



ANALYSE

Compromission du domaine
d'Echelon

CELLULE SOC

Septembre 2024

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

Table des matières

Liste des figures	3
1. Vues d'ensemble.....	4
2. Analyse de l'extraction de données	6
3. Analyse de la compromission initiale	7
4. Analyse de l'escalade de privilèges.....	9
5. Analyse des actions de persistance	11
Annexe	12
Alerte close (Faux Positif)	12
Probables faux positifs (à vérifier)	12
Case #4	12
Case #5	12
Alertes à approfondir	13

Liste des figures

Section 1 :

Figure 1 - Alertes concernées par le case.....	4
Figure 2 - Liste des tâches du case.....	4
Figure 3 - Liste des TTPs relevées dans le case.....	5

Section 2 :

Figure 4 - Extraction de données : déroulement et actifs impactés.....	6
Figure 5 - Extraction de données : IoCs.....	6

Section 3 :

Figure 6 - Compromission initiale : déroulement.....	7
Figure 7 - Compromission initiale : actifs impactés.....	7
Figure 8 - Détails Phishing et Infiltration.....	7
Figure 9 - Compromission initiale : IoCs.....	8

Section 4 :

Figure 10 - Escalade de privilèges : déroulement et analyse de capture réseau..	9
Figure 11 - Analyse de capture réseau : détails	9
Figure 12 - Analyse des hashes relevés.....	10
Figure 13 - Escalade de privilèges : IoCs	10

Section 5 :

Figure 14 - Persistance : déroulement des actions.....	11
Figure 15 - Persistance : ajout de clé Run dans le registre.....	11
Figure 16 - Persistance : Tâche planifiée (script de reverse shell)	11
Figure 17 - Persistance : création d'un compte à privilèges.....	11
Figure 18 - Persistance : IoCs.....	11

1. Vues d'ensemble

All (8)

Type: Alert (7)IDS (1)

Source: SIEM (7)Snort (1)

Reference ^	Type ^	Title ^	Source ^	Severity ^	Attributes	Date ^
20230831164518	IDS	Trafic DNS inhabituel via TCP	Snort	H	4	08/31/23 16:45
<div>None</div> <div></> None</div>						
t120240928085833-1	Alert	Voyage impossible - connexions depuis plusieurs pays en un temps réduis	SIEM	H	0	09/28/24 8:58
<div>None</div> <div></> None</div>						
t120240928085834-4	Alert	Signalement de phishing de l'utilisateur	SIEM	H	0	09/28/24 8:58
<div>None</div> <div></> None</div>						
t220240928093635-1	Alert	Scan SMB	SIEM	H	0	09/28/24 9:36
<div>None</div> <div></> None</div>						
t220240928093636-2	Alert	Scan LDAP	SIEM	H	0	09/28/24 9:36
<div>None</div> <div></> None</div>						
t320240928101030-1	Alert	Création d'une tâche planifiée	SIEM	H	0	09/28/24 10:10
<div>None</div> <div></> None</div>						
t320240928101030-2	Alert	Modification de clés de registre RUN	SIEM	H	0	09/28/24 10:10
<div>None</div> <div></> None</div>						
t320240928101030-3	Alert	Ajout d'un utilisateur dans le groupe Domain Administrators	SIEM	H	0	09/28/24 10:10
<div>None</div> <div></> None</div>						

Figure 1 - Alertes concernées par le case

List of tasks (10 of 10)					
	Group	Task	Date	Assignee	Actions
<input type="checkbox"/>	default	Analyse de l'extraction de données Closed after 2 minutes	09/28/24 9:00	Analyst	
<input type="checkbox"/>	default	Extraction de données : Remédiation (1) Closed after a few seconds	09/28/24 9:04	Analyst	
<input type="checkbox"/>	default	Extraction de données : Remédiation (2) Started 7 hours ago	09/28/24 9:08	Admin	
<input type="checkbox"/>	default	Liste des TTPs Closed after 6 hours	09/28/24 9:17	Analyst	
<input type="checkbox"/>	default	Analyse de la compromission initiale Closed after 8 minutes	09/28/24 9:23	Analyst	
<input type="checkbox"/>	default	Analyse de l'escalade de privilèges Closed after an hour	09/28/24 9:36	Snort	
<input type="checkbox"/>	default	Compromission initiale : Remédiation Closed after 19 minutes	09/28/24 9:36	Admin	
<input type="checkbox"/>	default	Escalade de privilèges : Remédiation Started 4 hours ago	09/28/24 11:19	Admin	
<input type="checkbox"/>	default	Analyse des actions de persistance Closed after 3 hours	09/28/24 11:38	Analyst	
<input type="checkbox"/>	default	Persistance : Remédiation Started 37 minutes ago	09/28/24 15:07	Admin	

Figure 2 - Liste des tâches du case

Extraction de données :

T1048.003 "Exfiltration over Unencrypted Non-C2 Protocols"

T1027 "Obfuscated Files or Information"

Compromission initiale :

T1598 "Phishing for information"

T1027 "Obfuscated Files or Information"

T1078.003 "Valid Accounts : Local Accounts"

Escalade de privilèges :

T1021.002 "Remote Services: SMB"

T1135 "Network Share Discovery"

T1078.001 "Valid Accounts : Default Accounts"

T1018 "Remote System Discovery"

Persistance :

T1136 "Create Account" & **T1098** "Account Manipulation"

T1547.001 "Boot or Logon Autostart Execution: Registry Run Keys"

T1053.005 "Scheduled Task" & **T1059.001** "Command and Scripting Interpreter: Powershell"

Figure 3 - Liste des TTPs relevées dans le case

2. Analyse de l'extraction de données

A

Echelon/Analyst

Déroulement des actions adverses

1. L'adversaire a acquis le domaine loginmicrosooft[.]com

2. L'adversaire a infiltré le SI d'Echelon (cf. "Analyse de la compromission initiale")

3. L'adversaire a compromis le compte svcmysql (cf. "Analyse de l'escalade de privilèges")

4. L'adversaire a obtenu puis encodé (en hexadécimal) des données d'identification sur le domaine Echelon

5. L'adversaire a transmis les données volées encodées depuis le Contrôleur de Domaine sous la forme de requêtes DNS réalisées via TCP et envoyées vers l'IP malveillante

A

Echelon/Analyst

Actifs impactés

Compte utilisateur : svcmysql

Équipement : Serveur Contrôleur de Domaine d'Echelon

Données.

Données d'identification de plusieurs comptes utilisateurs transmis via DNS après encodage en hexadécimal. Echantillon relevé :

- (cn=Fabien%20Ayot,ou=France,ou=Users,dc=echelon,dc=local:Echelon2023!)
- (cn=Maurelle%20Bourdette,ou=France,ou=Users,dc=echelon,dc=local:MyP@ssw0rd123)
- (cn=Marthe%20Sylvain,ou=France,ou=Users,dc=echelon,dc=local:maurelle.bourdette1968)
- (cn=Madeleine%20Brousse,ou=France,ou=Users,dc=echelon,dc=local:StrongPassword)
- (cn=Christian%20Monty,ou=France,ou=Users,dc=echelon,dc=local:ceuAZEi13zF5D6!Sblze)
- (cn=svcmysql,ou=France,ou=Domain%20Admin,dc=echelon,dc=local:IdV;6EW4eTH@2HTo#J9!nvwio)
- (cn=Loyal%20Dupont,ou=France,ou=Users,dc=echelon,dc=local:Echelon2023!)
- (cn=Serge%20Bouchard,ou=France,ou=Users,dc=echelon,dc=local:poaFE..z12d)
- (cn=administrator,ou=France,ou=Domain%20Admin,dc=echelon,dc=local:kcoRZ412VCa/;!EZnoca)
- (cn=Millard%20Belisle,ou=France,ou=Users,dc=echelon,dc=local:Echelon1..)
- (cn=Jacquenet%20Vaillancour,ou=Users,ou=France,dc=echelon,dc=local:IL0veLila)
- (cn=www-data,ou=France,ou=Web,dc=echelon,dc=local:W3BS3RV.1202301)
- (cn=John%20Elom,ou=France,ou=Users,dc=echelon,dc=local:MPssw0iStronEn0gh)
- (cn=root,ou=France,ou=SQL%20Admin,dc=echelon,dc=local:toor)
- (cn=Sabrina%20Pels,ou=France,ou=Users,dc=echelon,dc=local:Jean&Jeanne2004)
- (cn=Eric%20Judo,ou=France,ou=Users,dc=echelon,dc=local:Ramzy!SFunny)

Figure 4 - Extraction de données : déroulement et actifs impactés

☐ other

53

Destination port DNS over TCP

No reports available

☐ ip

103[.]251[.]167[.]20

Risky IP Destination IP

No reports available

☐ domain

loginmicrosooft[.]com

Risky Domain

No reports available

Figure 5 - Extraction de données : IoCs

3. Analyse de la compromission initiale

A

Echelon/Analyst

Déroulement de la compromission initiale

1. L'adversaire a envoyé un mail de spearphishing à l'utilisateur John Elom contenant une pièce jointe malveillante (voir "Vecteur de compromission initiale" ci-dessous)

2. L'utilisateur a ouvert la pièce jointe malveillante

3. Un code javascript a provoqué une redirection vers une page malveillante (voir "Vecteur de compromission initiale")

4. L'adversaire a récupéré les identifiants de l'utilisateur

5. L'adversaire a utilisé les identifiants volés pour se connecter depuis l'IP malveillante 103[.]251[.]167[.]20 (voir "Infiltration dans le SI d'Echelon" ci-dessous)

Figure 6 - Compromission initiale : déroulement

A

Echelon/Analyst

Actifs impactés :

Compte utilisateur / boîte de messagerie john.elom[.]@echelon[.]com

Figure 7 - Compromission initiale : actifs impactés

A

Echelon/Analyst

Infiltration dans le SI d'Echelon en utilisant des identifiants volés

Cf Alerte t120240923071409-1 "Voyage impossible - connexions depuis plusieurs pays en un temps réduits"

Connexion le 23/9/2024 à 6h10

Depuis l'IP malveillante 103[.]251[.]167[.]20 repérée dans l'extraction de données

Connexion presque simultanée avec autre connexion (apparemment légitime) depuis un autre pays

Type de connexion : interactive (donc utilisation du mot de passe, sans doute récupéré suite au phishing analysé dans le log ci-dessous)

IP interne attribuée : 10[.]0[.]2[.]166

A noter : pas de MFA pour aucune des deux connexions concernées dans l'alerte.

A

Echelon/Analyst

Vecteur de compromission initiale : mail de phishing

Cf Alerte t120240923071410-4 "Signalement de phishing de l'utilisateur"

Analyse de l'en-tête :

Mail reçu à 6h06

Adresse Mail de l'expéditeur : msa@communication[.]microsoft[.]com (typosquatting similaire au domaine loginmicrosoft[.]com utilisé dans l'extraction de données)

IP expéditrice : 121[.]186[.]71[.]183

Analyse de la pièce jointe :

Code javascript obfusqué par encodage base64

Le code a pour fonction d'opérer une redirection vers une url, sans doute à des fins de vol d'identifiants

Hash (SHA-256) du script desobfusqué : e55a236a7bd0bb9644df5b5fb3488aa35e8ee6ee23b7ca49af0f75868e984e79

L'url de redirection commence par https://[.]x17qszcdzlh6hb560dedk[.]65nlskaa2[.]ru/dP5x/#

Le compte utilisateur john.elom[.]@echelon[.]com est explicitement utilisé dans l'url de redirection, ce qui suggère une attaque ciblée

Figure 8 - Détails Phishing et Infiltration


























<input type="checkbox"/>	   	domain	communication[.]microsooft[.]com
			 Risky Domain  No reports available
<input type="checkbox"/>	   	ip	121[.]186[.]71[.]183
			 Risky IP  No reports available
<input type="checkbox"/>	   	url	hxxps://x17qszcdzxlh6hb560dedk[.]65nlspaa2[.]ru/dP5x/#
			 Risky url  No reports available
<input type="checkbox"/>	   	hash	e55a236a7bd0bb9644df5b5fb3488aa35e8ee6ee23b7ca49af0f75868e984e79
			 SHA-256  Malicious Script  No reports available

Figure 9 - Compromission initiale : IoCs

4. Analyse de l'escalade de privilèges

A Echelon/Analyst

Déroulement des actions adverses

1. L'adversaire a compromis le compte utilisateur John Elom (cf. Tâche "Analyse de la compromission initiale")
2. L'adversaire a effectué un scan SMB (Alerte t220240928093635-1) pour rechercher les ressources et fichiers partagés sur le domaine d'Echelon
3. L'adversaire a trouvé les identifiants du compte svcmysql dans le fichier pass_adm_dom_svcmysql.txt (cf. "Analyse de la capture" réseau ci-dessous)
4. L'adversaire a utilisé le compte svcmysql pour effectuer un scan LDAP (Alerte t220240928093636-2).

A Echelon/Analyst

Analyse de la capture réseau

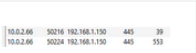
- La capture ne contient pas de traces de trafic LDAP (port 389)
- La capture contient deux "conversations" de trafic SMB entre l'IP interne 10.0.2.66 et le DC d'Echelon sur 192.168.1.150 (voir image1 ci-dessous)
- L'adversaire a accédé aux dossiers "\\IPC\$" et "\\TEMP"
- Dans le dossier "\\TEMP", l'adversaire a trouvé plusieurs fichiers (voir image2 ci-dessous)
- L'adversaire a notamment eu accès au fichier contenant les identifiants du compte svcmysql (voir image3 ci-dessous)
- La capture ne contient pas de trafic relatif aux hashes qui ont été ajoutés aux observables (voir "Analyse des hashes" ci-dessous)

Figure 10 - Escalade de privilèges : déroulement et analyse de capture réseau

A Echelon/Analyst

"Conversations" SMB

- source : ports 50216 et 50224 sur IP 10.0.2.66
- destination : port 445 sur Contrôleur de Domaine (192.168.1.150)



Source	Destination	Port	Protocol
10.0.2.66	192.168.1.150	445	SMB
10.0.2.66	192.168.1.150	555	SMB

image1.png

A Echelon/Analyst

Liste des fichiers trouvés dans le dossier 192.168.1.150\\TEMP :




image2.png

A Echelon/Analyst

Accès au fichier pass_adm_dom_svcmysql.txt




image3.png

Figure 11 - Analyse de capture réseau : détails

A
Echelon/Analyst

Analyse des hashes ajoutés aux observables

- hash b972f1622bdf57455e43a2a74094be6478e89dac55c570c1f26d1da8455d35bc
 - identifié comme malicieux (Trojan) sur plusieurs plateformes de CTI. Cf <https://www.virustotal.com/gui/file/b972f1622bdf57455e43a2a74094be6478e89dac55c570c1f26d1da8455d35bc/detection>
- hash 25abf45e40710b775479c3881a2fd4392f78ad8aec1ce603da39245448f27f8e
 - Non malicieux, correspond au processus explorer.exe (<https://www.virustotal.com/gui/file/25abf45e40710b775479c3881a2fd4392f78ad8aec1ce603da39245448f27f8e/detection>)

Figure 12 - Analyse des hashes relevés

☐
☒
☒
☐
☐
☐
☐
hash

b972f1622bdf57455e43a2a74094be6478e89dac55c570c1f26d1da8455d35bc

SHA-256
Trojan

No reports available

Figure 13 - Escalade de privilèges : IoCs

5. Analyse des actions de persistance

A Echelon/Analyst

Déroulement des actions adverses

1. L'adversaire a utilisé le compte utilisateur john.elom pour ajouter une clé de registre RUN afin de lancer le programme BGInfo.exe au démarrage
2. L'adversaire a utilisé le compte svcmysql pour créer un compte "admin_backup" dans le groupe Admin sur le Contrôleur de Domaine
3. L'adversaire a utilisé le compte svcmysql pour créer une tâche planifiée sur le Contrôleur de Domaine pour pouvoir y exécuter arbitrairement des commandes powershell

Figure 14 - Persistance : déroulement des actions

A Echelon/Analyst

Ajout d'une clé de registre RUN

Commande utilisée : REG ADD "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /t REG_SZ /v "BGInfo Sysinternals" /d "C:\Program Files\Bginfo.exe" /f

- La fonction de la clé est de lancer le programme "Bginfo.exe" au démarrage (clé RUN).
- On note l'utilisation de la fonctionnalité "/f" pour ne pas requérir de confirmation pour valider l'ajout de la clé
- Le programme Bginfo.exe (s'il s'agit du programme légitime) sert à récupérer et afficher sur le bureau des informations système

Figure 15 - Persistance : ajout de clé Run dans le registre

A Echelon/Analyst

Création d'une tâche planifiée

- La tâche planifiée est l'exécution d'un script powershell. Le contenu du script est obfusqué par un encodage en base64
- Le hash du script desobfusqué est 5ff01a325fa0f78ae2791f6497646e91f707ea8f9a607803e5c39e7f5b14abce
- Le script utilise plusieurs paramètres visant à éviter la détection et certaines mesures de sécurité (-NoP ; -Nonl ; -W hidden ; -Exec Bypass)
- Le script établit une connexion TCP vers l'IP malveillante 103[.]251[.]167[.]20
- Le script capture le flux de données de cette connexion TCP afin de pouvoir envoyer et recevoir des données
- Le script prévoit la réception et l'exécution de commandes powershell
- Le script capture et envoie les résultats des commandes exécutées
- Le script ferme la connexion TCP une fois que la boucle de communication (réception/exécution de commandes + envoi des résultats) est terminée

En résumé, le but de l'adversaire est d'exécuter périodiquement le script permettant la prise de contrôle du DC d'Echelon via l'exécution à distance de commandes powershell

Figure 16 - Persistance : Tâche planifiée (script de reverse shell)

A Echelon/Analyst

Ajout d'un compte à privilèges

L'adversaire a créé le compte "admin_backup" dans le groupe Admin du Contrôleur de Domaine d'Echelon afin de pouvoir s'y identifier même si les accès des comptes existants déjà compromis sont réinitialisés

Figure 17 - Persistance : création d'un compte à privilèges

<input type="checkbox"/> registry	REG ADD "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /t REG_SZ /v "BGInfo Sysinternals" /d "C:\Program Files\Bginfo[.]exe" /f
	Run keys Persistence
	No reports available
<input type="checkbox"/> hash	5ff01a325fa0f78ae2791f6497646e91f707ea8f9a607803e5c39e7f5b14abce
	SHA-256 Malicious Script Persistence
	No reports available

Figure 18 - Persistance : IoCs

Annexe

Alerte close (Faux Positif)

- Référence et nom de l'alerte : t120240928085834-5 « Signalement de phishing de l'utilisateur »
- L'analyse du mail suspect révèle qu'il ne comporte pas d'élément malveillant
- Création d'un case dédié (case #2) et clôture comme faux positif :

Close Case #2

You are about to close Case #2. Are you sure you want to continue ?

Incident

Status * ☐ True Positive ☐ False Positive ☐ Indeterminate ☐ Other

Investigation shows that there is nothing malicious (email with clean attachment ...)

Summary * **B I H S %** **Preview**

Spam publicitaire sans élément malveillant

Cancel * Required field Close case

Probables faux positifs (à vérifier)

Case #4

- Référence et nom de l'alerte : t220240928093636-3 « Scan NMAP »
- L'IP source est l'IP interne 192.168.1.100 qui correspond au serveur interne dédié au scan du réseau
- Vérifier avec l'équipe technique si le scan est effectivement légitime avant de clore l'alerte

Case #5

- Référence et nom de l'alerte : t220240928093636-4 « Scan http »
- Trafic web sur un port inhabituel
- Pas d'IoC lié à la compromission du Domaine Echelon, pas de trace dans la capture réseau analysée pour l'escalade de privilèges
- A approfondir

Alertes à approfondir

Case #3 « Connexions à distance suspectes » :

- Références et noms des alertes :
 - t120240928085833-2 « Voyage impossible »
 - t120240928085833-3 « Connexions depuis un pays non autorisé »
- Les identifiants des comptes utilisateurs concernés (erci.judo et sabrina.pels) font partie des données exfiltrées dans la compromission du Domaine Echelon
- Les adresses IP externes ne font pas partie des IoCs relevés dans la compromission du Domaine Echelon
- Les noms d'hôte semblent être légitimes
- Utilisation d'authentification à facteurs multiples (MFA)
- Vérifier avec les utilisateurs pour qualifier les alertes.