Carochan

Rapport d'Incident :
Analyse et Plan d'Action

Analyste : N. Clerbout

I. Investigation

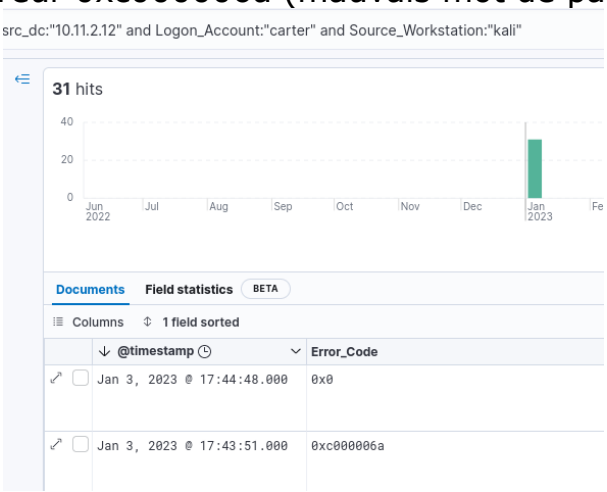
Alerte : (ALE-1) Multiple authentication failures followed by success

Détails d'investigation :

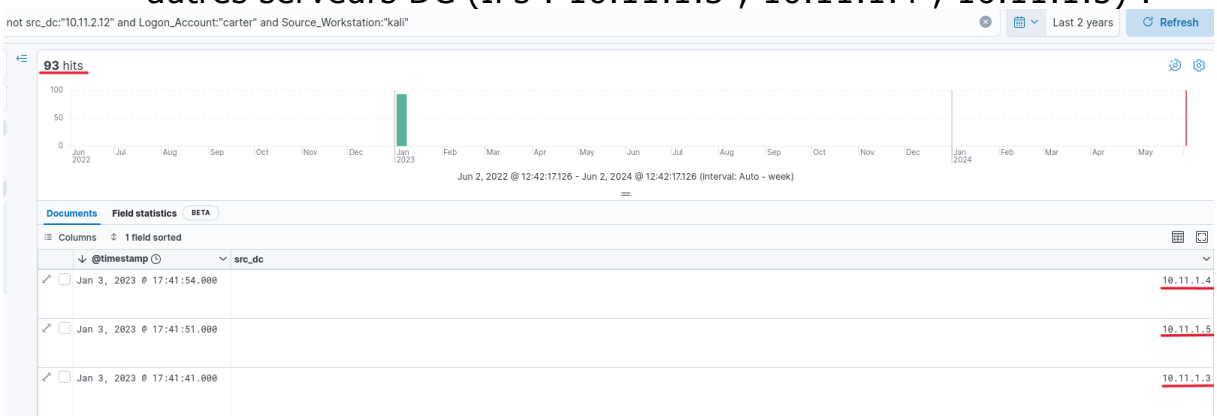
- Date de l'alerte : 03/01/2023 à 17h30
- Observables :
  - Hostname : kali
  - IP : 10.11.2.12
  - Username : carter

- 31 tentatives de connexion en moins de 20 minutes (voir index « windows_events » du SIEM) :

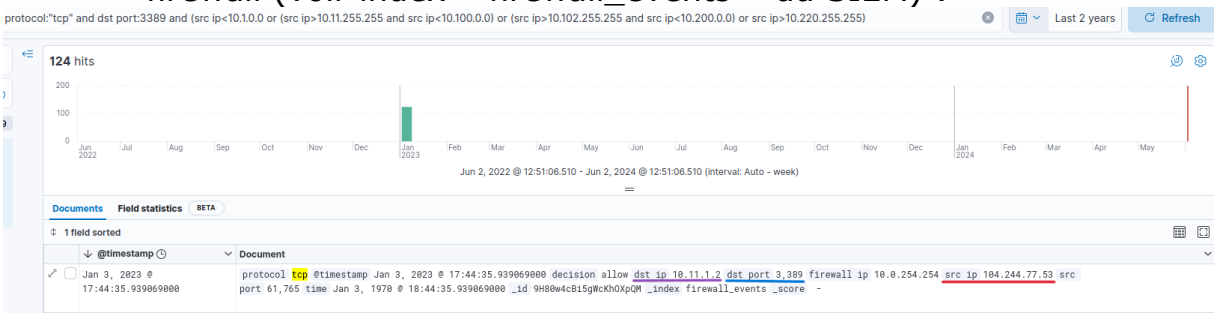
- 1 réussite (Code Erreur 0x0) après 30 échecs. Tous les échecs ont le Code Erreur 0xc000006a (mauvais mot de passe) :



- Sur la même période de 20 minutes, 93 tentatives (au total) additionnelles avec même hostname et même username sur 3 autres serveurs DC (IPs : 10.11.1.3 ; 10.11.1.4 ; 10.11.1.5) :



- Sur cette période de 20 minutes, 124 connexions depuis une IP externe sur le port 3389 enregistrées dans les logs du firewall (voir index « firewall_events » du SIEM) :



Le port 3389 est le port usuel pour le protocole RDP.
L'adresse IP externe est 104.244.77.53. Cette IP est associée au domaine frantech.ca, propriété de BuyVM. Connu pour autoriser le trafic TOR.
La connexion a été établie avec la DMZ du site Europe (IP 10.11.1.2).

Indicateurs de compromission :

- IP 104.244.77.53
- Domaine frantech.ca
- TTPs :
  - T1021.001 (Remote Services / Remote Desktop Protocol)
  - T1078.002 (Valid Accounts / Domain Accounts)
  - T1110 (Brute Force)

Actifs impactés :

- Serveurs EU-DC01, -DC02, -DC03 et -DC04 : DCs du domaine carochan.com.
- Compte utilisateur « carter ».

Informations supplémentaires :

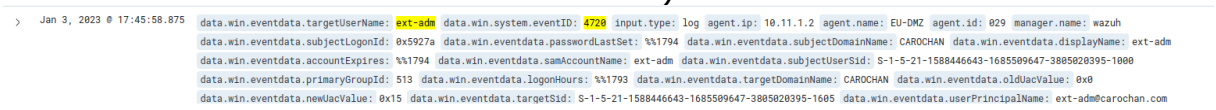
Source et raison de levée de l'alerte	Qualification de l'alerte	Justification de la qualification
Source : SIEM (événements Windows)	Vrai positif	Fréquence des tentatives cohérente avec une attaque Brute Force automatisée. Signes de connexion depuis l'extérieur via trafic TOR.

Alerte : (ALE-2) Privileged user created

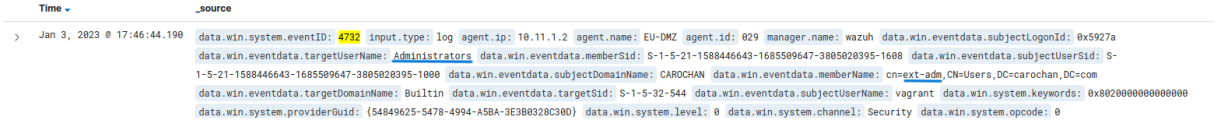
Détails d'investigation :

- Date de l'alerte : 17/05/2023 à 10h02
- Observable :
    - Username : ext-adm

- EventID 4720 indiquant la création de l'utilisateur ext-adm (Voir index « wazuh-alerts » de l'EDR) :



- EventID 4732 indiquant l'ajout de ext-adm au groupe Administrators (à noter : compte « vagrant » dans le champ data.win.eventdata.subjectUserName) :



Indicateurs de compromission :

- TTPs :
    - T1136.002 (Create Account / Domain Account)
    - T1098 (Account Manipulation)

Actifs impactés :

- DMZ (zone démilitarisée) du site Europe : « EU-DMZ ».
- DCs du domaine carochan.com.
- Compte utilisateur « vagrant »
- Groupe d'utilisateurs Administrators.

Informations supplémentaires :

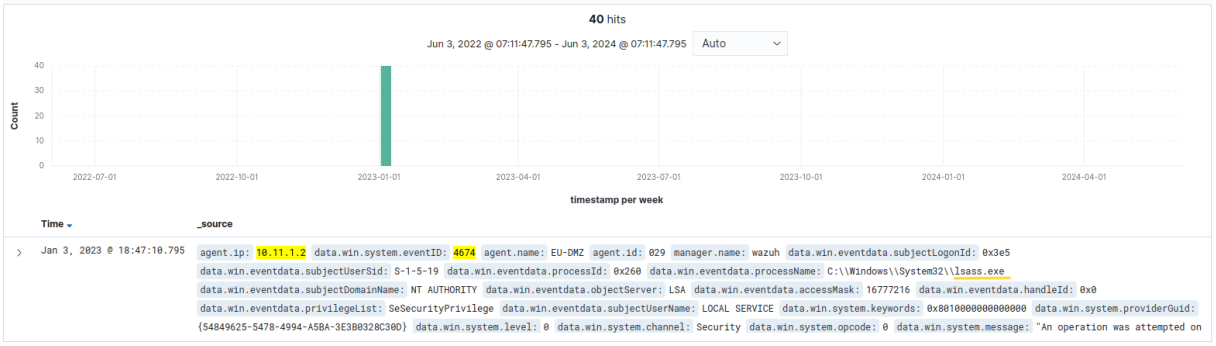
Source et raison de levée de l'alerte	Qualification de l'alerte	Justification de la qualification
Source : EDR (événements Windows)	Vrai positif	Création d'un compte puis ajout de ce compte à un groupe utilisateurs à privilèges via la DMZ et donc depuis l'extérieur du réseau.

Alerte : (ALE-3) Potential memory dump of lsass process detected

Détails d'investigation :

- Date de l'alerte : 03/01/2023 à 18h30
- 3 observables :
  - Filename : C:\Windows\System32\lsass.exe
  - IP : 10.11.1.2
  - Hostname : dc.carochan.com

- 40 logs pour cette adresse IP et le nom de fichiers lsass.exe (voir index « wazuh-archives » de l'EDR) :



- 2188 logs supplémentaires pour les adresses IP 192.168.56.102 (machine WINDOWS_DC_TEST – agent 004 dans Wazuh) et 192.168.56.103 (machine TEST_WEF – agent 069 dans Wazuh).

Indicateurs de compromission :

- TTPs :
  - T1003.001 (OS Credential dumping / LSASS Memory)

Actifs impactés :

- DMZ du site Europe : « EU-DMZ ».
- Machines de test WINDOWS_DC_TEST et TEST_WEF.

Informations supplémentaires :

Source et raison de levée de l'alerte	Qualification de l'alerte	Justification de la qualification
Source : EDR (événements Windows)	Vrai positif	Appels du processus lsass via la DMZ.

Alerte : (ALE-4) SMB scan detected

Détails d'investigation :

- Date de l'alerte : 04/01/2023 à 18h00
- Observables :
  - Port de destination 445
  - 9 adresses IP sources : 10.11.2.53 ; 10.11.2.57 ; 10.11.2.71 ; 10.11.2.92 ; 10.11.2.119 ; 10.11.2.159 ; 10.11.2.198 ; 10.11.2.215 ; 10.11.2.247

- 324 logs correspondants (voir index « firewall-events » du SIEM) :

- L'adresse IP 10.11.2.57 est également destinataire d'une communication sur le port 445 depuis l'adresse IP 10.10.0.238 (qui fait partie du LAN utilisateurs) :

Indicateurs de compromission :

- TTPs :
  - T1021.002 (Remote Services : SMB/Windows Admin Shares)
  - T1135 (Network Share Discovery)

Actifs impactés :

- LAN serveurs (10.11.0.0/16) de la zone Europe.
- Machine utilisateur d'adresse IP 10.10.0.238.

Informations supplémentaires :

Source et raison de levée de l'alerte	Qualification de l'alerte	Justification de la qualification
Source : SIEM (événements firewall) Les adresses IP sources font partie du sous-réseau « LAN serveurs » de la zone Europe mais ne correspondent pas à des machines répertoriées	Vrai positif	Utilisation d'adresses IP du LAN Serveurs de la zone Europe sans machines correspondantes. Caractéristiques d'un scan SMB.

Alerte : (ALE-5) Nmap scanner detected

Détails d'investigation :

- Date de l'alerte : 05/01/2023 à 14h00
- Observables :
  - IP source : 10.11.2.13
  - IPs destinataires : multiples sur le réseau 10.11.0.0/16
  - Port destinataire : 9182
- Plus de 43 000 connexions depuis l'IP 10.11.2.13 vers le port 9182 entre le 2 et le 7 janvier (voir index « firewall_events » du SIEM).
- L'adresse IP 10.11.2.13 correspond au serveur EU-MNT01 qui est un serveur hébergeant l'outil de monitoring Prometheus. Le port 9182 est le port utilisé par défaut pour l'exporteur Windows associé à l'outil Prometheus (https://github.com/prometheus/prometheus/wiki/Default-port-allocations).

Indicateurs de compromission :

- TTPs :
  - T1046 (Network Service Discovery)

Actifs impactés :

- Serveur EU-MNT01.
- LAN Serveurs de la zone Europe (10.11.0.0/16).

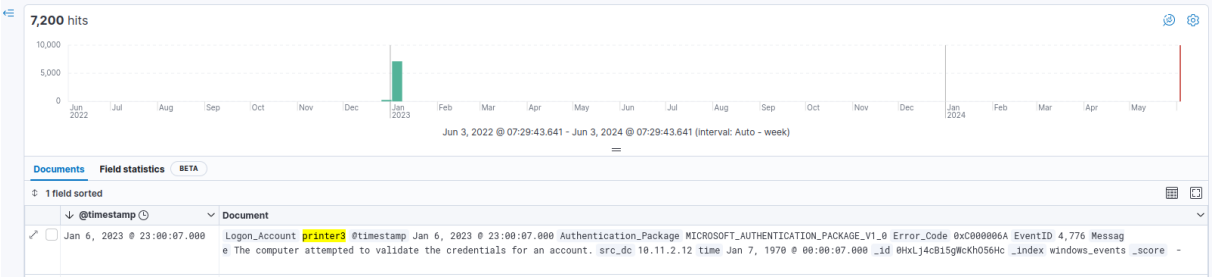
Informations supplémentaires :

Source et raison de levée de l'alerte	Qualification de l'alerte	Justification de la qualification
Source : SIEM (événements firewall) Connexions nombreuses et fréquentes sur de multiples machines sur le port 9182.	Faux positif	Comportement normal du service de monitoring Prometheus avec exporteur Windows, à partir du serveur dédié EU-MNT01

Alerte : (ALE-6) Massive authentication failures

Détails d'investigation :

- Date de l'alerte : 05/01/2023 à 21h07
- Observables :
  - IP : 10.11.2.12
  - Username : printer3
  - Error_Code : 0xC000006A
- 7200 échecs d'authentification au total (toutes adresses IPs confondues) pour le compte printer3 sur les premiers jours du mois de janvier 2023 (voir index « windows_events » du SIEM) :



- Les adresses IP concernées sont
  - 10.11.2.12
  - 10.11.1.3
  - 10.11.1.4
  - 10.11.1.5

Indicateurs de compromission :

- TTPs :
  - T1018 (Remote System Discovery)
  - T1021.002 (Remote Services : SMB/Windows Admin Shares)
  - T1110 (Brute Force)

- T1135 (Network Share Discovery)

Actifs impactés :
- Serveurs DCs de la zone Europe.
- DMZ de la zone Europe
- Imprimante 3 de la zone Europe : EU-PRT3 (IP 10.3.2.3).

Informations supplémentaires :

Source et raison de levée de l'alerte	Qualification de l'alerte	Justification de la qualification
Source : SIEM (événements Windows)	Faux positif	Pas de succès d'authentification suite aux nombreux échecs. Probable problème de configuration de l'accès à l'imprimante 3.

Alerte : (ALE-7) Malicious e-mail detected

Détails d'investigation :
- Date de l'alerte : 19/02/2023 à 15h00
- Adresse mail du destinataire : romeo.hernandez@carochan.com.
- Adresse mail de l'envoyeur : julie@closedclassrooms.com.
- Pas de pièce jointe.
- Pas de lien dans le corps du message.
- Le nom de domaine closedclassrooms.com n'est pas reconnu comme malicieux. (https://talosintelligence.com/reputation_center/lookup?search=closedclassrooms.com)
- Pas de provocation de sentiment d'urgence dans le titre ou corps du message. Le contenu est de caractère publicitaire / promotionnel.

Indicateurs de compromission :

Actifs impactés :
- Boîte email de l'utilisateur romeo.hernandez

Informations supplémentaires :

Source et raison de levée de l'alerte	Qualification de l'alerte	Justification de la qualification
Signalement utilisateur. Emetteur inconnu	Faux positif	Pas d'élément malicieux donc pas d'incident de sécurité à craindre.

II. Analyse

Dossier #1 : Brute Force attack

Alertes :

- ALE-1 : « Multiple authentication failures followed by success »

Caractéristiques :

- La totalité des serveurs DC de la zone Europe sont sollicités pour ces tentatives d'authentification.
- Nombre et fréquences des tentatives d'authentification semblent indiquer une attaque Brute Force automatisée.
- Authentification réussie après de nombreux échecs : compromission d'un compte utilisateur

Commentaires/observations :

Scénario :

- Accès initial (TA0001) par Brute Force sur le compte utilisateur « carter » via RDP.

Dossier #2 : Suspicious remote administration of accounts and privileges

Alertes :

- ALE-2 : « Privileged user created »
- ALE-3 : « Potential memory dump of lsass process detected »

Caractéristiques :

- Opérations liées à la gestion des utilisateurs et accès effectuées depuis l'extérieur du réseau de Carochan (via la DMZ).

Commentaires/observations :

Scénario :

- Accès aux identifiants (TA0006) par dump mémoire de LSASS.
- Accès initial (TA0001) et Persistance (TA0003) par création puis manipulation d'un compte avec Elévation de Privilèges (TA0004).

Dossier #3 : SMB Scan

Alertes :

- ALE-4 : « SMB Scan detected »

Caractéristiques :

- Plusieurs adresses IP du LAN Servers de la zone EU impliquées.
- Une adresse IP du Lan Utilisateurs de la zone EU impliquée.

Commentaires/observations :

Scénario :

- Acteur malicieux ayant eu accès à certains LAN de la zone EU et réalisant une Découverte des ressources partagées sur le réseau (T1021.002 ; T1135).

III. Plans d'action

Dossier #1 : Brute Force attack

Plan d'action :

- Isoler et nettoyer le compte « carter » : révocation du token d'authentification, réinitialisation du mot de passe.
- Analyse forensique des Serveurs DC de la zone Europe.
- Durcir les politiques d'authentification : nombre / fréquence de tentatives avant blocage du compte.
- Appliquer l'authentification à plusieurs facteurs.
- Configurer SNORT pour interdire le trafic vers et depuis l'IP 104.244.77.53.

```
reject tcp 104.244.77.53 any <> $HOME_NET any (msg: «IP 104.244.77.53 detected»;
sid: 1000001; rev:1;)
```

- Mettre à jour la configuration des GPOs relatives aux accès anonymes.

Dossier #2 : Suspicious remote administration of accounts and privileges

Plan d'action :

- Supprimer le compte utilisateur « ext-adm ».
- Isoler et auditer le compte utilisateur « vagrant » ; révoquer son token d'authentification, réinitialiser son mot de passe.
- Audit du groupe utilisateurs « Administrators ». Vérifier la bonne application des politiques de sécurité (pas de comptes domaines dans le groupe des administrateurs locaux).
- Vérifier l'application des politiques de sécurité relatives à LSASS (Credential Guard activé).
- Configurer Snort pour surveiller les appels au service Kerberos depuis la DMZ de la zone Europe.

```
alert tcp 10.11.1.2 any <> $HOME_NET 88 (msg: «traffic towards port 88 from EU-
DMZ»; sid: 1000002; rev: 1;)
```

Dossier #3 : SMB Scan

Plan d'action :

- Déterminer la façon dont l'attaquant a eu accès aux LANs Servers et Utilisateurs de la zone EU.
- Revoir la segmentation réseau (changer les masques de sous-réseaux) pour éviter un trop grand nombre d'adresses IP disponibles non utilisées.
- Vérifier la configuration de la GPO « Do Not Allow Anonymous Enumeration of SAM Accounts and Shares »