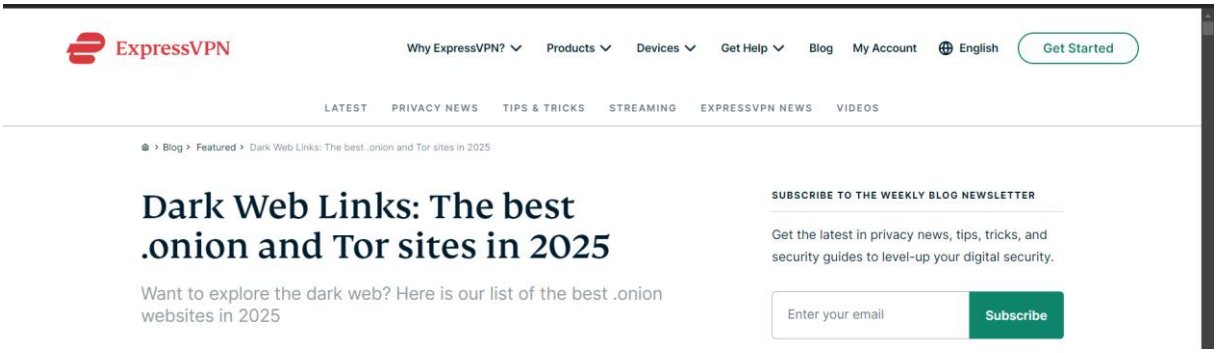


---

3. Téléchargement et Préparation des Forums

a) Procédure de la recherche

Ce site nous a donné plusieurs onion liens pour accéder à des **Dark web search engines** comme AHMIA, Haystak, Torch ...**:**

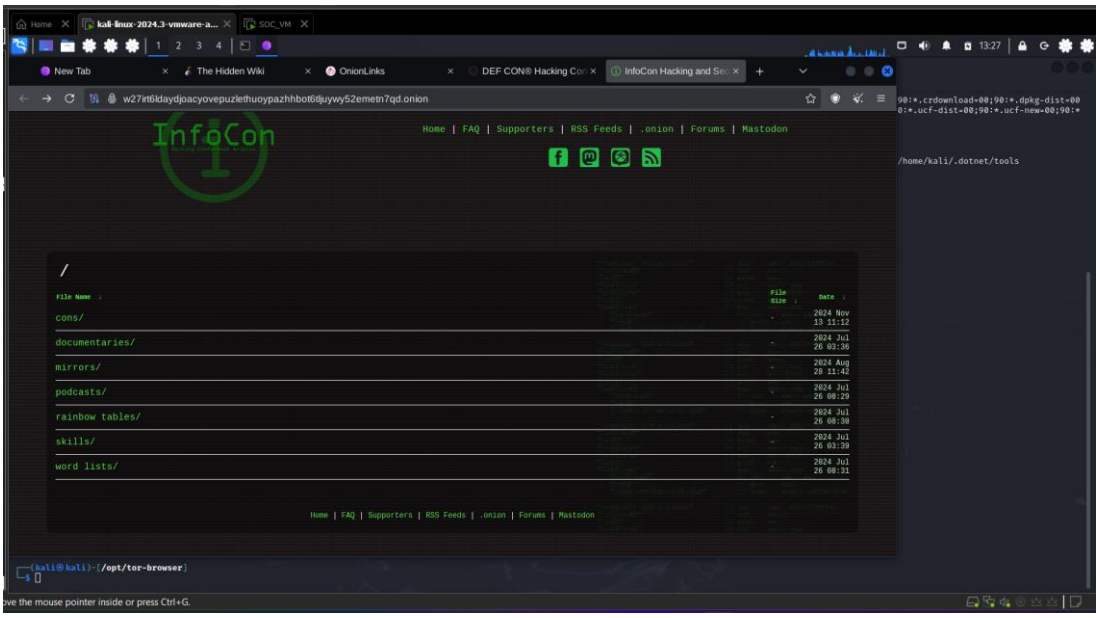


On a aussi choisi **The Hidden Wiki** pour naviguer sur le dark web dans le cadre de mon projet, car c'est un point de départ organisé et populaire. Ce répertoire fournit des liens vers des sites .onion classés par catégories (marchés, forums, services, etc.), ce qui permet d'accéder rapidement à des ressources pertinentes tout en ayant une vue d'ensemble du contenu disponible sur le dark web.

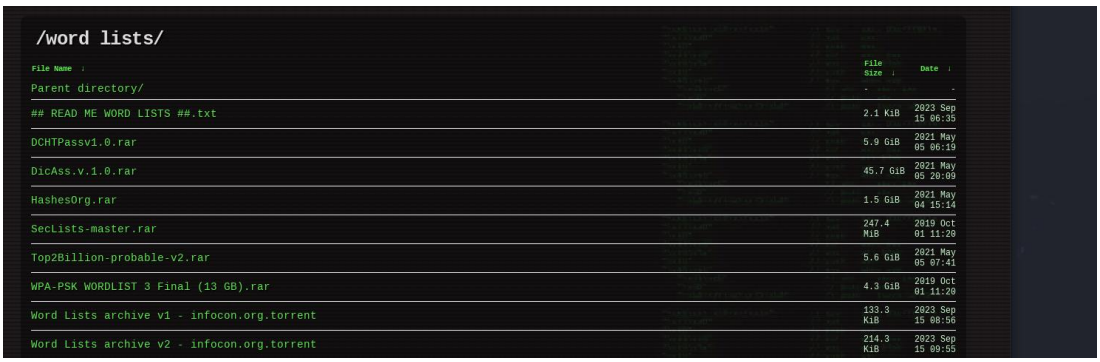
b) Procédure de téléchargement

Après avoir navigué sur plusieurs liens .onion, nous avons pu identifier des sites permettant de télécharger des forums. Ces forums constituent une source précieuse pour notre projet, car ils peuvent être analysés afin de comprendre les outils, les méthodes, et les interactions au sein des communautés du dark web.

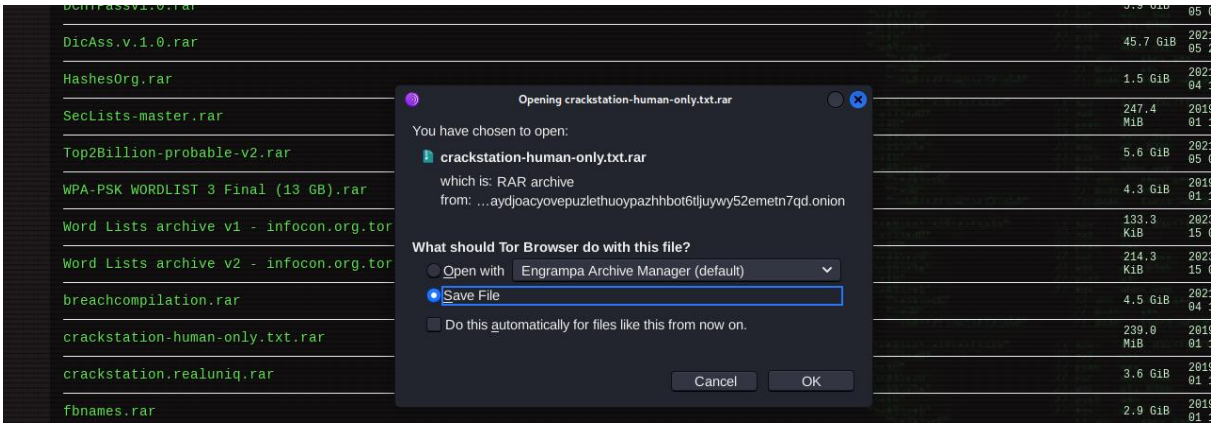
Alors, on a entré dans cette page InfoCon



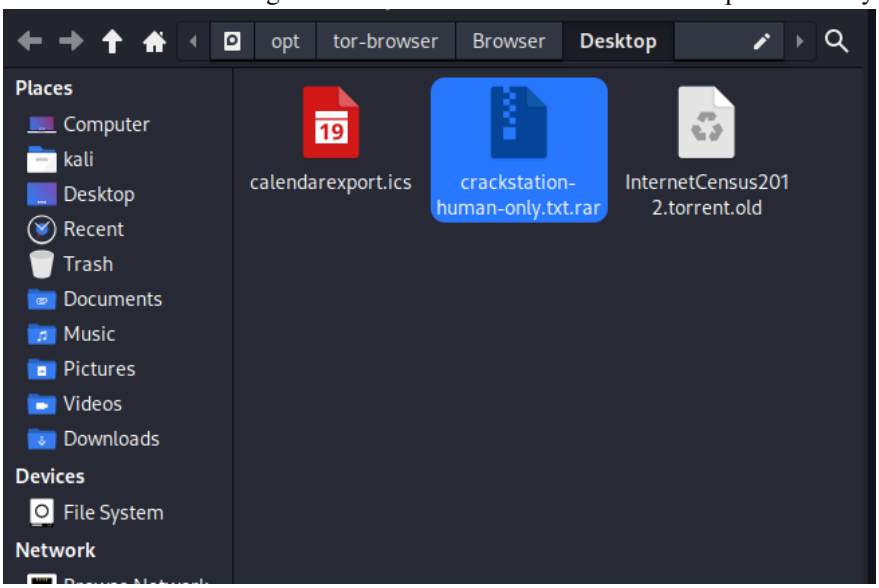
Sélectionner un fichier pour le téléchargé



Et juste débuter le téléchargement



On a finalement téléchargé 3 différents forums de 2 différents liens pour les analysés



---

4. Magic Bytes

a) Définition de "Magic Bytes"

Les **magic bytes** (ou magic numbers) sont des séquences spécifiques de bytes présentes au début des fichiers, servant à identifier leur type ou leur format. Ces signatures permettent aux systèmes ou aux applications de reconnaître un fichier indépendamment de son extension. Par exemple :

- Les fichiers PNG commencent par 89 50 4E 47 (en hexadécimal).
- Les fichiers PDF commencent par %PDF.

Lien avec le reverse engineering

Dans le contexte du **reverse engineering**, les magic bytes sont essentiels pour analyser et comprendre le comportement des fichiers suspects ou malveillants. En identifiant rapidement le type de fichier à partir de ces signatures, les experts peuvent :

1. **Déterminer la cible** : Identifier si un fichier exécutable ou script est déguisé avec une fausse extension.
2. **Analyser des binaires** : Savoir si le fichier contient un format compressé ou crypté.
3. **Faciliter l'extraction d'informations** : Orienter l'utilisation d'outils spécifiques (par ex., analyseurs hexadécimaux, décompresseurs).

Ces signatures jouent ainsi un rôle clé dans l'investigation de logiciels malveillants ou la rétroconception d'applications et d'outils présents sur des forums suspects.

b) Identification utilisant la commande 'file'

```
┌──(kali㉿kali)-[/opt/tor-browser/Browser/Desktop]
└─$ file calendarexport.ics
calendarexport.ics: iCalendar calendar file

┌──(kali㉿kali)-[/opt/tor-browser/Browser/Desktop]
└─$ file crackstation-human-only.txt.rar
crackstation-human-only.txt.rar: RAR archive data, v5

┌──(kali㉿kali)-[/opt/tor-browser/Browser/Desktop]
└─$ file InternetCensus2012.torrent.old
InternetCensus2012.torrent.old: BitTorrent file
```

En utilisant la commande 'file', on a identifié que ce sont des fichiers :

- « iCalendar» : Généralement utilisé pour stocker des événements de calendrier.
- « RAR v5 » : Pouvant contenir des données compressées.
- « BitTorrent » : probablement lié au projet Internet Census 2012.

NB : Le projet Internet Census 2012 a cartographié l'utilisation des adresses IP et identifié les appareils non sécurisés connectés à Internet.

c) Identification utilisant la commande 'strings'

```
┌──(kali㉿kali)-[/opt/tor-browser/Browser/Desktop]
└─$ strings calendarexport.ics
BEGIN:VCALENDAR
PRODID:-//vBulletin 6//EN
VERSION:2.0
CALSCALE:GREGORIAN
BEGIN:VEVENT
UID:5b69b20e-8b26-425c-bd52-9cf12f7726d0
DTSTAMP:20250113T185136Z
SUMMARY:Airplane Hacking Contest Registration Closes July 15 2019
DESCRIPTION:https://aviationvillage.org/hack-an-airplane-contest/\nAirplane
  Hacking Contest Registration Closes July 15 2019
URL:https://ezdhgsy2aw7zg54z6dqsutrduhl22moami5zv2zt6urr6vub7gs6wfad.onion/node/228588
DTSTART;VALUE=DATE:20190715
END:VEVENT
END:VCALENDAR
```

Elle révèle des informations sur un événement de calendrier intitulé "Airplane Hacking Contest Registration Closes July 15 2019". Le fichier comprend des détails tels que l'UID, le horodatage (20250113T185136Z), une description contenant un lien vers un site web, ainsi que la date de début de l'événement (20190715) et encore plus en bas, il y avait beaucoup de data.

```
┌──(kali㉿kali)-[/opt/tor-browser/Browser/Desktop]
└─$ strings InternetCensus2012.torrent.old
d8:announce44:udp://tracker.openbittorrent.com:80/announce13:announce-listll44:udp://tracker.openbittorrent.com:80/a
nnounceel36:https://tracker.infocon.org/announceel35:https://tracker.defcon.org/announceee7:comment20:Internet Censu
s 201210:created by25:Transmission/2.52 (13304)13:creation datei1363476636e8:encoding5:UTF-84:infod5:filesld6:length
i4960421e4:pathl11:code.tar.gzeed6:lengthi190008690e4:pathl4:data10:hostprobes6:1.zpaqeed6:lengthi131048681e4:pathl4
:data10:hostprobes8:100.zpaqeed6:lengthi134504803e4:pathl4:data10:hostprobes8:101.zpaqeed6:lengthi34737890e4:pathl4:
data10:hostprobes8:102.zpaqeed6:lengthi35047847e4:pathl4:data10:hostprobes8:103.zpaqeed6:lengthi34342846e4:pathl4:da
ta10:hostprobes8:104.zpaqeed6:lengthi131935530e4:pathl4:data10:hostprobes8:105.zpaqeed6:lengthi133176992e4:pathl4:da
ta10:hostprobes8:106.zpaqeed6:lengthi133232457e4:pathl4:data10:hostprobes8:107.zpaqeed6:lengthi135545765e4:pathl4:da
ta10:hostprobes8:108.zpaqeed6:lengthi136099826e4:pathl4:data10:hostprobes8:109.zpaqeed6:lengthi184657553e4:pathl4:da
ta10:hostprobes7:11.zpaqeed6:lengthi136802823e4:pathl4:data10:hostprobes8:110.zpaqeed6:lengthi135020113e4:pathl4:dat
a10:hostprobes8:111.zpaqeed6:lengthi137789650e4:pathl4:data10:hostprobes8:112.zpaqeed6:lengthi138063957e4:pathl4:dat
a10:hostprobes8:113.zpaqeed6:lengthi137538558e4:pathl4:data10:hostprobes8:114.zpaqeed6:lengthi136334846e4:pathl4:dat
a10:hostprobes8:115.zpaqeed6:lengthi132964552e4:pathl4:data10:hostprobes8:116.zpaqeed6:lengthi134232536e4:pathl4:dat
a10:hostprobes8:117.zpaqeed6:lengthi135419739e4:pathl4:data10:hostprobes8:118.zpaqeed6:lengthi1367300074e4:pathl4:dat
a10:hostprobes8:119.zpaqeed6:lengthi185249957e4:pathl4:data10:hostprobes7:12.zpaqeed6:lengthi131065330e4:pathl4:data
10:hostprobes8:120.zpaqeed6:lengthi135380511e4:pathl4:data10:hostprobes8:121.zpaqeed6:lengthi134552884e4:pathl4:data
10:hostprobes8:122.zpaqeed6:lengthi136187544e4:pathl4:data10:hostprobes8:123.zpaqeed6:lengthi134331372e4:pathl4:data
10:hostprobes8:124.zpaqeed6:lengthi135672053e4:pathl4:data10:hostprobes8:125.zpaqeed6:lengthi131014617e4:pathl4:data
10:hostprobes8:126.zpaqeed6:lengthi129263766e4:pathl4:data10:hostprobes8:128.zpaqeed6:lengthi128874118e4:pathl4:data
10:hostprobes8:129.zpaqeed6:lengthi184741615e4:pathl4:data10:hostprobes7:13.zpaqeed6:lengthi126221076e4:pathl4:data1
0:hostprobes8:130.zpaqeed6:lengthi125462607e4:pathl4:data10:hostprobes8:131.zpaqeed6:lengthi124767102e4:pathl4:data1
0:hostprobes8:132.zpaqeed6:lengthi125181154e4:pathl4:data10:hostprobes8:133.zpaqeed6:lengthi125767649e4:pathl4:data1
0:hostprobes8:134.zpaqeed6:lengthi124675839e4:pathl4:data10:hostprobes8:135.zpaqeed6:lengthi125535700e4:pathl4:data1
0:hostprobes8:136.zpaqeed6:lengthi126411637e4:pathl4:data10:hostprobes8:137.zpaqeed6:lengthi125565167e4:pathl4:data1
0:hostprobes8:138.zpaqeed6:lengthi126549271e4:pathl4:data10:hostprobes8:139.zpaqeed6:lengthi189444254e4:pathl4:data1
0:hostprobes7:14.zpaqeed6:lengthi127220128e4:pathl4:data10:hostprobes8:140.zpaqeed6:lengthi127746945e4:pathl4:data10
:hostprobes8:141.zpaqeed6:lengthi127034415e4:pathl4:data10:hostprobes8:142.zpaqeed6:lengthi126920488e4:pathl4:data10
:hostprobes8:143.zpaqeed6:lengthi126447349e4:pathl4:data10:hostprobes8:144.zpaqeed6:lengthi126766133e4:pathl4:data10
:hostprobes8:145.zpaqeed6:lengthi126942964e4:pathl4:data10:hostprobes8:146.zpaqeed6:lengthi127338609e4:pathl4:data10
:hostprobes8:147.zpaqeed6:lengthi126409306e4:pathl4:data10:hostprobes8:148.zpaqeed6:lengthi126909020e4:pathl4:data10
:hostprobes8:149.zpaqeed6:lengthi183699166e4:pathl4:data10:hostprobes7:15.zpaqeed6:lengthi126724546e4:pathl4:data10:
hostprobes8:150.zpaqeed6:lengthi128673440e4:pathl4:data10:hostprobes8:151.zpaqeed6:lengthi126329573e4:pathl4:data10:
hostprobes8:152.zpaqeed6:lengthi126130919e4:pathl4:data10:hostprobes8:153.zpaqeed6:lengthi125967799e4:pathl4:data10:
hostprobes8:154.zpaqeed6:lengthi126437311e4:pathl4:data10:hostprobes8:155.zpaqeed6:lengthi126305527e4:pathl4:data10:
hostprobes8:156.zpaqeed6:lengthi126630502e4:pathl4:data10:hostprobes8:157.zpaqeed6:lengthi126112362e4:pathl4:data10:
hostprobes8:158.zpaqeed6:lengthi126647961e4:pathl4:data10:hostprobes8:159.zpaqeed6:lengthi183170830e4:pathl4:data10:
hostprobes7:16.zpaqeed6:lengthi126128571e4:pathl4:data10:hostprobes8:160.zpaqeed6:lengthi129395880e4:pathl4:data10:h
ostprobes8:161.zpaqeed6:lengthi129255018e4:pathl4:data10:hostprobes8:162.zpaqeed6:lengthi129992774e4:pathl4:data10:h
ostprobes8:163.zpaqeed6:lengthi129483373e4:pathl4:data10:hostprobes8:164.zpaqeed6:lengthi129653355e4:pathl4:data10:h
ostprobes8:165.zpaqeed6:lengthi129354055e4:pathl4:data10:hostprobes8:166.zpaqeed6:lengthi129377446e4:pathl4:data10:h
ostprobes8:167.zpaqeed6:lengthi129424397e4:pathl4:data10:hostprobes8:168.zpaqeed6:lengthi128866595e4:pathl4:data10:h
ostprobes8:169.zpaqeed6:lengthi184029239e4:pathl4:data10:hostprobes7:17.zpaqeed6:lengthi129466103e4:pathl4:data10:ho
stprobes8:170.zpaqeed6:lengthi130255505e4:pathl4:data10:hostprobes8:171.zpaqeed6:lengthi115435967e4:pathl4:data10:ho
stprobes8:172.zpaqeed6:lengthi133097993e4:pathl4:data10:hostprobes8:173.zpaqeed6:lengthi130046520e4:pathl4:data10:ho
stprobes8:174.zpaqeed6:lengthi129392277e4:pathl4:data10:hostprobes8:175.zpaqeed6:lengthi127063056e4:pathl4:data10:ho
```

Les informations affichées incluent des détails sur les trackers utilisés (comme tracker.openbittorrent.com et tracker.defcon.org), la méthode d'encodage (UTF-8), et des données associées aux "hostprobes" avec leurs longueurs et chemins respectifs.

d) Identification utilisant 'binwalk'

```
┌──(kali㉿kali)-[/opt/tor-browser/Browser/Desktop]
└─$ binwalk InternetCensus2012.torrent.old

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             BitTorrent file
```

Le résultat indique que ce fichier est un **fichier BitTorrent**, détecté dès le premier octet (offset 0). Cela confirme qu'il s'agit d'un fichier utilisé pour le partage de données via le protocole BitTorrent. Aucun autre contenu caché ou signature supplémentaire n'a été identifié.

```
└─$ binwalk crackstation-human-only.txt.rar

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0×0             RAR archive data, version 5.x
11910142      0×B5BBFE        JBOOT STAG header, image id: 3, timestamp 0×393BE93E, image size: 909458185 bytes, ima
ge JBOOT checksum: 0×33D0, header JBOOT checksum: 0×1523
13271426      0×CA8182        JBOOT STAG header, image id: 10, timestamp 0×58018671, image size: 288505043 bytes, im
age JBOOT checksum: 0×4E8F, header JBOOT checksum: 0×2646
24406177      0×17468A1       gzip compressed data, ASCII, has header CRC, has 9479 bytes of extra data, last modifi
ed: 2026-08-05 03:34:44
24987075      0×17D45C3       JBOOT STAG header, image id: 11, timestamp 0×595DE4B5, image size: 461246613 bytes, im
age JBOOT checksum: 0×BD04, header JBOOT checksum: 0×4B2D
35847020      0×222FB6C       JBOOT STAG header, image id: 13, timestamp 0×1E2D4E90, image size: 260222217 bytes, im
age JBOOT checksum: 0×D4EC, header JBOOT checksum: 0×D9B2
38361519      0×24959AF       JBOOT STAG header, image id: 7, timestamp 0×9B1FBA21, image size: 2101632229 bytes, im
age JBOOT checksum: 0×C781, header JBOOT checksum: 0×6709
50331783      0×3000087       JBOOT STAG header, image id: 6, timestamp 0×59A81969, image size: 4047538541 bytes, im
age JBOOT checksum: 0×D8C8, header JBOOT checksum: 0×AA85
55491483      0×34EBB9B       MySQL ISAM compressed data file Version 1
56248335      0×35A480F       JBOOT STAG header, image id: 7, timestamp 0×A98D33FC, image size: 2730425504 bytes, im
age JBOOT checksum: 0×50C5, header JBOOT checksum: 0×7FFE
68481227      0×414F0CB       JBOOT STAG header, image id: 2, timestamp 0×933240A1, image size: 890357633 bytes, ima
ge JBOOT checksum: 0×165C, header JBOOT checksum: 0×B1A4
^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B84234418      0×50550B2       JBOOT STAG header, image id: 0, timestamp 0×4508DB
6F, image size: 3422667315 bytes, image JBOOT checksum: 0×335, header JBOOT checksum: 0×A546
^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B102794458     0×62084DA       Uncompressed Adobe Flash SWF file, Version 16, Fil
e size (header included) 120547532
127488319     0×799513F       JBOOT STAG header, image id: 4, timestamp 0×B613465F, image size: 3066294182 bytes, im
age JBOOT checksum: 0×C8E0, header JBOOT checksum: 0×961C
134369551     0×802510F       JBOOT STAG header, image id: 2, timestamp 0×773089B, image size: 621634090 bytes, imag
e JBOOT checksum: 0×A463, header JBOOT checksum: 0×103B
136259968     0×81F2980       JBOOT STAG header, image id: 16, timestamp 0×E0509E51, image size: 384435437 bytes, im
age JBOOT checksum: 0×D102, header JBOOT checksum: 0×BC92
138318647     0×83E9337       AU audio data, 3271916408 sample rate, 2857059756 channels
140569603     0×860EC03       JBOOT STAG header, image id: 14, timestamp 0×7A9D5241, image size: 1659335101 bytes, i
mage JBOOT checksum: 0×D1D4, header JBOOT checksum: 0×7AB9
143571019     0×88EB84B       Broadcom header, number of sections: 1530503227,
181063297     0×ACACE81       JBOOT STAG header, image id: 6, timestamp 0×8D66016E, image size: 193438162 bytes, ima
ge JBOOT checksum: 0×4135, header JBOOT checksum: 0×AF47
182532153     0×AE13839       JBOOT STAG header, image id: 10, timestamp 0×BC467400, image size: 1342605755 bytes, i
mage JBOOT checksum: 0×CBCE, header JBOOT checksum: 0×CB53
185672266     0×B11224A       MP3 ID3 tag,
196279631     0×BB2FD4F       JBOOT STAG header, image id: 15, timestamp 0×EF377AEB, image size: 873343858 bytes, im
age JBOOT checksum: 0×6873, header JBOOT checksum: 0×123B
209405875     0×C7B47B3       JBOOT STAG header, image id: 9, timestamp 0×84D3B1E, image size: 3099206858 bytes, ima
ge JBOOT checksum: 0×C672, header JBOOT checksum: 0×6447
213566215     0×CBAC307       Cisco IOS experimental microcode, for ""
217813040     0×CFB9030       JBOOT STAG header, image id: 14, timestamp 0×3080ABE3, image size: 2129657226 bytes, i
mage JBOOT checksum: 0×5621, header JBOOT checksum: 0×75E2
237248411     0×E241F9B       JBOOT STAG header, image id: 13, timestamp 0×83848B44, image size: 1435737729 bytes, i
mage JBOOT checksum: 0×19B3, header JBOOT checksum: 0×DB54
```

Le fichier est identifié comme une **archive RAR version 5.x**, et l'analyse révèle plusieurs signatures de données internes, notamment :

- **Données compressées en gzip**, ce qui suggère la présence de fichiers compressés supplémentaires.
- **Plusieurs en-têtes JBOOT STAG**, souvent associés à des micrologiciels embarqués.
- **Un fichier Adobe Flash SWF non compressé**, ce qui peut indiquer du contenu multimédia ou interactif.
- **Un fichier audio avec des métadonnées ID3 MP3**, laissant supposer la présence d'un fichier audio.
- **Un microcode d'IOS Cisco**, ce qui peut signifier que des éléments liés à des équipements réseau sont inclus.

Ces résultats suggèrent que cette archive contient une grande diversité de types de fichiers, possiblement liés à du reverse engineering ou à l'analyse de micrologiciels.

```
└─$ binwalk calendarexport.ics

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
```

Le résultat n'affiche aucune donnée détectable ou exploitable. Cela indique qu'aucune structure particulière ou signature connue n'a été trouvée dans le fichier analysé.

---

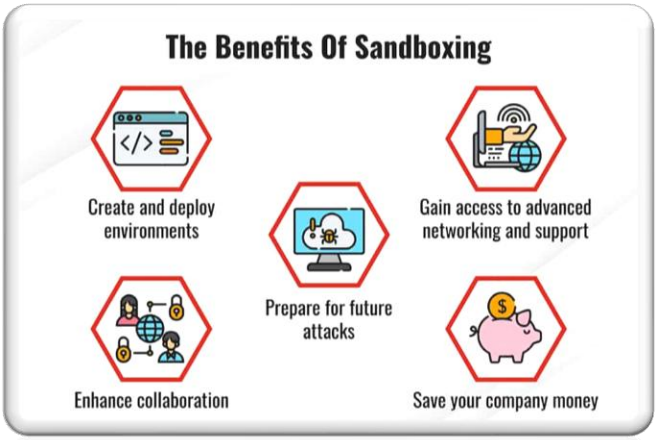
5. Reverse Engineering et sandboxing des Forums d'Exploit

a) Introduction au reverse engineering et sandboxing

Le reverse engineering est un processus capable de remonter à l'origine d'un programme ou d'un logiciel. En matière de cybersécurité, il s'agit d'analyser une attaque en étudiant les différentes étapes de sa réalisation. Le reverse engineering est un outil très utile pour la sécurité informatique, mais il interroge quant à sa légalité. C'est pourquoi il doit être utilisé dans un contexte strict, dans un but unique, celui de mieux comprendre les cyberattaques pour mieux s'en défendre.

Le sandboxing est une pratique de sécurité dans laquelle vous utilisez un environnement isolé, ou une « sandbox », pour les tests. Dans le sandbox que vous exécutez, analysez le code dans un environnement sûr et isolé sans affecter l'application, le système ou la plateforme.

Le Sandboxing est très efficace lors de la mise en place d'une défense contre les menaces zero-day, qui sont des menaces qui n'ont pas été observées auparavant ou qui correspondent à tout malware connu dans le fichier. Même si les filtres d'e-mail réguliers peuvent analyser les e-mails pour détecter les expéditeurs malveillants, les types de fichiers et les URL, les menaces zero-day apparaissent tout le temps et peuvent être manquées par la filtration traditionnelle. Le Sandboxing offre un plus grand niveau de protection, en particulier lorsqu'un e-mail malveillant passe par les filtres mis en place par votre fournisseur.



Lorsque le sandboxing est utilisé pour les tests, il crée un endroit sûr pour installer et exécuter un programme, en particulier un programme suspect, sans exposer le reste de votre système. Si l'application contient un code malveillant, elle peut s'exécuter dans le sandbox sans affecter les autres composants de votre réseau.

b) Outils utilisés

Les outils utilisés incluent :

- **HybridAnalysis** : Plateforme en ligne qui analyse les fichiers et URL suspects en exécutant leurs comportements dans un environnement sécurisé (sandbox) pour détecter les activités malveillantes.
- **Virustotal** : Service en ligne qui scanne les fichiers et URLs à l'aide de dizaines d'antivirus et outils de détection pour identifier les menaces potentielles.

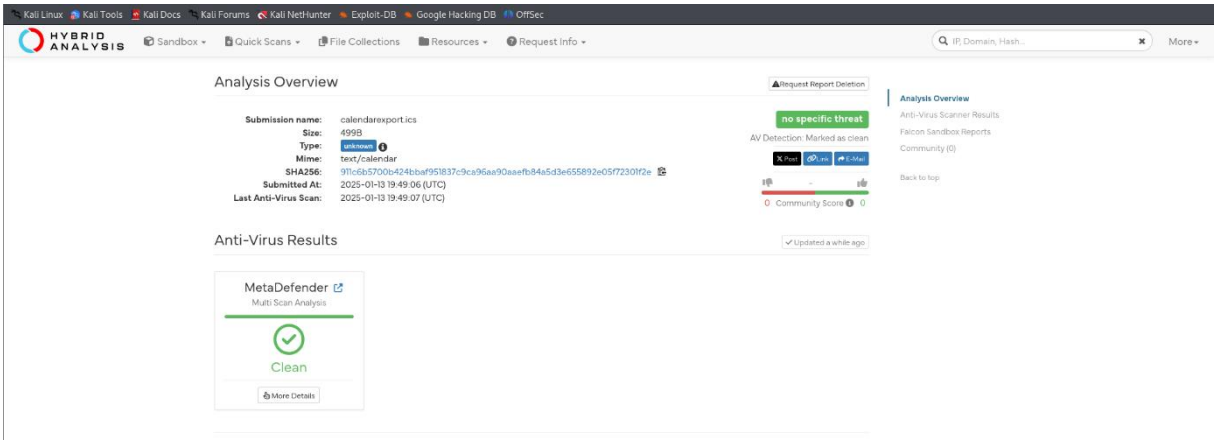
c) Analyse des forums

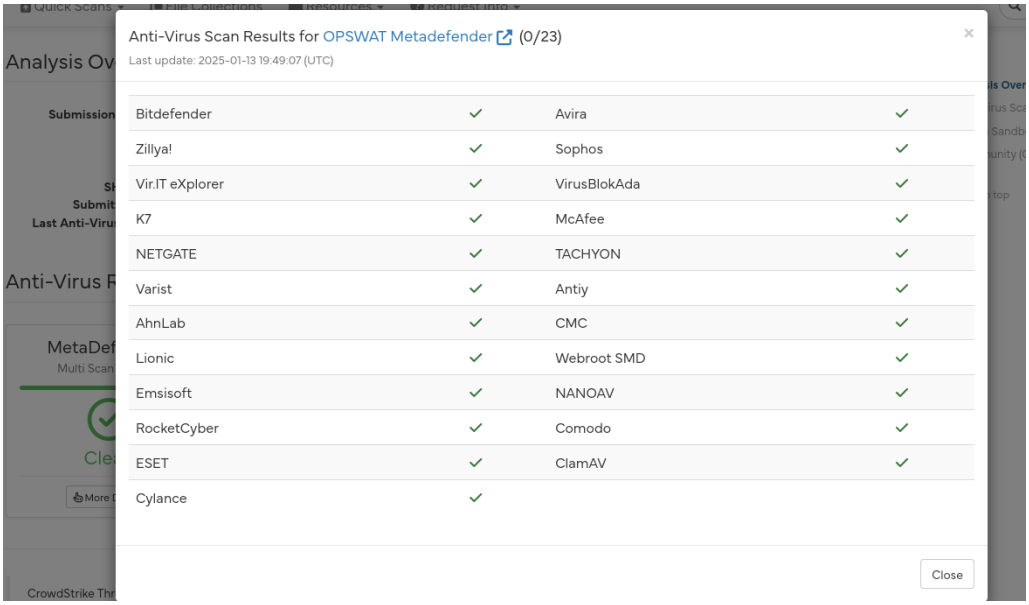
Au premiers temps, on a fait haché les forums

```
┌──(kali㉿kali)-[/opt/tor-browser/Browser/Desktop]
└─$ md5sum calendarexport.ics
741a91e68d7d48402c4696930c28572b  calendarexport.ics

┌──(kali㉿kali)-[/opt/tor-browser/Browser/Desktop]
└─$ md5sum crackstation-human-only.txt.rar
67297f0628dedc54cc885656ff06bcbd  crackstation-human-only.txt.rar

┌──(kali㉿kali)-[/opt/tor-browser/Browser/Desktop]
└─$ ls
calendarexport.ics  crackstation-human-only.txt.rar  InternetCensus2012.torrent.old

┌──(kali㉿kali)-[/opt/tor-browser/Browser/Desktop]
└─$ md5sum InternetCensus2012.torrent.old
0908a243e97f5bdd43c590048bdde819  InternetCensus2012.torrent.old
```

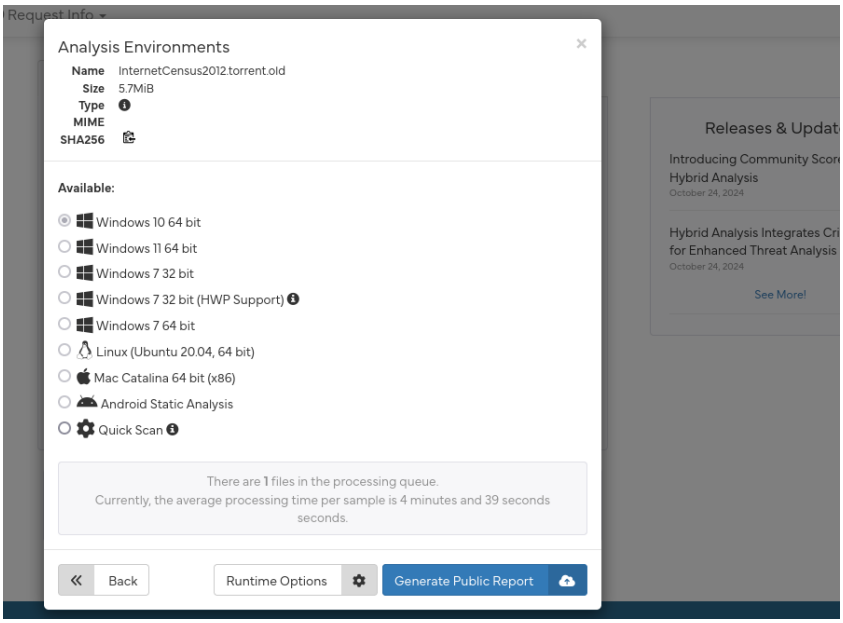
Chaque fichier a été examiné pour découvrir ses fonctionnalités cachées en Utilisant :

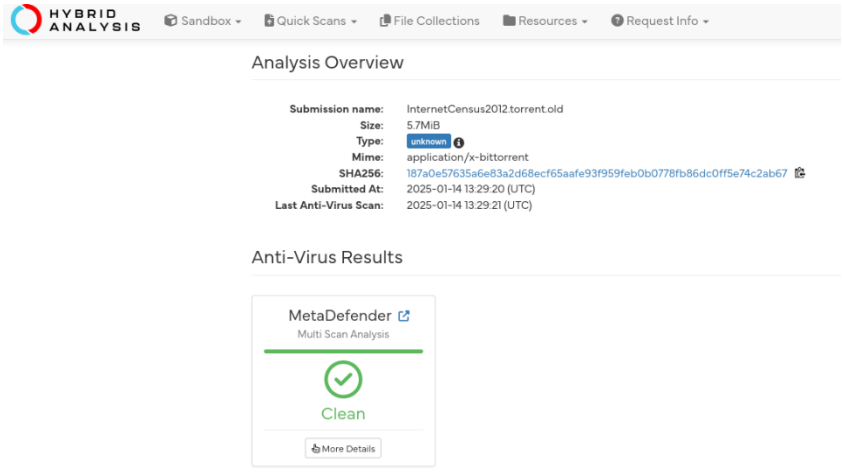
Hybrid Analysis :

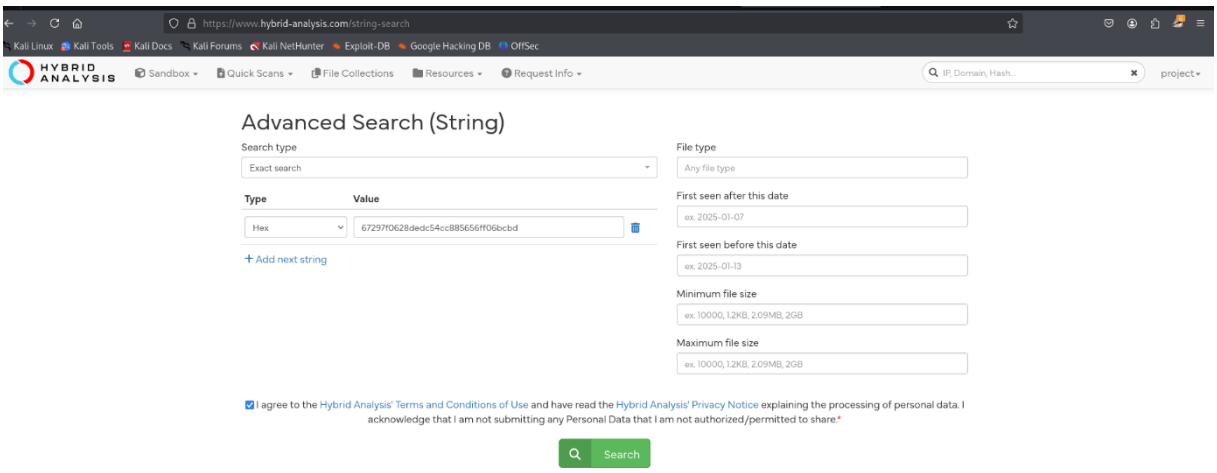


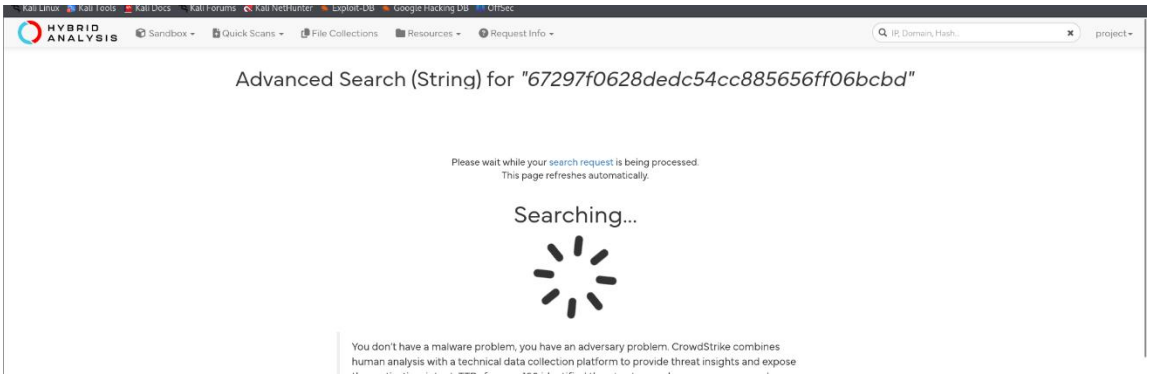


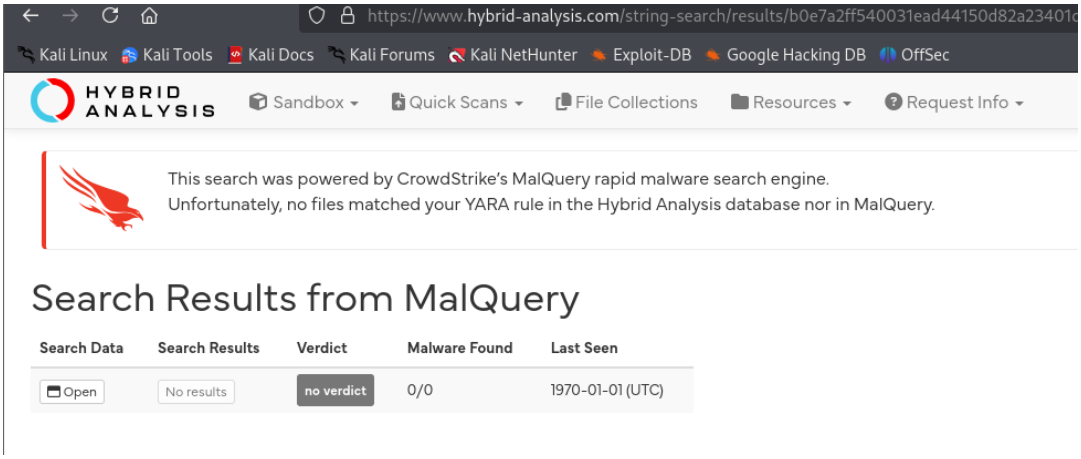
On a même essayé plusieurs environnement


Request Info
Analysis Environments
Name InternetCensus2012.torrent.old
Size 5.7MiB
Type
MIME
SHA256
Available:
Windows 10 64 bit
Windows 11 64 bit
Windows 7 32 bit
Windows 7 32 bit (HWP Support)
Windows 7 64 bit
Linux (Ubuntu 20.04, 64 bit)
Mac Catalina 64 bit (x86)
Android Static Analysis
Quick Scan
There are 1 files in the processing queue.
Currently, the average processing time per sample is 4 minutes and 39 seconds seconds.
Back
Runtime Options
Generate Public Report
Releases & Updat
Introducing Community Scor
Hybrid Analysis
October 24, 2024
Hybrid Analysis Integrates Cri
for Enhanced Threat Analysis
October 24, 2024
See More!

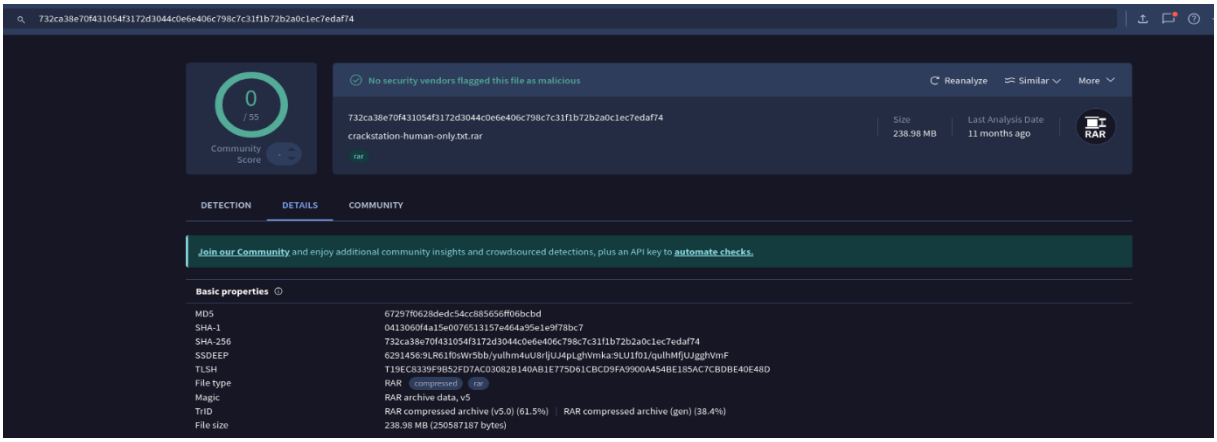

HYBRID ANALYSIS
Sandbox
Quick Scans
File Collections
Resources
Request Info
Analysis Overview
Submission name: InternetCensus2012.torrent.old
Size: 5.7MiB
Type: unknown
Mime: application/x-bittorrent
SHA256: 187a0e57635a6e83a2d68ecf65aafe93f959feb0b0778fb86dc0ff5e74c2ab67
Submitted At: 2025-01-14 13:29:20 (UTC)
Last Anti-Virus Scan: 2025-01-14 13:29:21 (UTC)
Anti-Virus Results
MetaDefender
Multi Scan Analysis
Clean
More Details

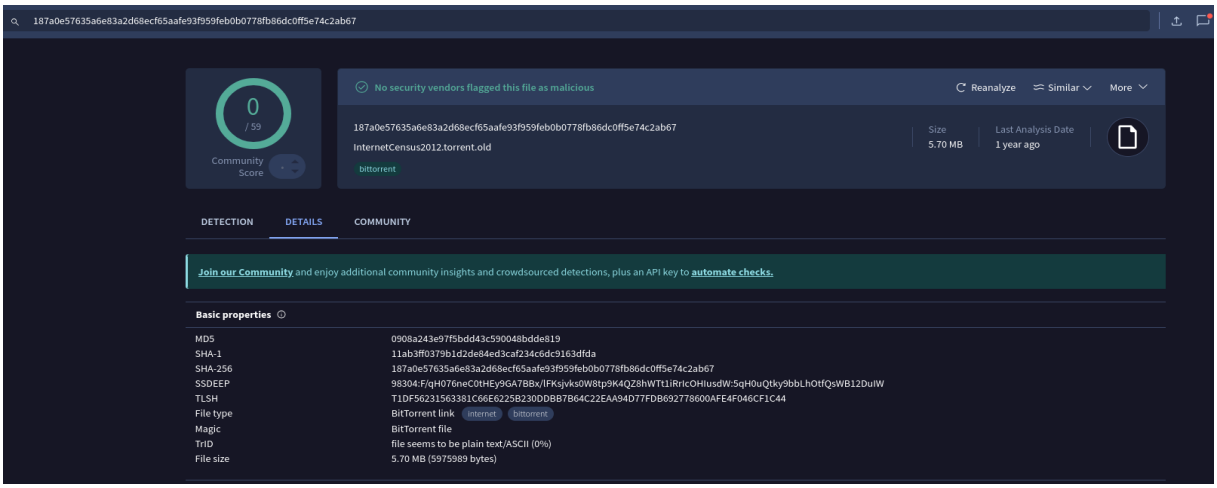

https://www.hybrid-analysis.com/string-search
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
HYBRID ANALYSIS
Sandbox
Quick Scans
File Collections
Resources
Request Info
project
Advanced Search (String)
Search type
Exact search
Type
Value
Hex
67297f0628dedc54cc885656ff06bcbd
+ Add next string
File type
Any file type
First seen after this date
ex. 2025-01-07
First seen before this date
ex. 2025-01-13
Minimum file size
ex. 10000, 1.2KB, 2.09MB, 2GB
Maximum file size
ex. 10000, 1.2KB, 2.09MB, 2GB
I agree to the Hybrid Analysis' Terms and Conditions of Use and have read the Hybrid Analysis' Privacy Notice explaining the processing of personal data. I acknowledge that I am not submitting any Personal Data that I am not authorized/permitted to share.*
Search

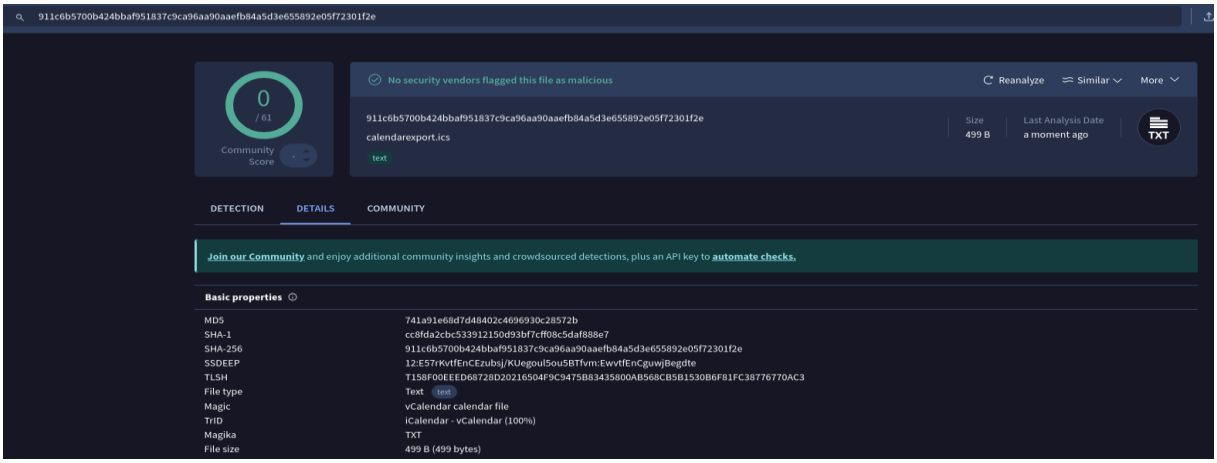

HYBRID ANALYSIS
Sandbox
Quick Scans
File Collections
Resources
Request Info
project
Advanced Search (String) for "67297f0628dedc54cc885656ff06bcbd"
Please wait while your search request is being processed.
This page refreshes automatically.
Searching...
You don't have a malware problem, you have an adversary problem. CrowdStrike combines human analysis with a technical data collection platform to provide threat insights and expose


https://www.hybrid-analysis.com/string-search/results/b0e7a2ff540031ead44150d82a23401c
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
HYBRID ANALYSIS
Sandbox
Quick Scans
File Collections
Resources
Request Info
This search was powered by CrowdStrike's MalQuery rapid malware search engine.
Unfortunately, no files matched your YARA rule in the Hybrid Analysis database nor in MalQuery.
Search Results from MalQuery
Search Data
Search Results
Verdict
Malware Found
Last Seen
Open
No results
no verdict
0/0
1970-01-01 (UTC)

VirusTotal :


732ca38e70f431054f3172d3044c0e6e406c798c7c31f1b72b2a0c1ec7edaf74
0
/ 55
Community Score
No security vendors flagged this file as malicious
Reanalyze
Similar
More
732ca38e70f431054f3172d3044c0e6e406c798c7c31f1b72b2a0c1ec7edaf74
crackstation-human-only.txt.rar
rar
Size
238.98 MB
Last Analysis Date
11 months ago
RAR
DETECTION
DETAILS
COMMUNITY
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Basic properties
MD5
67297f0628dedc54cc885656ff06bcbd
SHA-1
0413060f4a15e0076513157e464a95e1e9f78bc7
SHA-256
732ca38e70f431054f3172d3044c0e6e406c798c7c31f1b72b2a0c1ec7edaf74
SSDEEP
6291456:9LR61f0sWr5bb/yulhm4uU8rljUJ4pLghVmka:9LU1f01/qulhMfjUJgghVmF
TLSH
T19EC8339F9B52FD7AC03082B140AB1E775D61CBCD9FA9900A454BE185AC7CBDBE40E48D
File type
RAR
compressed
rar
Magic
RAR archive data, v5
TrID
RAR compressed archive (v5.0) (61.5%)
RAR compressed archive (gen) (38.4%)
File size
238.98 MB (250587187 bytes)





Finalement, après avoir exploré et analysé les données téléchargées, nous n'avons trouvé aucun contenu malveillant. Cette expérience nous a principalement permis de maîtriser les méthodes d'analyse, renforçant ainsi nos compétences en investigation et en compréhension des outils du dark web.

---

6. Implications de Sécurité et Risques

a) Risques liés aux forums

- Propagation de logiciels malveillants : Les forums malveillants sont des vecteurs de diffusion de virus, vers et chevaux de Troie, menaçant la sécurité des systèmes informatiques.
- Vol de données sensibles : Les informations personnelles ou professionnelles peuvent être compromises et échangées sur ces plateformes, entraînant des violations de la confidentialité.
- Escroqueries et fraudes : Les forums malveillants facilitent des activités illégales telles que le phishing, l'usurpation d'identité et d'autres formes de fraude en ligne.

b) Mesures de prévention

- Éducation et sensibilisation : Former les utilisateurs aux dangers des forums malveillants et aux signes d'activités suspectes est essentiel pour renforcer la vigilance.

- Politiques de sécurité strictes : Mettre en place des stratégies de gestion des risques liés aux logiciels malveillants, incluant des contrôles d'accès rigoureux et des protocoles de réponse aux incidents, est crucial pour protéger les systèmes.
- Surveillance proactive : Utiliser des outils de surveillance pour détecter et signaler les activités suspectes sur le réseau permet une réaction rapide aux menaces potentielles.

c) Rôle du reverse engineering et du sandboxing

Ces techniques permettent une compréhension approfondie des menaces, facilitant leur neutralisation.

---

7. Défis et Limites du Projet

a) Problèmes rencontrés

Difficultés à accéder à des forums fiables.

Risques techniques lors du traitement des fichiers malveillants.

b) Limites

Les analyses ont été effectuées sur un échantillon limité de forums, ce qui peut réduire la portée des conclusions.

---

8. Conclusion et Perspectives

a) Résumé des découvertes

Nous avons exploré plusieurs liens .onion, téléchargé des forums et procédé à leur analyse. Aucun contenu malveillant n'a été trouvé, mais cette expérience nous a permis de maîtriser les techniques d'analyse et d'améliorer nos compétences en investigation.

b) Perspectives d'avenir

Développement d'outils automatisés pour l'analyse de fichiers malveillants.

Collaboration accrue entre les chercheurs en cybersécurité.

c) Suggestions

Élargir les échantillons pour une meilleure compréhension des tendances sur le Dark Web.

---

9. Bibliographie

Exploit Forum, Initial Access Brokers, and Cybercrime on the Dark Web - Flare

https://www.cyber-management-school.com/ecole/les-fondamentaux-de-la-cybersecurite/quest-ce-que-le-reverse-engineering/#:~:text=Le%20reverse%20engineering%20est%20un,diff%C3%A9rentes%20%C3%A9tapes%20de%20sa%20r%C3%A9alisation.

https://www.fortinet.com/fr/resources/cyberglossary/what-is-sandboxing#:~:text=Le%20sandboxing%20est%20une%20pratique,le%20syst%C3%A8me%20ou%20la%20plateforme.

https://en.wikipedia.org/wiki/Magic_number_(programming)

https://digital.ai/catalyst-blog/exploring-reverse-engineering-benefits-misuse-and-the-role-of-application-hardening/

https://www.forcepoint.com/cyber-edu/sandbox-security

https://www.expressvpn.com/blog/best-onion-sites-on-dark-web/?srsltid=AfmBOooVzih0FDODeEsuo4hx3Cp3S-KeRd-_mZdaXkYt9coK5sCRayWI

https://www.hybrid-analysis.com/

https://www.virustotal.com/gui/home/upload