Indicator of compromise (IoC)

AUTEUR : BENJAMIN DELAUTRE

Ioc – kézaco ?

- Un indicateur de compromission (en anglais, ***indicator of compromise*** ou ***IOC***), en sécurité informatique, est une trace laissée sur un réseau ou dans un système d'exploitation qui indique, avec un haut niveau de certitude, une intrusion informatique.

- En (trop ?) simple :

  - Les ***IoC*** sont utilisés après qu'une attaque ait été contenue, lorsque l'organisation a besoin de savoir où, quoi et comment.

  - Les ***IoA*** se concentrent sur une attaque en cours qui peut être active et doit être contenue.

IoC – kézaco ?

- Les ***IoC*** peuvent être utilisés pour alimenter la détection en amont des tentatives d'attaque (***IoA*** – ***Indicators of Attack***)

- Les grands réseaux peuvent avoir des milliers d'***IoC***. C'est pourquoi la plupart des preuves sont regroupées et chargées dans des systèmes de gestion des événements de sécurité (***SIEM*** pour ***Security Information and Event Management System***) pour aider les enquêteurs à organiser les données.

Pourquoi parler des ***IoC*** ?

- Détecter les menaces est aussi important que protéger ou être capable de répondre en cas d'une attaque.
- Une bonne connaissance des ***IoC*** permettra de mieux surveiller la sécurité d'un espace
- Une attaque est souvent un processus long
  - Phase de reconnaissance
  - Phase d'intrusion et présence
  - Mouvement latéral
  - Acquisition des privilèges administrateurs
  - Puis… l'attaque survient !

Exemples de *IoC*

- Trafic sortant inhabituel
  - Trafic sortant à des heures inhabituelles ?
- Activité provenant de régions géographiques étranges
  - Adresse IP chinoise tentant d'accéder à la SWDE ?
- Échecs d'authentification élevés
  - Tentative de trouver un compte volé qui donne accès au réseau ?
- Irrégularités de l'activité des supers utilisateurs sur des données sensibles

Exemples de *IoC*

- Augmentation du nombre de lectures de bases de données
  - Niveau de lecture inhabituelle de base données ? Sur des cartes de crédits ?
- Demandes excessives sur des fichiers importants
  - Plus de 200 requêtes sur « secret_du_*Directeur.php* » d'un compte avec moins de privilèges ?
- Changements de configuration suspects
  - Quelqu'un est-il en train de se créer une *backdoor* ?
- Inondation du trafic vers un site ou un emplacement spécifique
  - Ralentissement du réseau ? Sites indisponibles ? Firewall surchargé ? Ca sent le *DDoS*

Utilisations ***IoC***

- les ***IoC*** peuvent être utilisés pour déterminer les causes d'une attaque et éviter tout exploit de la même vulnérabilité dans le futur.

- Les ***IoC*** sont utiles pour la phase de « leçon apprise » pour identifier quelles défenses de cybersécurité ont été mal configurées ou insuffisantes pour arrêter un attaquant.


That's all Folks!

Sources :

- https://blog.f-secure.com/fr/les-5-phases-dune-cyber-attaque-le-point-de-vue-du-pirate/
- https://attacksimulator.com/blog/how-to-recognize-indicators-of-compromise/
- https://soteria-lab.com/blog/article/comment-reagir-pendant-et-apres-une-cyberattaque/
- https://www.nouvellespublications.com/cybersecurite-comment-reagir-pendant-apres-et-avant-une-d-attaque-3016.html
- https://fr.wikipedia.org/wiki/Indicateur_de_compromission
- https://www.proofpoint.com/fr/threat-reference/indicators-compromise