WAVESTONE

LETTRE DU CERT-WAVESTONE

N°7

SOMMAIRE

DOSSIER

LA NUIT LA PLUS LONGUE : RETOUR SUR UNE GESTION DE CRISE DANS LE CADRE D'UNE ATTAQUE D'ENVERGURE

Nous vous proposons une histoire vraie, basée sur des faits réels, mais anonymisée et romancée pour vous faire vivre les coulisses de la gestion d'une attaque ciblée.

Près de 15 membres du CERT-Wavestone ont été mobilisés pendant près de deux semaines sur cette affaire : participation à la cellule de crise de la Direction Générale, pilotage des investigations et de la préparation du plan de défense, point de contact pour les forces de l'ordre... nos équipes ont pu participer à un large panel d'activités de gestion de crise.

Ceci est leur histoire.

Prologue - La Qualification

[Gérôme] Jeudi soir, 18h30, un consultant entre dans mon bureau :

- *J'ai un client qui vient de m'appeler, il semble avoir un incident important avec des systèmes métiers touchés, il voudrait qu'on l'aide.*

Immédiatement, j'ai demandé à Vincent, le responsable technique de notre équipe de réponse à incident, d'appeler le client pour qualifier la situation.

[Vincent] Je me rappelle, c'était un jeudi soir et je descendais du RER juste avant de prendre mon bus… lorsque j'ai reçu un appel de Gérôme pour m'indiquer qu'un de nos clients avait besoin de notre aide pour une affaire de vol de données. À ce moment-là, nous n'avions pas beaucoup d'informations.

J'ai me suis isolé afin de pouvoir rapidement appeler notre contact, le RSSI de l'entité France. Ce dernier m'a alors présenté le contexte global : ils ont découvert un malware sur un de leur serveur qui volerait peut être des données de leurs clients. J'ai alors cherché à en savoir un peu plus :

- *Comment avez-vous détecté ce malware et qu'est-ce qui vous fait penser qu'il vole des données de vos clients ?*
- *Et bien nous avons installé un outil de solidification sur nos serveurs et ce dernier a levé des alertes sur un fichier. Au début, nous avons juste supprimé le fichier… mais il est revenu quelques temps après. Du coup je l'ai transmis à un de nos partenaires pour effectuer une analyse… et je viens de recevoir un pré-rapport : le programme crée des fichiers, les chiffre et semble les récupérer au travers d'un autre programme. Toutefois, nous ne savons pas quelles sont les données qui sont mises dans ces fichiers…*
- *Qu'a de particulier ce serveur ?*
- *Il s'agit d'un serveur local sur un de nos sites. Nous avons plus d'une centaine de sites en France. Nous souhaitons vérifier s'il n'y a pas d'autres sites qui seraient touchés…*
- *Quel type de données voit passer ce serveur ?*
- *Il s'agit surtout de données personnelles de nos clients…*

À ce moment-là, j'ai décidé de déclencher un ticket d'intervention CERT en mobilisant un de nos first responders. Il s'agit d'analystes du CERT-Wavestone formés aux premiers reflexes d'investigation qui se déplacent sur site pour démarrer les analyses et délivrer les premières actions de défense à nos clients. Je me souviens avoir appelé Ayoub dans la foulée pour le briefer sur ce qu'il allait devoir faire, le contexte, les premières informations récoltées, etc.

- *Ayoub, ta mission, que tu acceptes, est de te rendre chez VictimCorp afin d'évaluer le périmètre et l'étendue de l'attaque. Idéalement, commence à identifier des actions de correction urgentes et collecte les informations nécessaires pour que l'on qualifie rapidement le dimensionnement de l'équipe à déployer si besoin, ainsi que les compétences dont nous allons avoir besoin.*
- *Bien reçu, je m'organise et je pars avec notre kit d'outillage***.**

[Gérôme] Dès que Vincent m'a appris le sérieux de l'affaire et de la mobilisation d'un first responder, nous avons décidé, avec l'accord de notre client, de contacter un cabinet d'avocat spécialisé et un huissier. Vu le type et la sensibilité des données potentiellement exposées, il était crucial d'avoir un support juridique et d'intervenir dans les règles de l'art.

Le First Responder

[Ayoub] Le ton de Vincent au téléphone était un peu tendu, peut-être même urgent mais loin d'être alarmant. Il y a assez d'applications non maitrisées dans tout système d'information pour causer des flux ponctuels que l'on pourrait qualifier, à tort, de suspects… J'ai commencé néanmoins les préparatifs de voyage : outillage d'investigation (disques durs, boiter Tableau, vêtements de rechange pour une journée voire deux si besoin, billets de train, réservation d'hôtel, etc.).

Le lendemain matin, j'ai été accueilli sur site par le responsable sécurité de l'entité qui m'a présenté l'équipe qui travaillait sur l'incident : administrateurs systèmes, administrateurs réseaux… ainsi qu'un autre analyste forensic. Tout d'un coup l'affaire semblait un peu plus sérieuse qu'anticipée.

L'équipe m'a expliqué les éléments observés :

- *Un exécutable suspect a été identifié par un outil de solidification qui a été déployé sur des systèmes Windows.*
- *L'exécutable persistait malgré les nombreuses tentatives d'arrêt et de suppression.*
- *Des fichiers portant une extension inconnue ont été découverts sur des partages présents sur le système.*
- *Ces partages étaient quotidiennement renouvelés.*
- *Il n'était pas possible de lire les fichiers déposés.*

Craignant qu'il s'agisse de vieux serveurs Windows 2003, je demandais :

- *Le malware touche quelles versions de Windows ?*
- *Nous l'avons principalement identifié sur du Windows 2000 pour l'instant… c'est des machines métiers qui hébergent des applications très sensibles, c'était trop coûteux de les faire migrer…*

La tension était palpable et je comprenais les enjeux désormais : si les soupçons de VictimCorp étaient fondés, des milliers, voire dizaine de milliers, de données clients pouvaient être potentiellement impactées.

Nous nous sommes installés dans une petite salle avec un accès à distance à l'une des machines infectées. Ceci va bien sûr à l'encontre des bonnes pratiques d'investigation usuelles, mais nous possédions assez de machines infectées pour nous permettre une extraction plus aux normes plus tard, si cela se révélait nécessaire. Nous avions une réunion avec le DSI l'après-midi et il fallait rapidement des résultats factuels. Nous avons donc décidé de prendre ce risque.

Il était assez trivial de retrouver le malware en question : tous les binaires du répertoire C:\Windows\System\ dataient de 2009, excepté le malware qui affichait la date d'octobre 2014. Au passage, nous étions en mars 2015...

Beaucoup de questions restaient toutefois sans réponse :

- Combien de sites en France étaient impactés ?
- Était-ce limité au périmètre France ?
- Comment l'attaquant récupérait-il les fichiers créés ?
- Où se situait l'attaquant ?

Mais plus important encore, une question tacite que je n'avais pas anticipée trottait dans l'esprit de la Direction, une question qui a entrainé beaucoup de complications et qui aurait pu causer encore plus de dégâts...

[Gérôme] Resté à Paris, je suivais le déroulement des investigations à distance. À 11h, les premiers retours sur place alimentaient les suspicions d'une attaque importante. Le binaire observé était bien un malware qui réalisait de l'exfiltration de données. Celui-ci n'était pas connu des systèmes de protection classiques, il avait été adapté au contexte métier et technique. Nous étions face à une attaque d'une complexité non-négligeable mais surtout ciblée, visant délibérément les systèmes de notre client. Nous commencions à remonter la piste de la compromission. La tâche n'était pas aisée, peu de journaux existaient, les systèmes étaient tous à plat, il était difficile de trouver des points d'analyse.

En milieu de journée, d'autres informations de sources différentes et externes confirmaient les doutes. Il ne fallait plus attendre, la Direction devait être prévenue. Le DSI avait déjà été informé et il avait lui-même initié des premières actions vis-à-vis du comité de Direction. Mais vu la criticité des données et le nombre de systèmes touchés, il était nécessaire de passer en crise.

[Ayoub] Nous avons continué l'analyse afin d'identifier les mécanismes de persistance utilisés par le malware : clés de registres impactés, services créés, etc. Il s'est avéré qu'en termes de complexité technique, c'était probablement le malware le moins intéressant que l'on puisse rencontrer : exécution au niveau userland, clés de registre RUN pour assurer la persistance, nom commun à l'ensemble des versions des exécutables, etc. L'inspection de machines supplémentaires a permis d'identifier trois autres versions du malware. Ces différentes versions récupéraient les fichiers chiffrés et réinfectaient les autres systèmes si jamais ils étaient nettoyés : au total, il devait y avoir plus de 3000 machines infectées.

[Jean] Vendredi, 17h, alors que je venais de pusher mon dernier commit sur CERTitude, j'ai reçu un appel de Vincent, loin d'imaginer qu'il s'agissait là du premier pas dans l'équipe d'investigation de VictimCorp.

- *Salut Jean, tu as un peu de temps libre ?*
- *Pas beaucoup de temps, ma cérémonie de remise de diplôme est dans une heure et demie, à Bercy...*
- *Parfait ! Je vais t'envoyer deux exécutables, trouve moi tout ce que tu peux dessus.*

J'ai reçu dans la foulée un email chiffré contenant lesdits exécutables, puis ai entamé l'analyse des fichiers méchant1.exe et méchant2.exe, sans toutefois arriver à un résultat concluant dans la limite de temps imposée.

[Ayoub] À 18h, Vincent m'a appelé pour avoir des nouvelles :

- *Tu as besoin d'aide Ayoub ?*
- *Oh oui...*
- *Combien de personnes à peu près ?*
- *Illimité... la Direction a annoncé un budget illimité...*

À 21h, un représentant de la Direction est venu me voir, l'air assez sérieux en dépit de sa tenue sportive, et ferma la porte derrière lui.

- *Ayoub, il y a de vrais enjeux derrière cet incident. VictimCorp, c'est plusieurs centaines de milliers de collaborateurs. Pour être franc, je me demande s'il n'y a pas des possibilités de complicités internes.*

J'ai rappelé au client qu'au vu des éléments observés, tous les scénarios restaient possibles. En prévision, nous avons quand même bien suivi toutes les règles permettant d'amener l'affaire

devant un tribunal, en particulier en impliquant notre cabinet d'avocat partenaire.

La Crise

[Gérôme] Vendredi soir, la première réunion de crise a eu lieu, j'y étais présent pour représenter nos équipes d'investigation et aider à la gestion de la crise. Les conséquences étant potentiellement importantes, toutes les directions de l'entreprise étaient mobilisées et présentes. Le DSI et nos équipes firent un premier bilan des faits observés.

Tout de suite, la question de l'auteur des faits fut évoquée. Les informations techniques ont montré un code malveillant finement adapté au contexte client et présent depuis plusieurs mois. Toutes les pistes ont été évoquées et débattues, est-ce que cela pourrait être un interne ? Des complicités ? Sans écarter cette piste, nous avons expliqué que ce que nous avions observé peut également être le fruit d'un attaquant externe ayant pris le temps de comprendre le système du client.

Vint ensuite la question de la confidentialité à préserver autour de cet incident. La direction de la communication travaillait en parallèle sur une première posture au cas où l'incident viendrait à être connu. Il fut rapidement décidé d'isoler la cellule de crise opérationnelle dans un lieu particulier. Des membres de la DSI connaissant très bien le SI furent identifiés pour y participer. Nous décidions d'augmenter la taille de nos équipes d'investigation, 5 personnes étaient mobilisées sur le week-end.

Vendredi soir, nous avions la certitude qu'il s'agissait d'une attaque ciblée touchant les systèmes métiers. Certains comptes administrateurs avaient également été compromis, l'intégrité de l'Active Directory n'était pas garantie. Nous basculions la gestion de crise sur un système de messagerie parallèle au cas où l'attaquant y aurait accès. Mais nous étions toujours dans le flou sur la manière dont l'attaquant entrait dans le système d'information, accédait aux systèmes et exfiltrait les données. Ces incertitudes alimentaient également le scenario d'une fraude interne.

L'Enquête

[Ayoub] Florent m'a rapidement rejoint après mes premiers travaux de first responder. Je l'ai briefé sur la situation avant de continuer les analyses dont les objectifs étaient :

- Consolider la liste des indicateurs de compromission (IOC) des différentes versions du malware.
- Reconstruire la timeline d'infection.
- Identifier d'autres actifs compromis (comptes utilisateurs, machines Unix, etc.).

Nous travaillions en collaboration avec les équipes systèmes et réseaux afin d'identifier tout comportement malveillant dans le peu de journaux Windows qu'il y avait sur chaque machine.

En parallèle Vincent a demandé à l'ensemble des équipes d'activer la journalisation sur tous les équipements : routeurs, pare-feux, Windows, etc. afin d'avoir le maximum de visibilité sur le SI.

Après une journée d'épluchage de journaux, nous avons enfin trouvé la caverne d'Ali Baba tant convoitée : le camp de base de l'attaquant. Un serveur contenant des outils de scan réseaux, un utilisateur local non répertorié et inconnu de tous mais surtout des connexions à des heures suspectes durant la journée à différentes machines infectées. Nous remontions doucement le fil de l'attaque vers la source de la brèche.

[Gérôme] La journée de samedi était rythmée par deux réunions de crise avec la Direction Générale. Le cabinet d'avocats que nous avions mobilisé était maintenant présent également en cellule de crise. Les différents scénarios juridiques étaient évalués, à la fois sur les responsabilités de l'entreprise mais aussi sur sa capacité à réagir. Il fut décidé de porter plainte le plus tôt possible en fonction des investigations.

En parallèle, nous avons renforcé les équipes de notre côté et nous avons structuré une équipe d'investigation et une équipe de défense avec un responsable à la tête de chacune d'elle : Vincent pour l'investigation et Baptistin pour la défense. Nous avons également mobilisé un pilote global de la crise pour synchroniser nos équipes, celles du client, arbitrer les priorités et assurer les remontées d'information : j'ai pris ce rôle dans un premier temps avant de laisser la main à Chadi alors que je devais partir pour Singapour... Les créneaux avec la Direction Générale de 11h et 18h ont été confirmés, ils sont devenus nos référentiels pour les jours à venir et ont permis d'assurer un suivi régulier de la situation.

[Vincent] J'étais en repas de famille le samedi soir... mais mon téléphone n'arrêtait pas de sonner ! Nous étions en train de nous organiser pour venir renforcer l'équipe d'intervention, bien assurer la rotation des équipes pour respecter les contraintes d'horaires de travail, récupérer les informations des avocats, etc.

Finalement, nous avons décidé d'envoyer Ayoub se reposer et de conserver Florent pour assurer une continuité dans les

investigations. Baptistin et moi, qui avions suivi les analyses durant la journée, avons alors commencé à préparer nos affaires pour rejoindre Florent sur site dès le dimanche matin et débuter la mise en place des deux équipes.

Le train de six heures du matin était quelque peu… difficile. Arrivés sur site, nous avons commencé par rencontrer le RSSI pour lui expliquer la manière dont nous allions désormais procéder :

- *Nous connaissons la finalité de l'attaque : voler des données de vos clients. Et nous savons également le périmètre ciblé : la totalité des sites en France. Maintenant, l'objectif de la journée est d'identifier la chaîne qui mène l'attaquant aux serveurs en sur les sites. Compte tenu du volume d'actifs à analyser et d'informations à analyser nous allons nous appuyer sur vos équipes pour réaliser différents gestes d'investigation : collecter des données, analyser certains cas précis, etc.*
- *Parfait, nous avons également le RSSI opérationnel qui sera présent cet après-midi, il est actuellement absent.*
- *Nous ferons un point avec lui également quand il sera là. Pour la suite, à partir de demain, deux équipes seront formées : une pour conduire les investigations et une pour préparer la défense du système d'information et la survie des activités métiers. Nous avons identifié 8 personnes qui vont nous rejoindre et venir peupler ces équipes. Nous aurons besoin de vos experts pour nous aider à avancer également. Baptistin va dès maintenant commencer à travailler sur la défense, quant à moi je vais prendre en charge les investigations.*

Dès lors, nous nous sommes mis au travail avec des points de synchronisation réguliers à la fois avec notre client mais également avec nos responsables de crise : Gérôme et Chadi. Je me penchais en premier lieu sur le fameux serveur central. Après avoir demandé à Florent de nous créer un script d'alerting en cas de connexion de l'attaquant sur ce serveur, je me suis rapidement rendu compte que quelque chose clochait : le compte créé par l'attaquant était justement en train d'être utilisé !

- *Ah oui, c'est moi, déclara un des internes.*

Avant de poursuivre les investigations, nous avons alors dû faire un petit point d'équipe pour briefer les internes sur les réflexes d'investigation à avoir : discrétion pour ne pas révéler à l'attaquant qu'il est sous observation, traçabilité des actions d'investigation entreprises, communication et coordination. Face à l'absence d'outils de gestion de crise, j'ai alors demandé à ce que nos analystes qui allaient arriver le lendemain nous apportent MI6 : notre « MIcro Système d'Information Sécurisé », une plateforme sur laquelle nous avons tous les outils nécessaires pour opérer une bonne gestion de crise : messagerie, espace de stockage, wiki, ticketing, agenda partagé, etc.

Les bonnes pratiques assimilées par les internes, nous avons alors repris les investigations sur le serveur central : de nombreux documents internes avaient été accédés et parcourus à partir du compte de l'attaquant. Il s'agissait de documents d'architectures techniques, de procédures métiers, de description de certains produits, etc. Mais ce n'est pas tout, nous avions également trouvé des traces de navigation sur des sites type dropbox. Sans pouvoir confirmer l'exfiltration des données à ce stade, les doutes étaient tout de même de plus en plus forts. La découverte d'outils de cartographie du réseau, de rebond et plus globalement d'outils offensifs nous ont permis de catégoriser ce serveur comme étant le camp de base de l'attaquant : l'actif par lequel l'attaquant se connecte systématiquement avant d'accéder aux serveurs locaux des sites.

L'ambiance était plutôt studieuse, sans stress. Tout le monde avançait sur ses activités tranquillement. Les premières pizzas de la journée sont arrivées et nous avons alors mangé ensemble pour partager quelques informations, bonnes pratiques et retours d'expérience.

Le RSSI opérationnel est alors arrivé. Baptistin et moi avons pu commencer à discuter avec lui pour alimenter le plan de défense mais également pour orienter certaines investigations. Les échanges étaient peu fructueux car peu de systèmes de sécurité étaient en place ou efficaces.

Et puis soudain, tout s'accéléra : l'alarme installée par Florent retentit.

L'attaquant était là, dans l'enceinte cyber de notre client. Là, à commettre ses méfaits. Le niveau de stress est alors monté de trois crans, mais il fallait garder la tête froide. Ne pas faire d'erreur pour ne pas montrer à l'attaquant que nous le traquions… tout en déclenchant les captures adéquates pour pouvoir analyser ses activités et remonter le fameux fil !

L'attaquant n'était resté que quelques minutes. Mais ce fut largement suffisant pour nous donner une première information cruciale : il s'était connecté au camp de base en passant par le poste de travail… d'un administrateur du domaine ! L'AD était donc très certainement compromis et nous avons alors commencé à intégrer la notion de reconstruction dans le plan de défense…

L'analyse s'est poursuivie sur le poste de l'administrateur mais nous avons rapidement statué qu'il ne s'agissait là encore que

d'un simple rebond… depuis un serveur web cette fois !

- *Mais… je le connais ce serveur, dit un analyste de l'équipe de sécurité opérationnelle de VictimCorp. Nous avons effectué un audit de sécurité dessus l'an dernier, il y avait plein de failles partout et les middlewares étaient obsolètes…*
- *Qu'avez-vous fait du coup ? demandai-je alors.*
- *Quelques actions, mais c'était trop couteux de faire évoluer le système en profondeur.*

Quel dommage qu'il faille à chaque fois attendre les incidents et les crises pour enfin dérouler les actions de sécurisation ! Ah… le fameux fardeau du pentester (http://www.securityinsider-solucom.fr/2015/03/le-fardeau-du-pentesteur.html), comme dirait Arnaud…

Nos efforts se sont ensuite portés sur le serveur web et en particulier les logs de l'Apache. Nous avons alors rapidement identifié les accès de l'attaquant à un fichier particulier : un webshell qu'il avait déposé au préalable, notamment en exploitant les vulnérabilités de dépôt de fichiers identifiées lors de l'audit… Dès lors, nous avons commencé à analyser le code du webshell mais ce dernier était assez bien protégé. Je l'ai donc transmis à notre équipe d'analyse pour avoir un bilan complet.

Après une nouvelle pizza et sur la base de nos différentes découvertes, nous décidions de mettre en place de nouveaux mécanismes de surveillance. VictimCorp ne disposant pas de SIEM ou log manager, j'ajoutais WATS (Wavestone Attacker Tracking System) à ma liste d'outils requis. WATS est notre outil de surveillance de circonstance basé sur des technologies opensource : ELK et OSSEC. L'objectif n'est pas d'opérer une surveillance généralisée comme un SIEM classique, mais plutôt d'être en capacité de traquer des indicateurs très précis (un login, une IP, un nom de fichier, etc.) sur un grand ensemble de logs.

[Jean] Dimanche après-midi, j'ai entendu le son du vibreur de mon téléphone professionnel. Il s'agissait encore de Vincent, mais il semblait plus stressé que l'avant-veille :

- *C'est encore moi, désolé de te déranger un dimanche. Est-ce qu'un déplacement hors de Paris t'est possible dès ce soir ? C'est en lien avec les souches malveillantes que tu as analysées vendredi. Je te transmets un mail avec tous les outils dont nous allons avoir besoin, mets ça dans ton sac !*

[Vincent] Le lundi, 10 consultants de Wavestone étaient mobilisés dans les locaux du client. La cellule de crise était constituée, les rôles étaient clairs, la phase de montée en crise était terminée. Ne restait que le plus complexe, comprendre l'ensemble de cette attaque et en gérer les conséquences.

A 6h, le DSI de VictimCorp passait me prendre en voiture pour m'emmener à la première réunion de crise de la journée. La décision fut rapidement prise d'isoler la cellule de crise et les opérationnels sur un autre site pour continuer à mener les investigations et préparer la défense : passé le weekend, nous ne pouvions plus maîtriser la confidentialité de l'attaque en plein milieu des openspace de VictimCorp…

Le temps de briefer l'équipe d'investigation complètement formée et de mettre en œuvre les différentes rotations des équipes pour assurer une efficacité optimale des analystes, midi était déjà là… et les pizzas aussi !

Les binômes d'analystes ont ensuite repris leurs activités. L'équipe en charge de poursuivre les investigations sur le système du serveur web compromis alimentait les autres équipes d'analyse en actifs, comptes, IP ou fichiers suspects.

L'analyse du webshell n'avait malheureusement pas donné grand-chose : il s'agissait d'un webshell commun avec des modifications mineures pour faciliter quelques tâches d'exécution de commandes et protéger son propre code.

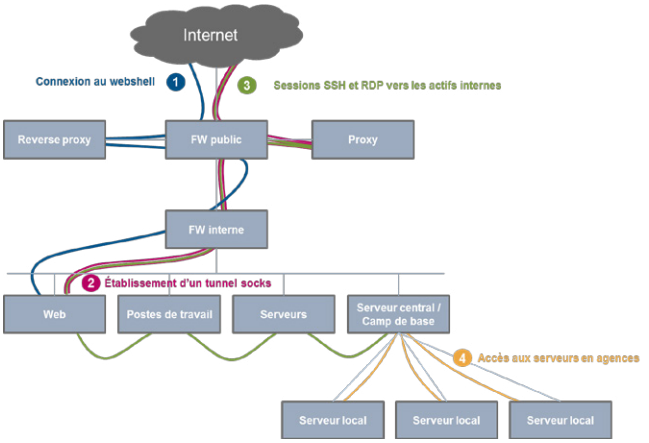
De mon côté, je m'attelais à comprendre le schéma de l'attaquant, son profil, ses ressources et motivations…

En fin de journée, nous avions dressé un important inventaire des actifs et comptes compromis. C'est à ce moment-là que l'attaquant choisit de se reconnecter à son webshell, déclenchant les nombreuses alertes et captures que nous avions positionnées… et ravivant le stress de certains qui n'avaient pas dormi depuis beaucoup trop longtemps… Je me rappelle encore de certaines personnes qui criaient « L'attaquant est connecté !!! Il est connecté !!! ». Des moments où il est important de garder son calme, ne rien faire d'autre qu'observer.

L'orage passé, nous avons pu analyser en détails chaque action menée par l'attaquant. Enfin, nous avions la vision complète. Le silence et le calme prirent le pas sur l'excitation, ça y est. Nous savions.

Il était maintenant temps de formaliser toute notre connaissance du mode opératoire de l'attaquant pour pouvoir alimenter la plainte qui allait être déposée et répondre aux questions des différents enquêteurs des forces de l'ordre.

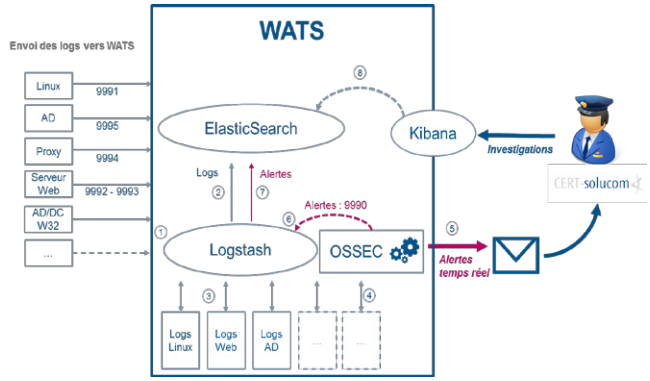
Enfin, il était surtout temps d'aller dormir… mais seulement après une nouvelle part de pizza !



La Surveillance

[Jean] L'attaquant se connectait tous les jours à heure à peu près fixe, nous avons alors pensé qu'un système de surveillance plus évolué nous permettrait de suivre sa progression, découvrir de nouveaux postes et comptes compromis, etc. Notre client ne possédant pas de solution de surveillance, nous avons déployé l'outil WATS, le mini SIEM Wavestone regroupant la pile ELK et OSSEC, que nous avons alimenté en grande partie à l'aide des journaux des Domain Controllers, des firewalls, des proxy, des antivirus et des UNIX. Un vidéoprojecteur avait été installé dans la salle d'investigation, et projetait sur un mur les différents dashboards : nombre de connexions aux comptes compromis par l'attaquant, graphes de son activité, serveurs de rebond, etc. Lorsque nous approchions 18h, heure habituelle de connexion de l'attaquant, tous les yeux étaient rivés sur cet écran improvisé.

Plus tard dans la semaine, nous avons également dû mettre en place un mécanisme de surveillance des informations dérobées par l'attaquant.



Le client ne disposait pas d'outil de gestion centralisée des serveurs qui étaient infectés et nous avons alors dû déployer un service de monitoring sur ces serveurs de manière plutôt précaire. Ainsi, de la même manière que l'attaquant exfiltrait ses informations, nous remontions nos journaux de surveillance, via une chaîne de trois serveurs, dont un DC, afin qu'ils soient envoyés vers WATS.

La Défense

[Hélène] Les premières journées (et nuits) d'investigations ont montré qu'il allait falloir rapidement commencer à préparer un plan de défense, dans le but d'endiguer l'attaque et de se prémunir d'éventuelles récidives : c'est à ce moment-là que Yassir, Fabien et moi sommes intervenus dans l'équipe de défense, sous le pilotage de Baptistin.

Mardi matin, nous avons rejoint sur place l'équipe Wavestone qui travaillait déjà sur les investigations. Arrivés sur les lieux, il n'y a plus l'ombre d'un doute, c'est la crise et nous sommes face à une attaque de grande ampleur. Immédiatement, j'ai rencontré l'équipe d'investigation sur place pour un briefing sur les premiers résultats de leurs analyses. À ce stade, le scénario de l'attaque et le mode opératoire de l'attaquant se dessinaient. Nous n'avions toutefois pas encore la vision exhaustive du SI et des éventuels points d'interconnexion prestataires, partenaires, filiales internationales… Dès lors, Baptistin a lancé le premier groupe de réflexion sur l'élaboration du plan de Défense. Tout de suite, des questions se posaient : par où commencer ? Comment se répartir les tâches ? Il fallait envisager tous les scénarios : et si le mode opératoire identifié à date n'était pas le seul ? Et si l'attaquant avait d'autres points d'entrée sur le SI ? Et si d'autres récidives conduisaient à la dégradation voire la destruction de systèmes ou données du client ?

Au-delà des mesures à mettre en œuvre pour supprimer le mode opératoire connu de l'attaquant (supprimer ses accès sur les systèmes, fermer les portes ouvertes…), nous devions nous préparer au scénario le plus critique : l'attaque reprend de plus belle (avec un plan B fonctionnel) et d'autres systèmes sont menacés de destruction (un air de Sony…).

Pour cela, nous nous sommes préparés à isoler une partie du SI pour éviter une propagation de l'attaque.

L'idée était que si ce scénario venait à se produire, on devrait isoler la partie du SI attaquée de sorte à ne laisser passer que les flux critiques pour assurer un minimum vital des activités Métiers.

Partant de ces différents scénarios, nous avons commencé à lister les actions à réaliser et mesures de sécurisation à mettre en œuvre, et nous avons par la suite enrichi ce plan tout au long de notre période d'intervention.

Le plan de défense s'est structuré pour faire émerger plusieurs chantiers :

- Un dispositif de surveillance : permettant d'agir et d'avancer sur les prochaines étapes tout en gardant l'œil sur les points stratégiques du SI.
- Une cellule de support : permettant de traiter les éventuels effets de bord des mesures appliquées.
- Une task force de suppression du mode opératoire connu de l'attaquant : permettant de s'assurer qu'aucune étape réalisée par l'attaquant ne peut être reproduite.
- Un processus d'isolation maîtrisée : permettant de confiner les impacts engendrés si les scénarios « nouvelle attaque » ou « dégradation » venaient à arriver.
- Des actions de sécurisation court, moyen et long terme : permettant de renforcer et pérenniser le niveau de sécurité du SI en adéquation avec les besoins du secteur.

Quelques heures plus tard… les tâches étaient réparties entre les différents membres de l'équipe. De mon côté, j'avais en charge la mise en place de la cellule de support et la préparation des actions en vue d'une potentielle isolation du SI… le sprint des investigations allait désormais laisser place à un marathon de sécurisation !

Mardi après-midi, je partais à la rencontre du responsable de la Cellule Support pour préparer un processus d'escalade spécifique. L'objectif : traiter efficacement les effets de bord des actions qui seront entreprises (remontées d'incidents sur des potentiels dysfonctionnements Métier et/ou IT).

Dès le mardi soir, un premier processus était formalisé et les principaux acteurs concernés aux différents niveaux (N1, N2, N3) étaient briefés !

Mercredi matin, soit 24 heures après le début de notre intervention, les premières actions étaient traitées, le scénario nominal se déroulait comme prévu.

La cellule de surveillance se mettait en place avec les outils de Jean ; en parallèle, je rencontrais certains Métiers afin d'essayer de déterminer avec eux l'ensemble des flux cruciaux et nécessaires au fonctionnement de leur activité. Bref, un travail de plusieurs mois en temps normal qu'il a fallu réaliser en moins de 3 jours ! L'objectif était d'identifier ensemble les actions à entreprendre pour qu'un fonctionnement en mode dégradé soit envisageable en cas d'isolation partielle (il ne faut pas oublier qu'à ce moment, le pire pouvait encore se produire).

Au bout des premiers échanges, ce n'était pas évident…

- *Bonjour les Métiers, dans le cas où nous devrions isoler en urgence en partie votre réseau du SI central, quels flux souhaiteriez-vous voir impérativement passer ?*
- *Tous !*
- *Bon… alors, reprenons…*

La nuit la plus longue

[Chadi] Chaque jour depuis le début l'attaque, nous nous réunissions à 14h pour préparer la réunion de crise DG. L'objectif était clair : donner une vision synthétique et stratégique à la Direction, afin qu'elle puisse prendre les décisions. Les premiers jours, les échanges ont beaucoup tourné autour de l'investigation, de l'attaquant et des impacts immédiats de l'attaque. Petit à petit, le principal centre d'intérêt est devenu la stratégie de défense à court et moyen termes. À ce sujet, le Directeur Général a été très clair « j'assumerai les erreurs passées, je ne les accepterai plus à l'avenir ». Dans le cadre du dépôt de plainte en cours, appuyé par des avocats spécialisés, il nous demanda de lui garantir que les données n'étaient plus à risque, et qu'il pouvait l'annoncer aux autorités.

Le DSI s'était engagé à apporter une réponse claire au plus tard le jeudi, à la première heure. Il nous restait l'après-midi et la nuit pour trouver une solution. Le défi était double : d'une part, nous devions protéger les données de la société et de ses clients. D'autre part, nous ne voulions pas simplement couper l'accès de l'attaquant, car nous ne savions pas à ce stade s'il dispose d'autres points d'entrée, et cela aurait été lui dévoiler qu'il avait été découvert.

Nous n'avions que peu de temps, et chaque acteur avait un avis sur la stratégie à adopter. Certains pensaient qu'il fallait surtout couper l'accès de l'attaquant pour protéger les données, d'autres mettaient l'accent sur le fait que cela ne l'empêcherait pas de revenir par une autre porte d'entrée que nous n'aurions pas encore identifiée.

Le manque de sommeil et la fatigue n'aidant pas, les discussions atteignaient une tension extrême, les désaccords explosaient au grand jour, et des noms d'oiseaux commençaient même à voler. S'ensuit alors la nuit la plus longue. Je me suis alors isolé avec Vincent pour réfléchir au calme sur la stratégie la plus rationnelle

à adopter et ainsi la communiquer à l'équipe de Défense pour pilotage et mise en place.

À 22h, nous avons eu un échange direct avec le DSI. Il nous regarda droit dans les yeux, et énuméra en comptant sur ses doigts :

- *Un, vous me faites une synthèse ce soir me décrivant clairement la situation et la solution proposée. Deux, vous ne réalisez aucune action contraire à la demande de notre DG. Trois, je vous souhaite une bonne nuit, car ce soir je vais border mes enfants que je n'ai presque pas vus depuis une semaine !*

À 1h du matin, les équipes techniques me parlèrent d'une idée qu'ils venaient d'avoir : un honeypot. Il s'agissait de laisser l'attaquant se connecter, mais de le bloquer dans un espace réseau isolé (une « bulle »), où il n'aurait, dans les faits, accès à rien. De cette manière, nous assurions la protection des données, tout en nous donnant la possibilité de surveiller ses actions ! Comment n'y avions-nous pas pensé plus tôt ? Le temps de valider la faisabilité technique de la chose, j'écrivis au DSI pour lui proposer cette solution. Il la valida dans la foulée.

Aux alentours de 2h du matin, j'ai alors demandé aux membres les plus fatigués de l'équipe de se reposer. De manière peu surprenante, j'ai rencontré une certaine résistance : l'excitation de l'action les poussait à ne pas vouloir s'arrêter en chemin.

Une équipe technique de relève travailla jusqu'au petit matin pour mettre en place les mesures nécessaires à notre plan. Ainsi, à 8h du matin, nous avons pu annoncer que les mesures étaient en place, et les données protégées le mieux possible.

La sortie de crise

[Chadi] Dès lors, deux activités distinctes se sont déroulées en parallèle entre jeudi et le lundi suivant.

D'un côté, nous avons suivi la démarche judiciaire. Des agents des forces de l'ordre nous ont rendu visite à la cellule de crise, et ont recueilli notre déposition, au titre d'experts en sécurité. Leur but était de comprendre le déroulé précis des évènements, la manière dont l'investigation avait été menée, les résultats obtenus, et la manière dont ils souhaitaient reprendre le dossier. Nous leur avons donc fourni tous les éléments à notre disposition.

De l'autre côté, nous avons mis en place une surveillance très spécifique sur la zone de l'attaquant. Elle consistait en un moniteur qui émettait une alerte visuelle 24h/24, 7j/7, dès qu'une connexion à la bulle était détectée.

[Jean] Le système de surveillance WATS en place était alors fonctionnel, mais ne permettait de tracer l'attaquant que sur les critères que nous connaissions déjà : comptes utilisés et serveurs infectés. Nous avions besoin de découvrir si d'autres serveurs avaient été compromis par l'attaquant en dehors du périmètre France que nous surveillions déjà. Vincent a alors proposé que nous utilisions CERTitude, notre outil de recherche d'indicateurs de compromission à large échelle. Malheureusement, nos critères incluaient les outils ayant servi au rebond de l'attaquant (dont PsExec) et nous avons alors eu un grand nombre de faux positifs, sans pour autant découvrir de nouveaux serveurs compromis. Il a alors été décidé de créer une procédure et un script de contrôle à dérouler et exécuter par chacun des pays sous supervision des analystes de notre cellule d'investigation.

Cette étape terminée et les outils de surveillance et détection étant en place, j'ai alors pu me retirer de l'équipe d'investigation et entamer une nouvelle mission.

[Hélène] Pendant ce temps, nous avons continué à rassembler les Métiers afin de cartographier l'ensemble de leurs flux cruciaux. Des premiers versions de matrices de flux ont vu le jour, pendant que d'autres étaient encore en cours de construction.

Nous avons alimenté les mesures de sécurisation du plan de défense avec les retours complémentaires obtenus par l'équipe d'investigations, qui avait désormais une vision complète du mode opératoire de l'attaquant et des outils qu'il utilisait.

[Chadi] Le vendredi, à la veille du week-end, l'attaquant a tenté de se connecter deux fois et de mener ses actions habituelles. L'excitation était à son comble : le piège avait fonctionné ! Les tentatives ont été multiples, puis il a fini par se déconnecter, sans action supplémentaire.

La fin de semaine a été calme. Après nous être assurés que le moniteur d'alerte serait bien surveillé nuit et jour, toute l'équipe a pu se reposer pour la première fois depuis le début de la crise. Quelques managers de VictimCorp et Vincent sont tout de même restés mobilisables durant le week-end en cas d'alerte sur le moniteur… juste au cas où. Le début de semaine suivante a été marqué par l'absence de nouvelle connexion. L'attaquant avait très certainement compris : il avait perdu ses accès au SI.

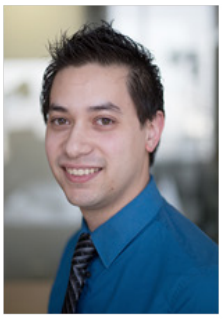
La cellule de crise a alors été levée, et s'en est suivie une longue

période de sécurisation globale du SI : il s'agissait de l'ensemble des mesures du plan de défense qui n'étaient pas directement liées au mode opératoire de l'attaque mais qui allaient permettre de sécuriser le SI de manière globale et pérenne. De tous les scénarios envisagés par l'équipe de Défense, c'était donc bien le plus souhaitable qui avait eu lieu ! Ouf..

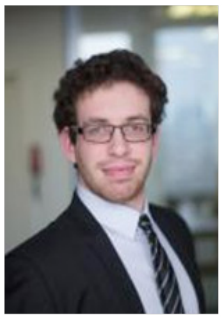
Finalement, ces actions sont venues alimenter la création d'un plan de transformation numérique de l'ensemble des métiers de VictimCorp, un projet à plusieurs centaines de millions d'euros...

Par ordre d'apparition


Gérôme


Vincent


Ayoub


Jean


Florent


Chadi


Baptistin


Arnaud


Hélène

DOSSIER

LES NOUVEAUX OUTILS DE LA SÉCURITÉ OPÉRATIONNELLE

Ces dernières années ont été marquées par la recrudescence des cyber-attaques, et a fortiori, l'apparition de nouveaux moyens de défense, de détection et de réaction.

Nous vous proposons de revenir sur trois nouveaux mécanismes :

/ Les solutions de type « EDR », ces outils « next-gen » pour les postes de travail.

/ Les plateformes « SIRP », la panacée de la coordination de la réponse à incident ?

/ Les techniques de Machine Learning appliquées à la cybersécurité.

EDR, CES OUTILS « NEXT-GEN » SONT-ILS UTILES CONTRE LES MENACES ACTUELLES ?

Au vu des différentes attaques qui assaillent le quotidien des entreprise et par rebond des investigateurs et analystes sur incident, l'assertion suivante reflète assez fidèlement le niveau de protection des systèmes d'information :

« La présence d'un antivirus, HIPS, IDS sur le système cible ne présente que peu, voire aucun challenge pour l'attaquant. »

Certes, ces solutions forcent l'attaquant à prendre quelques précautions standards qui relèvent plus du bon sens que de l'ingéniosité :

/ Réserver de nouveaux noms de domaine.

/ Recompiler le programme malveillant.

/ Éviter les scans massifs...

Mais les mécanismes de détection et de prévention actuels n'empêchent aucunement l'attaquant de pénétrer dans le réseau de l'entreprise, encore moins de se propager sur les partages et postes internes des collaborateurs.

Fort de ce constat, plusieurs acteurs mettent en valeur une vague d'outils « innovants » afin de répondre à trois problématiques majeures identifiées par les entreprises :

/ Détecter une attaque avancée.

/ Obtenir plus de visibilité sur le terminal (poste et serveur).

/ Remédier à distance les nuisances d'une attaque.

Avant d'aborder en détail le fonctionnement de ces nouvelles solutions marketing-ment appelées EDR, « Endpoint Detection and Response » ou encore « anti-APT endpoint », prenons le temps de souligner les limites des solutions classiques.

LIMITES DES SOLUTIONS CLASSIQUES

Solutions antivirales

Les solutions antivirales, positionnées tant au niveau du terminal qu'au niveau des serveurs de messagerie présentent des fonctions de sécurité indispensables et permettent de se protéger contre les menaces et attaques diffuses. Toutefois, force est de

constater que ces outils ne sont pas équipés pour détecter, encore moins bloquer, une attaque ciblée qui utilise un malware inconnu voire dans certains cas aucun malware (cf. Hacking team attack).

Sans forcément naviguer dans le monde obscur de l'obfuscation manuelle du code, il est assez trivial de contourner tous les antivirus du marché via une simple exécution en mémoire. En effet, un antivirus scanne automatiquement tout fichier qui est écrit sur le disque. Dès lors, un malware qui s'exécute uniquement en mémoire via l'une des nombreuses techniques existantes (dropper, injection de processus, injection de DLL, etc.) contourne toutes les protections présentes sur le terminal.

Intrusion Detection System

Les solutions IDS en contrepartie font face à un problème encore plus challenging : l'obsolescence des signatures. La protection qu'offre un IDS est aussi efficace que sa base de signatures. Certes il est possible et recommandé d'implémenter des règles de corrélation comportementales, via un SIEM à titre d'exemple, mais peu d'entreprises prennent le temps d'étudier et mettre en place ces règles-là soit par manque de temps, de ressource, d'expertise ou à cause des limitations des outils du marché.

ENDPOINT DETECTION & RESPONSE : UNE NOUVELLE APPROCHE

De plus en plus d'éditeurs s'intéressent à la problématique du poste de travail afin d'offrir une solution qui puisse détecter intelligemment une attaque mais également mener une investigation à distance et effectuer des actions de remédiation.

Nous aborderons en détails chacune de ces trois fonctionnalités afin d'apporter un éclairage sur la valeur ajoutée de ces outils par rapport aux solutions antivirales classiques, mais également mettre en évidence leurs limitations face à une véritable attaque ciblée.

Acteurs du marché

De manière très macroscopique, il est possible de distinguer quatre constellations importantes d'acteurs dans l'univers des EDR :

- Des pure-players qui sont dédiés au domaine de l'EDR et focalisent toute leur énergie sur les différents aspects du sujet : SentinelOne, Cylance, Carbon Black, etc.
- Des acteurs globaux, ces géants de l'informatique et de la sécurité : RSA, Cisco et Palo Alto proposent également des solutions EDR, principalement issus de rachat de pure-players mais qui ont généralement l'avantage de bien s'intégrer avec leurs solutions classiques.
- Acteurs spécialisés en investigation numérique (Digital Forensics - DFIR) : certains acteurs tels que Guidance et FireEye se sont fortement inspirés de leurs interventions sur des incidents afin de développer des outils EDR.
- Enfin, contre toute attente, les éditeurs de solutions antivirales qui agrémentent leur antivirus de quelques fonctionnalités inspirés du monde EDR.

Détection des menaces

L'une des attentes majeures d'un EDR est bien sûr sa capacité de détecter des attaques avancées pour lesquelles aucun IOC (Indicateur de compromission) n'est disponible. Nous nous limiterons donc aux solutions proposant un moteur de détection intelligent et autonome.

Quatre techniques de détection sont généralement employées par les acteurs du marché.

Détection de l'exploitation d'une vulnérabilité

Cette approche typiquement adoptée par des acteurs tels que FireEye, Confer (racheté par Carbon Black) ou encore Palo Alto profite d'un constat assez simple.

Qu'elle soit connue ou non (zéro-day) une vulnérabilité est exploitée via des techniques classiques, répertoriées et surtout dénombrables : dépassement de tampon, retour à des instructions, injection DLL, préparation du tas, etc.

Ces solutions ciblent donc la manifestation de ces techniques-là dans la mémoire des processus lancés sur le système et lèvent une alerte le cas échéant.

Ceci dit, afin d'avoir un niveau de visibilité satisfaisant sur le système, il est nécessaire de détourner une partie non négligeable des appels systèmes effectués par le système d'exploitation, intervenir dans le maniement des objets par le noyau, etc. Autant d'opérations qui peuvent facilement causer des dénis de service voire endommager le système.

Aussi l'approche généralement suivie est de ne surveiller que les processus souvent exploités par les attaquants i.e : une zéro-day sur flash aurait en revanche de grandes chances d'être détectée par ces outils. Une zéro-day sur le process smb.exe qui gère le partage de fichiers aurait beaucoup de chance de passer inaperçue.

Détection d'un comportement malveillant

Contrairement à la détection de l'exploitation d'une vulnérabilité, qui intervient dans les phases amont d'une attaque, la détection d'un comportement malveillant suppose que l'attaquant a pris, ou est en train de prendre, la main sur le poste.

Certains outils tels que Carbon Black, RSA ou encore SentinelOne préfèrent ainsi se concentrer sur des enchainements d'actions qui sont caractéristiques d'une attaque. À titre d'exemple, un éditeur de texte (notepad) qui exécute un processus cmd.exe et ouvre une connexion sur le port 443 d'un serveur hébergé dans un autre continent, est synonyme d'une action pour le moins suspecte et sera (dans l'idéal) remontée comme telle par ces outils.

L'inconvénient majeur de ce mode de détection est bien entendu le nombre de faux positifs que cela peut générer. Un exemple assez parlant se présente sous la forme des documents Office, qui pour peu qu'ils embarquent une macro un tant soit peu complexe, sont instantanément détectés par certaines de ces solutions comme des malwares. L'une des principales raison est l'écriture massive dans les répertoires temporaires de l'utilisateur %APPDATA% ou %TEMP% d'icônes, d'images, etc. comportement assez similaire à celui d'un malware.

Détection via sandbox

Certains éditeurs, principalement les acteurs de solutions antivirales, proposent une mise à jour de leur agent afin d'inclure des « capacités EDR ». Ceci est certes séduisant d'un point de vue déploiement et exploitation, mais bien souvent la mise à jour de l'agent n'ajoute qu'une étape de validation externe dans le processus de détection : si un fichier présent sur le disque ne correspond à aucune signature mais est tout de même considéré comme suspect, via une analyse statique du dit-fichier, ce dernier est envoyé à une sandbox qui l'exécute dans un environnement virtuel afin de statuer sur son état.

Outre le temps de détection inhérent à l'envoi et l'analyse du fichier sur un serveur distant ainsi que les potentiels problématiques de déploiement dans le cloud d'une telle sandbox, la détection se base toujours sur l'inspection des fichiers présents sur le disque uniquement et n'inspecte pas les processus qui tournent en mémoire sur l'endpoint.

Par ailleurs, le fait d'avoir un écart entre l'environnement d'exécution du malware (machine virtuelle - sandbox) et l'environnement de dépôt du fichier (terminal) introduit un biais qui peut se révéler fatal. En effet, plusieurs malwares se servent de cet écart afin de conditionner l'exécution de la charge utile malveillante et ainsi tromper les systèmes de sandboxing.

Détection via apprentissage

Contrairement aux outils de détection réseau, très peu d'acteurs EDR se sont aventurés dans le domaine de la détection des menaces via l'apprentissage du comportement de l'utilisateur.

Les techniques de détection présentées précédemment identifient bien des écarts, mais ces écarts sont renseignés sous forme de « liste noire » de comportements connus pour être malveillants. Là est la nuance qui ne va pas sans rappeler les principes des signatures, quoique sous une forme plus raffinée.

C'est ainsi que des acteurs tels que Triumfant suivent une approche assez intéressante : ils construisent un modèle mathématique qui décrit l'état nominal de l'activité d'un utilisateur sur un poste de travail. Toute variation par rapport à cet état : utilisation du privilège se_debug pour la première fois, présence de cinq comptes actifs sur le poste au lieu d'un seul, etc. remonte une alerte sécurité, qui sera validée ou non par l'opérateur.

Des acteurs comme Guidance s'inspirent de cette démarche mais modélisent plutôt le comportement de l'ensemble du parc informatique, ce qui permet effectivement de détecter un malware qui se propage sur le SI, mais pourrait faire défaut lors d'une attaque ciblée qui n'impacte que quelques postes.

Synthèse

Ces mécanismes de détection sont bien sûr très complémentaires et certains éditeurs n'hésitent pas à s'inspirer de plusieurs approches pour construire leur moteur de détection, toutefois ceci ne couvre pas l'intégralité des menaces. De ce fait, presque toutes les solutions incorporent un flux d'intelligence communiqué par les laboratoires de recherche des éditeurs, des clients, etc.

Ces flux d'intelligence reposent sur les traditionnels indicateurs de compromission (IOC), qui reprennent finalement les avantages, et surtout limitations, de la détection via signatures depuis longtemps proposée par les antivirus...

Capacités d'investigation

L'un des besoins majeurs mis en avant par les entreprises est la possibilité d'obtenir l'état de du terminal et de collecter des informations techniques à un instant t. Ceci se traduit par exemple par la récupération sur demande des artefacts suivants :

- Les processus et services actuellement présents sur l'endpoint.
- La liste des fichiers présents dans le répertoire %AppData%.
- Une copie de la mémoire vive.

Ce qui autrefois nécessitait un script powershell développé à la main, peut maintenant s'effectuer presque instantanément depuis une console centralisée et ainsi offrir une vision exhaustive de l'état du parc informatique.

Outre le gain indéniable en efficacité, la fiabilité des résultats en est également améliorée. En effet, les fonctions de recherches

à distance présentes nativement sur Windows sont limitées à l'espace utilisateur (ring 4) et ne peuvent pas détecter les processus/fichiers/clés de registres cachés par des malwares avancés (ring 0).

Ceci représente en effet l'atout majeur d'un agent installé sur le poste, pourvu qu'il soit installé au niveau du noyau et implémente des fonctions bas niveau.

Beaucoup d'éditeurs vont un cran plus loin en exposant des API permettant d'automatiser ces actions redondantes de recherche. Le format des IOC supportés varie d'un éditeur à un autre selon les choix stratégiques effectués : YARA pour Guidance qui a un background investigation, OpenIOC pour CarbonBlack et FireEye, alors que RSA supporte de nombreux formats. Néanmoins presque tous les éditeurs convergent petit à petit vers le support de l'ensemble des formats.

Aussi, afin d'approfondir certaines analyses suite à une alerte, les éditeurs n'hésitent pas à s'interfacer avec des outils de sandbox tiers, ou propres à l'éditeur afin de mener des analyses plus avancées, c'est le cas de Cisco, Hexis, et tant d'autres.

Options de remédiation

Le troisième aspect naturellement traité par les EDR est bien sûr la remédiation à distance des terminaux. Avant de traiter ce sujet néanmoins, il est intéressant de considérer la réelle valeur ajoutée d'une telle fonctionnalité. En effet, supprimer un fichier, DLL, processus à distance ne garantit aucunement l'éradication du malware. Certains malwares tels que Greyfish s'attaquent par exemple au BIOS et peuvent persister après le formatage du disque.

Toutefois, les incidents quotidiens n'impliquent pas systématiquement un malware aussi complexe que Greyfish et la possibilité de supprimer une clé de registre de persistance classique pourrait bien faciliter la vie de nombre d'analystes.

Du fait de cette problématique, d'un côté des éditeurs comme FireEye proposent uniquement d'isoler le poste infecté ce qui garantit un certain confinement de la menace, d'un autre côté des éditeurs comme Carbon Black ou Guidance proposent d'agir au niveau du système afin d'effectuer des opérations avancées au niveau du noyau et tenter de remédier le poste.

Enfin, d'autres acteurs comme Cisco ou RSA permettent de supprimer à distance quelques artefacts mais cela ne traite que superficiellement l'infection.

Un acteur peu connu en France, Triumfant permet lui d'effectuer des opérations chirurgicales au niveau de la mémoire afin de corriger les altérations du malware (tables IDT, SSDT, etc.) et traiter ainsi des malwares assez complexes.

Attention par contre, si la console de l'outil EDR tombe dans de mauvaises mains, elle peut devenir une arme de cyberdestruction assez massive.

CONCLUSION

Les solutions classiques antivirales, IDS, etc. présentent certes des protections faillibles mais il est illusoire de penser que les « nouvelles » solutions du marché fournissent des résultats parfaits et infaillibles, surtout sur l'aspect détection.

Un antivirus reste de mise, en particulier pour se protéger des malwares basiques et ne pourra être remplacé par un EDR.

Au final, la valeur ajoutée d'un tel outil se situerait plus au niveau des options de collecte d'artefacts, de recherche d'IOC voire de remédiation à distance qui faciliteront grandement les opérations des équipes de réponse à incident en cas d'attaque d'ampleur.

Ces outils devront cependant être particulièrement sécurisés pour ne pas être eux-mêmes des vecteurs facilitateurs de l'attaque. .

SIRP, QUELLE VALEUR AJOUTÉE ?

LE SIRP, UNE PLATEFORME DÉDIÉE À LA GESTION DES INCIDENTS DE SÉCURITÉ

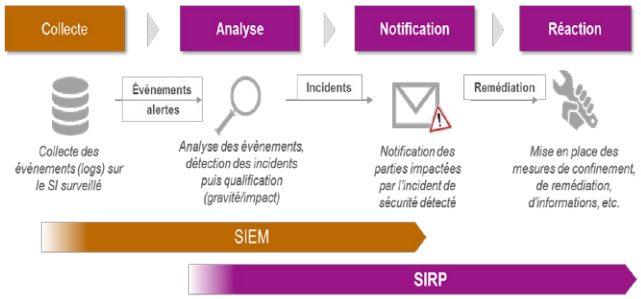
Comme son nom l'indique, un SIRP est une plateforme d'aide à la réponse à incident. Contrairement à un SIEM, dont l'objectif principal est de corréler les logs pour en extraire des alertes de sécurité, le SIRP participe à la gestion des alertes émises. En cela il se rapproche plus d'un outil de gestion de ticket (type ITSM) largement utilisé par les équipes d'exploitation SI au quotidien.

Il est néanmoins dédié à la gestion des alertes et incident de sécurité grâce à des fonctionnalités spécifiques (avec des workflows de traitement spécifiques, la gestion des IOC et de la threat intelligence, l'interfaçage avec le SIEM et les autres outils de sécurité, etc.). L'objectif du SIRP est d'aider les analystes ainsi que leurs managers dans leur travail quotidien et plus globalement d'améliorer l'efficacité des activités de réponse à incident.

POSITIONNEMENT DU SIRP DANS L'ENVIRONNEMENT DE DÉTECTION

Le SIRP, en tant que plateforme de réponse à incident peut se positionner dans le « prolongement du SIEM », notamment pour

faciliter l'analyse, les notifications et l'organisation de la réaction.



PRINCIPALES FONCTIONNALITÉS : COLLABORATION, STANDARDISATION ET AUTOMATISATION

La plateforme de SIRP, en tant que point central pour la gestion des incidents de sécurité, offre des fonctionnalités propres à ses utilisateurs (analystes, responsable de SOC, RSSI, etc.). En cela, elle dépasse, fonctionnellement et en termes de sécurité, les plateformes ITSM utilisés usuellement. En particulier une plateforme de SIRP complète et mature doit être en mesure d'apporter les gains suivants :

/ Une collaboration accrue, via :

- Des workflows ou playbooks (processus de gestion des incidents, assimilables à des arbres de décisions/ traitement) par défaut (i.e. fournies avec la solution) et facilement et hautement personnalisables. Par exemple, un workflow de traitement d'un malware détecté sur un poste de travail, avec une branche dédiée à la gestion d'un ransomware.

- Un interfaçage avec l'ITSM corporate (ou les ITSM dans le cas d'un SI / une organisation très éclatée) afin de pouvoir communiquer de manière transparente (et ce sans changer les habitudes, sur la base des outils existants) avec les autres équipes IT (ex. équipes réseau, poste de travail, helpdesk, etc.).

/ Une efficacité améliorée dans le traitement des incidents, via :

- La centralisation et l'accessibilité offerte par la plateforme à tous les analystes avec des rôles bien définis (N1, N2, N3, responsable MSSP, responsable SOC, RSSI BU, etc.), permettant notamment de gérer les priorités (automatiquement ou par assignation des incidents) ainsi que la continuité du traitement via la gestion des rotations d'équipes (dans le cadre d'un service en 24/7 par exemple).

- L'automatisation des actions d'analyse et de levée de doute réalisées habituellement manuellement par les analystes via l'interfaçage du SIRP avec certaines solutions existantes : puit(s) de logs, IDS, proxys, antivirus, et solution(s) de threat intelligence. Ces intégrations permettent au SIRP d'aller récupérer des informations complémentaires relatives à l'incident pour l'enrichir.

Par exemple, pour une alerte créée dans le SIRP via le SIEM et originalement générée par plusieurs alertes IDS, le SIRP pourrait automatiquement (ou sur simple demande de l'analyste) aller chercher dans :

- Pour la recherche de traces / de marqueurs :
  - » Les logs (du proxy Web) s'il retrouve trace de la requête et de la réponse.
  - » La CMDB ou référentiels LDAP/AD pour récupérer des informations relatives aux machines concernées par l'alerte (nom, type, département, OS, dernier utilisateur connecté, etc.).
  - » L'antivirus poste de travail : les alertes et version de l'antivirus.
  - » La sandbox mail/réseau : les derniers éléments de menaces potentielles identifiés mais laissés passer.
- Pour la contextualisation de la menace :
  - » Recherche d'informations relatives au cas en cours (marqueurs, menaces, cibles, etc.) dans sa propre base regroupant les incidents passés (notion de capitalisation).
  - » Une base de threat intelligence interne (ex. instance MISP) ou externe via soumissions de marqueurs à des plateformes externes / SaaS (par exemple à Virus Total, IBM Xforce, FireEye, Trend Micro, Palo Alto, etc.).
- Pour la qualification :
  - » A des applications externes (ex. envoi de hash ou URL vers Virus Total).
  - » A des solutions internes, par exemple envoi des fichiers suspects (remontés depuis une alerte antivirus ou IDS) vers une sandbox pour analyse dynamique (via exécution dans un environnement contrôlé).
  - » Vers les différentes solutions antivirus en place (antivirus sur les passerelles email, antivirus endpoints, etc.) permettant de vérifier de manière centralisée et industrielle si la menace est connue par les solutions de confinement en place.

- L'industrialisation / l'automatisation de la réponse. Bien que source de polémiques, l'automatisation de la réponse sur incident (notamment des actions de mitigation) est un sujet de discussion chez nombre d'entreprises. Certaines plateformes SIRP permettent, via des mécanismes similaires (interfaçage avec des solutions tierces en place) d'industrialiser les actions de confinement / mitigation. Par exemple en proposant à l'analyste un bouton « bloquer l'URL et l'IP désignée sur les proxys Web » ou encore « générer une signature pour le fichier désigné sur l'ensemble des antivirus ».

- Une industrialisation du traitement et des décisions portée par les workflow et un wiki intégré et géré par les analystes. Par exemple, une fiche réflexe pour la mitigation d'un ransomware ou d'un DDOS, une liste des contacts pour escalade dans telle business unit ou filiale, un exemple de rapport d'incident, une liste globale des lessons learned (plans d'actions d'amélioration identifiés post incident), etc.

Évidemment, l'interfaçage avec les solutions tierces n'est pas « naturel », le SIRP propose en général des API et supporte certaines solutions partenaires de l'éditeur, reste ensuite à s'assurer des capacités des solutions tierces avec lesquelles s'interfacer, soit au niveau de l'application via une API, à défaut au niveau de la base de données.

DES ATOUTS TRANSVERSES, TELLES QUE :

/ Des capacités de reporting avancées : les SIRP proposent des métriques propres à la gestion des menaces et incidents de sécurité (ex. répartition par type d'incidents, par impacts, respect des SLA, etc.) ainsi qu'un « reporting role based » (les indicateurs et rapports pour l'analyste N1 sont différents de celui du responsable de SOC ou encore du RSSI d'une business unit).

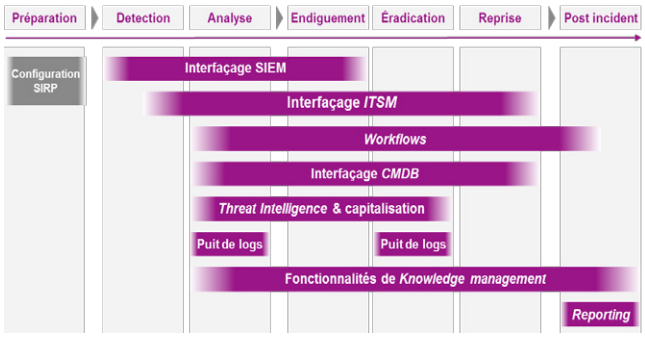
/ L'aide au respect des contraintes règlementaires via une confidentialité et une traçabilité accrue des informations et actions relatives aux incidents de sécurité. En effet, le SIRP, en tant solution dédiée et pensée secure by design, intègre son propre contrôle d'accès et moyens de chiffrement et est maitre des interfaces avec les solutions tierces (par exemple dans le cadre d'un interfaçage avec l'ITSM corporate seules les informations strictement nécessaires à l'opérateur de la tâche sont transmises à l'ITSM). Certaines solutions permettent d'avoir une traçabilité ainsi qu'un historique de tous les champs d'un incident (par exemple la criticité de l'incident créée à « haute », descendue à « moyenne » le 29/07/2016 par l' « analyse N2 Jean Dupont »).

/ La gestion (prise en compte, suivi, capitalisation) des « demandes de sécurité » (par exemple la campagne de recherche de marqueur sur demande de l'ANSSI).

/ L'aide à l'organisation de war room, gestion de crise, etc.

LE SIRP SUPPORTE L'ENSEMBLE DU PROCESSUS DE RÉPONSE À INCIDENT

Finalement, le SIRP, grâce à ses fonctionnalités intrinsèques et lorsqu'il est interfacé avec les solutions clés, apporte un gain sur les différentes phases de la réponse à incident.



INTÉGRATION DANS L'EXISTANT TECHNOLOGIQUE ET ORGANISATIONNEL

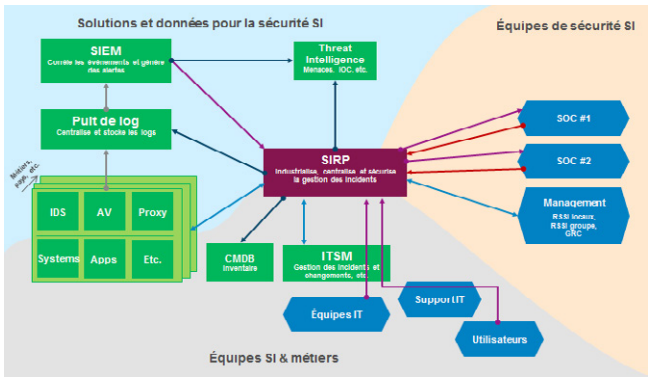
Le SIRP, en tant que brique centrale de la réponse à incident est à la croisée des chemins, entre les :

/ Informations techniques : évènements / logs, alertes, incidents, rapports, etc.

/ Les solutions de gestion du système d'information (CMDB, ITSM, etc.) et de sécurité (puit de logs, SIEM, IDS, antivirus, proxy, etc.).

/ Les équipes de sécurité et de production IT.

Le schéma ci-dessous offre une vue des échanges fonctionnels entre le SIRP est les éléments suscités :



S'ÉQUIPER D'UN SIRP

Même si cet outillage peut paraître très séduisant vu ses capacités, de nombreuses questions se posent avant de se lancer sur un projet d'acquisition.

PRIORISER SES BESOINS POUR DÉFINIR UNE PREMIÈRE CIBLE

Avant de se lancer dans le choix et le déploiement de son outil de SIRP, il s'agit, pour en tirer un maximum parti, d'évaluer son organisation et son niveau de maturité sur les aspects de la détection et réponse à incident pour ensuite définir la cible attendue

et enfin estimer l'écart (gap analysis) et notamment les points que le SIRP pourra et devra supporter.

Voici quelques questions à se poser :

- Sur l'existant : quelle est ma maturité sur la détection et la réponse à incident ? Comment sont répartis mes actifs ? Quelles sont les équipes qui les exploitent et gèrent les incidents ? Quels sont les processus existants ou manquants (traitement, escalade, communication, etc.) ? Quelles sont les solutions préventives et de détections principales ? Même si l'outillage pourra aider, il ne remplacera pas une organisation non fonctionnelle ou encore qui manque complètement de compétences.
- Quelles sont les contraintes règlementaires qui s'imposent à tout ou partie des métiers et du SI (LPM, PDIS, BALE, etc.) ? Le SIRP peut-il jouer un rôle dans cette mise en conformité ?
- Finalement, quels sont les gains attendus ? Par exemple, s'agit-il principalement de renforcer la communication entre plusieurs périmètres / équipes de supervision et gestion des incidents ? S'agit-il d'améliorer la traçabilité et la capitalisation d'informations ? S'agit-il aussi de standardiser et d'automatiser au maximum les actions d'analyse et/ou de réaction ?

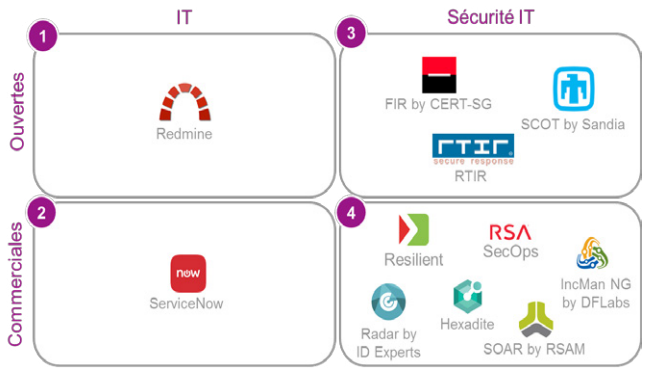
Un travail collaboratif est vivement encouragé afin de s'assurer que chacun puisse y trouver son compte pour choisir l'outil le mieux adapté aux besoins et en maximiser son adoption et donc sa valeur.

CHOISIR LA SOLUTION ADAPTÉE À SON CONTEXTE

La phase d'identification des besoins prend réellement toute son importance dans le processus de choix d'une solution SIRP. En effet, il existe une forte variété de solutions pouvant répondre à tout ou partie des attentes.

Ces solutions peuvent être classées suivants deux grands critères :

- La solution est-elle open source (issue d'un projet, gratuite et modifiable à souhait mais potentiellement sans support professionnel) ou au contraire commerciale (packagée et prête à l'emploi avec un support technique mais en contrepartie payante) ?
- La solution a-t-elle été créée dans l'objectif de gérer les incidents de sécurité IT ou au contraire est-elle issue du monde de la production IT et en ce sens une extension d'un outil de ticketing / ITSM ?



À noter par exemple :

1. Côté open source [3] : la plateforme FIR (Fast Incident Response) créée et maintenue par le CERT de la Société Générale.
2. Côté ITSM [2] : ServiceNow, leader de l'ITSM en SaaS qui a récemment ajouté une offre « Security Operation Management » supportée par 3 applications ServiceNow : « Security Incident Response », « Vulnerability Management » et « Threat Intelligence ».
3. Côté des pure players SOAR / SIRP [4] :
   - Resilient (acquis par IBM en mai 2016) qui propose sa solution éponyme dédiée. Resilient est certainement l'acteur historique sur le marché des SIRP.
   - RSA (division sécurité d'EMC, en cours de rachat par Dell) propose la solution « SecOps » intégrée à son offre « Advanced SOC ».
   - DFLabs, société italienne, dont la solution « IncMan » est le produit phare.

Typiquement, si vous êtes un CERT/CSIRT ou une seule équipe de réponse à incident à « forte expertise », un outil développé par un autre CERT/CSIRT (ex. FIR du CERT-SG), personnalisé et exploité par vos soins constitue certainement le meilleur choix.

A contrario si votre société utilise une solution ITSM largement déployée et que celle-ci offre un module de gestion des incidents de sécurité, peut-être faut-il porter un soin particulier à l'idée de capitaliser sur l'ITSM en évaluant soigneusement les fonctionnalités spécifiques aux incidents de sécurité.

Si vous avez un haut niveau de maturité, que vous recherchez définitivement des fonctionnalités avancées pour la réponse à incident et qui soient supportées par défaut (par exemple un plugin multi-SIEM, la multi-threat intelligence, etc.), peut-être est-il judicieux d'examiner les quelques pure-player du marché ; ceux-ci étant largement tirés par les États-Unis et ses MSSP (Managed Security Service Provider).

CONCLUSION

Un SIRP n'est bien sûr pas indispensable nous pouvons faire de la réponse à incident sans SIRP. Mais pour certains organismes, notamment les grandes entreprises réparties sur plusieurs plaques géographiques et/ou plusieurs sites, cela peut être intéressant. Un SIRP permet de gagner en efficacité sur le traitement des incidents (délais, qualité de la réponse, valorisation des actions, etc.), offre un reporting de la réponse à incident et assure une coordination entre les différentes équipes.

Mais comme toute nouvelle solution sur un système d'information, c'est par un accompagnement des différentes parties prenantes au changement que pourra passer sa bonne intégration.

MACHINE LEARNING ET CYBERSÉCURITÉ

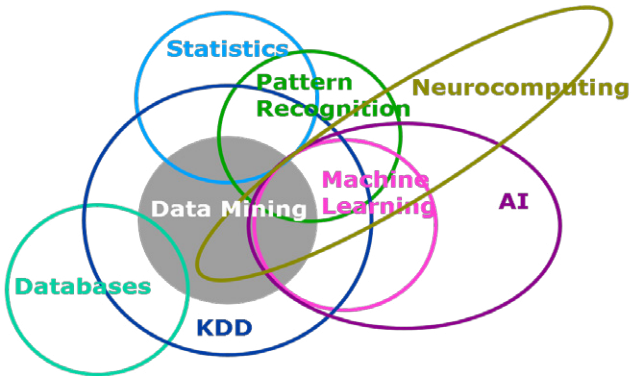
Tout le monde entend parler de « machine learning », d' « intelligence artificielle », de « big data », d' « analytics »... Qu'en est-il de ces concepts, et notamment du machine learning appliqués à la cybersécurité ?

MACHINE LEARNING, KESAKO ?

Le « machine learning » pourrait se définir tel que « le concept d'utiliser les données et des algorithmes pour permettre à une machine d'apprendre d'elle-même ».

LA THÉORIE, DES DOMAINES ET DES GRAPHES...

Contrairement à la modélisation statistique qui consiste en la formalisation de règles entre des variables sous la forme d'équations mathématiques, le machine learning désigne le concept d'un algorithme qui peut apprendre à partir des données sans s'appuyer sur des règles préprogrammées. En cela, le machine learning appartient au domaine de l'information et de l'intelligence artificielle.



LE MACHINE LEARNING S'APPUIE SUR LES RÉCENTS PROGRÈS TECHNOLOGIQUES

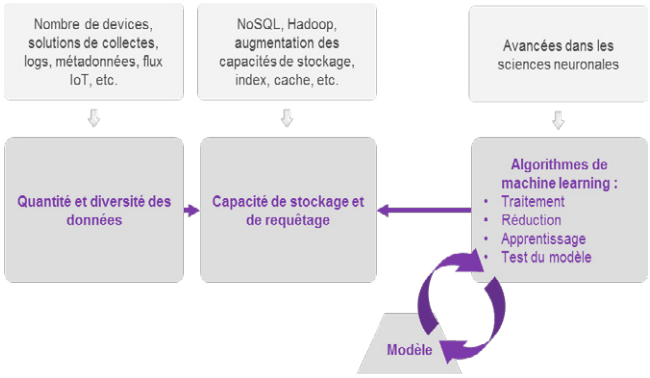
Les 3 principaux piliers du machine learning sont :

/ L'exploration de données (data mining), permise et justifiée par la quantité et la diversité des données aujourd'hui produites, potentiellement collectées et disponibles.

/ La reconnaissance de motifs (pattern recognition), permettant notamment de tisser des liens entre les données recueillies et de faire ressortir des motifs.

/ L'informatique neuronale (neurocomputing), comme moyen supplémentaire d'analyse, inspiré des réseaux neuronaux biologiques, comme le cerveau.

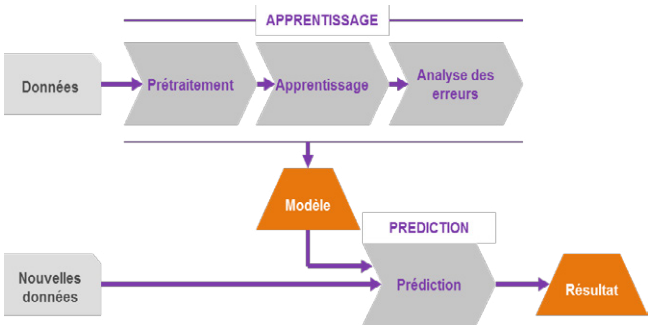
Ces capacités sont permises par les récents progrès technologiques, comme l'illustre le schéma ci-dessous :



Finalement, le machine learning constitue le « cerveau » qui permet d'extraire du sens depuis l'entrepôt de données.

COMMENT CELA FONCTIONNET-T-IL ?

Donner la capacité à une machine d'apprendre ne va pas de soi ! En voici les concepts clés :



Le processus peut se décomposer en plusieurs phases :

/ Le prétraitement des données, via la normalisation et l'épuration des données, permet de les rendre accessibles au traitement.

/ L'apprentissage, qui peut se baser sur plusieurs types d'algorithmes, parmi lesquels :

- L'apprentissage supervisé crée un modèle en se basant sur des exemples étiquetés obtenus à partir d'expériences passées. Il nécessite des données d'entrainement composées de 2 ensembles : premièrement des éléments/valeurs d'entrée (également appelés « features »), et secondement, une classe (ou «labels»), exemple : site Web de phishing vs. site sain. Le but du modèle créé est de prédire la classe pour des données où seules les features sont disponibles. Concrètement, pour qu'un programme apprenne à reconnaître une voiture, par exemple, il est « nourri » de dizaines de milliers d'images de voitures, étiquetées comme telles. Une fois entraîné, il peut reconnaître des voitures sur de nouvelles images.

- L'apprentissage profond ou non-supervisé vise à laisser le

soin (et le travail) à la machine (comprendre l'algorithme) de déterminer les classes en mettant en exergue les motifs communs et différences. Cette méthode se distingue de l'apprentissage supervisé par le fait qu'il n'y a pas de sortie a priori. Cette technique se base sur un « réseau de neurones » dans lequel les résultats de la couche de neurones vont servir d'entrée au calcul des autres couches. En mars 2016 le programme alphaGo ayant appris à jouer au jeu de go par cette méthode a battu le champion du monde Lee Sedol 4 parties à 1.

/ L'analyse des erreurs constituant une phase de test du modèle.

Ensuite, afin de valoriser les données classifiées, il s'agit de combiner les classes.

Cette phase est certainement plus délicate. En effet, la corrélation fait intervenir des règles liées aux métiers (à l'utilisation voulue du machine learning), mêlant des règles notamment faites d'expériences et d'exceptions.

DE NOMBREUSES APPLICATIONS POSSIBLES POUR UN MARCHÉ EN PLEIN BOOM

L'intelligence artificielle et plus précisément le machine learning a décidément le vent en poupe ! Des applications historiques telles la prévention de la fraude dans le milieu bancaire ou à la prédiction des maladies et à l'aide à la décision pour les soins associés (cf. Google DeepMind et London Eye Hospital), il existe de nombreux débouchés potentiels (dont cet article n'est pas l'objet).

Tiré par les grands et notamment Google, de nombreuses annonces au sujet du machine learning ont été publiées récemment, avec par exemple :

/ Google ayant rendu public courant mai ses puces « TPU » (Tensor Processing Unit) spécialement conçues pour être optimisées pour les opérations de réduction (opération élémentaire du machine learning), utilisable avec sa bibliothèque opensource nommée « TensorFlow ».

/ En juin, la société BrainChip (producteur de puces dédiées au machine learning) a racheté la société française « Spikenet Technology » offrant des « technologies multi-applicative de reconnaissance de formes en temps réel » avec par exemple des applications dans la surveillance des aéroports.

LE MACHINE LEARNING APPLIQUÉ À LA CYBERSÉCURITÉ

Intéressons-nous maintenant aux applications du machine learning à la cybersécurité et notamment à la détection d'incidents de sécurité.

DES MOTEURS DE DÉTECTION EN PLEINE ÉVOLUTION

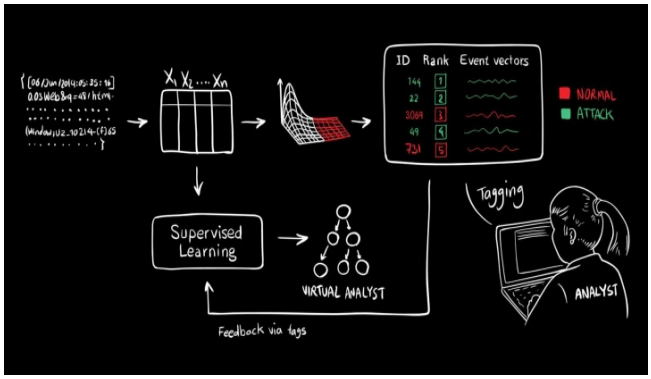
Avant d'évoquer les applications à proprement parler, dressons un rapide récapitulatif des solutions / moteurs de détections actuels, parmi lesquels :

/ Les méthodes historiques (de type « antivirus ») se basant sur des signatures : la solution cherche, notamment dans les fichiers, des traces des signatures connues comme faisant partie de malwares.

/ Les solutions plus avancées se basent sur l'émulation (i.e. exécution du malware présumé dans un environnement bac à sable) pour déterminer s'il en résulte un comportement malveillant ou non. Cela passe par une combinaison d'analyse comportementale (ex. il n'est pas « normal » qu'un binaire lise et réécrive un grand nombre de fichiers sur les périphériques de stockage, ce qui peut être le signe d'un ransomware) et de recherche d'indicateurs de compromission – IOC (ex. un fichier faisant des HTTP GET vers des URL / IP connus comme étant répertoriés comme un C&C).

/ De nouvelles solutions, d'analyse comportementale à grande échelle ingérant de grandes quantités (plusieurs Gbps) et variétés de données (flux, métadonnées, logs, etc.) à la recherche de déviances pouvant indiquer des actes malveillants.

C'est notamment sur ce dernier type de solutions que le machine learning peut apporter une réelle valeur ajoutée.



Parmi les grands éditeurs de solutions de sécurité, RSA (division sécurité d'EMC, en passe d'être racheté par Dell) a annoncé à la RSA conférence (mars 2016) l'intégration à la suite Security Analytics (le SIEM RSA sur la base des logs et des paquets réseaux) d'un moteur d'analyse comportemental temps réel basé sur le machine learning.

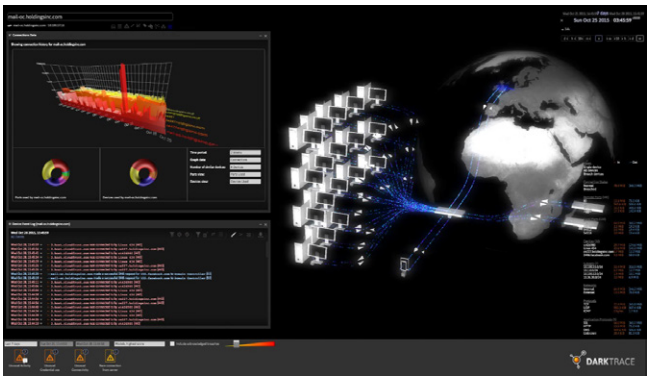
Du côté de « Big Blue », l'éditeur fournisseur de la plateforme de SIEM bien connue « Qradar » a annoncé en mai la sortie d'une déclinaison appliquée à la cybersécurité de sa plateforme de machine learning « Watson ».

IBM compte nourrir « Watson for cybersecurity » de son flux de Threat Intelligence « X-force » mais aussi des données moins structurées tels que des messages de SPAM, des malwares ainsi que des rapports de recherche, aidé par le partenariat établi sur

ce projet avec 8 universités nord-américaines. L'éditeur prévoit de traiter 15 000 documents par mois.

De taille plus modeste et plus proche de nous, la société DarkTrace, fondée en 2013 et basée en Angleterre, propose une solution de détection, nommée « Enterprise Immune System » qui n'utilise pas d'IOC mais uniquement des algorithmes de machine learning. Une déclinaison au monde des SI industriels est également disponible. L'éditeur indique un temps moyen d'apprentissage (capture des données, contextualisation manuelle, levée d'alerte, tunning de manière itérative, etc.) d'environ 2 semaines.

La solution, outre son moteur de détection différenciant, offre une interface particulièrement visuelle.



Nous avons récemment pu la voir fonctionner (en environnement de démo) et la challenger dans le cadre d'un RFP pour un client du cabinet. La solution semble particulièrement prometteuse. Darktrace a levé 65 millions de dollars début juillet pour continuer son développement.

Ce qui est particulièrement intéressant avec ces solutions est le fait qu'elles ne se concentrent pas seulement sur la détection de l' « infection initiale » mais aussi et surtout sur la détection des « symptômes » (post infection donc), offrant une visibilité accrue pour détecter les comportements malveillants.

UN MOYEN DE DÉTECTION COMPLÉMENTAIRE PLUTÔT QU'UNE FIN EN SOI

Le machine learning, même s'il n'est pas nouveau, a récemment fait ses preuves et de nombreuses applications (fraude, santé, assurance, etc.) sont envisageables. Cette combinaison rend le machine learning très tendance actuellement et intéressant pour les prochaines années.

Appliqué à la cybersécurité et à la détection d'incidents de sécurité, les grands acteurs du domaine (ex. RSA, IBM) enrichissent leur plateforme par des moteurs de détection basés sur du machine learning, et des sociétés « pure player » (ex. Darktrace) voient le jour et commercialisent des solutions dédiées. Cela dit, le marché semble est encore peu mature.

Aussi, très rares sont aujourd'hui les grands comptes ayant déployé une solution de détection d'incidents de sécurité principalement basée sur le machine learning. En effet, les équipes de sécurité sont souvent dépassées par les alertes des moyens de détection actuels sans qu'il y ait besoin d'en ajouter un. Un réel niveau de maturité SSI semble donc un prérequis avant de s'équiper d'une telle solution.

Dans tous les cas, le machine learning constitue une approche complémentaire car ne visant pas à détecter les mêmes évènements : son apport semble bien plus important sur le volet détection de comportements malveillants suite à compromission que sur la détection de la compromission elle-même.

Finalement, le machine learning appliqué à la cybersécurité apparait comme un moyen complémentaire et non une fin en soi : du côté des solutions, les capacités de visualisation, d'automatisation et de reporting semblent cruciales, côté humain, la disponibilité et la qualité de l'expertise restent plus que jamais nécessaires.

Bref, un sujet à suivre de près !

INTERVIEW

LA STRATÉGIE DE THREAT INTELLIGENCE D'UNE BANQUE INTERNATIONAL

Christian Karam est le directeur de la Cyber Threat Intelligence d'un grand groupe bancaire international. Basé à Singapour, il supervise le service en charge de fournir aux métiers une vision des menaces constamment actualisée, et aux équipes opérationnelles des renseignements précieux pour identifier les indicateurs de menaces, les techniques, tactiques et procédures qui permettent de gagner en efficacité dans la mitigation et la réponse face aux menaces. Christian Karam conduit également des activités reconnues de recherche et d'expertise en sécurité et cybercriminalité, après avoir travaillé pour Interpol.

La Threat Intelligence n'est pas un domaine très développé dans les entreprises, pourquoi ?

Dans la plupart des entreprises, cette activité n'est pas encore très répandue. Il s'agit d'un investissement important en termes de ressources humaines, c'est pour cela que peu d'entreprises ont aujourd'hui commencé à travailler sur le sujet. D'autant que les compétences sont très rares dans ce domaine… soit il s'agit d'anciens officiers de police qui ont déjà travaillé sur des sujets cyber, soit de chercheurs en cybersécurité…

À la base, il s'agit de reprendre le modèle du Total Information Awareness (TIA) des Américains. Un programme de Threat Intelligence doit servir à révolutionner les capacités de l'entreprise à détecter, classifier et identifier les attaquants et, *a fortiori*, permettre à l'entreprise de prendre des actions rapides pour se prémunir et déjouer les cyber-attaques.

Néanmoins, les banques ont bien compris l'intérêt de développer la Threat Intelligence : il s'agit de faire peur aux cybercriminels en leur faisant passer un message fort « nous savons qui vous êtes, nous savons d'où vous venez et nous pouvons vous faire arrêter ». L'objectif principal est bien l'attribution des attaques : qui attaque, avec quelles motivations, quelles sont leurs intentions, quelles sont leurs capacités ? Nous travaillons de concert avec les forces de l'ordre pour faire arrêter les attaquants. Nous devons faire en sorte que les cybercriminels considèrent que « ça ne vaut pas le coup » d'attaquer la banque : c'est trop compliqué techniquement et cela devient risqué.

La Threat Intelligence a également pour objectif d'identifier en quoi les cybercriminels peuvent être meilleurs que nous dans la défense et ainsi de rééquilibrer le rapport de force.

Comment structurer les activités de Threat Intelligence ?

Tout d'abord, il faut mettre en place le processus : qui va faire quoi, comment, avec qui… il faut délimiter les rôles et les responsabilités.

Ensuite, il y a toute la phase d'ingénierie : quels produits utiliser, comment les intégrer, quels sont les outils qui permettront d'être plus efficaces, de quelles sources de Threat Intelligence avons-nous besoin…

De manière concrète, nous avons mis en place un centre de renseignement (RENS) qui va travailler de concert avec le SOC, l'équipe anti-fraude et l'équipe d'investigation cybercrime.

C'est ce centre qui reçoit l'ensemble des différents flux de Threat Intelligence, qui les traite pour les autres équipes et qui définit le paysage de la menace (*threat landscape*) de la banque, à savoir ce qui est le plus intéressant à suivre en fonction de la zone géographique et de l'actualité cybersécurité.

Le centre RENS a été créé pour répondre aux problématiques opérationnelles et stratégiques :

- Sur le volet opérationnel, l'objectif est de fournir des informations utiles aux autres équipes pour les aider et les orienter dans leurs investigations et dans leur dé-

fense du SI. Globalement, nous essayons d'appliquer le modèle OODA (Observe, Orient, Decide and Act) pour nos opérations sécurité. Le centre RENS analyse et observe les attaques pour fournir les informations utiles afin d'orienter les autres équipes, notamment le SOC, à prendre les bonnes décisions avant d'agir dans le cadre de la protection ou de la défense du SI.

/ Sur le volet stratégique, il s'agit de prendre du recul sur l'état de la menace qui pèse sur l'entreprise et sur les attaques subies, en apportant une vision plus globale que l'attaque unitaire. Chaque affaire close est revue pour identifier des métriques et évaluer les capacités de l'attaquant. Nous identifions ensuite si notre défense est au même niveau ou meilleure que l'attaquant, en considérant les technologies déployées pour bloquer l'attaquant.

Ce travail d'évaluation est fait deux fois par mois et nous permet d'identifier là où nous devons effectuer des investissements.

Le centre fait également de la recherche externe : nous essayons de débusquer les attaquants en identifiant leurs infrastructures, leurs outils, leurs méthodologies, etc.

Aujourd'hui, nous disposons d'une dizaine d'analystes et nous avons un objectif de 35 analystes d'ici 3 ans. Pour comparaison, le SOC représente aujourd'hui environ 40 personnes avec une cible à 50 d'ici 3 ans.

Quelles difficultés rencontrez-vous dans la mise en œuvre de cette équipe ?

La principale difficulté est celle de la compétence. Peu de gens sont capables de faire ce type d'analyse : il faut des compétences en système, en réseau, en reverse engineering, en cybercriminalité…

Par ailleurs, nous avons des difficultés vis-à-vis des sources de Threat Intelligence : trouver une source de qualité est très compliqué. Le marché de la Threat Intelligence est essentiellement américain. Par conséquent, les indicateurs sont à 90% des données utiles pour l'Amérique du Nord et 10% seulement pour l'Europe et l'Asie.

Nous faisons également face à des problématiques culturelles :

/ « Tout collecter, tout savoir, prendre tous les signaux de tous les bruits » n'est pas quelque chose qui existe en Europe.

/ Nous sommes confrontés à la barrière de la langue dans de nombreux cas.

/ Les pays européens ont tendance à être beaucoup plus conservateurs que les autres sur la protection des données.

/ Il y a un cloisonnement très fort en Europe entre le secteur de la défense et le secteur privé.

Enfin, la législation n'est pas la même partout et nous pouvons nous retrouver face à des contraintes légales dans la collecte ou le partage d'informations au sein d'une même organisation répartie sur plusieurs plaques géographiques différentes.

Quels sont les investissements à considérer ?

Nous en avons déjà un peu parlé, mais globalement :

/ Des ressources compétentes.

/ Des flux de Threat Intelligence utiles et pertinents. Baser sa stratégie uniquement sur les flux est une mauvaise pratique car à terme il y aura énormément de faux positifs. Il est nécessaire de commencer par des sources internes pour prioriser les différents périmètres, puis d'enrichir le tout avec des sources externes. Il faut réaliser une cartographie des capacités de renseignement interne avant de se porter sur l'externe. Attention, car plus il y a de sources, plus il y a de travail pour les analystes… Il faut voir la Threat Intelligence comme le fait de « trouver une aiguille dans un tas d'aiguilles : toutes les attaques se ressemblent ! ». C'est d'autant plus vrai car les groupes d'attaquants cherchent réellement à s'imiter pour se camoufler : les États veulent se faire passer pour des groupes de cybercriminels afin de rester anonymes ; à l'inverse les groupes de cybercriminels adoptent les méthodes des États pour se légitimer.

/ Un outillage complet. Il existe deux principales typologies d'outils :

- Les Threat Intelligence Platforms (TIP) : pour la corrélation entre le renseignement interne et externe (sources, bulletins, vulnérabilités, etc.).
- Les Threat Intelligence Repositories : pour la consolidation des indicateurs et autres informations collectées.

En synthèse, construire sa stratégie de Threat Intelligence, c'est :

/ Cibler le périmètre sur lequel travailler : il est impossible de travailler sur l'ensemble du périmètre d'un grand groupe international… il est nécessaire de trier !

/ Créer l'organisation et les processus du service : attention aux compétences des analystes !

/ Cadrer les activités de Threat Intelligence (stratégique, opérationnelle, tactique et/ou technique) : ne pas surinvestir une activité inutile si l'organisation ne suit pas !

/ Construire l'outillage adéquat : TIP, TIR, sources de veilles internes puis externes… ni trop, ni trop peu !

/ Se guider par les résultats : ne pas hésiter à se réinventer régulièrement pour faire face à l'évolution des menaces !

Merci à Christian Karam d'avoir accepté cette interview !

CERT W

Le CERT-Wavestone associe un ensemble d'expertises techniques et métiers afin d'apporter une réponse globale aux incidents de sécurité. Plus de 45 profils expérimentés sont mobilisables au sein du CERT-Wavestone.

ACTUALITÉS

L'Eté n'a pas été de tout repos pour nos analystes : vol de données, chantâge, destruction du SI, ransomware, vengeance d'un ancien employé... nos clients ont été assaillis de toute part! L'hétérogénéité des affaires traitées nous rappelle que la plupart des attaques proviennent de cybercriminels peu qualifiés et non d'acteurs étatiques...

Retrouvez les publications de nos experts sur www.securityinsider-wavestone.com

Twitter @secuInsider

Pour vous abonnez à notre lettre CERT : cert@wavestone.com

ABONNEMENT : CERT@WAVESTONE.COM

RÉACTION SUR ATTAQUE OU SUSPICION

- Investigation numérique / Forensics
- Gestion de crise SI et métier
- Construction des plans de remédiation

THREAT INTELLIGENCE

- Evaluation de l'attractivité de l'entreprise
- Analyse et décryptage d'attaques
- Watch&Learn : Veille cybercriminalité

PRÉPARATION À LA DÉFENSE & À LA GESTION DE CRISE

- Définition et animation des processus CERT et SOC
- Red team & Purple team
- Exercices de crise

Directeur de la publication : Pascal Imbert

Responsable de la rédaction : Frédéric Goux
Contributeurs : Gérôme Billois, Baptistin Buchet, Hélène Dutilleul, Ayoub Elaassal, Chadl Hantouche, Mathieu Hartheiser, Jean Marsault et Vincent Nguyen.

Photographies : Getty images - Fotolia

Graphiques : Wavestone

Conception graphique : les enfants gâtés

Impression : Axiom Graphics

CERT-Wavestone

Responsable CERT : Matthieu Garin

cert@wavestone.com

2016 I © WAVESTONE - ISBN : 978-2-918872-31-3 / EAN : 9782918872313

WAVESTONE

www.wavestone.com

Wavestone est un cabinet de conseil, issu du rapprochement, début 2016, de Solucom et des activités européennes de Kurt Salmon (hors consulting dans les secteurs retail & consumer goods).

Dans un monde où savoir se transformer est la clé du succès, l'ambition de Wavestone est d'apporter à ses clients des réponses uniques sur le marché, en les éclairant et les guidant dans leurs décisions les plus stratégiques.

Wavestone rassemble 2 500 collaborateurs présents sur 4 continents. Il figure parmi les leaders indépendants du conseil en Europe, et constitue le 1er cabinet de conseil indépendant en France.