

Cyber Threat Intelligence en boucle courte avec un Honey Net

Laurent. Aufrechter (laurent.aufrechter@thalesgroup.com) - Thales

Lise de la Maisonneuve (lise.delamaisonneuve@thalesgroup.com) - Thales

Résumé :

Classiquement, les Honey Pots ont été utilisés pour mesurer les activités malveillantes sur Internet. Il s'agit de dispositifs de leurrage numérique plus ou moins évolués. Des Honey Pots ont ainsi été exposés avec comme objectif de découvrir de nouveaux modes d'attaque, ou des listes de mots de passe utilisées en « brut force ». La Cyber Threat Intelligence s'appuie en grande partie sur ce type de dispositifs. Cela permet de fournir des informations pertinentes à la majorité des entreprises et aux utilisateurs pour comprendre la spécificité de leurs menaces (opportunité, motivation, capacité).

Cependant, certaines sociétés sont particulièrement exposées du fait de leurs activités (banque...). Les informations produites par la Cyber Threat Intelligence doivent alors être complétées par une capacité locale.

Cette communication explique comment un Honey Net (sous-réseau hébergeant des Honey Pots) connecté au réseau d'entreprise peut permettre de créer une capacité de Cyber Threat Intelligence locale en interaction avec une cellule de Cyber Threat Intelligence de plus haut niveau.

Mots-clés :

Honey Pot, Honey Net, Cyber Threat Intelligence, stratégie de leurrage

1. Introduction

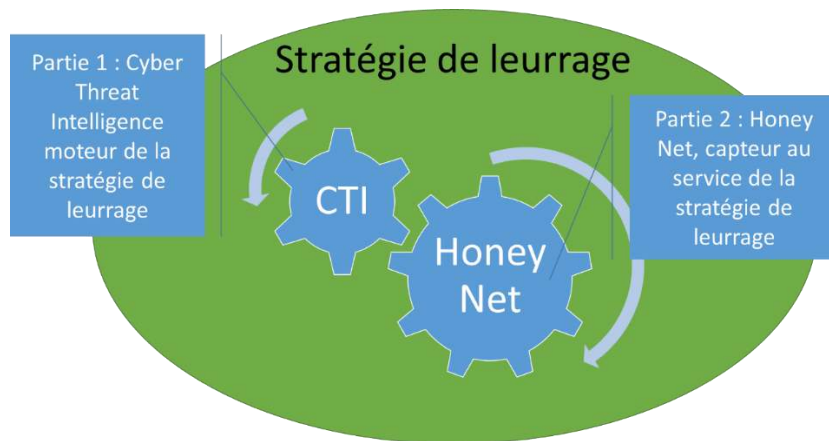
Le leurrage numérique peut prendre différentes formes, mettre en œuvre des techniques plus ou moins évoluées, et maintenant mettre en œuvre de l'intelligence artificielle, avec des réseaux de neurones profonds.

Mais le leurrage doit avoir un but. Celui-ci doit être défini par une stratégie de leurrage qui doit contenir deux éléments clés :

- Le besoin : il peut s'agir d'un besoin de détection, de recueil d'information...
- L'effet à obtenir : quels sont les éléments attendus en sortie du dispositif.

La stratégie doit permettre de définir les moyens de leurrage à mettre en œuvre avec un niveau de détail permettant la configuration d'un Honey Net le plus efficace possible.

Dans notre cas, il s'agit de créer une capacité de détection, et d'alimenter d'une base de données de Cyber Threat Intelligence permettant d'améliorer les capacités de détection et de réaction.



2. Cyber Threat Intelligence moteur de la stratégie de leurrage

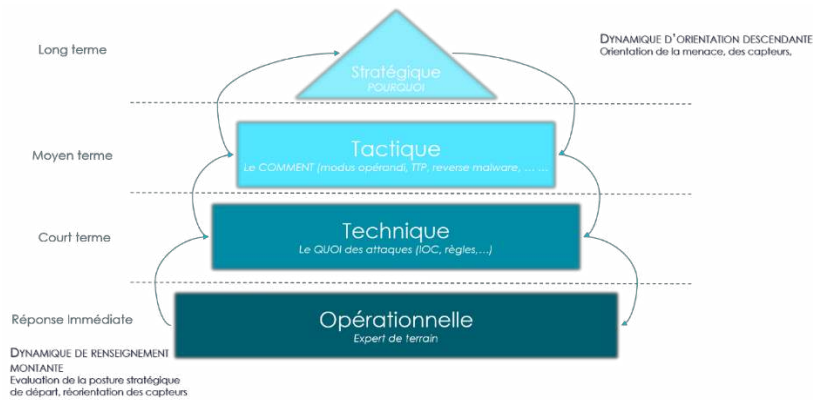
2.1. La Cyber Threat Intelligence, un vecteur de renseignement multi- niveaux

La Cyber Threat Intelligence mobilise par conséquent un ensemble d'outils et de techniques dont l'objectif est de permettre d'avoir la connaissance des éléments suivants :

- Adresses IP et noms de serveurs actuellement utilisés à des fins malveillantes.
- Élément permettant de détecter une attaque : on parle alors d'indicateurs de compromission (IoC).
- Modes opératoires des malwares utilisés par les attaquants.
- Groupes d'attaquants avec leurs modes opératoires privilégiés.
- Motivations de groupes d'attaquants liés à des États ou de grands groupes de cybercriminels.
- Etc.

Cette énumération ne prétend pas à l'exhaustivité des éléments qu'un service de CTI se doit d'apporter. Bien au contraire, cette liste démontre que la CTI s'appuie sur des informations diverses issues de sources recoupées afin d'apporter les renseignements les plus pertinents possible à des équipements réseau, à des administrateurs ou à des décideurs.

Parmi ces informations, on trouve des informations fournies depuis des années par les fournisseurs d'équipements (firewalls par exemple) et de logiciels (antimalware). Les activités liées à la CTI ont, donc, existé avant la création de cette désignation.



2.1.1. CTI opérationnelle

Tel le Monsieur Jourdain de Molière, tout le monde fait de la CTI depuis longtemps, sans le savoir vraiment. Les éditeurs d'antimalware, par exemple, analysent tous les malwares auxquels ils ont accès pour mettre à jour leurs produits. Le client final ne voit qu'une mise à jour de la base de données des signatures. De même, les éditeurs de pare-feu et de sondes réseau (IDS, IPS) font de même pour créer de nouvelles signatures ou identifier des adresses IP utilisées pour des actions malveillantes. C'est grâce à cette Cyber Threat Intelligence « discrète » que les utilisateurs sont protégés d'un grand nombre de menaces.

Cette Cyber Threat Intelligence peut être qualifiée de CTI opérationnelle. C'est en effet une CTI de terrain, réservée à des experts, répondant à des exigences de réactivité. Son objectif est, donc, de fournir des informations pour mettre à jour des moyens de défense des systèmes d'information déployés, et en cours d'utilisation. Elle a vocation à fournir des informations pour des équipements plus que pour des experts, même si certains des artefacts qu'elle produit peuvent être synthétisés dans des tableaux de bord.

Cette CTI opérationnelle n'est pas prise en compte par les DSI, ni les CISO, en tant que telle, parce qu'elle ne permet pas de prendre des décisions. Par exemple, qui sait dire combien de signatures de leurs sondes réseau concernent tel produit ? C'est pourtant un indicateur intéressant sur le nombre de vulnérabilités de ce produit, et sur le fait que ces vulnérabilités soient activement exploitées sur le terrain.

2.1.2. CTI tactique

Pour compléter cette CTI opérationnelle, première étape d'une posture de défense globale, des offres de Cyber Threat Intelligence se sont développées. Les activités effectuées dans le cadre de ces offres concernent des éléments qui ne sont plus uniquement orientés défense immédiate, mais s'inscrivent dans une stratégie plus globale.

La CTI technique s'inscrit dans une stratégie de détection. Elle est considérée comme une défense déployée à court terme, et continuellement renouvelée.

Le niveau tactique entre dans la sphère de l'analyse avancée des informations véhiculées par la CTI. En effet, il est nécessaire à ce niveau d'avoir une équipe d'experts techniques capable d'analyser une attaque (de lire les chaînes de TTP (Techniques, tactiques, procédures)) afin d'en faire ressortir ses spécificités, voire sa signature. Ce travail est d'autant plus important que se développe le « malware as a service ». Les groupes utilisent donc des outils

communs, d'où un phénomène de copycat entre attaquants pour leurrer la cible ou faire porter la responsabilité de l'attaque à un autre groupe.

Ces niveaux intermédiaires sont indispensables à la construction d'une connaissance de la menace qui pèse sur les entités.

2.1.3. CTI stratégique

Ce niveau de CTI est différent des niveaux précédents, à la fois par les produits qu'il délivre et le public qu'il vise. Mais surtout, par son objectif final : permettre la prise de décision. Il y a donc un changement de niveau de vision, par une prise de hauteur de vue.

Une cellule de CTI fournit des rapports permettant à leurs clients de mieux cerner les menaces dans leur domaine d'activité, leur permettant ainsi de mieux dimensionner leurs moyens de détection, que ce soit en termes de matériels, de procédures ou de ressources humaines.

La CTI n'est plus un flux technique enfoui dans un service lié à des équipements, mais un outil de réflexion et de facilitation de la prise de décision permettant aux entreprises de construire une stratégie de défense active en se préparant en fonction des adversaires probables. En changeant de niveau, cela permet aux RSSI de faire un choix éclairé quant aux outils à déployer, de savoir et de justifier où les déployer, et quelles sont les typologies de règles de détection à intégrer.

En résumé, de mettre en place une stratégie de détection optimisée en fonction des budgets disponibles ou de demander des budgets supplémentaires, le cas échéant.

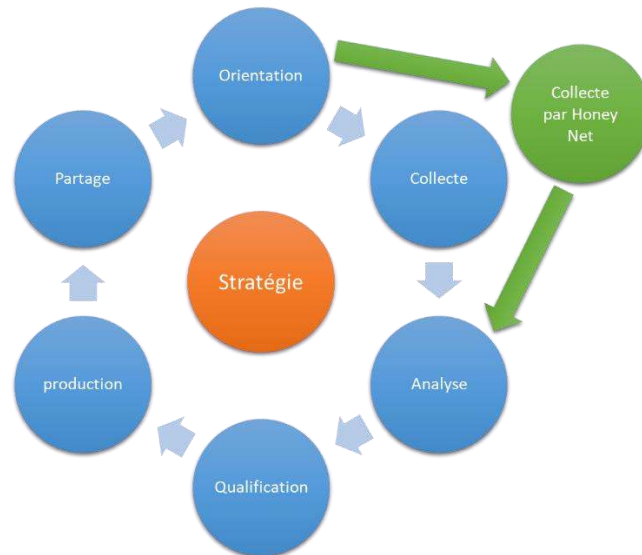
2.2. Limites de la CTI

Pour pouvoir produire des informations, il faut d'abord collecter des données liées aux attaques. C'est pour cela que le partage d'information est primordial, la collecte totale des informations étant impossible par une seule entité. Il faut donc compter sur la communauté cyber pour partager les informations vues à différents endroits. De plus, ces informations peuvent être généralistes ou très spécifiques. D'où le besoin pour une entité de capter ses propres informations.

Cela est d'autant plus important que les groupes d'attaquants achètent parfois des exploits qu'ils n'ont pas la capacité de développer eux-mêmes. Ces exploits ne sont pas vendus ni utilisés qu'une seule fois. Il est donc très probable qu'ils soient identifiés dans plusieurs attaques. Dès que les éléments permettant de les identifier et de les neutraliser seront identifiés par un premier acteur, s'il les diffuse, tous ceux les ayant reçus pourront alors compléter leurs moyens de détection ou, s'ils ont déjà été victimes de l'attaque, mettre en place des remédiations adaptées. Pour les autres, ces exploits restent inconnus et, dans la plupart des cas, indétectables. Les attaquants peuvent alors se déplacer dans le système d'information, y récupérer les éléments d'intérêt de manière discrète, et ceux pendant des mois.

Il faut donc que ces entités trouvent le moyen de réduire le délai entre l'attaque et la contre-mesure à mettre en œuvre. Pour cela, il est indéniable que l'étude de l'attaque dans un environnement neutre et protégé apportera de nouvelles informations déterminantes pour la résolution de l'incident et de ses conséquences. Pour ce faire, il faut mettre en place un ou des capteurs capables de collecter ses informations spécifiques tout en protégeant les analystes et le système.

La solution consiste à intégrer le Honey Net dans le dispositif global, en fonction de la stratégie de leurrage. En faisant un parallèle avec le cycle du renseignement, utilisé par les services de renseignements, le Honey Net assure un rôle de capteur local, en complément des autres sources d'informations, et s'inscrit donc naturellement dans ce cycle.



3. Honey Net

L'utilisation de Honey Pots est souvent perçue comme unitaire et technique. Connectés à Internet, ce sont des filets jetés à la mer qu'on relève de temps en temps pour « sentir l'air du temps », ou remettre à jour des listes d'adresses IP, de mots de passe, identifier une nouvelle vulnérabilité ou un nouveau mode d'action.

À l'intérieur d'une entreprise, un Honey Net n'a pas du tout le même cycle de mise en œuvre ni les mêmes objectifs. C'est un capteur technique configuré en fonction de la stratégie de leurrage.

Cependant, dans le cadre d'un projet, une étude sur les Honey Pots existants montre qu'il s'agit dans la grande majorité de dispositifs techniques. Ces outils sont faits pour être déployés, et ils enregistrent des informations dans des fichiers dans la plupart des cas. Certains ont une interface vers un environnement de Cyber Threat Intelligence et sont capables d'y remonter des artefacts, mais ils sont rares. Cowrie, par exemple, est un Honey Pot qui simule un serveur ssh et telnet, et qui est capable de remonter des informations vers une plateforme de CTI type MISP, par exemple.

Comme tout dispositif technique, un Honey Net n'a d'utilité que s'il s'inscrit dans une stratégie, or, la notion de stratégie de leurrage est aujourd'hui encore mal définie. S'il existe des articles sur le sujet¹, ils restent souvent superficiels, et aucun modèle standardisé n'existe pour définir ce type de stratégie.

¹ <https://securitybrief.com.au/story/six-benefits-of-initiating-a-deception-strategy-for-it-security-teams>
<https://medium.com/taslet-security/deception-as-a-strategy-for-cyber-security-b8e1c317fdaa>

Dans le cadre de ce projet, il a été choisi de déployer un Honey Net à l'intérieur de l'entreprise pour en faire un sous-réseau complet. Ce Honey Net a deux objectifs distincts : détecter des activités anormales et, à partir de ces activités, créer des artéfacts de Cyber Threat Intelligence.

3.1. Définition d'un Honey Net

Il n'existe pas de définition standard sur les Honey Net. La définition suivante² est cependant intéressante parce qu'elle regroupe un certain nombre d'éléments :

« A honeynet is a network set up with intentional vulnerabilities; its purpose is to invite attack, so that an attacker's activities and methods can be studied, and that information used to increase network security. A honeynet contains one or more honey pots, which are computer systems on the Internet expressly set up to attract and "trap" people who attempt to penetrate other people's computer systems. Although the primary purpose of a honeynet is to gather information about attackers' methods and motives, the decoy network can benefit its operator in other ways, for example by diverting attackers from a real network and its resources. The Honeynet Project, a non-profit research organization dedicated to computer security and information sharing, actively promotes the deployment of honeynets.

In addition to the honey pots, a honeynet usually has real applications and services so that it seems like a normal network and a worthwhile target. However, because the honeynet doesn't actually serve any authorized users, any attempt to contact the network from without is likely an illicit attempt to breach its security, and any outbound activity is likely evidence that a system has been compromised. For this reason, the suspect information is much more apparent than it would be in an actual network, where it would have to be found amidst all the legitimate network data. Applications within a honeynet are often given names such as "Finances" or "Human Services" to make them sound appealing to the attacker. »

Cette définition reprend les objectifs des Honey Pots, qui est de récupérer de l'information, en précisant que le Honey Net doit se faire passer pour un sous-réseau réaliste, représentatif de ce qu'on peut trouver dans le reste du système d'information de l'entreprise. Aucune information n'est donnée sur comment ce Honey Net est interfacé avec un outil d'exploitation des informations. Elle ne fait par contre aucune référence au fait qu'il puisse participer à la détection d'une attaque, ce qui ne peut être le cas que s'il est déployé dans un réseau d'entreprise.

3.2. Honey Net et détection

Lors d'une attaque, un des objectifs est de cartographier le système. Cela permet de repérer où sont les ressources ayant le plus de valeur. Il peut s'agir d'une base de données contenant des informations personnelles, des plans industriels, des données financières ou l'accès au contrôle de la production d'une usine. Lors de cette cartographie, les attaquants vont devoir explorer le réseau, souvent à partir d'un nœud du réseau leur donnant une visibilité sur le maximum d'ordinateurs. Par exemple, un nœud type Active Directory est une prise de grande valeur. Si le Honey Net est connecté au reste du réseau de l'entreprise, il est fort probable que tôt ou tard, les attaquants ont de grandes chances de s'y retrouver. Il existe plusieurs techniques pour les « aider » à

² <https://searchsecurity.techtarget.com/definition/honeynet>

trouver le Honey Net ou des nœuds en faisant partis. L'objectif est clairement d'essayer autant que faire se peut « d'aider » ces attaquants à le trouver.

Il existe plusieurs types de Honey Pot suivant le niveau d'interactions qu'ils offrent à l'attaquant. Certains sont très basics : ils présentent une page d'authentification qu'aucun mot de passe ne permet de déverrouiller. Ils sont qualifiés de Honey Pot basse interaction. D'autres simulent certains comportements d'un système, ce qui fait d'eux des Honey Pot de moyenne interaction. Enfin, on peut mettre en place un vrai serveur « moyennement » protégé mais très contrôlé pour créer un Honey Pot à forte interaction. Pour que les attaquants passent le maximum de temps dans un Honey Net, il faut combiner ces trois niveaux de Honey Pot. Sinon, les attaquants chercheront des cibles plus faciles, qui risquent d'être des nœuds du vrai système d'information. Cela doit cependant être fait avec précaution pour éviter que des nœuds du Honey Net ne soient utilisés par l'attaquant pour mener des actions malveillantes à l'intérieur ou l'extérieur du système d'information attaqué. Un système de type « bouton rouge » doit être disponible pour déconnecter facilement et rapidement le Honey Net. L'automatisation de cette déconnexion est un choix judicieux : mieux vaut perdre de l'information que de servir de vecteur d'attaque.

3.3. Infrastructure du Honey Net

Pour implémenter le Honey Net, nous avons fait le choix d'utiliser Docker et une infrastructure SDN.

Ces deux choix permettent d'avoir une malléabilité de notre outillage qui est forte, et qui permet facilement de créer un sous-réseau crédible au regard du reste du système d'information dans lequel il est implémenté. Typiquement, le changement de système d'exploitation des machines n'est pas trop pénalisant, même si les procédures d'installation des différents outils sont différentes. Comme notre objectif n'est jamais d'avoir des systèmes d'exploitation durcis, aucun effort n'est fait sur ces axes. Au contraire, utiliser des images Docker permet de choisir précisément la version du système que l'on veut, avec les vulnérabilités associées.

Cette infrastructure permet d'avoir un outil malléable, qui permet d'avoir un dispositif se fondant dans l'infrastructure hôte. Cet aspect prend toute sa valeur quand le Honey Net est vu comme un capteur du renseignement cyber : il est possible de réorienter le Honey Net si cela s'avère nécessaire, ou de compléter le dispositif. Le Honey Net n'est pas obligatoirement un dispositif positionné en un point unique d'un système d'information : il est possible de déployer plusieurs instances dont le contenu peut varier en fonction des informations recueillies dans le premier Honey Net impacté. Ces variations peuvent porter aussi bien sur la forme (nombre et types de machines, plan d'adressage IP...) que sur le fond (type et nom des documents exposés, type de services...).

Un choix important dans notre implémentation est de créer des événements dans une instance MISP. MISP est une plateforme de Cyber Threat Intelligence reconnue et largement disséminée. C'est un outil à la fois de travail pour les opérateurs, et de partage d'information. MISP intègre nativement la notion de partage contrôlé d'informations, car comme évoqué précédemment, la Cyber Threat Intelligence repose fortement sur le partage.

3.4. Réalisme des Honey Pot

Les répertoires partagés de Docker sont un bon moyen pour animer le Honey Net. Il existe plusieurs cas d'utilisation, mais le plus ludique est sans contestation possible l'animation d'une Webcam.

Un des Honey Pots de notre Honey Net est dédié à la simulation d'une console de vidéosurveillance. Ce choix a été fait pour plusieurs raisons : à la fois parce que c'était en phase avec des travaux internes, mais également parce que tout humain qui tombe sur une Webcam peut se retrouver captivé, pour peu qu'il s'y passe quelque chose. Et enfin, parce qu'un sous-réseau qui héberge une console de contrôle est certainement fréquenté par des administrateurs.

Une console de vidéosurveillance est basiquement un site Web qui met à disposition des images. Dans la première version, l'image présentée est un GIF animé, combinant plusieurs images fixes de pièces différentes. Le problème est que, quel que soit l'heure ou le jour de la semaine, les images sont les mêmes. Dans notre stratégie de leurrage, ce niveau est considéré comme suffisant car la console de vidéosurveillance n'est pas un élément de forte valeur.

Dans d'autres cas, elle pourrait être considérée comme un élément clé. Tout bon film présentant « le casse du siècle » montre l'importance des caméras de surveillance, mais au-delà de cet aspect anecdotique, une console de vidéosurveillance pourrait avoir une importance stratégique, par exemple sur un navire de la Marine Nationale.

Dans ce cadre, si une banque d'images est créée et que l'image présentée est stockée dans un répertoire partagé avec la machine hôte, il est facile de créer un programme qui va prendre les images de la bibliothèque, y ajouter la date et l'heure en surimpression, et écraser l'image affichée par le site. Ces traitements seraient invisibles d'un attaquant qui aurait pris le contrôle de notre site Web.

Il est possible de maintenir l'attaquant devant cette console pour lui faire perdre du temps : il faut par exemple avoir des images de personnes en discussion et qui prennent des notes sur un tableau... L'effort nécessaire pour mettre en place ce programme et la bibliothèque d'images serait fait ou non en fonction de la stratégie de leurrage.

3.5. Reconstruction après attaque

L'utilisation de Docker permet également de résoudre un problème important pour une infrastructure faite pour être compromise : la reconstruction des machines. Après une attaque, une fois que la décision a été prise de passer à l'action, il faut se préparer à l'attaque suivante sans pour autant perdre des informations. Écraser toutes les traces de l'attaque permet de redémarrer plus rapidement, mais cela réduit les chances de pouvoir se protéger d'une répétition d'une attaque identique. Il faut donc conserver les traces tout en redémarrant rapidement le Honey Net.

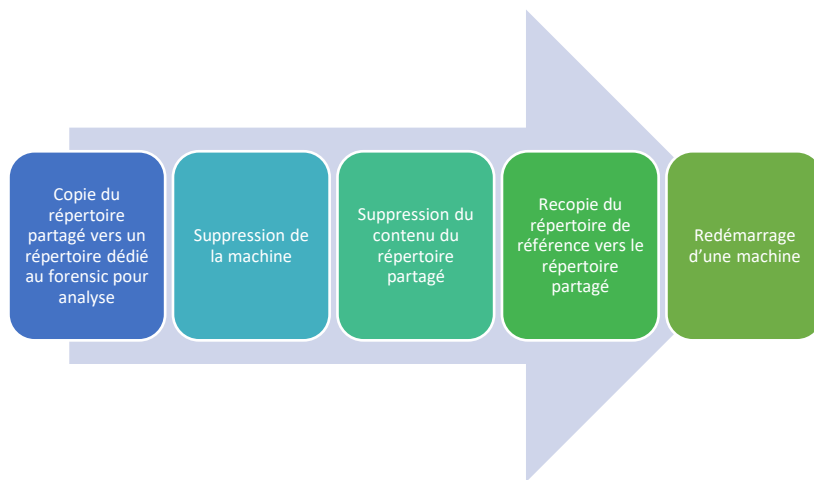
Quand une machine est démarrée à partir d'une image Docker, l'image elle-même n'est pas modifiée au cours de la vie de la machine. De fait, si une machine a été compromise, il suffit de la supprimer cette instance et d'en démarrer une nouvelle. Automatiquement, la machine est « désinfectée ».

Si cela est vrai dans un bon nombre de cas, dès qu'un répertoire est partagé entre la machine hôte et la « machine Docker », les modifications faites dans cette machine deviennent persistantes. Naturellement, supprimer la machine

et en créer une nouvelle n'est plus suffisant, puisque les données qu'elle utilise ont été compromises. Si pour des machines en production avec de vraies données, cela pose un problème sérieux, ce n'est pas le cas du Honey Net où les données ne sont pas des données de production. Cela peut se résoudre en stockant dans un répertoire non accessible des machines Docker une version de référence des données, et d'écraser le répertoire partagé avec ces données avant de redémarrer la machine.

Pour matérialiser cela, prenons l'exemple d'un serveur Web qui présente un site interne. Les données de référence sont stockées dans un répertoire qui n'est pas vu de la machine Docker. Si le site Web est compromis par un attaquant, et que celui-ci procède à un défaçage, le contenu du site Web sera altéré.

Une fois l'attaque identifiée, il faut alors effectuer les étapes suivantes :



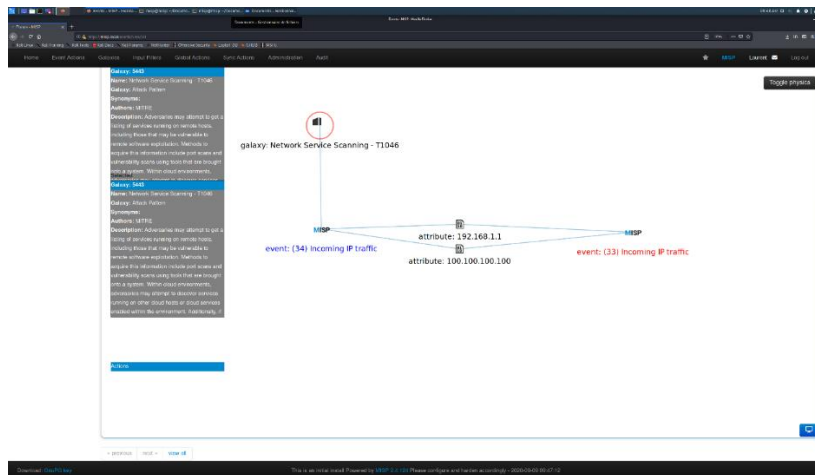
De cette manière, vue de l'extérieur, la machine est remise en état, mais aucun artéfact créé par l'attaquant n'a été perdu.

3.6. Exemple d'évènements créés dans MISP

Si la partie mise en place et gestion du cycle de vie des machines déployées dans le Honey Net est une partie intéressante, la création des évènements dans l'instance MISP est un point plus difficile.

Globalement, MISP permet de stocker des évènements auxquels sont attachés des attributs. Si les évènements ont peu de propriétés, à part un titre et un niveau de diffusion, les attributs sont fortement typés. Cela permet d'identifier chaque information avec une catégorie et une sous-catégorie. Par exemple, dans la catégorie « Network traffic », il y a « ip-src » pour les adresses IP sources et « ip-dst » pour les adresses IP cibles.

Ce typage permet de faire des calculs automatiques d'intersection entre deux évènements. Par exemple, si la même adresse IP source est utilisée dans deux évènements, MISP indiquera cette relation, et permettra de naviguer d'un évènement à l'autre. Il est également possible d'avoir une représentation graphique des évènements et de leurs liens.



La figure ci-dessus montre que les événements 33 et 34 ont en commun deux adresses IP.

Ces outils permettent de faciliter l'analyse des événements, et, si cela s'avère pertinent, de fusionner des événements.

En plus de ce typage, il est possible d'apposer des tags sur les événements et les attributs. Les tags ont été utilisés pour ajouter une information permettant de différencier plus facilement les attributs.

La création des événements nécessite un travail préparatoire d'analyse important. Il faut déterminer quelles sont les informations qui seront extraites à partir des traces d'attaques, comment elles sont catégorisées, attribut par attribut. D'autres questions qui sont loin d'être anodines doivent aussi être adressées, par exemple la stratégie permettant de décider que deux traces doivent être regroupées dans le même événement.

Tous ces éléments font partie de la stratégie de leurrage qui permet de savoir quels sont les types d'événements qui sont pertinents, et un inventaire des données d'entrée pour évaluer la richesse des attributs qu'il sera possible de créer.

À titre d'exemple, deux événements sont présentés.

3.6.1. Attaque de type Brut force contre un service

Dans notre implémentation, les attaques par brut force contre un service peuvent être détectées par deux Honey Pots différents. Dans ce document, un seul type sera présenté.

Le Honey Pot le plus simple en charge de détecter les attaques par brut force génère des logs très simples. Ils contiennent principalement l'heure, l'IP source, le type de service attaqué, et le compte et le mot de passe en clair.

Si le typage des attributs est simple pour les adresses IP, trouver le type de l'attribut pour contenir le compte et le mot de passe est moins trivial. Nous avons utilisé « Targeting data » en catégorie et « target-user » en type. Le choix du typage des attributs est important, mais surtout, il doit être cohérent. Dans notre cas, le fait que les informations soient créées par programme permet d'avoir un niveau de cohérence total.

Les tags utilisés sur les attributs permettent d'avoir le type de service attaqué.

L'analyse des logs générés par notre outillage n'est pas faite en continu. Pour l'instant, nous procédons par batch régulièrement. Cela permet de limiter les échanges avec MISP : il n'est pas utile de vérifier à chaque fois qu'un événement connexe au log existe déjà avant de décider s'il faut en créer un nouveau. Cela ne signifie pas pour autant que tout ce qui est détecté dans une période est stocké dans le même événement. Pour l'instant, le choix a été de créer un événement par IP source. Cela permet de ne pas surcharger la base en créant un événement par machine attaquée avec à chaque fois l'intégralité du dictionnaire d'attaque utilisé. Ce choix est important, car il est fait pour limiter le nombre d'événements créés, pour éviter de surcharger les opérateurs d'informations redondantes. Cela n'est pas anodin : un opérateur surchargé n'est pas un opérateur efficace.

Il faut noter que quand un attribut est créé dans un événement, s'il existe déjà, il n'y a pas de création de doublons. De fait, si le même dictionnaire de mots de passe est utilisé contre plusieurs machines ou plusieurs services, il n'y aura qu'un attribut par couple compte / mot de passe. Ces attributs peuvent être extraits par programme de la base MISP. Il est donc possible de les exporter pour archivage ou pour exploitation.

3.6.2. Requêtes DNS générées depuis un hôte du Honey Net compromis

Quand un hôte du Honey Net est compromis, ce qui est conforme à la définition de Honey Net, il est possible que l'attaquant cherche à télécharger des outils complémentaires, ou à prendre contact avec un serveur de Command & Control pour devenir un bot. Pour cela, il va chercher à entrer en contact avec une machine hébergée sur Internet. Soit il fera une requête directement avec l'adresse IP, soit il accèdera au site via son URL. Dans ce cas, une requête DNS sera automatiquement générée. Celle-ci sera vue par une sonde réseau qui remontera un log spécifique. Ce log est une demande de résolution de nom. La réponse doit revenir rapidement, qu'elle soit positive ou négative.

Dans notre stratégie de leurrage, il a été décidé d'ajouter un tag au niveau de l'événement pour identifier les résolutions de nom qui n'ont pas été résolues. En effet, c'est un cas qui survient quand un bot cherche le prochain serveur de Command & Control, qui repose en général sur un calcul de son nom. Cela signifie qu'un serveur va bientôt utiliser ce nom pour contrôler le réseau de bots. C'est une information particulièrement précieuse, car elle permet de préparer des règles de détection aussi simples qu'efficaces.

3.7. Interface technique avec la CTI

Centraliser des indicateurs de compromission dans un environnement de Cyber Threat Intelligence est loin d'être anodin : c'est un moyen de partage qui peut être aussi bien utilisé entre une entreprise et ses filiales qu'avec une ou plusieurs communautés. Ce partage est d'autant plus important que l'histoire nous a prouvé à maintes reprises que les attaquants passaient par le maillon le plus faible d'une chaîne. Si une entreprise mature du point de vue cyber est en relation avec des fournisseurs qui ne sont pas du même niveau, ceux-ci peuvent servir de vecteur d'attaque. Le partage d'informations de Cyber Threat Intelligence est un moyen efficace de renforcer les maillons les plus faibles des chaînes pour augmenter globalement le niveau de cyber sécurité.

La mise en place du Honey Net dans le cadre de ce projet comporte un environnement de partage d'informations de Cyber Threat Intelligence (MISP). Quand une activité suspecte est détectée dans le Honey Net, un log est envoyé vers le CSOC (Cyber Security Operation Center) pour avertir les opérateurs qu'une attaque est en cours. La création des événements avec leurs attributs fonctionne sur un cycle différent, puisqu'il s'adresse à des utilisateurs différents. En effet, le contenu du MISP ne concerne pas directement les opérateurs de niveau 1, mais plutôt les opérateurs des niveaux suivants qui vont être à même de créer des règles de détection et de les déployer dans la partie opérationnelle du système d'information.

La création automatique d'éléments dans MISP est une piste intéressante pour minimiser les activités manuelles, et également pour avoir une homogénéité forte du typage des données.

Cependant, au-delà des informations recueillies grâce au Honey Net, la plateforme de CTI doit être intégrée dans les processus de réponse à incident des entreprises.

4. Conclusion

Le passage d'une **CTI tactique à une CTI stratégique** requiert une identification claire du besoin, et la création d'une telle capacité ne peut se faire sans une analyse préalable. C'est pourquoi le point de **départ de travaux doit être la stratégie de leurrage**. Actuellement, la définition de cette stratégie est le maillon faible du dispositif. Celle-ci doit permettre de définir la structure et le contenu du Honey Net à mettre en place.

Elle doit également prendre en compte les moyens de détection disponible pour permettre d'exporter dans un format adéquat les informations vers les capteurs, pour éviter des étapes supplémentaires dans la mise en place de la détection.

L'utilisation d'un Honey Net à l'intérieur d'une entreprise peut servir à alimenter une capacité de Cyber Threat Intelligence locale permettant de mieux combattre les attaques les plus ciblées. Cette capacité locale doit permettre de faire le lien avec la Cyber Threat Intelligence « générale » dans un cycle permettant d'adapter le contenu du Honey Net en fonction de l'évolution de la menace. Les échanges entre les deux éléments doivent obligatoirement être bidirectionnels.

Pour cela, le Honey Net doit être à la fois riche et malléable : il doit pouvoir persuader les attaquants qu'ils sont effectivement dans un sous-réseau « normal », avec des informations réelles et de valeur. Cela implique un alignement du contenu en termes de système d'exploitation que de types de technologies. Si une entreprise est équipée uniquement de serveurs Windows, un sous-réseau où tout est basé sur Linux n'est ni réaliste ni intéressant. De fait, toutes les attaques sur le Honey Net ne seraient pas applicables sur l'environnement de production.

Il ne faut pas imaginer le Honey Net uniquement comme un sous-réseau particulier. Il peut être partitionné en plusieurs sous-réseaux avec plusieurs points d'accroche dans le réseau. Ces points d'accroche devront être positionnés à des endroits stratégiques : interfaces avec un réseau externe, machines servant à des fins d'administration ou permettant des opérations stratégiques pour l'activité de l'entreprise. À chacun des points de connexion d'un Honey Net, le contenu devra être pertinent pour motiver l'attaquant à utiliser ses moyens d'attaque, et ainsi permettre de les contrer.

La plateforme de CTI n'est pas un outil automatique : il faut qu'elle soit exploitée par des opérateurs qui seront capables, à partir des événements créés automatiquement, de produire des indices de compromission, mais surtout de comprendre la stratégie de l'attaquant, voire des attaquants si plusieurs attaques ont lieu en même temps. Et si possible de rattacher les attaques à des groupes connus, ou à des campagnes en cours.

C'est là que la vision globale portée par la stratégie de leurrage montre toute sa valeur : si une entreprise a été prévenue qu'un groupe particulier risque de les attaquer et que le Honey Net permet de rattacher une attaque en cours à ce groupe, les risques liés à cette attaque seront bien moindres. De fait, même si l'attaque n'a pas été détectée dans la partie opérationnelle du système d'information, les équipes internes sauront quels sont les éléments à chercher (canaux de Command & Control, malware avec un comportement précis...). La diminution du temps de réaction, le gain de temps dans l'évaluation du périmètre de l'attaque et de l'organisation des remédiations fera la différence entre une entreprise préparée et les autres.

Dans ce cadre, le leurrage numérique est un moyen efficace de participer à la protection des systèmes d'information.