Rapport d'Analyse Forensique

MOUHALHAL Abdelmonaim

Encadré par :

Christophe RAMON

Rapport d'Analyse Forensique

Résumé Exécutif

Une intrusion informatique a été détectée au sein des systèmes critiques de l'entreprise. Cette attaque a abouti au vol de données sensibles, notamment une recette secrète essentielle pour les activités de l'entreprise. Après analyse approfondie, il a été confirmé que l'attaquant a exploité des failles dans les configurations de sécurité pour accéder à des systèmes critiques via une attaque par force brute. Cette attaque a permis l'installation d'un malware persistant, l'exfiltration de données stratégiques, et la compromission de plusieurs systèmes internes.

Introduction

Ce rapport détaille les événements ayant conduit à l'incident de sécurité, les techniques utilisées par les attaquants, et les mesures recommandées pour éviter de futures intrusions. L'objectif principal est de fournir une vue d'ensemble claire et exploitable pour renforcer la posture de sécurité de l'entreprise.

Méthodologie

L'analyse a été menée en utilisant des outils avancés de forensic numérique, notamment :

- **Autopsy 4.21.0** : pour l'analyse des disques.
- **Volatility 2.6.1** : pour l'analyse mémoire et la détection de processus suspects.
- **Hayabusa v3.1.0** : pour l'analyse des journaux d'événements Windows.
- **VirusTotal** : pour la vérification de la réputation des fichiers et adresses IP suspectes.

Résultats de l'Analyse(Exclusif summary)

1. Points d'Entrée et Tactiques d'Intrusion

- **Technique d'accès initial** : Une attaque par force brute sur le compte administrateur de `CITADEL-DC01` depuis l'adresse IP `194.61.24.102` a permis de contourner les contrôles d'authentification.
- **Propagation interne** : Une fois le contrôle du domaine acquis, l'attaquant a utilisé le protocole RDP pour se déplacer latéralement vers `DESKTOP-SDN1RPT`.

2. Présence du Malware

- **Nom du malware** : `coreupdater.exe`
- **Localisation** : `C:\Windows\System32\coreupdater.exe`
- **Capacités identifiées** :
    - Exécution de commandes à distance.
    - Exfiltration de données.
    - Persistance via la modification des clés de registre pour un démarrage automatique.
- **Communication C2** : Le malware a établi une connexion avec l'adresse IP `203.78.103.109`, identifiée comme serveur Command and Control (C2).

3. Données Exfiltrées

- **Fichiers compromis** :
    - `Szechuan Sauce.txt`
    - `SECRET_Beth.txt`
    - `PortalGunPlans.txt`
- **Mode d'exfiltration** : Les fichiers ont été compressés en `loot.zip` puis exfiltrés vers un serveur externe.

4. Chronologie de l'Attaque

1. **Initialisation** : L'attaque par force brute débute à partir de l'IP `194.61.24.102`.
2. **Accès réussi** : Compromission de l'administrateur du contrôleur de domaine.
3. **Propagation** : Déploiement du malware sur les machines cibles et déplacement via RDP.
4. **Exfiltration** : Téléchargement des fichiers sensibles en archive et suppression locale pour masquer les traces.

Impact et Conséquences

L'exfiltration de la recette `Szechuan Sauce.txt` représente un risque stratégique majeur pour l'entreprise, en raison de la valeur commerciale et de la propriété intellectuelle associées à ce fichier. De plus, la compromission de systèmes critiques expose l'entreprise à des risques financiers, légaux, et réputationnels.

Recommandations

1. **Renforcer la Sécurité des Comptes :**
    - Implémenter une politique de mots de passe robustes.
    - Activer l'authentification multifactorielle (MFA).
2. **Limiter l'Accès RDP :**
    - Désactiver RDP pour les utilisateurs non essentiels.
    - Utiliser des solutions VPN sécurisées pour les connexions distantes.
3. **Surveillance Active :**
    - Mettre en place un système de détection d'intrusion (IDS) pour surveiller les activités réseau suspectes.
    - Analyser régulièrement les journaux d'événements.
4. **Réagir Rapidement :**
    - Déployer un plan de réponse aux incidents pour détecter et contenir rapidement toute activité malveillante.
    - Auditer et corriger les failles identifiées lors de cette analyse.
5. **Former les Employés :**
    - Sensibiliser les équipes aux pratiques de sécurité informatique.
    - Simuler des scénarios d'attaque pour tester les capacités de réponse.

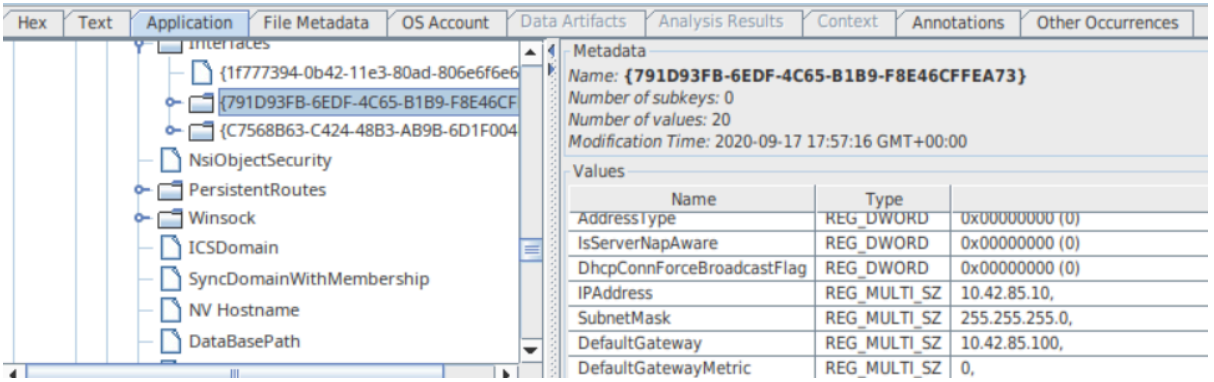
Conclusion

L'attaque sur les systèmes de l'entreprise met en évidence des faiblesses exploitables dans les contrôles d'accès et la surveillance réseau. En mettant en œuvre les recommandations de ce rapport, l'entreprise peut réduire considérablement ses risques et renforcer sa résilience face aux cybermenaces.

Liste des preuves

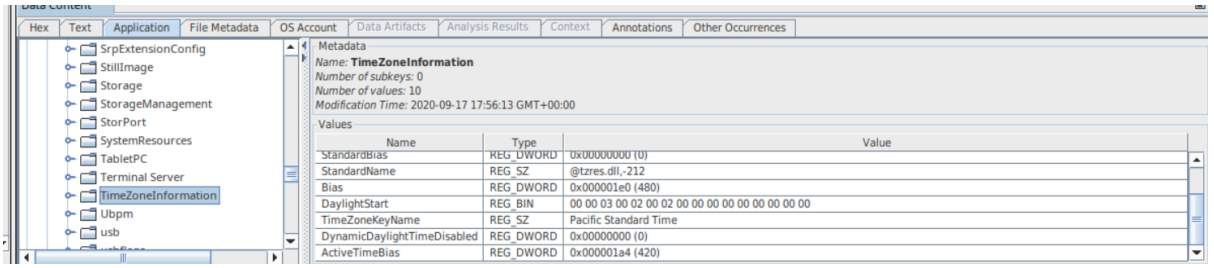
Carte d'Identité du Serveur

1. **Nom d'Hôte :** CITADEL-DC01
2. **Adresse IP :** 10.42.85.10



3. **Système d'Exploitation :** Windows Server 2012 R2 Standard Evaluation.
4. **Version :** Selon le registre, il correspond à la version Standard Evaluation.

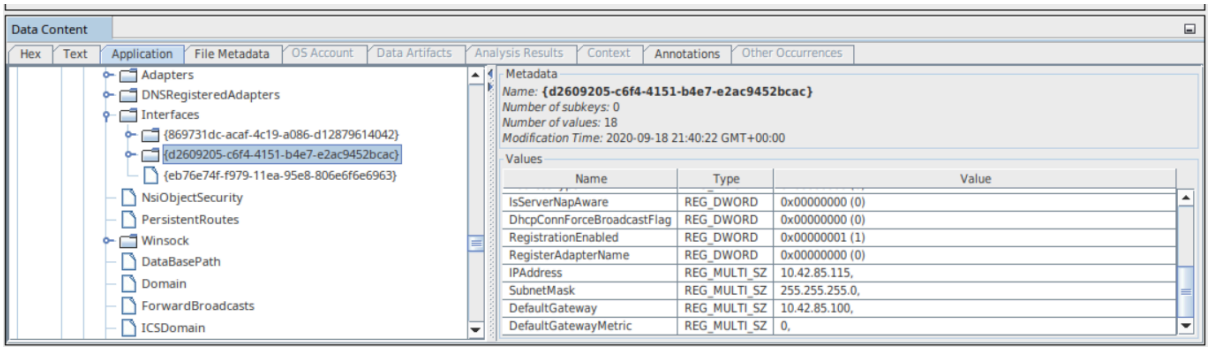
5. **Configuration du Fuseau Horaire :** Pacific Standard Time (PST)



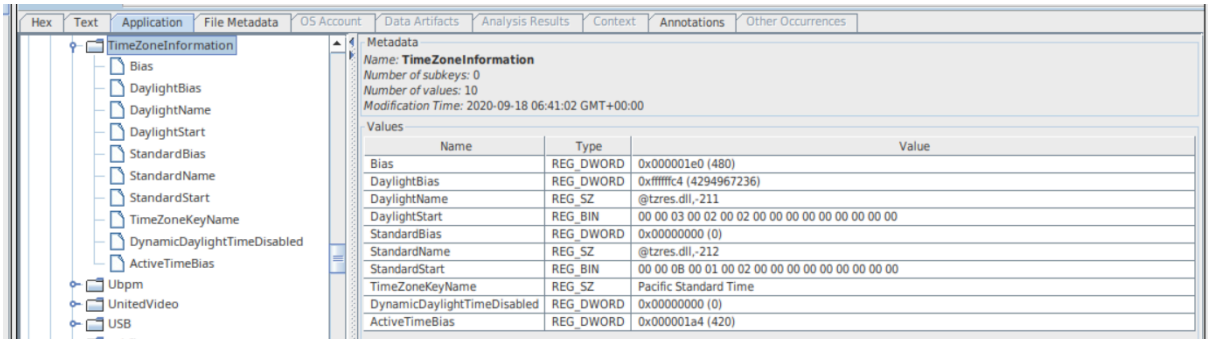
6. **Nombre d'Utilisateurs Configurés :** Les journaux indiquent plusieurs utilisateurs, mais le plus pertinent est `Administrator`.

Carte d'Identité du Poste de Travail

1. **Nom d'Hôte :** DESKTOP-SDN1RPT
2. **Adresse IP :** 10.42.85.115



3. **Système d'Exploitation :** Windows 10 Enterprise Edition
4. **Version :** Confirmée comme Enterprise Edition.
5. **Configuration du Fuseau Horaire :** Pacific Standard Time (PST)



6. **Nombre d'Utilisateurs Configurés :** Plusieurs utilisateurs notés ; activité principale observée sous un compte utilisateur principal.

Identification du Point d'Entrée

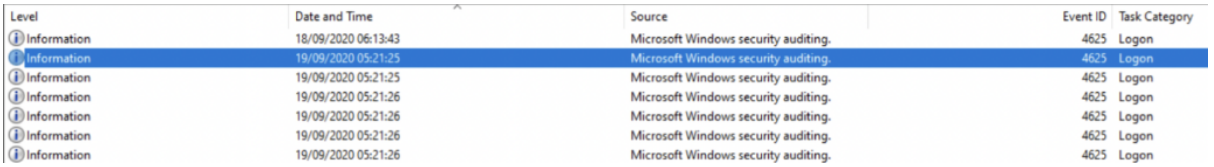
L'analyse des événements de sécurité dans le fichier **Security.evtx** a permis d'identifier le point d'entrée utilisé par l'attaquant pour compromettre le système. Voici les étapes clés de cette identification :

1. Détection des Tentatives de Connexion

- **Événement 4625** : Cet événement indique une tentative de connexion échouée. Il a été utilisé pour repérer les tentatives d'accès non autorisées.
- **Événement 4624** : Cet événement indique une connexion réussie. Il a permis de confirmer le moment où l'attaquant a réussi à s'authentifier.

2. Analyse des Tentatives Échouées

- Une machine nommée **Kali** (WorkStation Name: **Kali)** a été identifiée comme source de multiples tentatives de connexion infructueuses.



Level	Date and Time	Source	Event ID	Task Category
Information	18/09/2020 06:13:43	Microsoft Windows security auditing.	4625	Logon
Information	19/09/2020 05:21:25	Microsoft Windows security auditing.	4625	Logon
Information	19/09/2020 05:21:25	Microsoft Windows security auditing.	4625	Logon
Information	19/09/2020 05:21:26	Microsoft Windows security auditing.	4625	Logon
Information	19/09/2020 05:21:26	Microsoft Windows security auditing.	4625	Logon
Information	19/09/2020 05:21:26	Microsoft Windows security auditing.	4625	Logon
Information	19/09/2020 05:21:26	Microsoft Windows security auditing.	4625	Logon

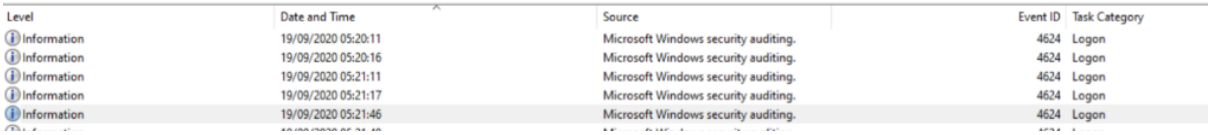
```
Timestamp · EventTitle · Hostname · Channel · Event ID · Record ID · AllFieldInfo · EvtxFile
2020-09-19 04:21:25.735 +01:00 · Logon failure · CITADEL-DC01.C137.local · Sec · 4625 · 7389 · AuthenticationPackageName: NTLM ¦ FailureReason: %
%2313 ¦ IpAddress: - ¦ IpPort: - ¦ KeyLength: 0 ¦ LmPackageName: - ¦ LogonProcessName: NtLmSsp ¦ LogonType: 3 ¦ ProcessId: 0x0 ¦ ProcessName: - ¦
 Status: 0xc000006d ¦ SubStatus: 0xc000006a ¦ SubjectDomainName: - ¦ SubjectLogonId: 0x0 ¦ SubjectUserName: - ¦ SubjectUserSid: S-1-0-0 ¦ TargetD
omainName:  ¦ TargetUserName: Administrator ¦ TargetUserSid: S-1-0-0 ¦ TransmittedServices: - ¦ WorkstationName: kali · /home/hello/Desktop/citde
lEvtx/Security_citadel.evtx
```

- Ces tentatives ont été enregistrées avec l'événement **4625**, montrant que l'attaquant a essayé de forcer l'accès au système.

```
2020-09-19 04:21:25.735 +01:00 · Logon failure · CITADEL-DC01.C137.local · Sec · 4625 · 7389 · AuthenticationPackageName: NTLM ¦ FailureReason: %
%2313 ¦ IpAddress: - ¦ IpPort: - ¦ KeyLength: 0 ¦ LmPackageName: - ¦ LogonProcessName: NtLmSsp ¦ LogonType: 3 ¦ ProcessId: 0x0 ¦ ProcessName: - ¦
 Status: 0xc000006d ¦ SubStatus: 0xc000006a ¦ SubjectDomainName: - ¦ SubjectLogonId: 0x0 ¦ SubjectUserName: - ¦ SubjectUserSid: S-1-0-0 ¦ TargetD
omainName:  ¦ TargetUserName: Administrator ¦ TargetUserSid: S-1-0-0 ¦ TransmittedServices: - ¦ WorkstationName: kali · /home/hello/Desktop/citde
lEvtx/Security_citadel.evtx

2020-09-19 04:21:25.955 +01:00 · Logon failure · CITADEL-DC01.C137.local · Sec · 4625 · 7390 · AuthenticationPackageName: NTLM ¦ FailureReason: %
%2313 ¦ IpAddress: - ¦ IpPort: - ¦ KeyLength: 0 ¦ LmPackageName: - ¦ LogonProcessName: NtLmSsp ¦ LogonType: 3 ¦ ProcessId: 0x0 ¦ ProcessName: - ¦
 Status: 0xc000006d ¦ SubStatus: 0xc000006a ¦ SubjectDomainName: - ¦ SubjectLogonId: 0x0 ¦ SubjectUserName: - ¦ SubjectUserSid: S-1-0-0 ¦ TargetD
omainName:  ¦ TargetUserName: Administrator ¦ TargetUserSid: S-1-0-0 ¦ TransmittedServices: - ¦ WorkstationName: kali · /home/hello/Desktop/citde
lEvtx/Security_citadel.evtx

2020-09-19 04:21:26.172 +01:00 · Logon failure · CITADEL-DC01.C137.local · Sec · 4625 · 7391 · AuthenticationPackageName: NTLM ¦ FailureReason: %
%2313 ¦ IpAddress: - ¦ IpPort: - ¦ KeyLength: 0 ¦ LmPackageName: - ¦ LogonProcessName: NtLmSsp ¦ LogonType: 3 ¦ ProcessId: 0x0 ¦ ProcessName: - ¦
 Status: 0xc000006d ¦ SubStatus: 0xc000006a ¦ SubjectDomainName: - ¦ SubjectLogonId: 0x0 ¦ SubjectUserName: - ¦ SubjectUserSid: S-1-0-0 ¦ TargetD
omainName:  ¦ TargetUserName: Administrator ¦ TargetUserSid: S-1-0-0 ¦ TransmittedServices: - ¦ WorkstationName: kali · /home/hello/Desktop/citde
lEvtx/Security_citadel.evtx

2020-09-19 04:21:26.391 +01:00 · Logon failure · CITADEL-DC01.C137.local · Sec · 4625 · 7392 · AuthenticationPackageName: NTLM ¦ FailureReason: %
%2313 ¦ IpAddress: - ¦ IpPort: - ¦ KeyLength: 0 ¦ LmPackageName: - ¦ LogonProcessName: NtLmSsp ¦ LogonType: 3 ¦ ProcessId: 0x0 ¦ ProcessName: - ¦
 Status: 0xc000006d ¦ SubStatus: 0xc000006a ¦ SubjectDomainName: - ¦ SubjectLogonId: 0x0 ¦ SubjectUserName: - ¦ SubjectUserSid: S-1-0-0 ¦ TargetD
omainName:  ¦ TargetUserName: Administrator ¦ TargetUserSid: S-1-0-0 ¦ TransmittedServices: - ¦ WorkstationName: kali · /home/hello/Desktop/citde
lEvtx/Security_citadel.evtx
```

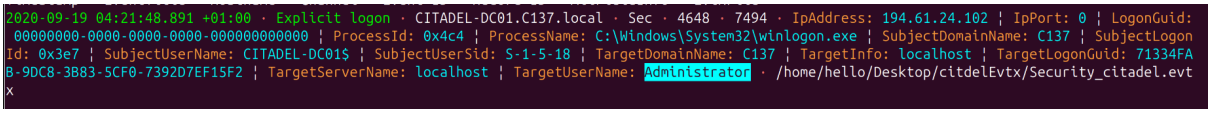
3. Succès de l'Attaque par Force Brute

- L'attaquant a finalement réussi à s'authentifier (**Événement 4624)** après **95 tentatives** en quelques secondes entre (05:21:25 – 05:21:46). **timeline :05:21:25 début de brute force**



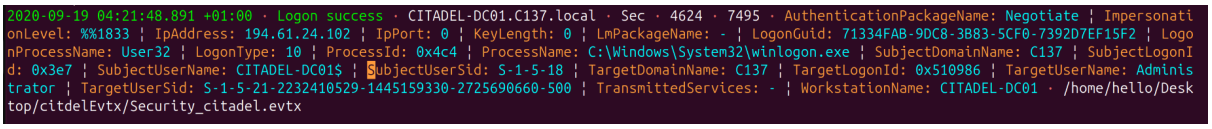
Level	Date and Time	Source	Event ID	Task Category
Information	19/09/2020 05:20:11	Microsoft Windows security auditing.	4624	Logon
Information	19/09/2020 05:20:16	Microsoft Windows security auditing.	4624	Logon
Information	19/09/2020 05:21:11	Microsoft Windows security auditing.	4624	Logon
Information	19/09/2020 05:21:17	Microsoft Windows security auditing.	4624	Logon
Information	19/09/2020 05:21:46	Microsoft Windows security auditing.	4624	Logon

- Le compte ciblé était **CITADEL\Administrator**, un compte privilégié. (logs Hayabusa)



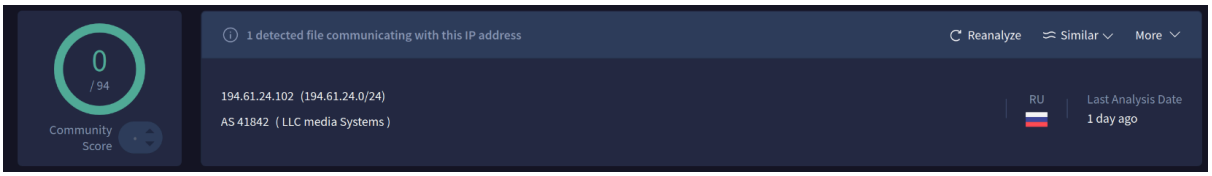
```
2020-09-19 04:21:48.891 +01:00 · Explicit logon · CITADEL-DC01.C137.local · Sec · 4648 · 7494 · IpAddress: 194.61.24.102 ¦ IpPort: 0 ¦ LogonGuid:
 00000000-0000-0000-0000-000000000000 ¦ ProcessId: 0x4c4 ¦ ProcessName: C:\Windows\System32\winlogon.exe ¦ SubjectDomainName: C137 ¦ SubjectLogon
Id: 0x3e7 ¦ SubjectUserName: CITADEL-DC01$ ¦ SubjectUserSid: S-1-5-18 ¦ TargetDomainName: C137 ¦ TargetInfo: localhost ¦ TargetLogonGuid: 71334FA
B-9DC8-3B83-5CF0-7392D7EF15F2 ¦ TargetServerName: localhost ¦ TargetUserName: Administrator · /home/hello/Desktop/citdelEvtx/Security_citadel.evt
x
```

- L'adresse IP source de l'attaque était **194.61.24.102**. (logs Hayabusa)



```
2020-09-19 04:21:48.891 +01:00 · Logon success · CITADEL-DC01.C137.local · Sec · 4624 · 7495 · AuthenticationPackageName: Negotiate ¦ Impersonati
onLevel: %%1833 ¦ IpAddress: 194.61.24.102 ¦ IpPort: 0 ¦ KeyLength: 0 ¦ LmPackageName: - ¦ LogonGuid: 71334FAB-9DC8-3B83-5CF0-7392D7EF15F2 ¦ Logo
nProcessName: User32 ¦ LogonType: 10 ¦ ProcessId: 0x4c4 ¦ ProcessName: C:\Windows\System32\winlogon.exe ¦ SubjectDomainName: C137 ¦ SubjectLogonI
d: 0x3e7 ¦ SubjectUserName: CITADEL-DC01$ ¦ SubjectUserSid: S-1-5-18 ¦ TargetDomainName: C137 ¦ TargetLogonId: 0x510986 ¦ TargetUserName: Adminis
trator ¦ TargetUserSid: S-1-5-21-2232410529-1445159330-2725690660-500 ¦ TransmittedServices: - ¦ WorkstationName: CITADEL-DC01 · /home/hello/Desk
top/citdelEvtx/Security_citadel.evtx
```

(L'adresse IP provient de la Russie, mais elle n'est pas identifiée comme suspecte sur VirusTotal)



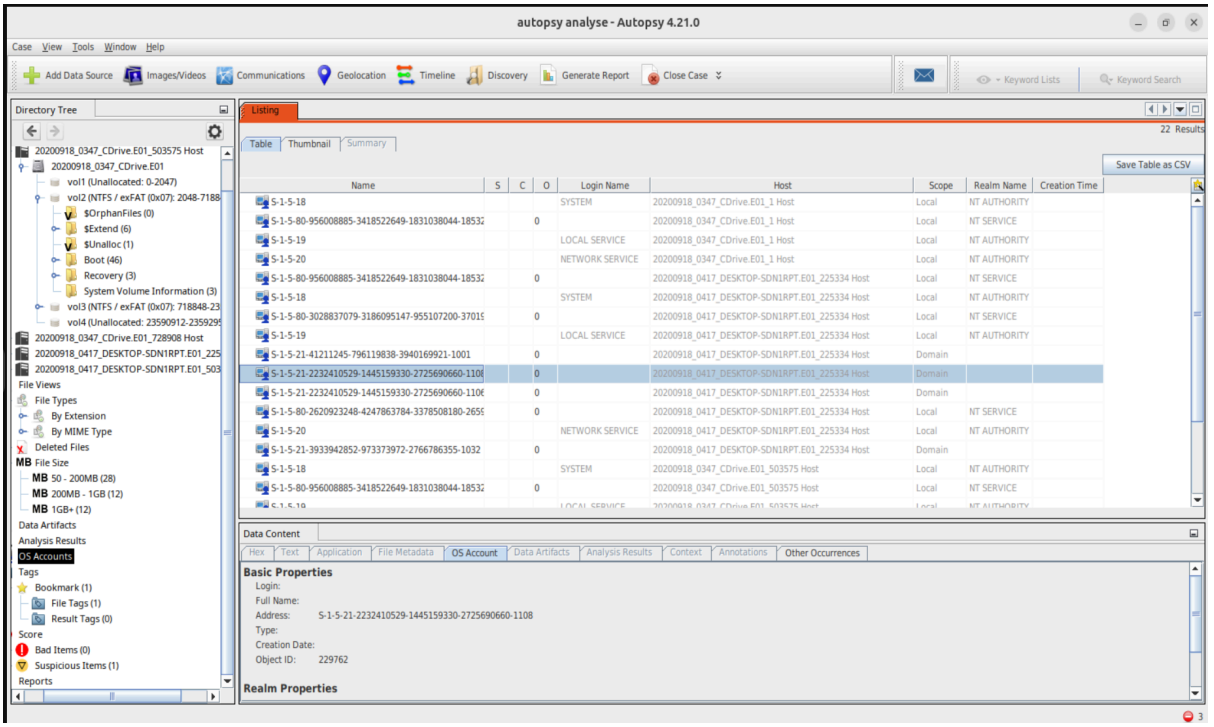
- **timeline : 04:21:48 +1 : authentification réussi a CITADEL\Administrator**

4. Protocole et Méthode d'Accès

- L'attaquant a d'abord accédé au contrôleur de domaine **CITADEL-DC01**, puis s'est déplacé vers une autre machine du réseau, **DESKTOP-SDN1RPT**.

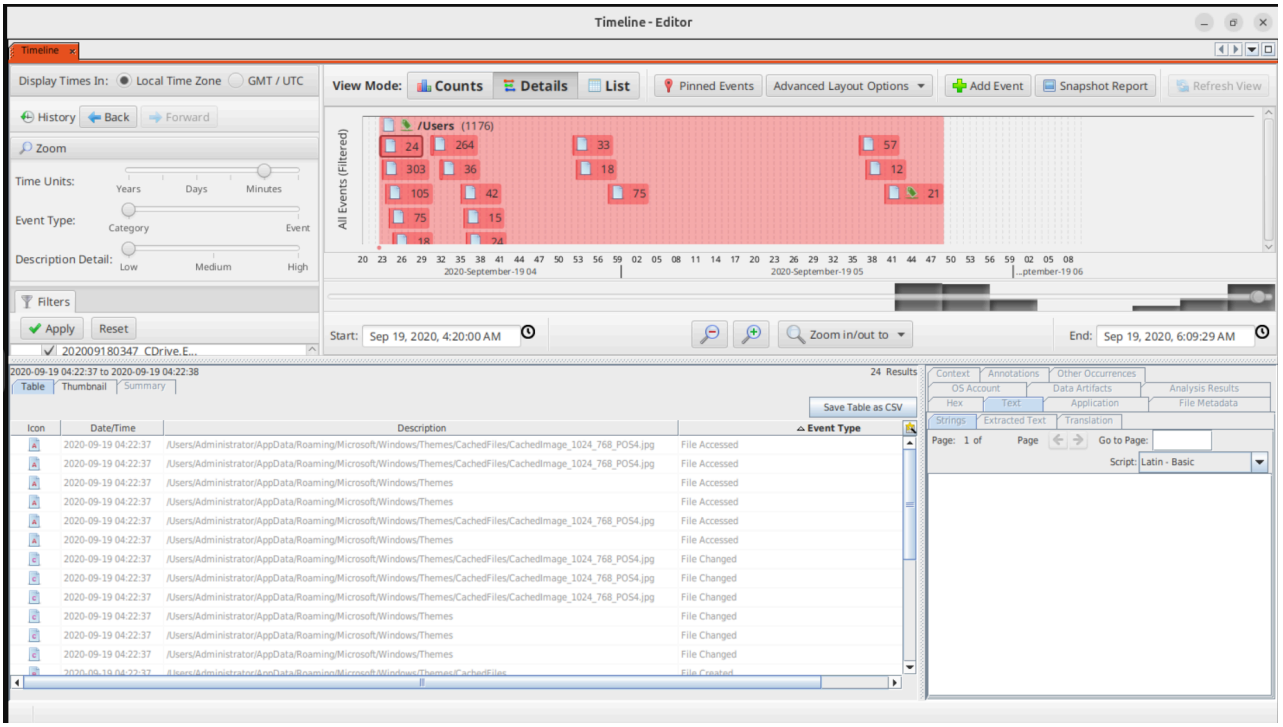
```
2020-09-19 04:22:37.422 +01:00 · Logon success · CITADEL-DC01.C137.local · Sec · 4624 · 7532 · AuthenticationPackageName: Negotiate ¦ Impersonati
onLevel: %%1833 ¦ IpAddress: 194.61.24.102 ¦ IpPort: 0 ¦ KeyLength: 0 ¦ LmPackageName: - ¦ LogonGuid: 059920FB-D27B-8AFC-EE4B-1F360D291C15 ¦ Logo
nProcessName: User32 ¦ LogonType: 10 ¦ ProcessId: 0xce8 ¦ ProcessName: C:\Windows\System32\winlogon.exe ¦ SubjectDomainName: C137 ¦ SubjectLogonI
d: 0x3e7 ¦ SubjectUserName: CITADEL-DC01$ ¦ SubjectUserSid: S-1-5-18 ¦ TargetDomainName: C137 ¦ TargetLogonId: 0x51c10f ¦ TargetUserName: Adminis
trator ¦ TargetUserSid: S-1-5-21-2232410529-1445159330-2725690660-500 ¦ TransmittedServices: - ¦ WorkstationName: CITADEL-DC01 · /home/hello/Desk
top/citdelEvtx/Security_citadel.evtx

2020-09-19 04:22:37.422 +01:00 · Admin logon · CITADEL-DC01.C137.local · Sec · 4672 · 7533 · PrivilegeList: SeSecurityPrivilege SeTakeOwnershipPr
ivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeEnableDelegationPrivilege SeIm
personatePrivilege ¦ SubjectDomainName: C137 ¦ SubjectLogonId: 0x51c10f ¦ SubjectUserName: Administrator ¦ SubjectUserSid: S-1-5-21-2232410529-14
45159330-2725690660-500 · /home/hello/Desktop/citdelEvtx/Security_citadel.evtx
```

TargetUserSid :



- **Connexion réussie (ID de l'événement 4624)** :
  - **LogonType: 10** indique une connexion RDP .
  - **AuthenticationPackageName: Negotiate** suggère l'utilisation de mécanismes d'authentification standard, tels que Kerberos ou NTLM, qui sont couramment utilisés pour RDP.
  - **IpAddress: 194.61.24.102** montre l'adresse IP distante depuis laquelle la session RDP a été initiée.
  - **ProcessName: C:\Windows\System32\winlogon.exe** indique que le processus système responsable du traitement de la connexion est **winlogon.exe**.
- **Connexion administrateur (ID de l'événement 4672)** :
  - Le compte **Administrator** a été utilisé pour cette connexion, et il inclut un ensemble de privilèges élevés, tels que **SeSecurityPrivilege**, **SeBackupPrivilege**, **SeDebugPrivilege**, etc., qui sont généralement associés à des actions administratives.

Cela confirme que la connexion est une session RDP initiée par l'utilisateur **Administrator** sur **CITADEL-DC01**.



- **timeline : 04:22:37 +1 : authentification depuis CITADEL a DESKTOP-SDN1RPT.**

5. Périphérique d'Entrée

- Le point d'entrée initial dans le réseau a été identifié comme étant **CITADEL-DC01**, le contrôleur de domaine. Cela indique que l'attaquant a ciblé un système critique pour obtenir un accès privilégié.

Conclusion

hypothèses : L'attaquant a utilisé une **attaque par force brute** sur le compte administrateur via RDP, exploitant une vulnérabilité dans la politique de sécurité (probablement un mot de passe faible ou une absence de verrouillage après plusieurs échecs). Une fois l'accès obtenu, l'attaquant a pu se déplacer latéralement dans le réseau, compromettant d'autres systèmes.

Recommandations

- **Renforcer les politiques de mot de passe** : Imposer des mots de passe complexes et activer le verrouillage de compte après un nombre défini d'échecs.
- **Limiter l'accès RDP** : Restreindre l'accès RDP aux adresses IP autorisées et utiliser un VPN pour sécuriser les connexions distantes.
- **Surveiller les événements de sécurité** : Mettre en place une surveillance proactive des événements 4624 et 4625 pour détecter rapidement les tentatives d'intrusion.

- **Segmenter le réseau** : Limiter les déplacements latéraux en segmentant le réseau et en isolant les systèmes critiques comme les contrôleurs de domaine.

Déplacement Latéral

1. **Un Déplacement Latéral a-t-il Été Détecté ?** Oui.
2. **Méthode Utilisée :**
   - RDP de `CITADEL-DC01` à `DESKTOP-SDN1RPT`.
3. **Période :** Immédiate après l'accès initial au Contrôleur de Domaine.

Renseignement sur les Menaces, Premier Tour

Indicateurs de Compromission (IOCs) :

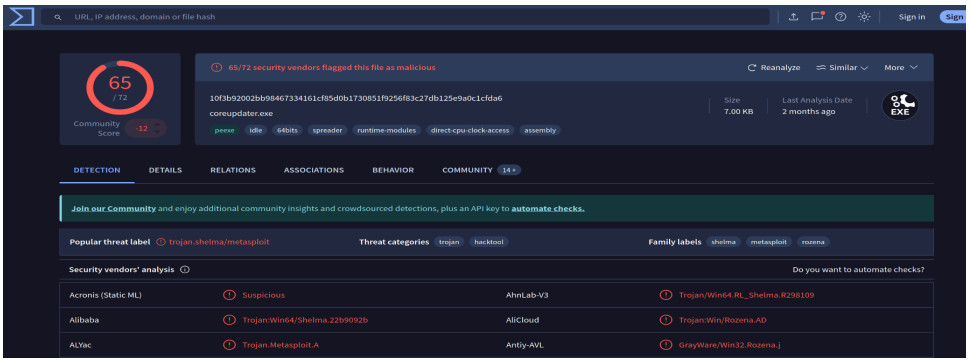
1. **Adresse IP :** 194.61.24.102
   - Localisation : Russie
   - Activité : Associée à des tentatives de force brute et des connexions RDP.
2. **Fichier Malware :** coreupdater.exe

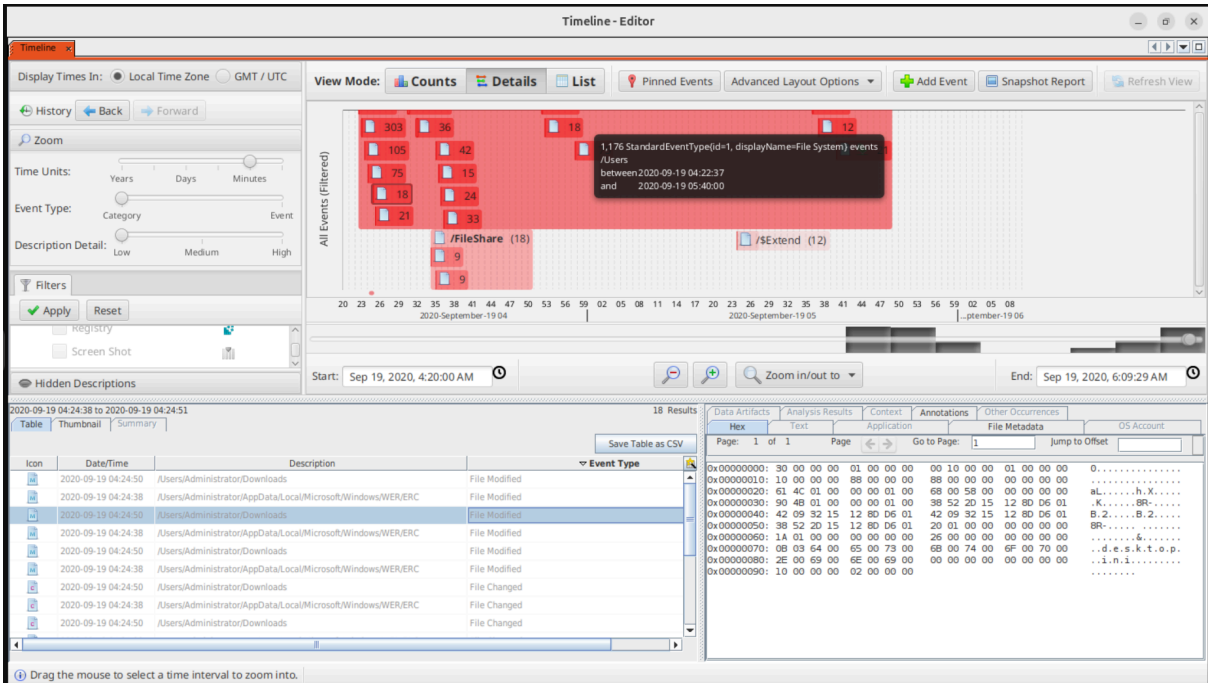
   Lors de l'analyse avec **Volatility**, un processus suspect, **coreupdater (PID 3644)**, a été détecté sans processus parent, une caractéristique typique des malwares.

```
Volatility 3 Framework 2.20.1
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime  ExitTime File output

4       0       System  0xe0005f273040  98      -       N/A     False   2020-09-19 01:22:38.000000 UTC       N/A     Disabled
204     4       smss.exe        0xe00060354900  2       -       N/A     False   2020-09-19 01:22:38.000000 UTC       N/A     Disabled
324     316     csrss.exe       0xe000602c2080  8       -       0       False   2020-09-19 01:22:39.000000 UTC       N/A     Disabled
404     316     wininit.exe     0xe000602cc900  1       -       0       False   2020-09-19 01:22:40.000000 UTC       N/A     Disabled
412     396     csrss.exe       0xe000602c1900  10      -       1       False   2020-09-19 01:22:40.000000 UTC       N/A     Disabled
452     404     services.exe    0xe00060c11080  5       -       0       False   2020-09-19 01:22:40.000000 UTC       N/A     Disabled
460     404     lsass.exe       0xe00060c0e080  31      -       0       False   2020-09-19 01:22:40.000000 UTC       N/A     Disabled
492     396     winlogon.exe    0xe00060c2a080  4       -       1       False   2020-09-19 01:22:40.000000 UTC       N/A     Disabled
640     452     svchost.exe     0xe00060c84900  8       -       0       False   2020-09-19 01:22:40.000000 UTC       N/A     Disabled
684     452     svchost.exe     0xe00060c9a700  6       -       0       False   2020-09-19 01:22:40.000000 UTC       N/A     Disabled
800     452     svchost.exe     0xe00060ca3900  12      -       0       False   2020-09-19 01:22:40.000000 UTC       N/A     Disabled
808     492     dwm.exe 0xe00060d09680  7       -       1       False   2020-09-19 01:22:40.000000 UTC       N/A     Disabled
848     452     svchost.exe     0xe00060d1e080  39      -       0       False   2020-09-19 01:22:41.000000 UTC       N/A     Disabled
928     452     svchost.exe     0xe00060d5d500  16      -       0       False   2020-09-19 01:22:41.000000 UTC       N/A     Disabled
1000    452     svchost.exe     0xe00060da2080  18      -       0       False   2020-09-19 01:22:41.000000 UTC       N/A     Disabled
668     452     svchost.exe     0xe00060e09900  16      -       0       False   2020-09-19 01:22:41.000000 UTC       N/A     Disabled
1292    452     Microsoft.Acti  0xe00060f73900  9       -       0       False   2020-09-19 01:22:57.000000 UTC       N/A     Disabled
1332    452     dfsrs.exe       0xe00060fe1900  16      -       0       False   2020-09-19 01:22:57.000000 UTC       N/A     Disabled
1368    452     dns.exe 0xe00060ff3080  16      -       0       False   2020-09-19 01:22:57.000000 UTC       N/A     Disabled
1392    452     ismserv.exe     0xe00060ff7900  6       -       0       False   2020-09-19 01:22:57.000000 UTC       N/A     Disabled
1556    452     VGAuthService.  0xe000614aa200  2       -       0       False   2020-09-19 01:22:57.000000 UTC       N/A     Disabled
1600    452     vmtoolsd.exe    0xe00061a30900  9       -       0       False   2020-09-19 01:22:57.000000 UTC       N/A     Disabled
1644    452     wlms.exe        0xe00061a9a800  2       -       0       False   2020-09-19 01:22:57.000000 UTC       N/A     Disabled
1660    452     dfssvc.exe      0xe00061a9b2c0  11      -       0       False   2020-09-19 01:22:57.000000 UTC       N/A     Disabled
1956    452     svchost.exe     0xe0006291b7c0  30      -       0       False   2020-09-19 01:23:20.000000 UTC       N/A     Disabled
796     452     vds.exe 0xe000629b3080  11      -       0       False   2020-09-19 01:23:20.000000 UTC       N/A     Disabled
1236    452     svchost.exe     0xe000629926c0  8       -       0       False   2020-09-19 01:23:21.000000 UTC       N/A     Disabled
2056    640     WmiPrvSE.exe    0xe000629de900  11      -       0       False   2020-09-19 01:23:21.000000 UTC       N/A     Disabled
2216    452     dllhost.exe     0xe00062a26900  10      -       0       False   2020-09-19 01:23:21.000000 UTC       N/A     Disabled
2460    452     msdtc.exe       0xe00062a2a900  9       -       0       False   2020-09-19 01:23:21.000000 UTC       N/A     Disabled
3724    452     spoolsv.exe     0xe000631cb900  13      -       0       False   2020-09-19 03:29:40.000000 UTC       N/A     Disabled
3644    2244    coreupdater.ex  0xe00062fe7700  0       -       2       False   2020-09-19 03:56:37.000000 UTC       2020-09-19 03:56:52.000000 UTC  Disabled
3796    848     taskhostex.exe  0xe00062f04900  7       -       1       False   2020-09-19 04:36:03.000000 UTC       N/A     Disabled
3472    3960    explorer.exe    0xe00063171900  39      -       1       False   2020-09-19 04:36:03.000000 UTC       N/A     Disabled
400     1904    ServerManager.  0xe00060ce2080  10      -       1       False   2020-09-19 04:36:03.000000 UTC       N/A     Disabled
3260    3472    vm3dservice.ex  0xe00063299280  1       -       1       False   2020-09-19 04:36:14.000000 UTC       N/A     Disabled
2608    3472    vmtoolsd.exe    0xe00062ede1c0  8       -       1       False   2020-09-19 04:36:14.000000 UTC       N/A     Disabled
2840    3472    FTK Imager.exe  0xe00063021900  9       -       1       False   2020-09-19 04:37:04.000000 UTC       N/A     Disabled
3056    848     WMIADAP.exe     0xe0006313f900  5       -       0       False   2020-09-19 04:37:42.000000 UTC       N/A     Disabled
2764    640     WmiPrvSE.exe    0xe00062c0a900  6       -       0       False   2020-09-19 04:37:42.000000 UTC       N/A     Disabled
```

   L'examen du cache web avec **Autopsy** a révélé une connexion HTTP vers l'IP **194.61.24.102**, associée au téléchargement du fichier **coreupdater.exe**

, identifié comme un cheval de Troie par **VirusTotal.**





timeline : 04:24:50 +1 téléchargement du fichier coreupdater.exe probable

```
hello@hello-HP-EliteBook-x360-1030-G2:~/volatility3$ python3 vol.py -f /home/hello/Desktop/citadeldc01.mem windows.filescan.FileScan | grep "coreupdater.exe"
0x130ddf20 100.0\Windows\System32\coreupdater.exereupdater.exe.2424urv.partial
0x2082ff20      \Windows\System32\coreupdater.exereupdater.exe
0x52317f20      \Windows\System32\coreupdater.exereupdater.exe.2424urv.partial
0x5faa4f20      \Windows\System32\coreupdater.exereupdater.exe
```

étant donné que le nom est associé à des comportements malveillants, cela soulève des suspicions. Les variations de nom comme `coreupdater.exereupdater.exe.2424urv.partial` peuvent aussi indiquer un fichier partiellement téléchargé ou une tentative de camouflage.

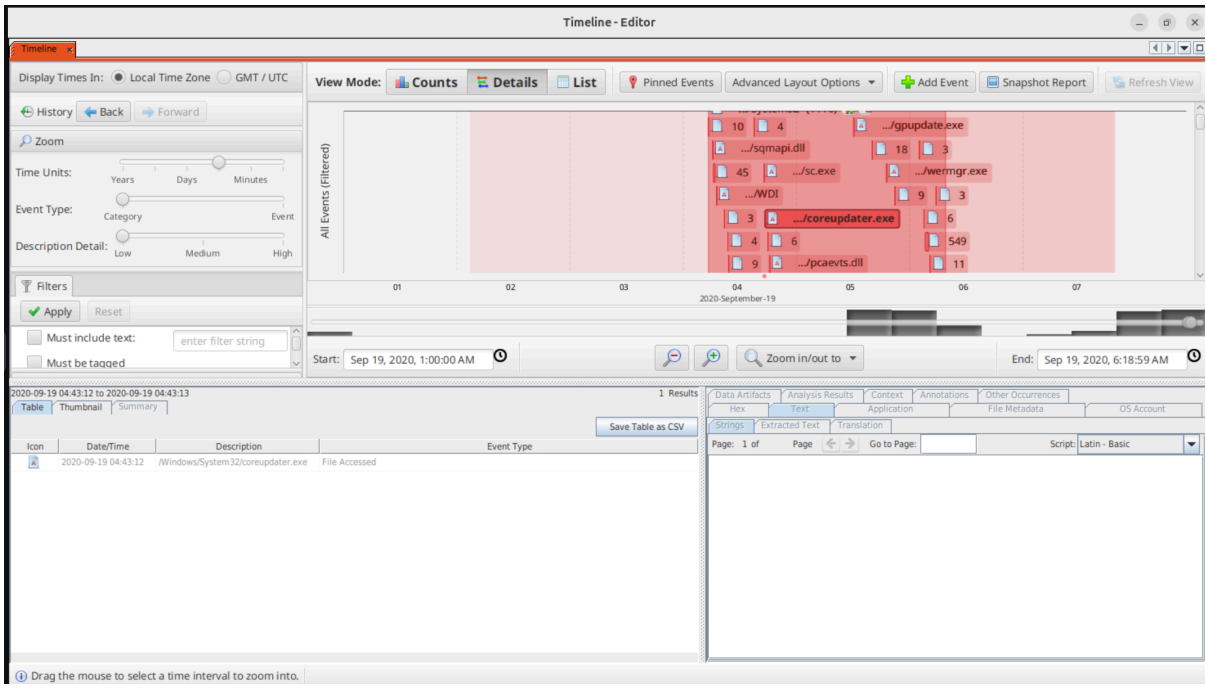
Les fichiers avec des suffixes comme `.2424urv.partial` suggèrent qu'il pourrait s'agir de fichiers malveillants qui sont en cours d'exécution ou ont été téléchargés partiellement. Ces fichiers partiels sont souvent créés lors du téléchargement ou de l'exécution de logiciels malveillants et peuvent ne pas avoir été complètement chargés en mémoire

- Le fichier a été installé dans **C:\Windows\System32 (event 7045),** en tant que service, ce qui confirme sa persistance. (**hayabusa logs**):

“””2020-09-19 04:42:42.676 +01:00 ǁ DESKTOP-SDN1RPT.C137.local ǁ Sys ǁ **7045** ǁ info ǁ 958 ǁ Svc

Installed ǁ Svc: coreupdater ¦ Path: C:\Windows\System32\coreupdater.exe ¦ Acct: LocalSystem

¦ StartType: auto start ǁ ServiceType: user mode service”””



- **une désactivation de la protection en temps réel** de **Windows Defender** (**hayabusa logs**):

“”2020-09-19 04:39:45.247 +01:00 ǁ DESKTOP-SDN1RPT.C137.local ǁ Defender ǁ 5001 ǁ high ǁ 36

ǁ Windows Defender Real-time Protection Disabled ǁ Product Name: %%827 ¦ Product Version:

4.18.2009.2 ǁ Product Name: %%827 ¦ Product Version: 4.18.2009.2””

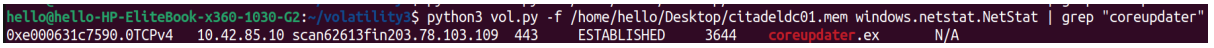
Liste des IOCs Curés :

- `194.61.24.102` : Origine des attaques par force brute et RDP.
- `10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6` : Fichier malware.(Capacités : Exécution de commandes, persistance)

Analyse du payload

Activités Observées sur CITADEL-DC01 :

1. Installation du malware `coreupdater.exe`, configuré comme un service de démarrage.
2. Établissement de connexions réseau vers une IP malveillante : `203.78.103.109` identifier (**netstat** et **netscan**)

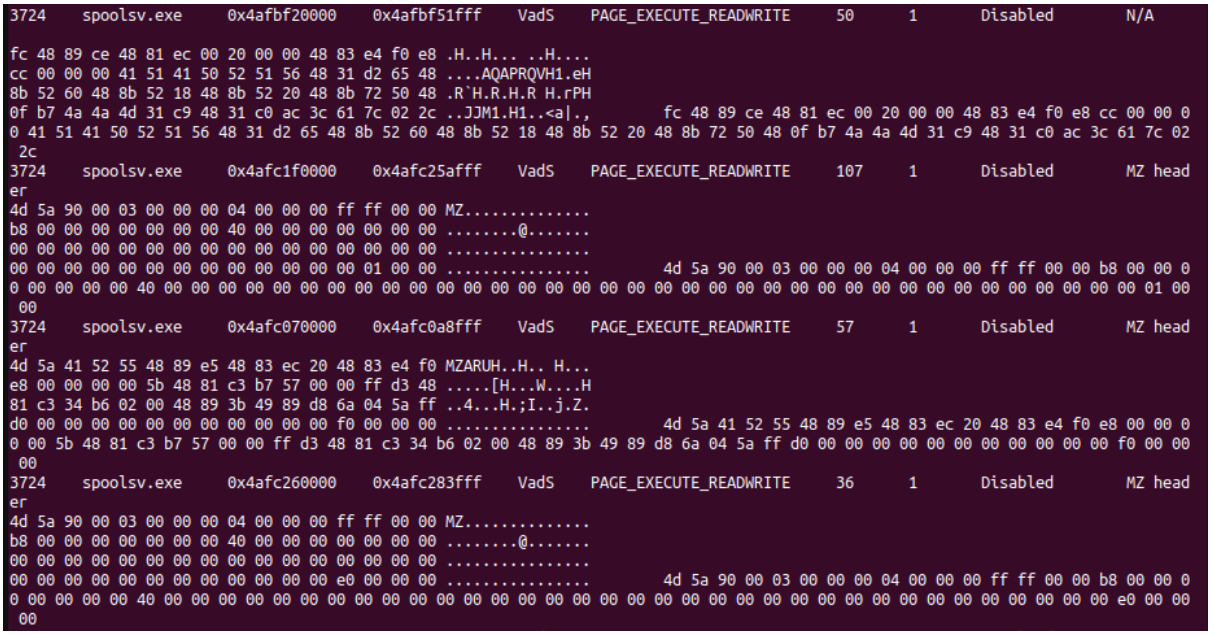


La sortie indique qu'une connexion réseau TCP est établie entre l'ordinateur local (adresse IP 10.42.85.10) et une machine distante (adresse IP 203.78.103.109), en utilisant le port sécurisé HTTPS (443). Cette connexion est liée au processus "coreupdater.ex", avec un identifiant de processus (PID) 3644, suggérant qu'un processus de mise à jour est en cours d'exécution.

3. (Thaïlande).

Decimal:	3410913133
Hostname:	203.78.103.109
ASN:	18362
ISP:	Netway Communication Co. Ltd.
Services:	Datacenter
Country:	Thailand
State/Region:	Krung Thep Maha Nakhon
City:	Bangkok
Latitude:	13.7500 (13° 44′ 59.91″ N)
Longitude:	100.5168 (100° 31′ 0.53″ E)

4. L'utilisation de **malfind** permet de constater que le processus **spoolsv.exe** apparaît à plusieurs reprises et est identifié comme un code suspect



hypothèse : Création d'une porte dérobée via spoolsv.exe.

Analyse du processus `spoolsv.exe` dans le cadre d'un examen de sécurité

Le processus `spoolsv.exe` est généralement un composant légitime du système Windows, responsable de la gestion des tâches d'impression (spooler d'impression). Cependant, il est parfois ciblé pour l'injection de malwares. L'examen des segments mémoire et des comportements associés à ce processus peut fournir des indices précieux sur des activités malveillantes potentielles.

Contexte du processus `spoolsv.exe`

- **Nom du processus** : `spoolsv.exe` est un processus légitime utilisé par Windows pour gérer le spooler d'impression.
- **Localisation** : Normalement, `spoolsv.exe` se trouve dans le répertoire système : `C:\Windows\System32\spoolsv.exe`.

Comportements suspects

Certaines plages mémoire associées à ce processus montrent des comportements qui suggèrent des anomalies.

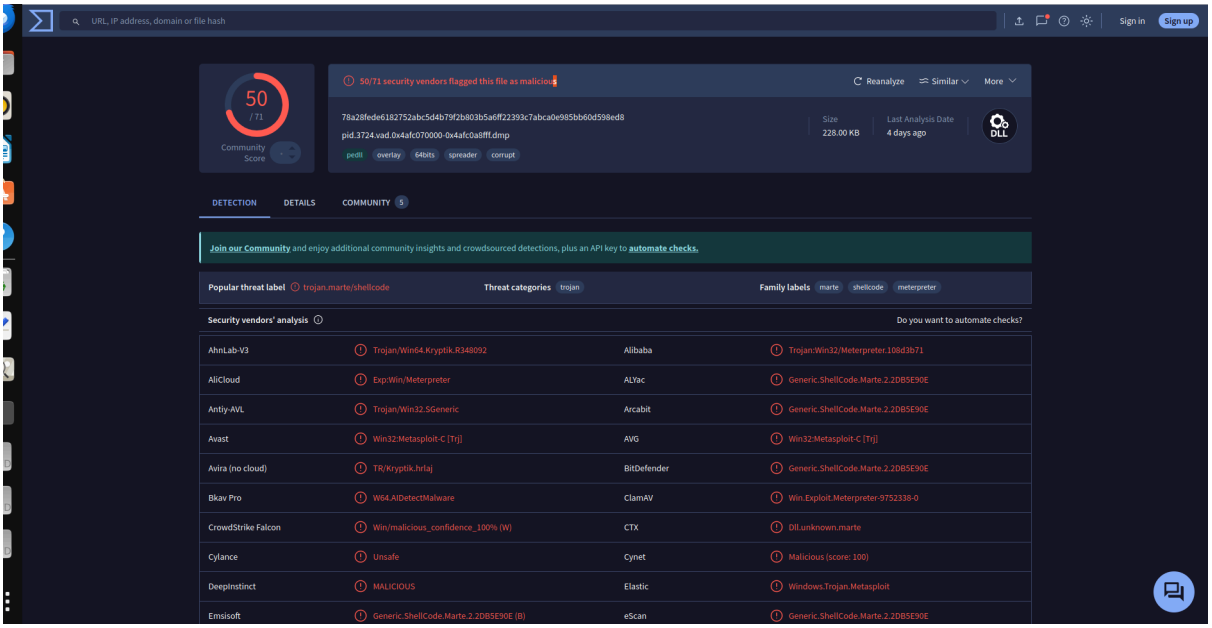
1. **Plages mémoire avec permissions `PAGE_EXECUTE_READWRITE`** Les plages mémoire suivantes sont configurées avec des permissions `PAGE_EXECUTE_READWRITE`, permettant à la fois l'exécution de code et son écriture dans la même zone mémoire. Ces permissions sont fréquemment utilisées par les malwares pour injecter du code dans des processus légitimes, tels que `spoolsv.exe`, et contourner la détection antivirus.
    - 0x4afbf20000 à 0x4afbf51fff (50 Ko)

    - 0x4afc1f0000 à 0x4afc25afff (107 Ko)
    - **0x4afc070000 à 0x4afc0a8fff (57 Ko)**
    - 0x4afc260000 à 0x4afc283fff (36 Ko)
2. **Présence d'en-têtes MZ** Les en-têtes MZ, caractéristiques des fichiers exécutables Windows (.exe), ont été détectés dans plusieurs segments mémoire associés au processus `spoolsv.exe`. Cela suggère la possibilité d'injection de fichiers exécutables malveillants dans ce processus légitime.
    - 0x4afc1f0000 à 0x4afc25afff
    - **0x4afc070000 à 0x4afc0a8fff**
    - 0x4afc260000 à 0x4afc283fff
3. **Code hexadécimal suspect** Des extraits du code hexadécimal associé à ces segments mémoire montrent des instructions typiques des fichiers exécutables Windows, ce qui renforce l'hypothèse d'une tentative d'injection de malwares.
   Exemples d'extraits hexadécimaux :
    - `fc 48 89 ce 48 81 ec 00 20 00 00 48 83 e4 f0 e8 ...`
    - `4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 ...`
    - `4d 5a 41 52 55 48 89 e5 48 83 ec 20 48 83 e4 f0 ...`

Évaluation du risque

- **Suspicion de malwares** : L'existence de segments mémoire avec des en-têtes MZ et des permissions d'exécution et d'écriture dans le processus `spoolsv.exe` est un indicateur fort de compromission. Cela suggère la possibilité d'injection de malwares.
- **Injection de code** : L'injection de malwares dans `spoolsv.exe` permettrait à ces derniers de s'exécuter directement en mémoire, sans écrire sur le disque, ce qui complique leur détection par les solutions antivirus classiques.

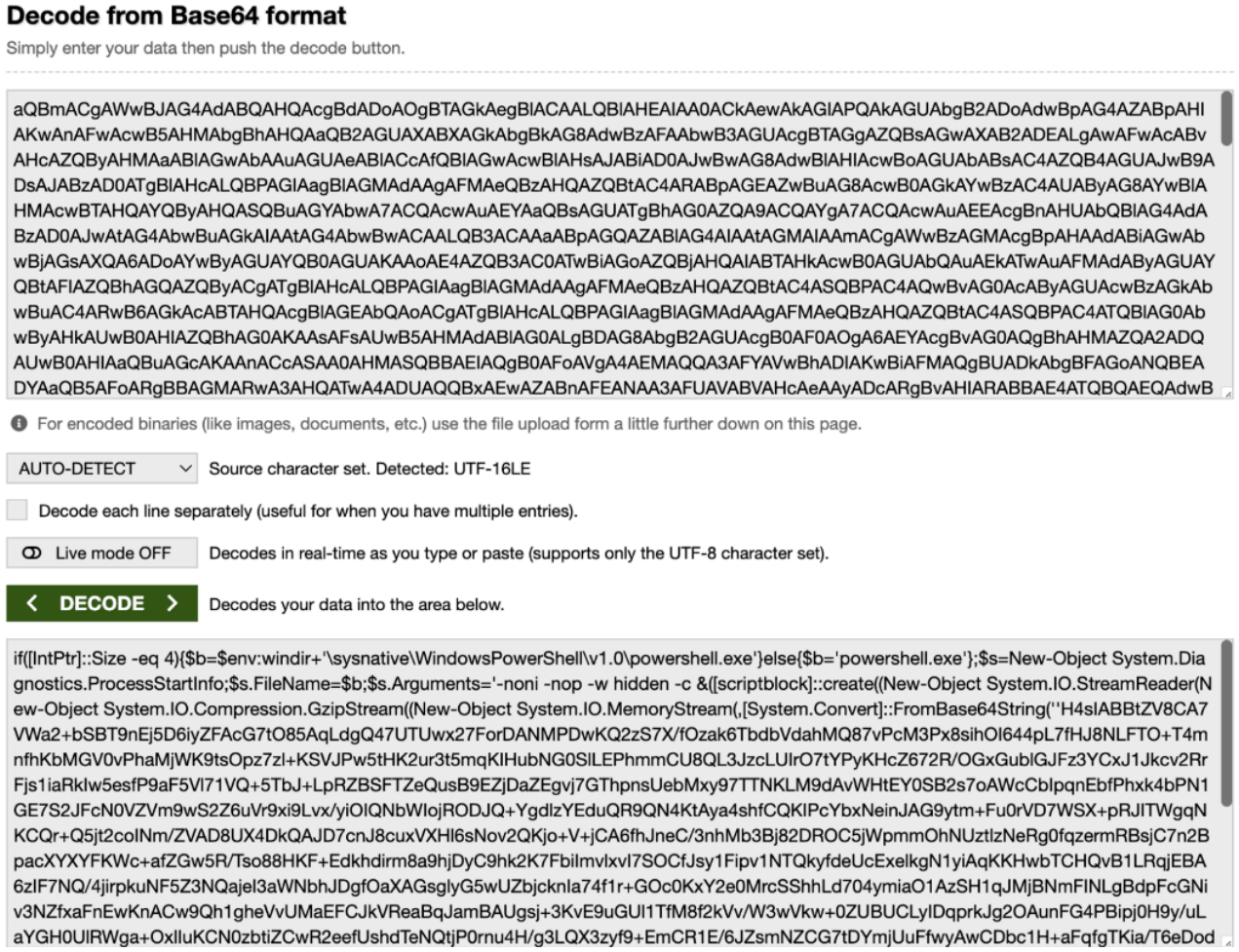
Nous allons examiner ce processus afin de valider cette hypothèse. À cette fin, nous soumettrons le dump du processus **spoolsv.exe** à VirusTotal pour en analyser la légitimité, comme le montre la figure ci-dessous.



> On constate que `spoolsv.exe` présente les mêmes caractéristiques que `coreupdater.exe`, ce qui laisse supposer que `spoolsv.exe` pourrait s'être injecté dans `coreupdater.exe`

Registre

après savoir examiné le fichier registry.key du contrôleur de domaine. on remarqué deux clés de registre inhabituelles, à savoir 9sEoCawv et CTzcLy6E apres avoir analyser cela, nous examinons la clé de registre **9sEoCawv**, qui est encodée en base64. Nous tentons ensuite de la déchiffrer, comme illustré dans l'image ci-dessous.



Il s'agit d'un script PowerShell. Cela nous renvoie des données au format GZip. En utilisant un autre outil de décompression, nous obtenons à nouveau des données en PowerShell, semblant implémenter une technique d'injection de code en mémoire dans un processus distant. Cela suscite la question de savoir si l'attaquant n'a pas tenté d'exfiltrer des données

Description Technique :

- `Volatility` a révélé des pages mémoire injectées dans `spoolsv.exe`, contenant du code exécutable. Les journaux réseau ont indiqué un trafic sortant vers `203.78.103.109` via les ports `443` .

Analyse du Malware

Un Malware a-t-il été Utilisé ? Oui.

1. **Localisation sur le Disque :**
    - Trouvé à : `C:\Windows\System32\coreupdater.exe`
2. **Première Apparition :** Peu après l'attaque par force brute.
3. **Source :** Téléchargé via HTTP depuis `194.61.24.102`.
4. **Méthode de Livraison :** Déploiement manuel après accès RDP.
5. **Communication C2 :** Connecté à `203.78.103.109` (Thaïlande).
6. **Capacités :**
    - Exécution de commandes à distance.
    - Exfiltration de données probables.
    - Persistance via un service de redémarrage automatique.
7. **Détails de Persistance :**
    - Clés de registre modifiées pour garantir l'exécution au démarrage.

Renseignement sur les Menaces, Deuxième Tour

Nouveaux IOCs Identifiés :

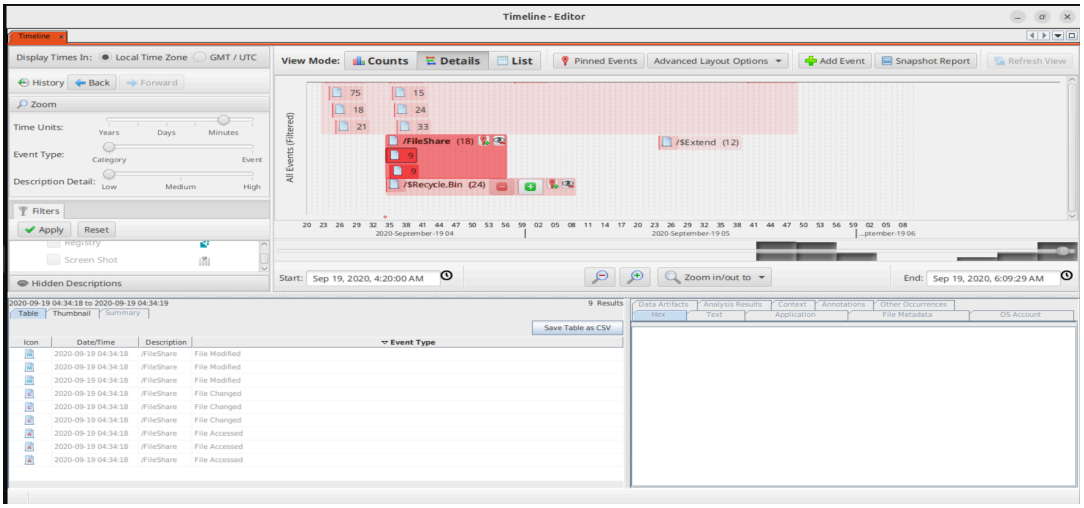
- Adresse IP : `203.78.103.109`
    - Activité : Infrastructure malveillante hébergeant le serveur C2.
    - Contexte : Liée à des campagnes de malware et des activités d'exfiltration(probables) .

Liste des IOCs Mise à Jour :

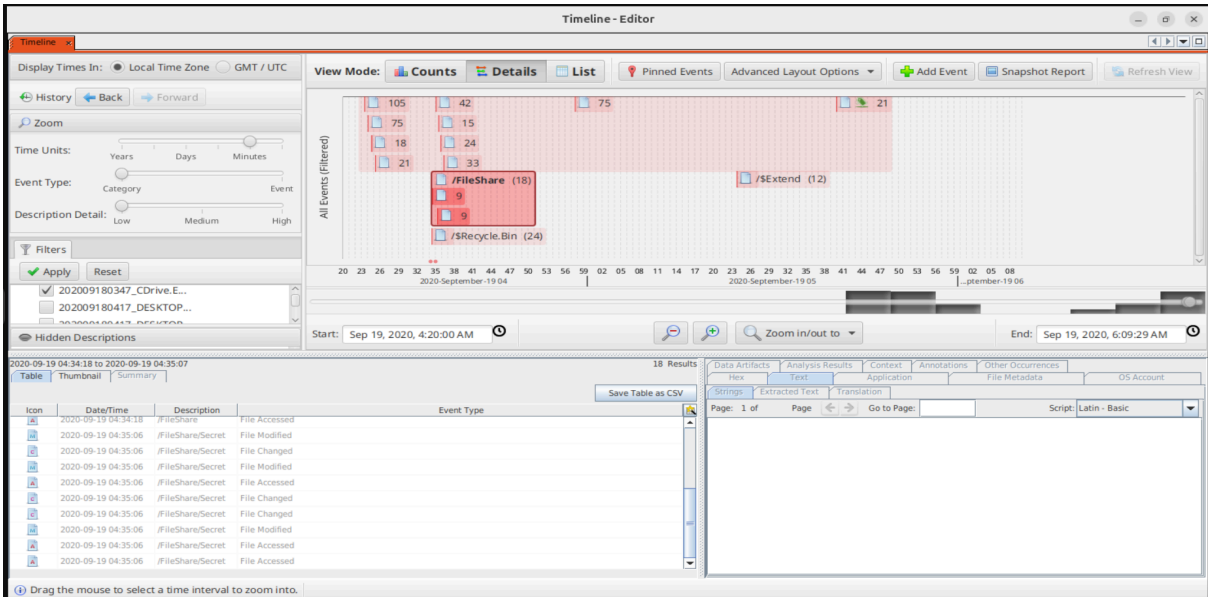
1. `194.61.24.102` (Origine des attaques par force brute).
2. `203.78.103.109` (Serveur C2).
3. `10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6` (Hash du malware).

Analyse des Données Sensibles

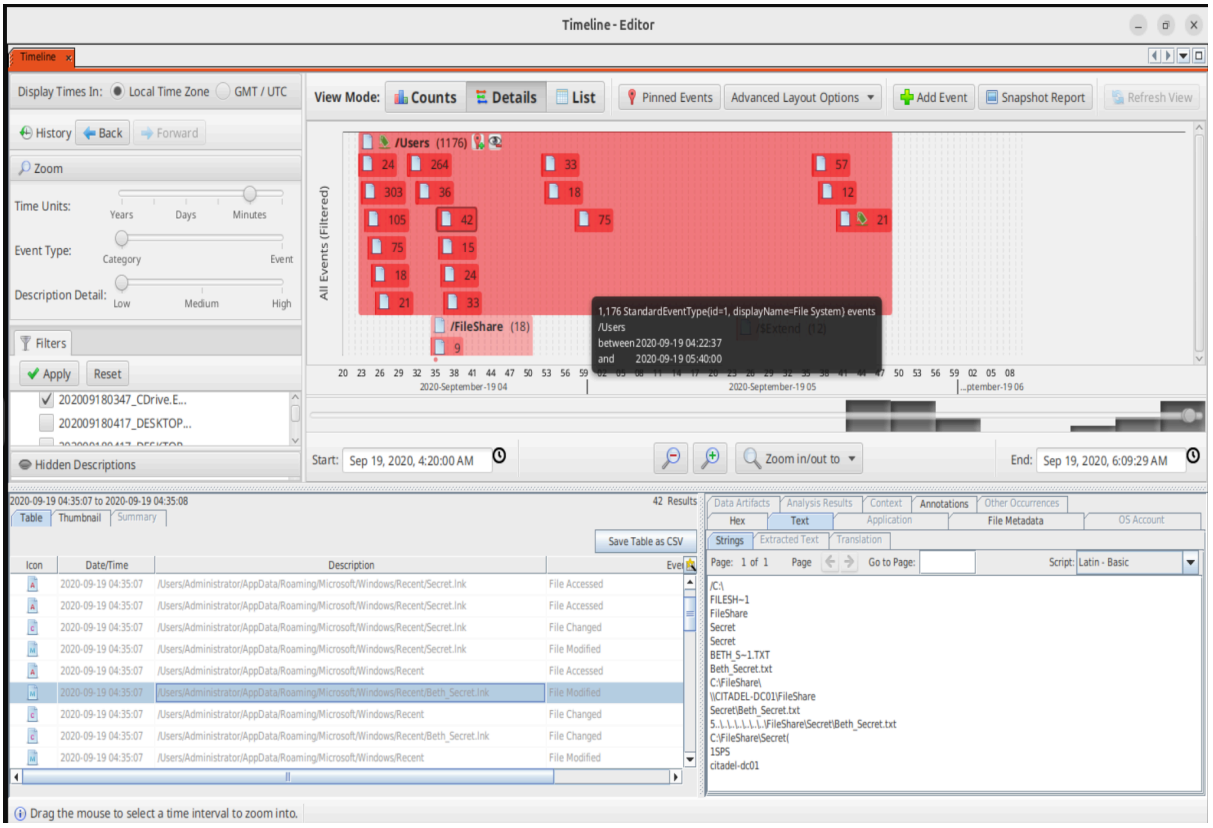
Fichiers récemment ouverts :



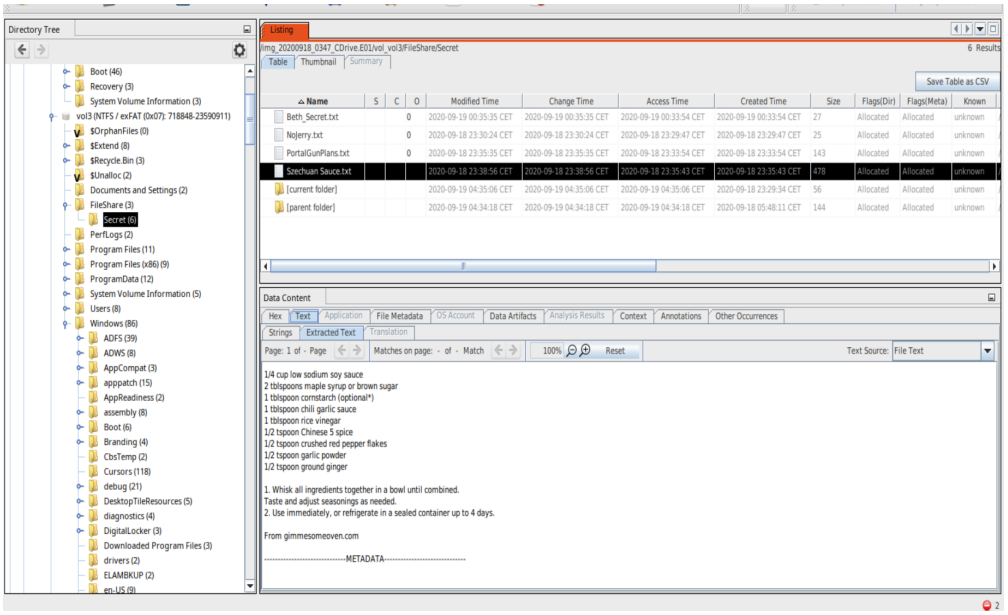
04:34:18 +1 : accès et modification de fichier dans `C:\FileShare`



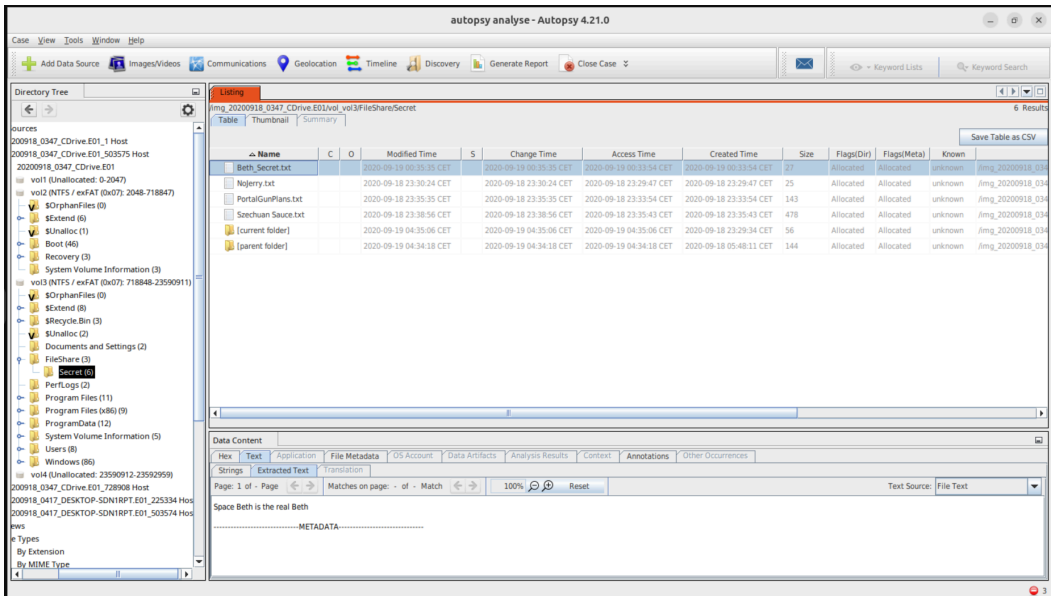
`04:35:07` : accès et modification de fichier dans `C:\FileShare\Secret\`



1. **Fichiers Critiques Identifiés :**
    - Szechuan Sauce.txt

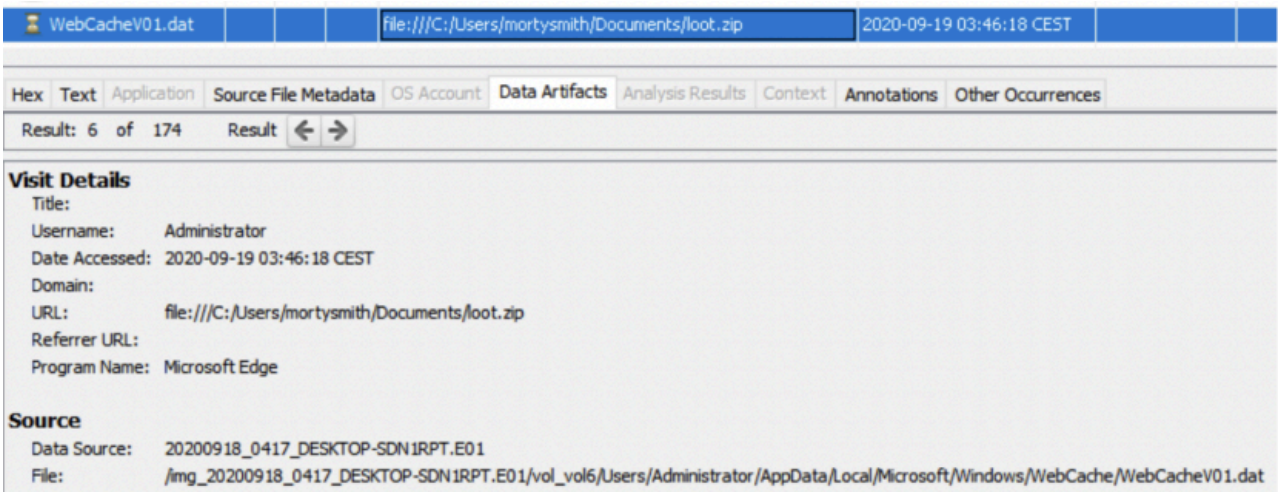


- `SECRET_Beth.txt`

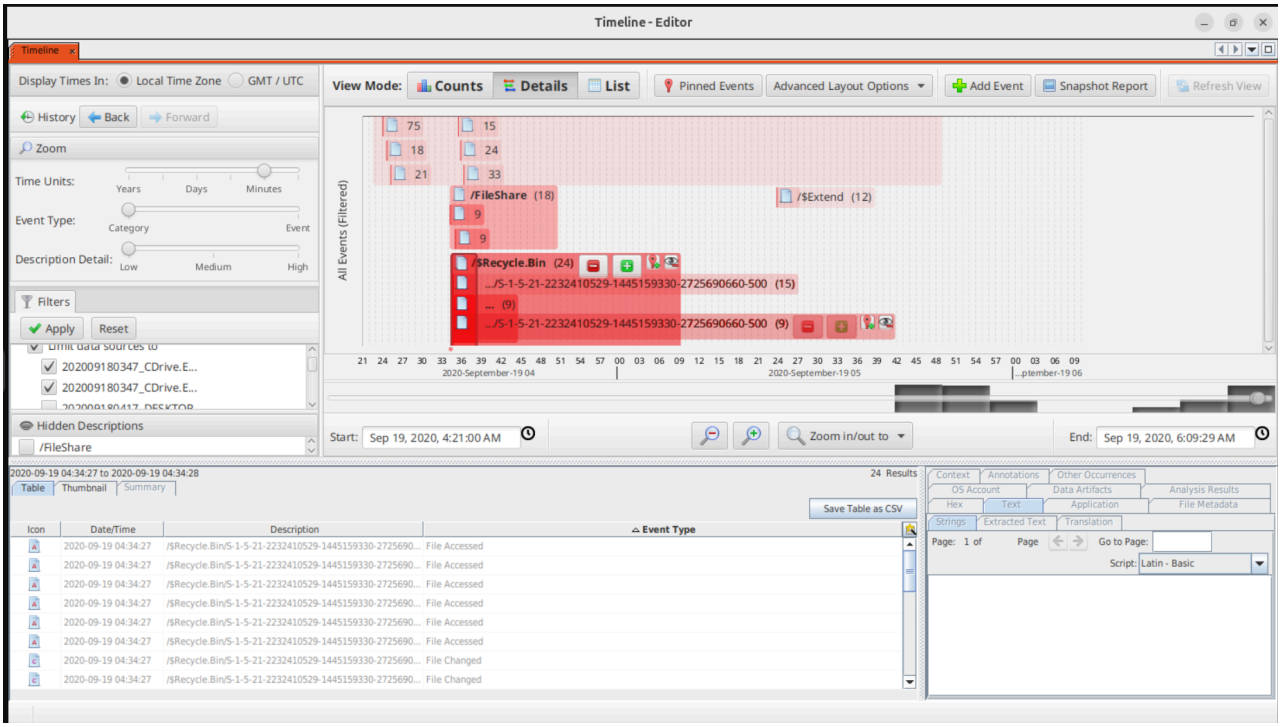


2. **Localisation des Fichiers :**
   - Stockés dans `C:\FileShare\Secret\`.

3. **Détails d'Exfiltration :**
   - Les fichiers ont été compressés dans `loot.zip` et téléchargés.



1. Activité dans `$Recycle.Bin` (04:34:27) :



	A	B	C	D	E	F	G
1	Icon	Date/Time	Description	Event Type			
2	true	2020-09-19 04:34:27	/$Recycle.Bin/S-1-5-21-2232410529-1445159330-2725690660-500	File Modified			
3	true	2020-09-19 04:34:27	/$Recycle.Bin/S-1-5-21-2232410529-1445159330-2725690660-500/$IU2L112.txt	File Accessed			
4	true	2020-09-19 04:34:27	/$Recycle.Bin/S-1-5-21-2232410529-1445159330-2725690660-500	File Changed			
5	true	2020-09-19 04:34:27	/$Recycle.Bin/S-1-5-21-2232410529-1445159330-2725690660-500/$IU2L112.txt	File Created			
6	true	2020-09-19 04:34:27	/$Recycle.Bin/S-1-5-21-2232410529-1445159330-2725690660-500/$IU2L112.txt	File Accessed			
7	true	2020-09-19 04:34:27	/$Recycle.Bin/S-1-5-21-2232410529-1445159330-2725690660-500	File Modified			
8	true	2020-09-19 04:34:27	/$Recycle.Bin/S-1-5-21-2232410529-1445159330-2725690660-500/$IU2L112.txt	File Created			
9	true	2020-09-19 04:34:27	/$Recycle.Bin/S-1-5-21-2232410529-1445159330-2725690660-500	File Changed			
10	true	2020-09-19 04:34:27	/$Recycle.Bin/S-1-5-21-2232410529-1445159330-2725690660-500	File Accessed			
11	true	2020-09-19 04:34:27	/$Recycle.Bin/S-1-5-21-2232410529-1445159330-2725690660-500	File Accessed			
12	true	2020-09-19 04:34:27	/$Recycle.Bin/S-1-5-21-2232410529-1445159330-2725690660-500/$RU2L112.txt	File Changed			
13	true	2020-09-19 04:34:27	/$Recycle.Bin/S-1-5-21-2232410529-1445159330-2725690660-500	File Accessed			
14	true	2020-09-19 04:34:27	/$Recycle.Bin/S-1-5-21-2232410529-1445159330-2725690660-500	File Changed			
15	true	2020-09-19 04:34:27	/$Recycle.Bin/S-1-5-21-2232410529-1445159330-2725690660-500/$IU2L112.txt	File Modified			
16	true	2020-09-19 04:34:27	/$Recycle.Bin/S-1-5-21-2232410529-1445159330-2725690660-500	File Modified			
17	true	2020-09-19 04:34:27	/$Recycle.Bin/S-1-5-21-2232410529-1445159330-2725690660-500/$IU2L112.txt	File Changed			
18	true	2020-09-19 04:34:27	/$Recycle.Bin/S-1-5-21-2232410529-1445159330-2725690660-500/$IU2L112.txt	File Created			
19	true	2020-09-19 04:34:27	/$Recycle.Bin/S-1-5-21-2232410529-1445159330-2725690660-500/$IU2L112.txt	File Accessed			
20	true	2020-09-19 04:34:27	/$Recycle.Bin/S-1-5-21-2232410529-1445159330-2725690660-500/$IU2L112.txt	File Changed			
21	true	2020-09-19 04:34:27	/$Recycle.Bin/S-1-5-21-2232410529-1445159330-2725690660-500/$IU2L112.txt	File Modified			
22	true	2020-09-19 04:34:27	/$Recycle.Bin/S-1-5-21-2232410529-1445159330-2725690660-500/$RU2L112.txt	File Changed			
23	true	2020-09-19 04:34:27	/$Recycle.Bin/S-1-5-21-2232410529-1445159330-2725690660-500/$RU2L112.txt	File Changed			
24	true	2020-09-19 04:34:27	/$Recycle.Bin/S-1-5-21-2232410529-1445159330-2725690660-500/$IU2L112.txt	File Modified			
25	true	2020-09-19 04:34:27	/$Recycle.Bin/S-1-5-21-2232410529-1445159330-2725690660-500/$IU2L112.txt	File Changed			
26							
27							
28							
29							
30							

- **Fichiers `$IU2L112.txt` et `$RU2L112.txt`** :
  - Création, modification et accès répétés à ces fichiers dans le dossier `$Recycle.Bin`, qui est utilisé par Windows pour stocker les fichiers supprimés.
  - Ces fichiers pourraient contenir des données sensibles qui ont été supprimées mais récupérées ou manipulées par un attaquant.
- **Activité suspecte** :
  - La modification et l'accès répétés à ces fichiers suggèrent une tentative de récupération ou de manipulation de données supprimées, potentiellement dans le cadre d'une exfiltration.

---

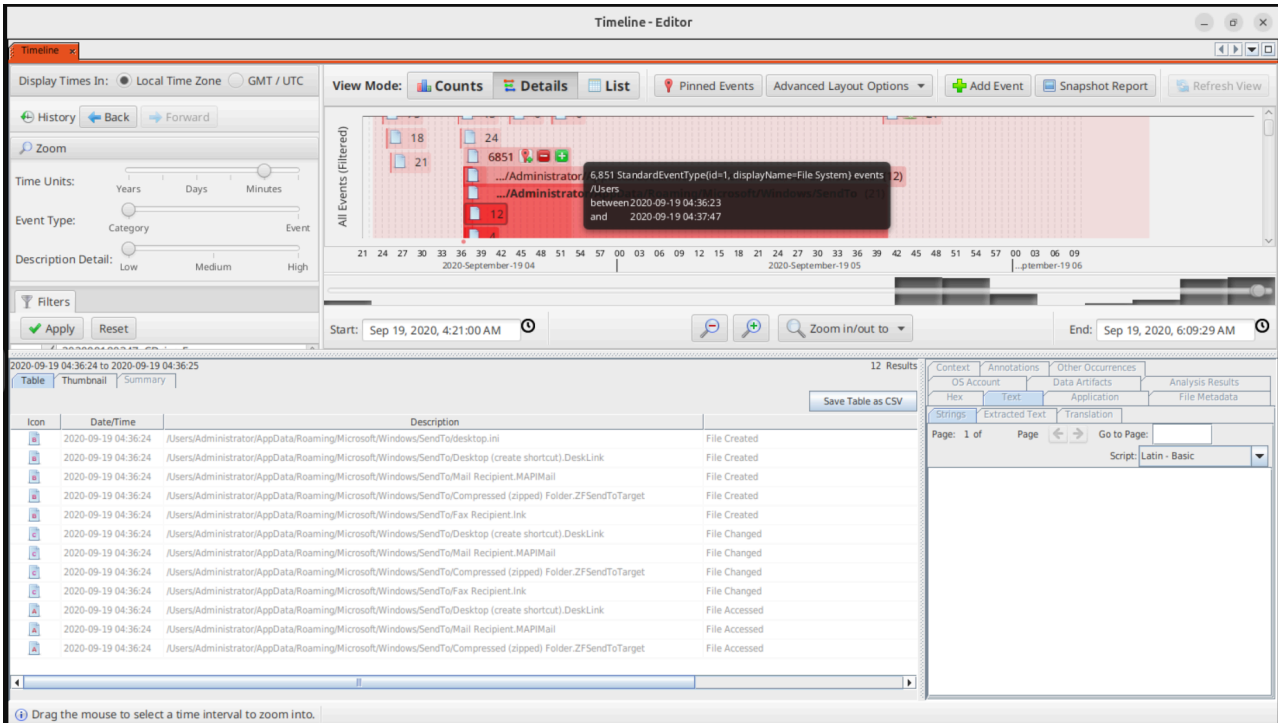
2. Activité dans `FileShare` (04:34:18 et 04:35:06) :

	A	B	C	D
1	Icon	Date/Time	Description	Event Type
2	true	2020-09-19 04:34:18	/FileShare	File Accessed
3	true	2020-09-19 04:34:18	/FileShare	File Changed
4	true	2020-09-19 04:34:18	/FileShare	File Modified
5	true	2020-09-19 04:34:18	/FileShare	File Modified
6	true	2020-09-19 04:34:18	/FileShare	File Changed
7	true	2020-09-19 04:34:18	/FileShare	File Modified
8	true	2020-09-19 04:34:18	/FileShare	File Changed
9	true	2020-09-19 04:34:18	/FileShare	File Accessed
10	true	2020-09-19 04:34:18	/FileShare	File Accessed
11	true	2020-09-19 04:35:06	/FileShare/Secret	File Modified
12	true	2020-09-19 04:35:06	/FileShare/Secret	File Changed
13	true	2020-09-19 04:35:06	/FileShare/Secret	File Modified
14	true	2020-09-19 04:35:06	/FileShare/Secret	File Accessed
15	true	2020-09-19 04:35:06	/FileShare/Secret	File Changed
16	true	2020-09-19 04:35:06	/FileShare/Secret	File Changed
17	true	2020-09-19 04:35:06	/FileShare/Secret	File Modified
18	true	2020-09-19 04:35:06	/FileShare/Secret	File Accessed
19	true	2020-09-19 04:35:06	/FileShare/Secret	File Accessed
20				

- **Dossier `FileShare`** :
  - Plusieurs événements "File Modified", "File Changed" et "File Accessed" indiquent une activité intense sur ce dossier, qui est souvent utilisé pour partager des fichiers sur un réseau.
  - Le sous-dossier `Secret` a également été modifié et consulté, ce qui suggère que des fichiers sensibles ont été ciblés.
- **Scénario possible** :
  - Un attaquant a pu accéder à ce dossier pour identifier et exfiltrer des fichiers sensibles.

---

3. Activité dans SendTo (04:36:24 et 04:36:43) :

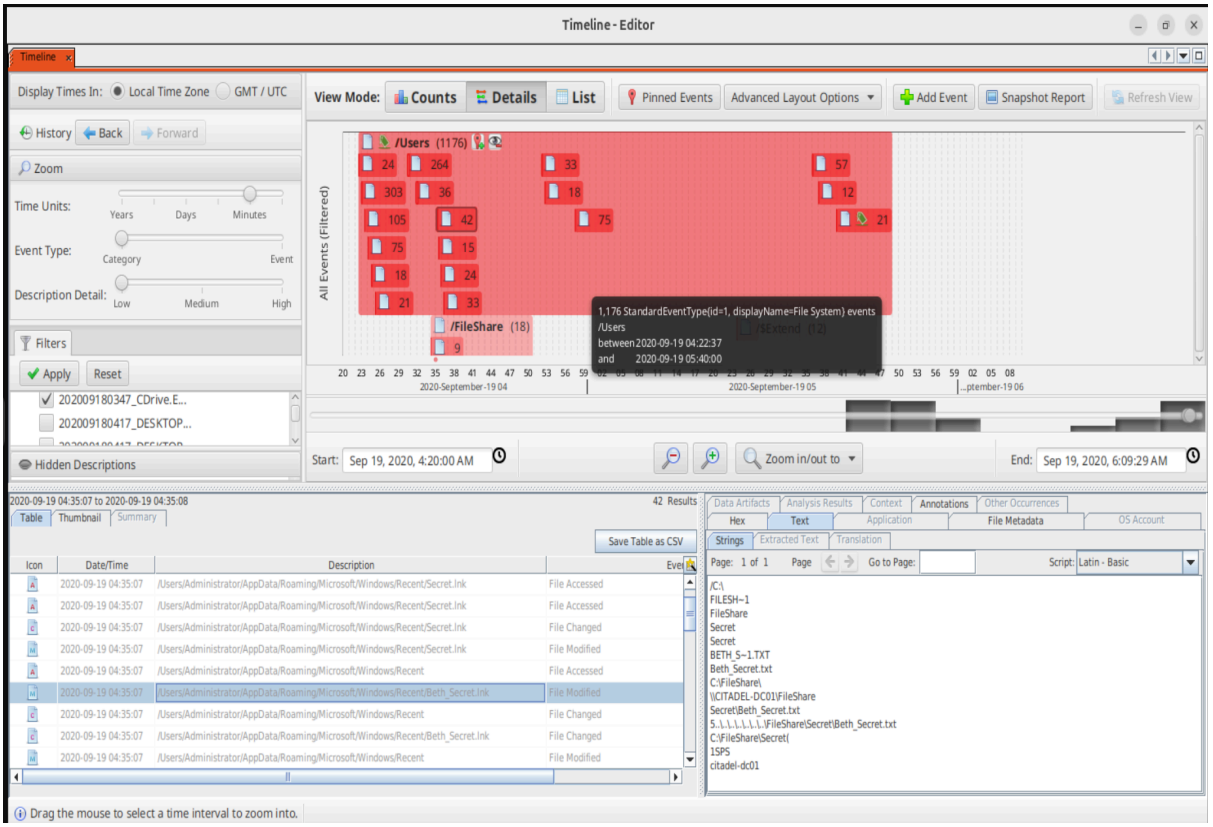


	A	B	C	D
1	Icon	Date/Time	Description	Event Type
2	true	2020-09-19 04:36:24	/Users/Administrator/AppData/Roaming/Microsoft/Windows/SendTo/desktop.ini	File Created
3	true	2020-09-19 04:36:24	/Users/Administrator/AppData/Roaming/Microsoft/Windows/SendTo/Desktop (create shortcut).DeskLink	File Changed
4	true	2020-09-19 04:36:24	/Users/Administrator/AppData/Roaming/Microsoft/Windows/SendTo/Mail Recipient.MAPIMail	File Changed
5	true	2020-09-19 04:36:24	/Users/Administrator/AppData/Roaming/Microsoft/Windows/SendTo/Desktop (create shortcut).DeskLink	File Accessed
6	true	2020-09-19 04:36:24	/Users/Administrator/AppData/Roaming/Microsoft/Windows/SendTo/Mail Recipient.MAPIMail	File Accessed
7	true	2020-09-19 04:36:24	/Users/Administrator/AppData/Roaming/Microsoft/Windows/SendTo/Desktop (create shortcut).DeskLink	File Created
8	true	2020-09-19 04:36:24	/Users/Administrator/AppData/Roaming/Microsoft/Windows/SendTo/Mail Recipient.MAPIMail	File Created
9	true	2020-09-19 04:36:24	/Users/Administrator/AppData/Roaming/Microsoft/Windows/SendTo/Compressed (zipped) Folder.ZFSendToTarget	File Changed
10	true	2020-09-19 04:36:24	/Users/Administrator/AppData/Roaming/Microsoft/Windows/SendTo/Fax Recipient.lnk	File Changed
11	true	2020-09-19 04:36:24	/Users/Administrator/AppData/Roaming/Microsoft/Windows/SendTo/Compressed (zipped) Folder.ZFSendToTarget	File Accessed
12	true	2020-09-19 04:36:24	/Users/Administrator/AppData/Roaming/Microsoft/Windows/SendTo/Compressed (zipped) Folder.ZFSendToTarget	File Created
13	true	2020-09-19 04:36:24	/Users/Administrator/AppData/Roaming/Microsoft/Windows/SendTo/Fax Recipient.lnk	File Created
14				

- **Fichiers dans SendTo** :
  - Création et modification de fichiers tels que `desktop.ini`, `Desktop (create shortcut).DeskLink`, `Mail Recipient.MAPIMail`, et `Bluetooth File Transfer.LNK`.
  - Ces fichiers sont liés aux options du menu "Envoyer vers" dans Windows, qui permet d'envoyer des fichiers vers des destinations spécifiques (par exemple, un e-mail, un dossier compressé, ou un appareil Bluetooth).
- **Indicateurs d'exfiltration** :
  - La création de ces fichiers pourrait indiquer qu'un attaquant a configuré des moyens pour exfiltrer des données via des e-mails, des dossiers compressés, ou des transferts Bluetooth.

---

4. Activité dans `Recent` et `AutomaticDestinations` (04:35:07 et 04:36:25) :



	A	B	C	D
1	Icon	Date/Time	Description	Event Type
2	true	2020-09-19 04:36:25	/Users/Administrator/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations/1bc392b8e104a00e.automaticDestinations-ms	File Modified
3	true	2020-09-19 04:36:25	/Users/Administrator/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations/1bc392b8e104a00e.automaticDestinations-ms	File Changed
4	true	2020-09-19 04:36:25	/Users/Administrator/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations/1bc392b8e104a00e.automaticDestinations-ms	File Accessed
5	true	2020-09-19 04:36:25	/Users/Administrator/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations/1bc392b8e104a00e.automaticDestinations-ms	File Created
6	true	2020-09-19 04:36:25	/Users/Administrator/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations	File Modified
7	true	2020-09-19 04:36:25	/Users/Administrator/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations	File Changed
8	true	2020-09-19 04:36:23	/Users/Administrator/AppData/Local/Microsoft/Terminal Server Client/Cache/bcache24.bmc	File Modified
9	true	2020-09-19 04:36:23	/Users/Administrator/AppData/Local/Microsoft/Terminal Server Client/Cache/bcache24.bmc	File Changed
10	true	2020-09-19 04:36:23	/Users/Administrator/AppData/Local/Microsoft/Terminal Server Client/Cache/bcache24.bmc	File Changed
11	true	2020-09-19 04:36:23	/Users/Administrator/AppData/Local/Microsoft/Terminal Server Client/Cache/bcache24.bmc	File Modified
12	true	2020-09-19 04:36:23	/Users/Administrator/AppData/Local/Microsoft/Terminal Server Client/Cache/bcache24.bmc	File Created
13	true	2020-09-19 04:36:23	/Users/Administrator/AppData/Local/Microsoft/Terminal Server Client/Cache/bcache24.bmc	File Accessed
14	true	2020-09-19 04:36:23	/Users/Administrator/AppData/Local/Microsoft/Terminal Server Client/Cache/bcache24.bmc	File Accessed
15	true	2020-09-19 04:36:23	/Users/Administrator/AppData/Local/Microsoft/Terminal Server Client/Cache/bcache24.bmc	File Created
16	true	2020-09-19 04:36:25	/Users/Administrator/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations	File Accessed
17	true	2020-09-19 04:36:25	/Users/Administrator/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations	File Changed
18	true	2020-09-19 04:36:25	/Users/Administrator/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations	File Modified
19	true	2020-09-19 04:36:25	/Users/Administrator/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations/1bc392b8e104a00e.automaticDestinations-ms	File Created
20	true	2020-09-19 04:36:25	/Users/Administrator/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations/1bc392b8e104a00e.automaticDestinations-ms	File Accessed
21	true	2020-09-19 04:36:25	/Users/Administrator/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations/1bc392b8e104a00e.automaticDestinations-ms	File Changed
22	true	2020-09-19 04:36:25	/Users/Administrator/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations/1bc392b8e104a00e.automaticDestinations-ms	File Modified
23	true	2020-09-19 04:36:25	/Users/Administrator/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations	File Accessed
24	true	2020-09-19 04:36:25	/Users/Administrator/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations	File Accessed
25	true	2020-09-19 04:36:25	/Users/Administrator/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations/1bc392b8e104a00e.automaticDestinations-ms	File Modified
26	true	2020-09-19 04:36:23	/Users/Administrator/AppData/Local/Microsoft/Terminal Server Client/Cache/bcache24.bmc	File Created
27	true	2020-09-19 04:36:25	/Users/Administrator/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations/1bc392b8e104a00e.automaticDestinations-ms	File Changed
28	true	2020-09-19 04:36:23	/Users/Administrator/AppData/Local/Microsoft/Terminal Server Client/Cache/bcache24.bmc	File Accessed
29	true	2020-09-19 04:36:23	/Users/Administrator/AppData/Local/Microsoft/Terminal Server Client/Cache/bcache24.bmc	File Changed
30	true	2020-09-19 04:36:23	/Users/Administrator/AppData/Local/Microsoft/Terminal Server Client/Cache/bcache24.bmc	File Modified
31	true	2020-09-19 04:36:25	/Users/Administrator/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations	File Modified

- **Fichiers `Secret.lnk` et `Beth_Secret.lnk`** :
    - Création, modification et accès répétés à ces fichiers `.lnk` (raccourcis) dans le dossier `Recent`. Ces fichiers pourraient pointer vers des ressources sensibles ou des dossiers ciblés pour l'exfiltration.
- **Fichiers `automaticDestinations-ms`** :

- Ces fichiers stockent l'historique des fichiers récemment ouverts dans Windows. Leur modification pourrait indiquer qu'un attaquant a consulté ou manipulé des fichiers récents pour identifier des cibles d'exfiltration.

---

5. Activité dans `Terminal Server Client` (04:35:54 et 04:36:23) :

	A	B	C	D
1	Icon	Date/Time	Description	Event Type
2	true	2020-09-19 04:35:54	/Users/Administrator/AppData/Local/Microsoft	File Accessed
3	true	2020-09-19 04:35:54	/Users/Administrator/AppData/Local/Microsoft	File Changed
4	true	2020-09-19 04:35:54	/Users/Administrator/AppData/Local/Microsoft	File Modified
5	true	2020-09-19 04:35:54	/Users/Administrator/AppData/Local/Microsoft/Terminal Server Client	File Modified
6	true	2020-09-19 04:35:54	/Users/Administrator/AppData/Local/Microsoft/Terminal Server Client	File Changed
7	true	2020-09-19 04:35:54	/Users/Administrator/AppData/Local/Microsoft	File Changed
8	true	2020-09-19 04:35:54	/Users/Administrator/AppData/Local/Microsoft/Terminal Server Client/Cache	File Created
9	true	2020-09-19 04:35:54	/Users/Administrator/AppData/Local/Microsoft	File Modified
10	true	2020-09-19 04:35:54	/Users/Administrator/AppData/Local/Microsoft	File Accessed
11	true	2020-09-19 04:35:54	/Users/Administrator/AppData/Local/Microsoft/Terminal Server Client	File Accessed
12	true	2020-09-19 04:35:54	/Users/Administrator/AppData/Local/Microsoft/Terminal Server Client	File Created
13	true	2020-09-19 04:35:54	/Users/Administrator/AppData/Local/Microsoft/Terminal Server Client	File Created
14	true	2020-09-19 04:35:54	/Users/Administrator/AppData/Local/Microsoft/Terminal Server Client	File Accessed
15	true	2020-09-19 04:35:54	/Users/Administrator/AppData/Local/Microsoft/Terminal Server Client	File Changed
16	true	2020-09-19 04:35:54	/Users/Administrator/AppData/Local/Microsoft/Terminal Server Client	File Modified
17	true	2020-09-19 04:35:54	/Users/Administrator/AppData/Local/Microsoft/Terminal Server Client/Cache	File Created
18	true	2020-09-19 04:35:54	/Users/Administrator/AppData/Local/Microsoft	File Modified
19	true	2020-09-19 04:35:54	/Users/Administrator/AppData/Local/Microsoft/Terminal Server Client/Cache	File Created
20	true	2020-09-19 04:35:54	/Users/Administrator/AppData/Local/Microsoft	File Changed
21	true	2020-09-19 04:35:54	/Users/Administrator/AppData/Local/Microsoft/Terminal Server Client	File Changed
22	true	2020-09-19 04:35:54	/Users/Administrator/AppData/Local/Microsoft/Terminal Server Client	File Modified
23	true	2020-09-19 04:35:54	/Users/Administrator/AppData/Local/Microsoft/Terminal Server Client	File Created
24	true	2020-09-19 04:35:54	/Users/Administrator/AppData/Local/Microsoft/Terminal Server Client	File Accessed
25	true	2020-09-19 04:35:54	/Users/Administrator/AppData/Local/Microsoft	File Accessed
26				

- **Fichiers `bcache24.bmc`** :
  - Création, modification et accès répétés à ces fichiers dans le dossier `Cache` du client Terminal Server. Ces fichiers sont utilisés pour stocker des données de session RDP.
  - Cela pourrait indiquer qu'une session RDP a été établie ou qu'un attaquant a utilisé RDP pour accéder au système.

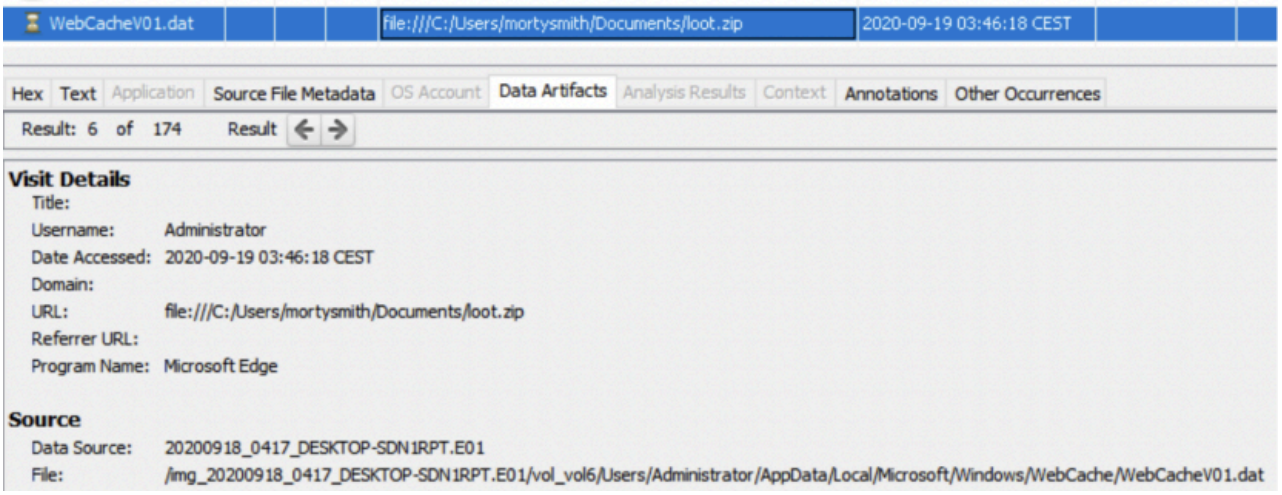
Indicateurs de Compromission (IoC) :

1. **Manipulation de fichiers dans `$Recycle.Bin`** :
   - Les fichiers supprimés ont été consultés et modifiés, ce qui pourrait indiquer une tentative de récupération de données.
2. **Activité intense dans `FileShare` et `SendTo`** :
   - Ces dossiers ont été ciblés pour l'exfiltration de données, avec des fichiers sensibles potentiellement compressés ou envoyés via des méthodes comme le courrier électronique ou Bluetooth.

3. **Utilisation de RDP (`Terminal Server Client`)** :
    - Les fichiers de cache RDP modifiés suggèrent une utilisation potentielle de RDP pour accéder au système ou exfiltrer des données.
4. **Consultation de l'historique des fichiers (`Recent` et `AutomaticDestinations`)** :
    - Les fichiers récemment ouverts ont été consultés, ce qui pourrait indiquer une reconnaissance pour identifier des cibles d'exfiltration.

Analyse du Vol de la Sauce Szechuan

1. **Méthode Utilisée :** Exfiltration des fichiers via `loot.zip`.

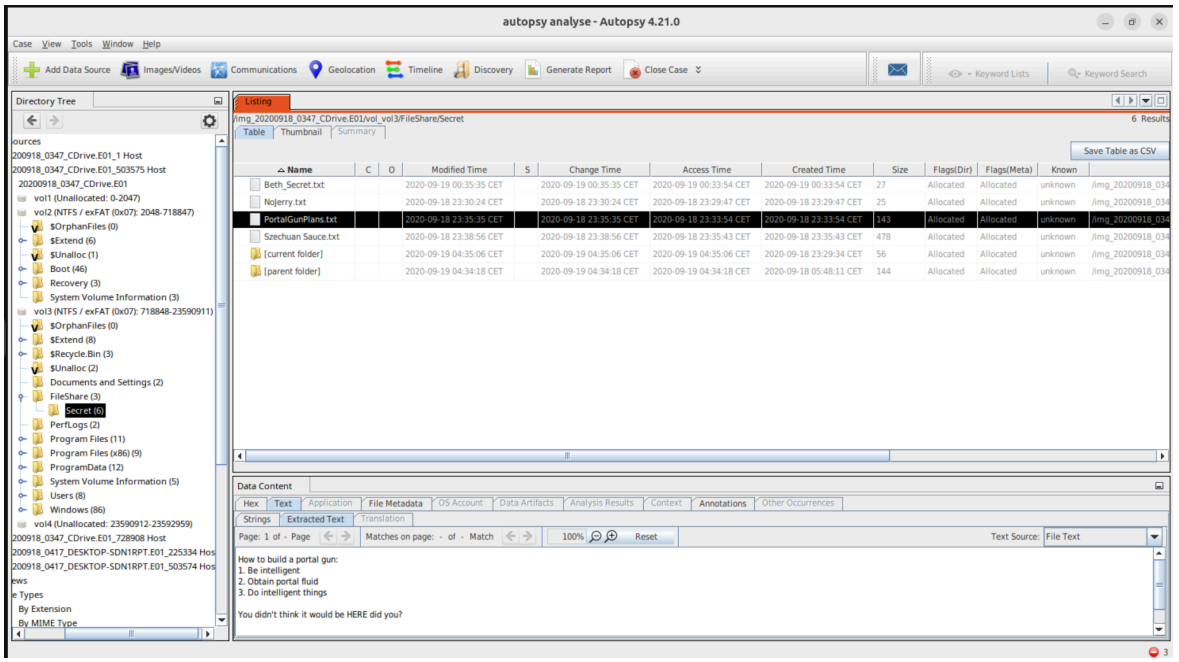


2. **Heure de l'Action :** Les journaux indiquent un accès à `Szechuan Sauce.txt` peu après l'installation du malware.

Autres Fichiers Sensibles

1. **Autres Fichiers Accédés :**

- `PortalGunPlans.txt`



- `NoJerry.txt`

2. **Heure de l'Action :** Accédés successivement après `Szechuan Sauce.txt`.

Fichiers Altérés

1. **Fichiers Altérés :**
   - `SECRET_Beth.txt` (Supprimé).
2. **Méthode Utilisée :** Suppression manuelle via l'explorateur de fichiers.
3. **Heure de l'Action :** Le timestamp correspond aux activités d'exfiltration.

Dernier Contact avec l'Adversaire

1. **Horodatage :** L'exfiltration a été finalisée ; le dernier contact connu est peu après la création de `loot.zip`.
2. **Fin de l'Activité :** La persistance du malware garantit un potentiel contact continu.

Recommandations

1. Appliquer des politiques de mot de passe robustes pour prévenir les attaques par force brute.
2. Désactiver l'accès RDP non nécessaire.

3. Effectuer des analyses régulières de malware.
4. Surveiller le trafic réseau pour détecter des activités suspectes.
5. Mettre en place un plan de réponse aux incidents pour gérer efficacement les violations.

Timeline

- **timeline :05:21:25 début de brute force a (CITADEL\Administrator) Security.evtx**
- **timeline :05:21:46 fin de brute force a (CITADEL\Administrator) Security.evtx**
- **timeline : 05:21:48 : authentification réussi a CITADEL\Administrator Security.evtx**
- **timeline : 05:22:37 : authentification depuis CITADEL a DESKTOP-SDN1RPT Security.evtx**
- **timeline : 05:24:50 compte compromis utilise Internet Explorer pour télécharger Meterpreter depuis l'adresse 194.61.24.102 via HTTP vers le contrôleur de domaine téléchargement du fichier coreupdater.exe**
- **timeline : 05:34:18 : Le fichier Secret_Beth.txt est supprimé du partage de fichiers du contrôleur de domaine**
- **timeline : 05:34:27 : Un fichier Beth_Secret.txt contenant un secret différent est créé sur le partage de fichiers du contrôleur de domaine**
- **timeline : 05:35:07 L'attaquant initie un mouvement latéral en utilisant le RDP pour se connecter au système Desktop-SDN1RPT**
- **timeline : 05:36:24 et 05:36:43 : Activité dans SendTo**
- **timeline : 05:46:18 Le fichier loot.zip est créé sur le système Desktop en utilisant l'Explorateur de fichiers puis exfiltration**