RAPPORT D'ANALYSE FORENSIQUE

Exfiltration de Données, Compromission d'Infrastructure & Ingénierie Sociale

Mohamed Rayen AKAICHI

Cible : Jean Martin (Stagiaire)
Période d'activité : 20 au 23 Octobre 2024
Date du rapport : 25 février 2026

Synthèse : L'utilisateur a orchestré un vol de données prémédité en utilisant des techniques d'obfuscation avancées (Stéganographie, Chiffrement caché). Il a tenté de manipuler les preuves temporelles (Timestomping) et a nettoyé ses traces via CCleaner après avoir exfiltré les bases clients, les données financières et les clés SSH critiques sur un support USB personnel.

Classification : CRITIQUE

Table des matières

1

1. Contexte et Périmètre de l'Analyse

1.1 Le Profil du Suspect

Jean Martin a intégré l'entreprise le 20 octobre 2024 en tant que stagiaire. Son départ précipité le 23 octobre (après seulement 3 jours), justifié par une fausse affectation au Ministère de l'Intérieur, a déclenché cette investigation.

1.2 Méthodologie et Environnement d'Analyse

Chaîne de Garde (Chain of Custody) : L'analyse a été réalisée sur une copie forensique (image disque) afin de garantir l'intégrité de la preuve originale.

— **Fichier source :** `img_TP_NVMe_UHPVN01J1CHYKR.E01`
— **Intégrité :** Hash vérifié (Conforme à l'original).

Outils Utilisés : Les logiciels suivants ont été employés pour l'extraction et l'analyse des artefacts :

— **Autopsy (v4.22.1) :** Analyse globale du système de fichiers, récupération des logs Windows (EVTX), analyse de la base de registre et des artefacts web.
— **VeraCrypt :** Montage des conteneurs chiffrés et accès aux volumes cachés (Hidden Volumes).
— **Firefox Portable Edition :** Analyse confinée du profil navigateur de l'utilisateur pour l'extraction de mots de passe et l'historique.

1.3 Chronologie d'Arrivée

— **20 Octobre - 20 :34** : Première ouverture de session. Configuration du poste.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags
All Users				2024-09-05 19:12:20 CEST	2024-09-05 19:12:20 CEST	2024-09-05 19:12:20 CEST	2024-09-05 19:12:20 CEST	48	Alloc
Default				2024-09-05 19:12:20 CEST	2024-09-05 19:12:20 CEST	2024-10-20 21:14:06 CEST	2024-09-05 19:58:13 CEST	336	Alloc
Default User				2024-09-05 19:12:20 CEST	2024-09-05 19:12:20 CEST	2024-09-05 19:12:20 CEST	2024-09-05 19:12:20 CEST	48	Alloc
Jean Martin				2024-10-20 21:01:52 CEST	2024-10-20 21:01:52 CEST	2024-10-23 11:16:07 CEST	2024-10-20 20:34:36 CEST	336	Alloc
Public				2024-10-20 20:36:17 CEST	2024-10-20 20:36:17 CEST	2024-10-23 11:09:02 CEST	2024-09-05 20:01:45 CEST	56	Alloc
[current folder]				2024-10-20 20:52:50 CEST	2024-10-20 20:52:50 CEST	2024-10-23 11:16:07 CEST	2024-09-05 19:58:13 CEST	56	Alloc
[parent folder]				2024-10-22 14:56:54 CEST	2024-10-22 14:56:54 CEST	2024-10-23 11:16:08 CEST	2019-12-07 10:03:44 CET	184	Alloc
desktop.ini				2024-09-05 20:00:39 CEST	2024-09-05 20:01:46 CEST	2024-10-23 11:15:33 CEST	2024-09-05 20:01:46 CEST	174	Alloc

FIGURE 1 – Création du compte utilisateur

1.4 Cartographie des Preuves (Architecture Logique)

L'analyse a permis de reconstruire l'environnement logique complexe mis en place par le suspect pour cloisonner ses activités :

— **Disque C : (Système)** : Contient les traces d'exécution (Logs), l'historique de navigation et les outils installés.
— **Disque D : (USB)** : Identifié comme *"USB-JM"*, marque **Verbatim Store'n'Go** (S/N : `NT302DEDGQSPOBSD`). Support de l'exfiltration.

— **Disque V : (Virtuel/Chiffré)** : Partition cachée VeraCrypt contenant les documents administratifs.
— **Disque Z : (Virtuel/Chiffré)** : Partition cachée VeraCrypt contenant les clés d'infrastructure.

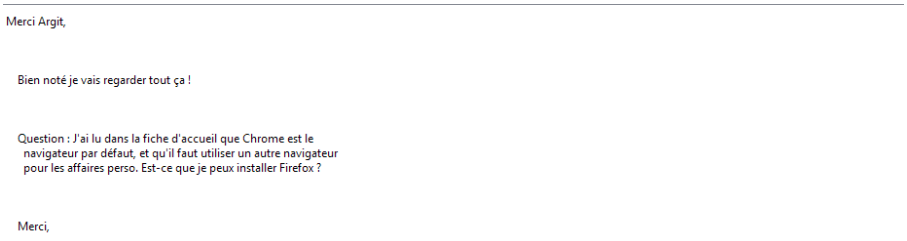
2

2. Chronologie (Timeline)

Reconstitution minute par minute basée sur les logs système, web et fichiers (CEST).

21 Octobre : La Collecte et la Préparation

— **11 :17 (Email)** : Le tuteur (Argit J.) envoie par email les documents internes (Procédures, Rapports).
— **11 :21 (Email)** : J. Martin demande l'autorisation d'installer **Firefox** pour "usage personnel". *Analyse : Stratégie pour éviter le traçage sur le navigateur par défaut (Chrome) géré par l'entreprise.*


Merci Argit,

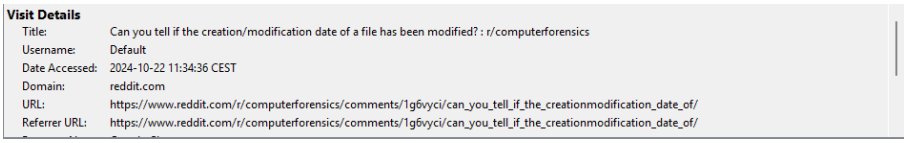
Bien noté je vais regarder tout ça !

Question : J'ai lu dans la fiche d'accueil que Chrome est le navigateur par défaut, et qu'il faut utiliser un autre navigateur pour les affaires perso. Est-ce que je peux installer Firefox ?

Merci,

FIGURE 2 – Demande d'installation de Firefox

— **13 :23 (Web)** : Recherche Google suspecte : *"effacer corbeille définitivement windows"*.


Visit Details

Title:	Can you tell if the creation/modification date of a file has been modified? : r/computerforensics
Username:	Default
Date Accessed:	2024-10-22 11:34:36 CEST
Domain:	reddit.com
URL:	https://www.reddit.com/r/computerforensics/comments/1g6vyci/can_you_tell_if_the_creationmodification_date_of/
Referrer URL:	https://www.reddit.com/r/computerforensics/comments/1g6vyci/can_you_tell_if_the_creationmodification_date_of/

FIGURE 3 – Historique de recherche suspect

— **13 :58 (Système)** : Installation de **CCleaner v6.29** (Dossier créé dans Program Files).
— **14 :21 - 17 :25** : Premiers tests de nettoyage avec CCleaner (3 exécutions).

22 Octobre : L'Armement et l'Ingénierie Sociale

— **10 :09 (Web)** : Recherches techniques avancées : *"VeraCrypt"*, *"Base64 encode"*, *"Steganography decode"*, *"Hidden volume"*.

FIGURE 4 – Recherches techniques d'obfuscation

FIGURE 5 – Recherches spécifiques VeraCrypt

— **Après-midi (Web - CRITIQUE)** : Recherches sur **Reddit (r/computerforensics)** concernant le **Timestomping** :
  — *"Can you tell if the creation/modification date of a file has been modified ?"*
  — *"Word documents analysis and track changes"*

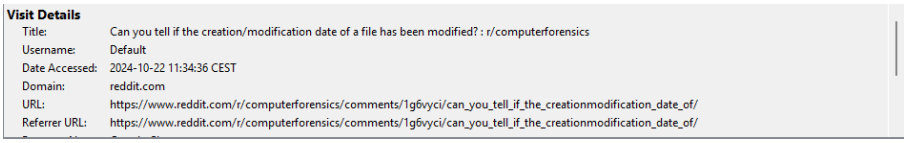


FIGURE 6 – Historique Reddit (Timestomping)

— **17 :58 (Fichier)** : Création du fichier `WallPaper-Ultra-HD (2).zip`. Bien qu'ayant une extension .zip, son entropie est de 8.0 (Maximum), indiquant un contenu chiffré.

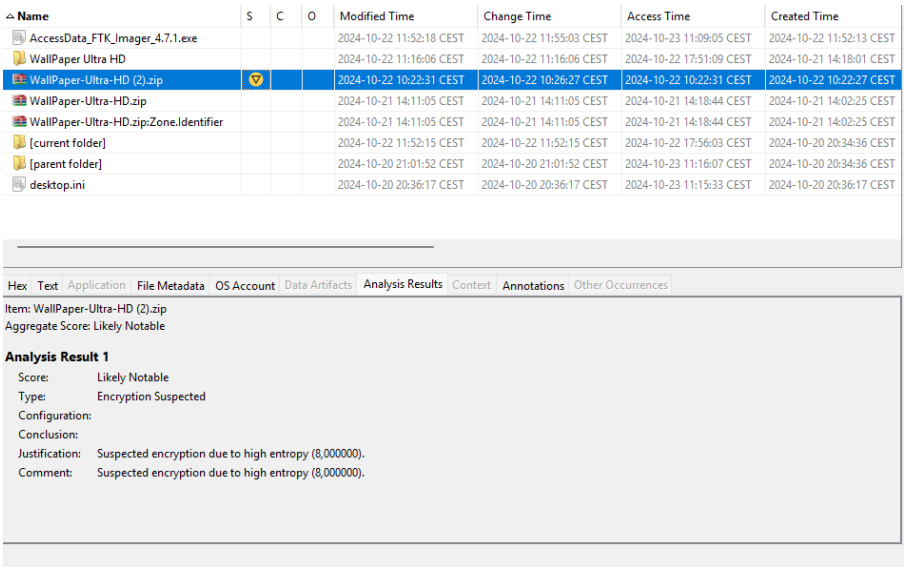
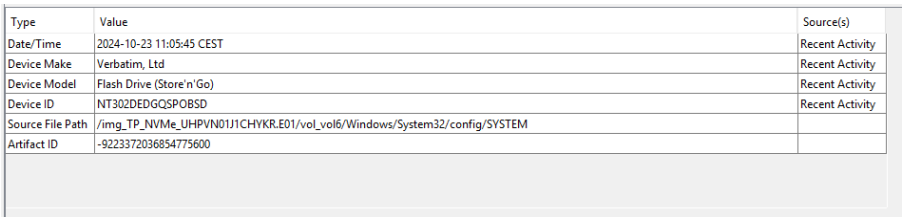


FIGURE 7 – Analyse du fichier ZIP chiffré

— **17 :56 (Email)** : Envoi du mail de démission prétextant une réception au **Ministère de l'Intérieur**. *Analyse : Mensonge (Social Engineering) pour justifier un départ immédiat sans éveiller les soupçons.*

23 Octobre : L'Exfiltration (Jour J)

— **11 :05 (Système)** : Connexion de la clé USB **Verbatim** (Event ID 2003/7045).



Type	Value	Source(s)
Date/Time	2024-10-23 11:05:45 CEST	Recent Activity
Device Make	Verbatim, Ltd	Recent Activity
Device Model	Flash Drive (Store'n'Go)	Recent Activity
Device ID	NT302DEDGQSPOBSD	Recent Activity
Source File Path	/img_TP_NVMe_UHPVN01J1CHYKR.E01/vol_vol6/Windows/System32/config/SYSTEM	
Artifact ID	-9223372036854775600	

FIGURE 8 – Preuve de connexion USB

— **11 :11** : Manipulation de l'image stéganographique `42.jpg`.
— **11 :12** : Montage du volume VeraCrypt `WallPaper-Ultra-HD (2).zip`.
— **11 :15** : Lancement final de **CCleaner** pour effacer les traces (Historique, Fichiers récents, Cache).

3

3. Analyse Technique des Vecteurs d'Attaque

3.1 La Chaîne de Dissimulation (Stéganographie & Chiffrement)

Le suspect a mis en place un mécanisme à double authentification complexe pour cacher les données volées.

3.1.1 Phase A : Le Secret Stéganographique

Une image anodine, `42.jpg`, servait de "coffre-fort" pour le mot de passe.

1. **Vecteur :** Image `42.jpg`.
2. **Clé d'extraction :** Le mot de passe `NGGYU-NGLYD!` (retrouvé dans le profil Firefox) a été utilisé avec un outil de stéganographie. Ce mot de passe fait référence au mème "Rickroll".
3. **Payload extrait :** Une chaîne encodée en Base64 : `U3Ryb25nU2VjcmVOVm9sdW1lUGFzc3dvcmQ==`
4. **Décodage :** Une fois décodée, la chaîne révèle le mot de passe maître : `StrongSecretVolumePassword`

3.1.2 Phase B : Le Conteneur VeraCrypt à Double Fond

Le fichier `WallPaper-Ultra-HD (2).zip` est un conteneur VeraCrypt utilisant la fonction de **Déni Plausible** (Hidden Volume).

— **Volume Externe (Leurre) :** S'ouvre avec le mot de passe `NGGYU-NGLYD!`. Contient uniquement un fichier `Test.xlsx` vide et un raccourci vers la vidéo YouTube "Never Gonna Give You Up". *But : Faire croire à l'enquêteur qu'il s'agit d'une blague.*

— **Volume Caché (Cible) :** S'ouvre avec le mot de passe `StrongSecretVolumePassword`. Contient les lecteurs **V :** et **Z :**.

3.2 Inventaire des Données Exfiltrées

L'exploration forensique des volumes cachés (V : et Z :) a révélé la nature critique des données dérobées :

— **Intelligence Économique (Lecteur V :)** :
  — `Base client.xlsx` : Fichier CRM complet (Contacts, Statuts, Prospects).
  — `Finances groupe.xlsx` : Transactions détaillées de l'année 2023.

FIGURE 9 – Contenu du volume caché V :

— **Infrastructure Critique (Lecteur Z :)** :
  — `baronnies` : **Clé Privée RSA (SSH)**.
  — `baronnies.pub` : Clé Publique associée.

Impact Technique : La compromission de la clé privée `baronnies` offre à l'attaquant un accès "root" ou administrateur persistant sur les serveurs de l'entreprise, sans besoin de mot de passe. C'est une porte dérobée (Backdoor) active.

3.3 Analyse Anti-Forensics (Contre-Mesures)

Le suspect a activement tenté d'empêcher l'analyse de son poste :

1. **Nettoyage Automatisé :** Utilisation intensive de CCleaner (8 occurrences en 48h).
2. **Timestomping :** Recherches documentées sur la modification des dates de fichiers pour fausser la chronologie légale.
3. **Leurres :** Utilisation de la culture Internet (Rickroll) pour ridiculiser une analyse superficielle.
4. **Partitionnement :** Utilisation de Firefox au lieu de Chrome pour éviter la synchronisation des historiques avec le compte Google de l'entreprise.

4

4. Preuves Matérielles et Traces Système

Les artefacts suivants sont archivés comme pièces à conviction :

— **System.evtx (Event 7045)** : Preuve de l'installation du pilote `veracrypt.sys` le 22/10.
— **Recent.lnk (JumpLists)** : Preuve de l'ouverture des fichiers sur D :, V : et Z : à 11 :14.
— **UsrClass.dat (Shellbags)** : Preuve de la navigation dans les dossiers de la clé USB.
— **Run Programs (Prefetch/SRUDB)** : Preuve de l'exécution de CCleaner à 11 :15.

FIGURE 10 – Installation de VeraCrypt

5

5. Conclusion et Recommandations

5.1 Conclusion

L'investigation démontre, hautement probable que Jean Martin est l'auteur d'un vol de données qualifié.

— Il avait les **moyens** (Compétences techniques, Outils installés).
— Il a eu l'**opportunité** (Accès légitime initial aux fichiers).
— Il a démontré l'**intention** (Recherches sur l'effacement de preuves, Mensonge sur son départ, Chiffrement caché).

5.2 Plan d'Action Immédiat

1. **Sécurité :** Révocation immédiate et remplacement de la paire de clés SSH `baronnies` sur l'ensemble du parc serveur. Audit des connexions entrantes récentes.
2. **Juridique :** Dépôt de plainte pénal pour vol de données, atteinte à un STAD et abus de confiance.
3. **RH :** Signalement de l'individu, notamment auprès du Ministère de l'Intérieur (utilisé comme faux prétexte).