

REPUBLIQUE DU SENEGAL



Un Peuple-Un But-Une Foi

Ministère de l'Enseignement Supérieur de la Recherche et de l'innovation Direction Générale
de l'Enseignement Supérieur Privé



BEM
School of
Technology

Rapport

Investigation numérique sur clé USB suspect

Présenté par :

Moustapha SY



Sommaire

Table des figures.....	1
Résumé.....	2
Glossaire.....	3
Introduction générale.....	4
Préparation de clé.....	5
Copie l'image de la clé.....	6
Analyse de l'image.....	7
Identifications des fichiers vulnérables.....	8
Détermination du vecteur d'infection	9

Table des figures

Figure 1 : Consultation de clé

Figure 2 : Formatage de la clé

Figure 3 : Premier etape avec ftk

Figure 4 : Deuxieme etape avec FTK

Figure 5 : Troisieme etape avec FTK

Figure 6 : Quatrieme etape FTK

Figure 7 : Cinquieme etape FTK

Figure 9 : Lancement de Autopsy

Figure 10 : Selection des filtres et recuperation des hash

Figure 11 : Affichage du resultat

Figure 12 : Identification du fichier malveillante

Figure 13 : Verification du fichier malveillant

Résumé

Une copie forensique complète de la clé usb a été créée à l'aide de FTK Imager afin de préserver l'intégrité des données et d'éviter toute modification du support original. Ensuite l'image est importée et analysée dans Autopsy.

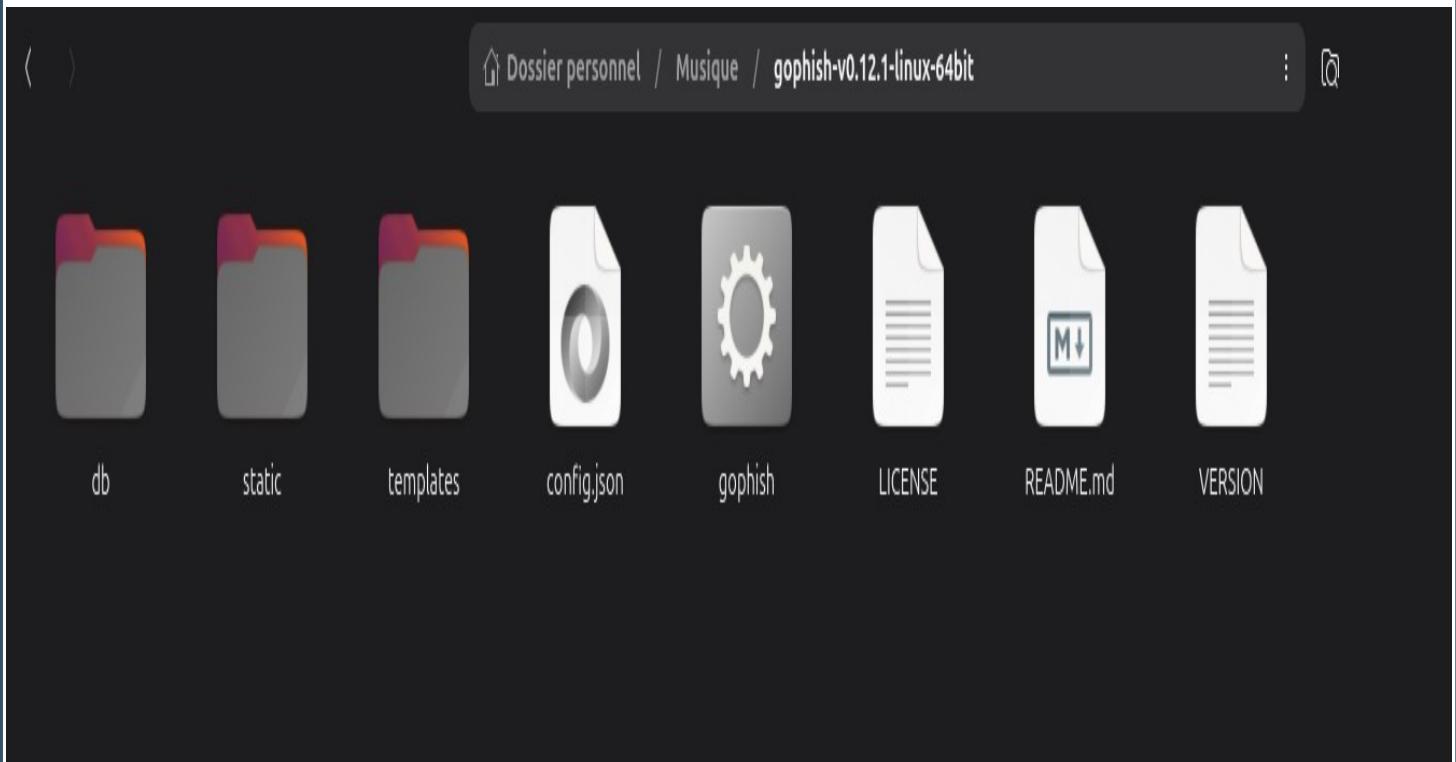
L'examen détaillé a permis d'identifier un élément suspect, notamment un fichier .exe exécutable non légitime. Maintenant pour vérifier que si c'est un fichier malveillant , nous avons utilisé un service en ligne ‘MetaDefender cloud’ , et ensuite de cela , effectivement le fichier est reconnu comme malveillant.

Glossaires

Introduction

Dans le cadre de la sécurité du système d'information, une clé usb suspecte a été introduite dans un poste de travail . L'objectif de cette investigation est de déterminer si la clé contient des éléments malveillant , de l'identifier et de déterminer le vecteur d'infection. Et nous allons utilisé un les outils FTK imager et Autopsy pour procéder à cela.

Préparation de clé



Ici on a mis un fichier malveillant Facture.exe avec d'autres fichiers

```
moustapha@moustapha: ~/Musique/gophish-v0.12.1-linux-64bit
moustapha@moustapha: ~/Musique/gophish-v0.12.1-linux-64bit
moustapha@moustapha:~/Musique/gophish-v0.12.1-linux-64bit$ sudo chmod +x gophish
[sudo] Mot de passe de moustapha :
moustapha@moustapha:~/Musique/gophish-v0.12.1-linux-64bit$ ls
config.json db gophish gophish_admin.crt gophish_admin.key gophish.db LICENSE README.md static templates VERSION
moustapha@moustapha:~/Musique/gophish-v0.12.1-linux-64bit$ 
```

Ici , on vient de formater la clé

```
moustapha@moustapha: ~/Musique/gophish-v0.12.1-linux-64bit
GNU nano 8.3                                         config.json

{
    "admin_server": {
        "listen_url": "0.0.0.0:3333",
        "use_tls": true,
        "cert_path": "gophish_admin.crt",
        "key_path": "gophish_admin.key",
        "trusted_origins": []
    },
    "phish_server": {
        "listen_url": "0.0.0.0:80",
        "use_tls": false,
        "cert_path": "example.crt",
        "key_path": "example.key"
    },
    "db_name": "sqlite3",
    "db_path": "gophish.db",
    "migrations_prefix": "db/db_",
    "contact_address": "",
    "logging": {
        "filename": "",
        "level": ""
    }
}
```

Maintenant , on ouvre FTK et on click sur ‘Create disk image’

```
moustapha@moustapha: ~/Musique/gophish-v0.12.1-linux-64bit
moustapha@moustapha:~/Musique/gophish-v0.12.1-linux-64bit$ nano config.json
moustapha@moustapha:~/Musique/gophish-v0.12.1-linux-64bit$ sudo ufw allow 3333
Omission de l'ajout de la règle existante
Omission de l'ajout de la règle existante (v6)
moustapha@moustapha:~/Musique/gophish-v0.12.1-linux-64bit$ sudo ufw status
État : actif

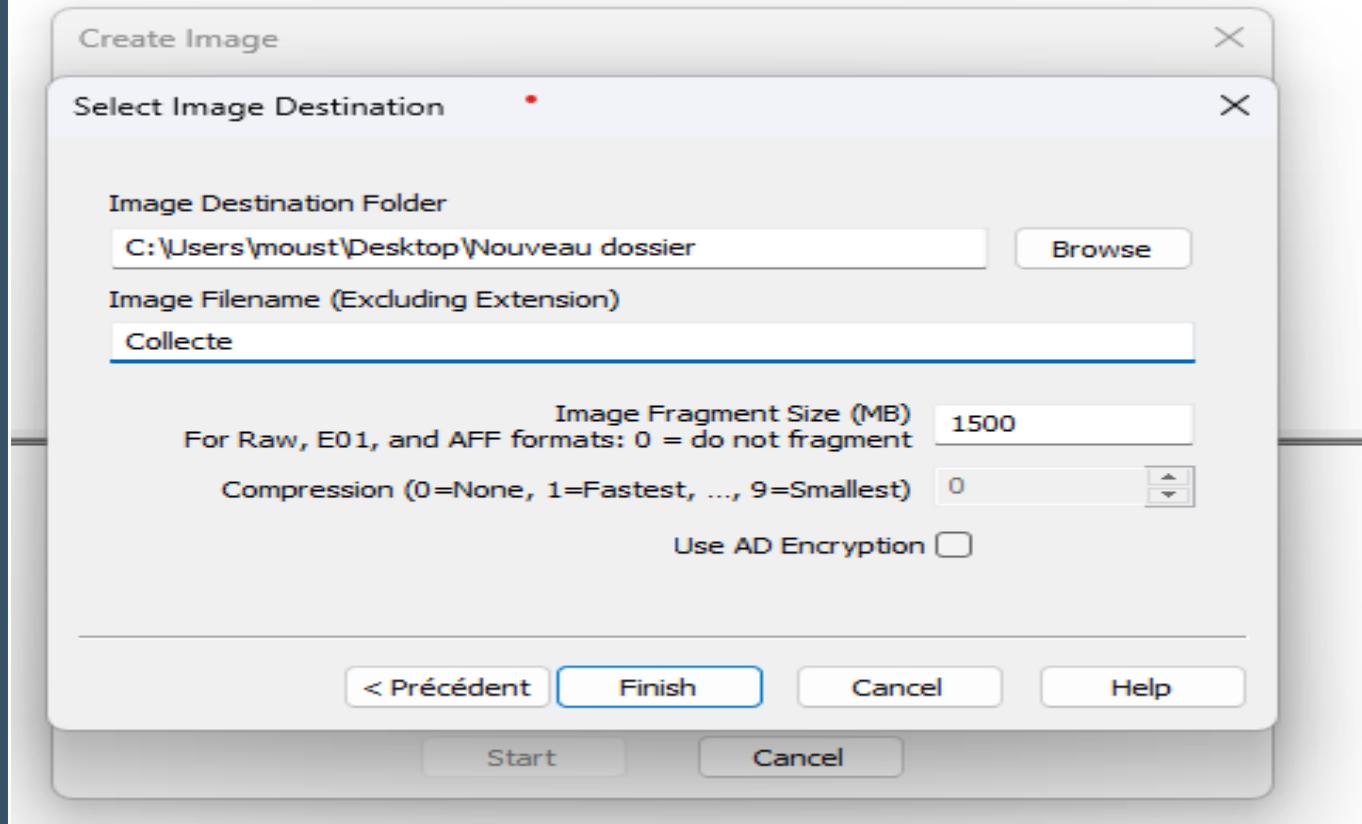
Vers          Action      De
---          -----
5044/tcp      ALLOW      Anywhere
5601/tcp      ALLOW      Anywhere
9200/tcp     DENY       Anywhere
5044          ALLOW      Anywhere
8220          ALLOW      Anywhere
3333          ALLOW      Anywhere
5044/tcp (v6) ALLOW      Anywhere (v6)
5601/tcp (v6) ALLOW      Anywhere (v6)
9200/tcp (v6) DENY       Anywhere (v6)
5044 (v6)     ALLOW      Anywhere (v6)
8220 (v6)     ALLOW      Anywhere (v6)
3333 (v6)     ALLOW      Anywhere (v6)

moustapha@moustapha:~/Musique/gophish-v0.12.1-linux-64bit$ 
```

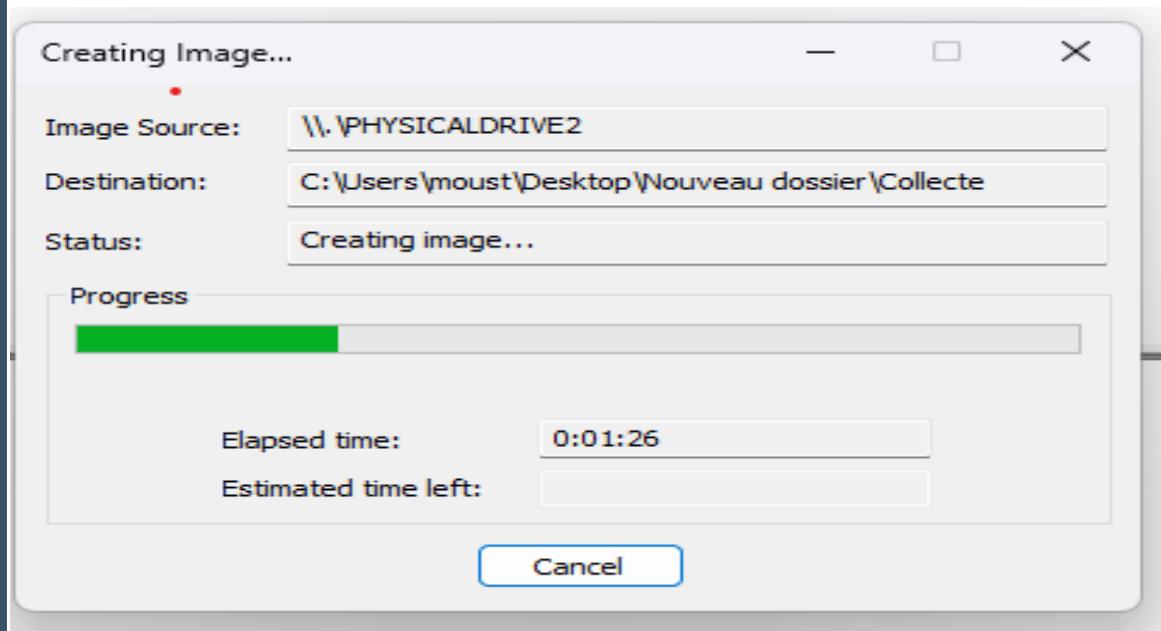
On choisi , ‘Physical drive’ puis ‘Raw dd’ pour faire une copie bit à bit’

```
moustapha@moustapha:~/Musique/gophish-v0.12.1-linux-64bit$ sudo ./gophish
time="2025-12-06T14:44:19Z" level=warning msg="No contact address has been configured."
time="2025-12-06T14:44:19Z" level=warning msg="Please consider adding a contact_address entry in your config.json"
goose: no migrations to run. current version: 20220321133237
time="2025-12-06T14:44:19Z" level=info msg="Starting IMAP monitor manager"
time="2025-12-06T14:44:19Z" level=info msg="Starting phishing server at http://0.0.0.0:80"
time="2025-12-06T14:44:19Z" level=info msg="Starting admin server at https://0.0.0.0:3333"
time="2025-12-06T14:44:19Z" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
time="2025-12-06T14:44:19Z" level=info msg="Starting new IMAP monitor for user admin"
time="2025-12-06T14:44:44Z" level=info msg="127.0.0.1 - - [06/Dec/2025:14:44:44 +0000] \"GET / HTTP/2.0\" 307 51 \" Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:145.0) Gecko/20100101 Firefox/145.0\""
time="2025-12-06T14:44:44Z" level=info msg="127.0.0.1 - - [06/Dec/2025:14:44:44 +0000] \"GET /login?next=%2F HTTP/2.0\" 200 1033 \" Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:145.0) Gecko/20100101 Firefox/145.0\""
time="2025-12-06T14:44:44Z" level=info msg="127.0.0.1 - - [06/Dec/2025:14:44:44 +0000] \"GET /images/logo_inv_small.png HTTP/2.0\" 200 1118 \"https://127.0.0.1:3333/login?next=%2F\" \" Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:145.0) Gecko/20100101 Firefox/145.0\""
time="2025-12-06T14:44:44Z" level=info msg="127.0.0.1 - - [06/Dec/2025:14:44:44 +0000] \"GET /images/logo_purple.png HTTP/2.0\" 200 4735 \"https://127.0.0.1:3333/login?next=%2F\" \" Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:145.0) Gecko/20100101 Firefox/145.0\""
time="2025-12-06T14:44:44Z" level=info msg="127.0.0.1 - - [06/Dec/2025:14:44:44 +0000] \"GET /css/dist/gophish.css HTTP/2.0\" 200 52514 \"https://127.0.0.1:3333/login?next=%2F\" \" Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:145.0) Gecko/20100101 Firefox/145.0\""
time="2025-12-06T14:44:45Z" level=info msg="127.0.0.1 - - [06/Dec/2025:14:44:45 +0000] \"GET /js/dist/vendor.min.js HTTP/2.0\" 200 324943 \"https://127.0.0.1:3333/login?next=%2F\" \" Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:145.0) Gecko/20100101 Firefox/145.0\""
time="2025-12-06T14:44:45Z" level=info msg="127.0.0.1 - - [06/Dec/2025:14:44:45 +0000] \"GET /images/favicon.ico HTTP/2.0\" 200 1150 \"https://127.0.0.1:3333/login?next=%2F\" \" Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:145.0) Gecko/20100101 Firefox/145.0\""
```

Ici on défini un case number



On met le chemin ou on doit mettre l'image, et apres ça on click sur finish > start



Drive/Image Verify Results

Sector count	15728640
MD5 Hash	
Computed hash	6d55692943afdc56072d3207de07095b
Report Hash	6d55692943afdc56072d3207de07095b
Verify result	Match
SHA1 Hash	
Computed hash	d6820cd2fb96f19e7305daa4a80b74821e90a
Report Hash	d6820cd2fb96f19e7305daa4a80b74821e90a
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Close

This screenshot shows a "Drive/Image Verify Results" window. It displays the following information:

- Sector count: 15728640
- MD5 Hash:
 - Computed hash: 6d55692943afdc56072d3207de07095b
 - Report Hash: 6d55692943afdc56072d3207de07095b
 - Verify result: Match
- SHA1 Hash:
 - Computed hash: d6820cd2fb96f19e7305daa4a80b74821e90a
 - Report Hash: d6820cd2fb96f19e7305daa4a80b74821e90a
 - Verify result: Match
- Bad Blocks List:
 - Bad block(s) in image: No bad blocks found in image

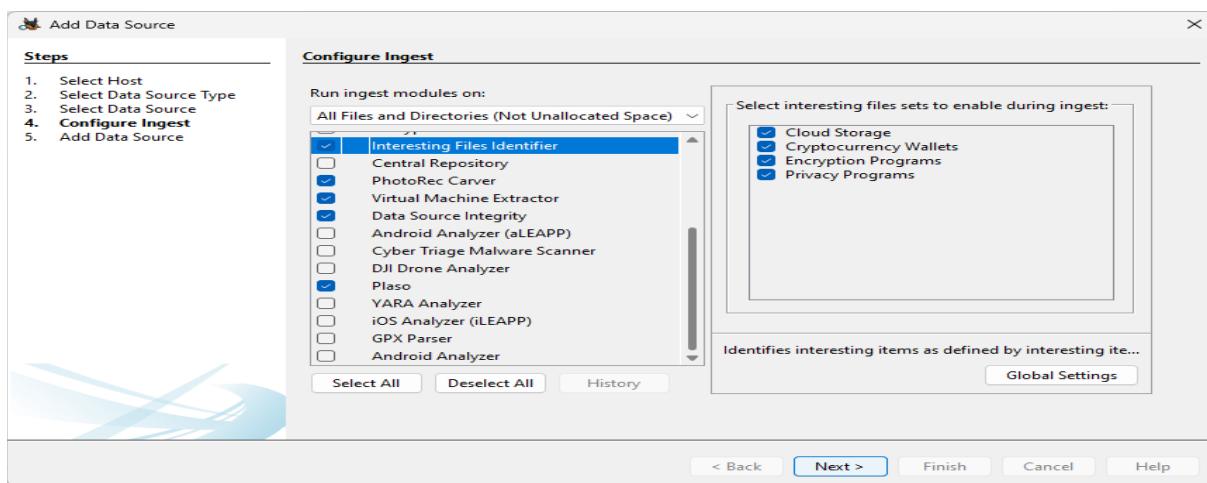
A "Close" button is located at the bottom of the window.

Maintenant l'image est entrain d'etre copier et apres la copie terminer , on peut voir en md5 et à SHA1

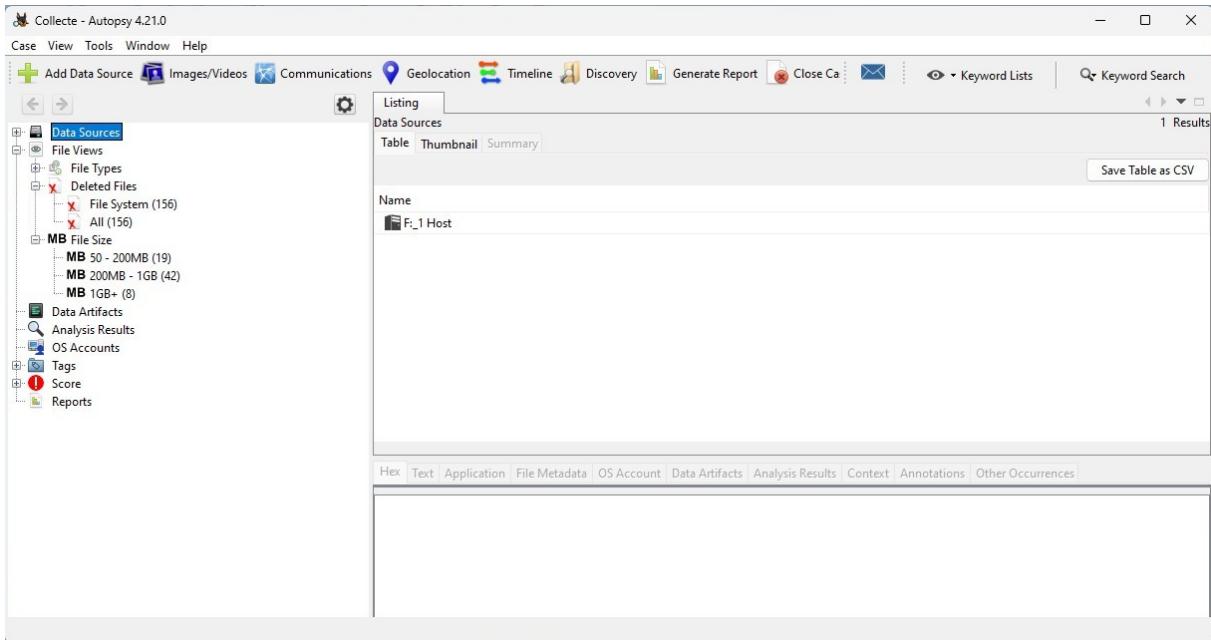
Analyse de l'image



Ici, on ouvre autopsy



On configure le ingest pour filtrer les éléments à recuperer



Ici , on a resultat de la recuperation

Name	S	C	O	Modified Time	Change Time	Access Time
000100000000029B4158BB8F				2023-02-18 18:23:34 GMT	2024-08-05 12:27:26 GMT	2024-10-14 00:25:57 GMT
0001000000000029D2B9AD878				2017-02-11 01:02:32 GMT	2024-08-05 12:27:26 GMT	2024-10-18 12:40:35 GMT
securityonion-2.4.110-20241010.iso				2024-10-22 14:16:16 GMT	2024-10-25 10:54:55 GMT	2024-10-25 11:03:49 GMT
securityonion-2.4.110-20241010.iso:Zone.Identifier				2024-10-22 14:16:16 GMT	2024-10-25 10:54:55 GMT	2024-10-25 11:03:49 GMT
securityonion-2.4.110-20241010.iso				2024-10-22 14:16:16 GMT	2024-10-24 10:03:35 GMT	2024-10-24 15:42:35 GMT
securityonion-2.4.110-20241010.iso:Zone.Identifier				2024-10-22 14:16:16 GMT	2024-10-24 10:03:35 GMT	2024-10-24 15:42:35 GMT
dt20_arw_win.cpk				2016-10-20 17:53:16 GMT	2024-08-05 12:08:18 GMT	2024-10-13 23:36:05 GMT
dt19_win.cpk				2016-10-20 17:40:00 GMT	2024-08-05 12:08:18 GMT	2024-10-13 23:36:05 GMT
dt20_eng_win.cpk				2016-10-20 17:40:16 GMT	2024-08-05 12:08:19 GMT	2024-10-13 23:36:05 GMT
dt20_fra_win.cok				2016-10-20 17:45:44 GMT	2024-08-05 12:08:19 GMT	2024-10-13 23:36:05 GMT

Ici , on a identifié un fichier nommé Facture.exe

Pour le moment on peut pas affirmer que cest un fichier malveillant , donc on va verifier avec un service en ligne nommé MetaDefence Cloud

The screenshot shows the analysis results for a file hash: 1F015CB6377151F1010A8EB935B941E5269975832696AB608237C2E89F86D490. The interface includes a navigation bar with links like 'Analyses bit par bit clé', 'Results | MetaDefender C...', 'trojan.exe - Le scanner anti-virus', 'Comment dupliquer une page', 'Télécharger un fichier | iLove...', and a search bar. Below the bar, it says 'Brave n'est pas votre navigateur par défaut' and 'Définir par défaut'. The main content area has tabs for 'Multiscanning' (26 engines, Threats Detected), 'Adaptive Sandbox' (Malicious), 'Deep CDR*' (Unsupported file type), 'Proactive DLP' (No Results Available), 'Vulnerabilities' (No Vulnerabilities Found), and 'Community feedback' (0 comments). A 'File Overview' table provides detailed technical information about the file, such as Category (Executable File), File Type (exe), File Extension (exe), TrID (53026CF7B2E48A6D1509026147F4FF57), SHA-1 (4F959905791980D316C94DE01D72A1...), SHA-256 (1F015CB6377151F1010A8EB935B941E...), and Company Name (Apache Software Foundation). A note at the bottom states: 'We value your privacy. We use cookies to enhance your browsing experience, serve personalized ads or content, and analyze our traffic. By clicking "Accept", you consent to our use of cookies. Please see our Cookie Policy.' with buttons for 'Accept All', 'Cookies Settings', and 'Reject All'.

Apres avoir mis le fichier dans site du service , 26 structures on affirmé que ce fichier est malveillant et peut compromettre un systeme , cest a dire ce fichier s'évolue comme un trojan.

Détermination du vecteur d'infection

ce fichier infecte le système après que la victime l'ait exécuté. La sténographie a été utilisée pour tromper l'utilisateur à cliquer sur une facture, et après click click, l'attaquant peut même accéder au webcam de la victime.