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 : Scan SMB détecté sur le réseau, indiquant un comportement de balayage potentiel visant à découvrir des services SMB ouverts.
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.

Type d'Alerte : Network Scan SMB
Source : SIEM
Date : 01/04/23 à 18:00
Firewall : 10.0.254.254
Port de Destination : 445 (protocole SMB)
Protocole : TCP
IP Source : Plage 10.11.2.0/24
IP Destination : Plage 10.11.0.0/16

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.

10.11.2.198, 10.11.2.92, 10.11.2.53, 10.11.2.71, 10.11.2.159, 10.11.2.247. Associées au réseau des serveurs . Ces adresses IP spécifiques mentionnées appartiennent à des plages réseau utilisées par Carochan. Cependant, elles ne sont pas répertoriées individuellement dans la CMDB comme étant associées à des équipements documentés, préoccupant.

10.210.1.4 et 10.210.1.5 : Associées à des services cloud et à des domaines de test, nécessitant une surveillance mais sans être des indicateurs de compromission immédiats.

10.10.1.135 et 10.10.3.74 : Associées à des machines d'utilisateurs qui ne devraient pas initier de scans SMB. 10.210.1.3 ayant communiqué avec le fichier malveillant "CHUJFIZ.EXE".

Port Utilisé : 445, qui est critique pour le partage de fichiers et peut être exploité par des attaques de propagation ou d'exfiltration de données.

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.

Serveurs : Réseau des serveurs (10.11.0.0/16), avec des tentatives de connexion vers des IPs diverses. (10.11.2.198, 10.11.2.92, 10.11.2.53, 10.11.2.71, 10.11.2.159, 10.11.2.247)
Utilisateurs impliqués : 10.10.1.135 et 10.10.3.74, déterminer l'origine de leur comportement suspect.
Infrastructure critique : Services SMB sur le réseau des serveurs.

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
Source:SIEM Balayage réseau SMB détecté, analysé par le firewall.	Risque: Elevé	Présence d'IPs non autorisées effectuant des scans SMB sur le réseau. |

II. Analyse

Dossier :

Alertes :

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

Caractéristiques

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

Commentaires/observations

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

La présence de machines utilisateurs dans les logs de scan est inquiétante et pourrait indiquer une compromission.
Les serveurs impliqués nécessitent une vérification approfondie pour éviter la propagation d'une éventuelle attaque. Les adresses IP spécifiques mentionnées appartiennent à des plages réseau utilisées par Carochan. Cependant, elles ne sont pas répertoriées individuellement dans la CMDB comme étant associées à des équipements documentés, ceci semble anormal et donc préoccupant.

Scénario :

Un attaquant potentiel a initié un scan SMB depuis des IPs de serveurs et de machines utilisateurs, ce qui suggère une recherche de services vulnérables.
Des machines compromises pourraient tenter de se propager en utilisant le protocole SMB.

III. Plans d'action

Dossier : SMB Scan Carochan

Plan d'action

Contenir la menace :

Bloquer les adresses IP suspectes identifiées :
10.11.2.198, 10.11.2.92, 10.11.2.53, 10.11.2.71, 10.11.2.159, 10.11.2.247, 10.10.1.135, 10.10.3.74, 10.210.1.3.
Restreindre l'accès au port 445 sur le pare-feu pour limiter les connexions SMB non autorisées.

Sécuriser les systèmes :

Vérifier les serveurs impactés pour détecter des scripts ou logiciels malveillants.
Analyser les machines utilisateurs (10.10.1.135, 10.10.3.74) pour identifier des signes de compromission.

Investiguer les activités :

Examiner les logs des scans SMB pour identifier les sources des scans et les cibles les plus touchées.

Renforcer la sécurité :

Configurer des alertes SIEM pour surveiller les scans SMB et les connexions suspectes au port 445.
Mettre en place des restrictions réseau pour limiter les scans internes.