



PLANS D'ACTION

Compromission du domaine
d'Echelon

CELLULE SOC

Septembre 2024

Version	Date	Propriétaire	Rédacteur / Autorité
1.0 Finale	30/09/2024	Cellule SOC	Nicolas Clerbout

Table des matières

Liste des figures	3
1. Remédiations pour l'extraction de données.....	4
2. Remédiations pour la compromission initiale.....	5
3. Remédiations pour l'escalade de privilèges	6
4. Remédiations pour les actions de persistance	7
5. Synthèse des actions à mettre en œuvre	8
Tâches du case restant à effectuer :	8

Liste des figures

Section 1 :

Figure 1 - Réaction immédiate : règle SNORT..... 4

Figure 2 - Actions à réaliser suite à la fuite de données..... 4

Section 2 :

Figure 3 - Plan d'action contre la compromission initiale..... 5

Section 3 :

Figure 4 - Plan d'action contre l'escalade de privilèges 6

Section 4 :

Figure 5 - Plan d'action face aux actions de persistance 7

Section 5 :

Figure 6 - Tâches à réaliser (TheHive)..... 8

1. Remédiations pour l'extraction de données

A Echelon/Analyst

Mise en place d'une règle de blocage sur SNORT

```
block tcp $HOME_NET any -> 103.251.167.20 53 (msg:"trafic DNS vers IP malveillante"; sid:10001; rev:1;)
```

Figure 1 - Réaction immédiate : règle SNORT

A Echelon/Analyst

a) Filtrage du trafic réseau :

Ajouter le domaine loginmicrosooft[.]com et l'IP 103[.]251[.]167[.]20 aux listes noires des différents firewall

b) Nettoyage de comptes utilisateur :

Supprimer les tokens d'identification et réinitialiser les mots de passe pour les comptes suivants :

- svcmysql (utilisé pour réaliser les requêtes DNS malveillantes)
- comptes dont les identifiants ont été exfiltrés (voir "Analyse de l'extraction de données" - Actifs impactés)

Figure 2 - Actions à réaliser suite à la fuite de données

2. Remédiations pour la compromission initiale

A

Echelon/Analyst

Actions sur compte utilisateur John Elom :

- Supprimer le mail malveillant et sa pièce jointe
- Révoquer le token d'identification et réinitialiser le mot de passe

Détection et prévention :

- Ajouter aux listes noires (firewall, Snort, serveur mail) + règles de détection SIEM et EDR :
 - domaine communication[.]microsooft[.]com ;
 - IP 121[.]186[.]71[.]183 ;
 - script de redirection (SHA-256 e55a236a7bd0bb9644df5b5fb3488aa35e8ee6ee23b7ca49af0f75868e984e79) ;
 - https[://]x17qszcdzxlh6hb560dedk[.]65nlsppaa2[.]ru
- Rechercher et nettoyer autres comptes/machines compromises (suppression de mails et scripts malveillants, réinitialiser mots de passe et révoquer tokens d'identification)

Mesures globales :

- Imposer l'authentification multi-facteurs (MFA) ;
- Interdire par GPO (stratégie de restriction logicielle) l'exécution de javascript depuis l'environnement de messagerie ;
- Rappeler les conseils de cyber-hygiène relatifs au phishing aux utilisateurs + organiser une campagne de formation/sensibilisation

Figure 3 - Plan d'action contre la compromission initiale

3. Remédiations pour l'escalade de privilèges

A Echelon/Analyst

Nettoyage de comptes

Révoquer les tokens d'identification et réinitialiser les mots de passe des comptes svcmysql et john.elom
(cf. remédiations concernant la compromission initiale et l'extraction de données)

Sécuriser les mots de passe

- Supprimer les fichiers contenant des mots de passe
- Interdire le stockage des mots de passe dans des fichiers en clair

Sécuriser les comptes de service

Interdire les connexions interactives aux comptes de service

Figure 4 - Plan d'action contre l'escalade de privilèges

4. Remédiations pour les actions de persistance

A

Echelon/Analyst

Nettoyage de comptes

- Supprimer le compte "admin_backup" créé par l'adversaire
- Révoquer les tokens d'identification et réinitialiser les mots de passe des comptes john.elom et svcmysql + autres comptes du groupe Admin du Contrôleur de Domaine

Nettoyage du Contrôleur de Domaine

- Supprimer la clé RUN "BGinfo Systemals" créée par l'adversaire
- Supprimer la tâche planifiée d'exécution du script powershell

Détection et Prévention

- Bloquer le trafic vers l'IP malveillante 103[.]251[.]167[.]20
- Mise à jour du SIEM et de l'EDR pour détecter le script powershell malveillant via son hash

Sauvegarde / Rétablissement

Mettre en place un second Contrôleur de Domaine à des fins de redondance et sauvegarde pour récupération en cas d'incident

Figure 5 - Plan d'action face aux actions de persistance

5. Synthèse des actions à mettre en œuvre

Tâches du case restant à effectuer :













<input type="checkbox"/>	Group	Task	Date	Assignee
<input type="checkbox"/>	  default	 Extraction de données : Remédiation (2) Started 7 hours ago	09/28/24 9:08	Admin
<input type="checkbox"/>	  default	 Compromission initiale : Remédiation Started 6 hours ago	09/28/24 9:36	Admin
<input type="checkbox"/>	  default	 Escalade de privilèges : Remédiation Started 5 hours ago	09/28/24 11:19	Admin
<input type="checkbox"/>	  default	 Persistence : Remédiation Started an hour ago	09/28/24 15:07	Admin

Figure 6 - Tâches à réaliser (TheHive)