Rapport d’Incident :
Analyse et plan d’action

Remplissez ce document avec les informations demandées, pour chaque alerte qui représente une menace. N’oubliez pas d’inclure des captures d’écran dans toutes les instances indiquées.

NB: Un seul gabarit est fourni par section. Copiez et collez le gabarit autant de fois que nécessaire pour représenter le nombre d’alertes et/ou dossiers concernés.

I. Investigation

Alerte : Potentiel dump de mémoire de lsass.exe détecté sur dc.carochan.com (10.11.1.2), avec des signes de manipulation de comptes et d'élévation de privilèges.
Risque: Elevé

Détails d’investigation

Reportez ici toutes les informations que vous avez pu recueillir sur l’alerte. Ajoutez ou enlevez des points au besoin.

Événement : Alerte liée à un dump mémoire de lsass.exe (Process ID : 608) le 01/03/23 à 18:30, détectée par l’EDR.
Source de l’alerte : Événements Windows, Event ID : 4674.
Entités observées :
Nom de fichier : C:\Windows\System32\lsass.exe
Adresse IP : 10.11.1.2
Nom d’hôte : dc.carochan.com

Détaillez ici les éléments qui permettent d’identifier cette menace dans l'avenir. Soyez le plus précis possible. Ajoutez ou enlevez des points au besoin.

Manipulation de Comptes : Ajout de l’utilisateur ext-adm au groupe Administrateurs le 15/05/2023 par vagrant depuis 10.11.1.2.
Création de Comptes : ext-adm créé et activé, indiquant une potentielle persistance.
Accès Anonyme Suspect : Tentative d'accès de type ANONYMOUS LOGON.
Tentatives de Réinitialisation de Mot de Passe : Plusieurs échecs pour ext-adm par vagrant.

Actifs impactés

Détaillez ici les machines, applications et utilisateurs impactés par cette alerte. Soyez le plus précis possible. Ajoutez ou enlevez des points au besoin.

Contrôleurs de Domaine : FR-SRV-DC01 (10.11.1.3) , FR-SRV-DC02 (10.11.1.4), FR-SRV-DC03 (10.11.1.5), FR-SRV-DC04 (10.11.2.12)

Utilisateur impliqué : vagrant, effectuant des modifications suspectes.

Informations supplémentaires

Remplissez le tableau avec les informations indiquées.

Source et raison de levée de l'alerte	Qualification de l'alerte *(faux positif ou incident vérifié)*	Justification de la qualification
Potentiel dump mémoire de lsass.exe, impactant les politiques de sécurité des DCs.	Risque: Elevé	Comportement anormal, modifications de comptes, et accès non autorisés identifiés.

II. Analyse

Dossier : Activités Malveillantes Ciblant les Comptes Privilégiés et le Contrôleur de Domaine FR-SRV-DC04

Alertes :

Listez ici les alertes regroupées dans ce dossier. Ajoutez ou enlevez des points au besoin.

- Multiple Authentication Failures Followed by Success
- Privileged User Created
- Potential Dump Memory

Caractéristiques

Détaillez ici les éléments communs qui réunissent ces alertes. Ajoutez ou enlevez des points au besoin.

Adresses IP :

10.11.2.12 (FR-SRV-DC04) impliquée dans les activités suspectes.
Tentatives de connexion bruteforce et manipulations suspectes sur les contrôleurs de domaine.
Serveur critique commun :

FR-SRV-DC04 comme point central des attaques.

Commentaires/observations

Si vous avez des observations à signaler par rapport à ce dossier, notez-les ici. Ajoutez ou enlevez des points au besoin.

L'utilisateur vagrant semble être au centre de l'activité suspecte.
La création et suppression rapide de comptes indiquent des efforts de dissimulation.

Scénario :

Un attaquant a compromis un compte privilégié (vagrant), utilisé pour élever des privilèges et modifier la structure des comptes, avec un potentiel dump de lsass.exe pour extraire des informations d'authentification.

III. Plans d'action

Dossier : Potentiel dump de mémoire de lsass

Plan d'action

Contenir la menace :

Suspendre les comptes vagrant et ext-adm.
Bloquer les adresses IP suspectes : 10.11.1.2, 10.11.1.3, 10.11.1.4, 10.11.1.5, et 10.11.2.12.

Sécuriser les systèmes :

Supprimer ext-adm du groupe Administrateurs.
Analyser et protéger lsass.exe en activant Credential Guard.
Auditer les actions passées des comptes vagrant et ext-adm.

Investiguer les activités :

Vérifier les logs des contrôleurs de domaine pour les événements ANONYMOUS LOGON et l'Event ID 4674.
Rechercher des connexions réseau suspectes entre les IPs identifiées.

Renforcer la sécurité :

Configurer des alertes SIEM pour surveiller les modifications de privilèges et les créations de comptes.
Restreindre les privilèges et l'accès à lsass.exe à des comptes autorisés.