L'automatisation comme mesure active de protection

Nicolas Audiot [1], Nicolas Loriot [1]

[1] *Airbus Cybersecurity, 1 boulevard Jean Moulin, Élancourt, France*

Abstract

Automation has been highly used as a mean to enhance the capabilities of security engineers, either to preserve them from routine tasks or to expand their scope of action. It has so far mostly revolved around passive actions (enhancing qualification of SOC alerts for instance). On a different track, we have observed the development of active measures to oppose an adversary, at first cautiously (NIPS) and now with more eagerness (EDR).

In the meantime, we observe increasingly prolific adversaries, especially ransomware actors, whose modus operandi revolves on a flash action on objectives phase rolled out outside of business hours. In this paper, we will try to venture ideas on how we could use automation to counter their speed and provide time for the defenders to react, using modifying or blocking actions system-wide for standard, poor-health IT systems.

Keywords

SOC, security operations centre, ransomware, centre des opérations de sécurité, rançongiciel, automation, automatisation, adversary, adversaire

1. Introduction

« Ah c'est dommage ». Cette phrase –ou des équivalents approchants– est souvent prononcée lors des analyses post-mortem de systèmes ayant fait l'objet d'une compromission, particulièrement suite à des attaques par rançongiciel. Elle est citée généralement autour de la présentation de l'élément clé ayant servi de pivot à l'adversaire, ce tout petit engrenage qui lui a permis de réussir son entreprise. 3 jours, 3 semaines ou 3 mois plus tard, elle vient surtout souligner un constat amer, format os de poulet coincé au travers de la gorge. Si seulement l'ancien VPN avait été dé-commissionné, si seulement la règle de pare-feu inutile avait été désactivée entre les deux zones, si seulement il y avait eu une double authentification… Cette envie de rejouer le dernier match du VI Nations 2021, mais que le 15 mette en touche plutôt que de vouloir relancer à la 80ème minute. Ces occasions manquées de faire des choses qui nous semblent a posteriori logiques sont légion.

Ces derniers mois ont mis l'accent sur les attaques par rançongiciels. À chaque nouveau rapport transparaît en filigrane une caractéristique majeure : l'attaque, ou au moins sa phase finale, a été exécutée très rapidement. D'expérience, nous avons constaté que cette phase d'action sur objectif (le moment où l'adversaire chiffre les disques durs) a généralement intentionnellement lieu la nuit ou en heures non ouvrées (HNO) du fuseau horaire de la victime. Parfois dans la nuit de jeudi à vendredi, comme si l'adversaire vous souhaitait un bon weekend, laissant le concept des 35h s'appliquer sur les 3 derniers jours restants de la semaine pour les plus chanceux et vous laisser mariner tout le weekend dans l'intention de vous faire céder à la tentation de payer la rançon pour reprendre les activités le lundi venu.

En tant que défenseurs, la problématique à laquelle nous avons à répondre est alors la suivante : comment contrer un adversaire qui planifie son attaque pour que la phase d'action sur objectifs coïncide avec les heures non ouvrées où, par définition, il y a peu ou pas de personnel pour réagir ?

Il convient de préciser que les réflexions qui suivent sont basées sur un début de détection nécessaire pour détecter l'adversaire. Cependant ce papier se concentrera sur les méthodes pour réagir au mieux dès les premiers signaux détectés, mêmes faibles.

C&ESAR '21: Computer Electronics Security Application Rendezvous, November 16-17, 2021, Rennes, France
EMAIL: nicolas.audiot@airbus.com (N. Audiot); nicolas.loriot@airbus.com (N. Loriot);

Avoir recours à l'automatisation dans plusieurs domaines et depuis plusieurs années pour remplacer du personnel ou accélérer son travail nous a permis d'atteindre un niveau de maturité, notamment sur ce qu'il est possible de faire ou ce qu'il convient d'éviter. Face à un adversaire caractérisé par sa vitesse et ayant l'avantage de l'initiative, est-il envisageable de faire appel à l'automatisation, non plus seulement pour augmenter les capacités de nos analystes, mais également pour qu'une fois revenus au niveau de progression de l'adversaire dans l'attaque, pouvoir reprendre l'initiative et interrompre son activité avant le moment fatidique ?

2. Situation

2.1. RETEX automatisation

2.1.1. Chéri.e, j'ai rétréci les temps de traitement

Au sein du SOC d'Airbus CyberSecurity, l'automatisation a été appliquée en premier pour accélérer la qualification des alertes. Cela a été nécessaire pour être en mesure de tenir des délais de réponse courts (inférieurs à l'heure) et pour faire face à l'augmentation de la charge de travail.

Cela a été fait en premier en développant des « playbooks » d'orchestration, dont le but était d'automatiser les phases d'enrichissement et de qualification des alertes. Les analystes ont commencé à développer des scripts reproduisant le travail manuel qu'ils effectuaient fréquemment. Ce travail est devenu une activité à part entière de plusieurs milliers d'heures cumulées au fil des années. Le temps de traitement est passé de quelques heures ou fraction d'heure à quelques minutes par alerte ; d'un traitement par des analystes de niveau 2 à un traitement majoritairement par des analystes de niveau 1.

Dans un second temps, l'intelligence artificielle (IA) a été mise à contribution. La première orientation a été de reproduire les raisonnements des analystes en phase de qualification. L'objectif était d'aller récupérer les éléments de conclusion qu'un analyste recherche pour les lui présenter sans qu'il ait à les collecter. Les modèles développés reproduisant les raisonnements des analystes, ceux-ci étaient en mesure de comprendre et expliquer les résultats qui leur étaient proposés. Cette « explicabilité » est une condition *sine qua non* en environnement opérationnel, où il est nécessaire de pouvoir appuyer la prise de décision.

Sur certaines tâches où nous avons commencé à l'appliquer, cela nous a permis des gains de temps jusqu'à 1 heure par jour, en fonction de la volumétrie. Cette automatisation a même pu mettre en lumière des travers, tels que des erreurs d'analyste dans leur classification : certains soucis se répétant avaient été à tort classifiés en faux positif par l'analyste le temps que le client corrige le souci.

Nous avons ensuite cherché à étendre l'usage de l'IA aux phases de levée de doute et de réponse à incident. Dans ces situations, il est parfois utile de savoir évaluer rapidement la compromission d'éléments d'un système d'information à partir d'un râteau assez large (dans les faits, se retrouver avec les empreintes de milliers de machines et devoir fournir une réponse le plus rapidement possible). En parallèle de la vérification de points statiques (mécanismes de persistance par tâche planifiée ou création de service par exemple), les modèles mis au point font apparaître des divergences par rapport à un état préalablement sain de chaque machine. Durant la phase de test certaines machines compromises n'ont pas été détectées par l'IA, les modèles étaient en erreur ; dans ces cas l'analyste reprenait les investigations. Les détections étaient toujours des vrais-positifs.

2.1.2. Retour d'expérience sur l(a tentative d)'intégration et le déploiement continus de règles en production

Nous avons également initié il y a quelques années des travaux pour accélérer le partage de règles entre les périmètres. Ces travaux ont été réalisés dans une chaîne d'intégration continue avec son déploiement (CI/CD) permettant de générer automatiquement le package de règles adaptées au SIEM visé et de déployer automatiquement ce dernier dans le SIEM en utilisant ses API. Cela est passé par plusieurs étapes. Le premier niveau d'automatisation a commencé d'abord par une volonté de capitaliser et de partager au mieux les règles qui peuvent l'être entre les différents périmètres en opération. Ce travail a terminé, après différents essais, sous la forme d'une capitalisation dans un outil

de gestion de configuration avec des capacités de forge logicielle. De là, nous avons eu deux courants de pensée dans nos équipes et nous avons testé les deux approches afin d'identifier la plus efficiente.

La première approche, modérée, avait comme objectif premier de mettre en gestion de configuration les nouvelles règles et parseurs associés afin qu'elles puissent être exportées facilement dans nos différents périmètres clients. Les règles étaient préparées sur un environnement simulé et testées avant d'être ajoutées au catalogue. Cet export était le fait d'un analyste qui gérait le périmètre et qui décidait alors quelles règles et parseurs parmi le catalogue il allait passer en production. L'automatisation se bornait à mettre à disposition des analystes un package régulièrement mis à jour.

La deuxième, plus ambitieuse, était de déployer un processus CI/CD sur cette chaîne de création de nouvelles règles. Là où la première option se bornait à mettre à disposition des packages adaptés aux formats des différents éditeurs que nous utilisions (ce qui est déjà une activité à part entière), cette deuxième option embrassait pleinement le principe CI/CD avec un développement de la règle, une compilation de cette dernière dans le format de l'outil cible, un déploiement automatique dans un environnement simulé avec le SIEM cible, une injection des logs pour simuler l'attaque et en fonction du résultat de la règle (c'est-à-dire une détection) le « commit » dans la forge était accepté ou refusé. La fin du processus allant ensuite jusqu'à déployer sur le périmètre de production la règle ainsi validée. Les leçons de cette deuxième méthode sont : si le déploiement est largement accéléré … le taux de faux positif est également en forte hausse générant une perte d'exploitation (surcharge) au niveau des opérateurs. Contrairement au prêt à porter, un système ne se satisfait que peu du concept de la taille unique. Chaque système a ses comportements propres et un même phénomène peut et doit se mesurer avec des seuils ajustés aux spécificités du client. En complément les méthodes de collectes peuvent avoir un impact sur les parseurs (par exemple, une remontée des logs Windows via différents agents qui peuvent formater différemment les messages). L'environnement simulé CI/CD n'est pas assez diversifié pour reproduire tous les cas des différents clients.

Cette deuxième option est donc à prendre uniquement si vous avez une très forte standardisation possible dans vos choix technologiques tant pour la partie SOC que les outils supervisés. L'environnement de test des règles doit représenter la combinatoire des outils et cas de déploiement de vos clients. Ce déploiement automatisé de règles doit se faire avec un marquage « pré production » des nouvelles règles qui nécessiteront souvent un affinage humain, soit pour réduire les faux positifs liés aux spécificités d'un périmètre client, soit pour rendre la règle effective car la règle initiale a été pensée avec trop de prérequis (une règle qui se base sur sysmon alors que tous les clients ne l'ont pas …) et donc ne détectera rien …

Pour ces différentes raisons, et car nos clients ont chacun leurs petites spécificités qui ne rendent pas aujourd'hui rentable d'avoir une reproduction fidèle de tous leurs cas dans notre environnement CI/CD, nous nous bornons à la première méthode agrémentée de quelques zestes de la deuxième. L'expérience nous a fait redescendre d'un cran le taux d'automatisation recherché pour l'alimentation de nos stratégies de détection.

2.2. Une posture de détection et d'armement dictée par les premiers APT publics

Dans les années 2010, la majorité de nos stratégies de détection et donc du fonctionnement de notre SOC et de notre équipe de réponse à incident étaient prévus pour lutter contre les adversaires dits « Advanced Persistent Threat » (APT). Ceux-ci avaient un niveau plus ou moins avancé suivant les acteurs, mais ils avaient surtout une vocation principale d'espionnage. L'objectif de l'attaquant était de rester sous le radar le plus longtemps possible afin de profiter de sa position acquise pour collecter un maximum de données sensibles et leur mise à jour au fil du temps.

Évidemment, les menaces plus classiques faisaient partie du champ de détection. Mais ces APT avaient une présence médiatique pour lesquels le jeu d'annonces sur la place publique était quasiment de trouver le cas où l'acteur était resté le plus longtemps sans se faire repérer. Nous pouvons rappeler l'exemple du groupe APT1 qui avait une moyenne de 356 jours avant détection et un record à 1764 jours [1]. À la vue de ces échelles, finalement, un weekend de perdu, bien que dommageable, était négligeable (en temps du moins).

La situation depuis ce rapport APT1 et la situation actuelle a évoluée (dans le bon sens) en étant constaté à moins d'un mois dans le dernier rapport M-Trends Report 2021 de FireEye Mandiant [2], en passant notamment de 416 en moyenne en 2011 à 24 en 2020.

La mise en place de SOC encore récents ou en projet pour certains acteurs industriels à l'époque de ces premiers APT publics n'ont pas poussé à avoir un personnel présent en HNO. Le budget et les efforts étaient principalement concentrés sur les heures ouvrées. Le fonctionnement HNO existait pour les cas de crise, déclenchés par les équipes en heures ouvrées.

Cela amène à une situation où, dans la majorité des cas, les dispositifs mis en place par le défenseur (côté SOC, IT ou métier) n'ont pas toujours été pensés pour amener une capacité de réaction. Ou du moins, la plupart du temps, pas pour obtenir des réponses rapides et ordonnées.

2.3. RETEX opérationnel

En premier, même si ce n'est pas quelque chose qui a été recherché, l'automatisation a eu tendance à faire disparaître certains aspects métier. Ce qui a été plus pénalisant, cela a pu se traduire en perte de compétences, ce qui est grave d'un point de vue opérationnel. L'exemple le plus frappant pour nous a été l'automatisation du traitement des alertes évoqué au 2.1. Le niveau d'attente placé sur cette capacité et les impératifs qui la régissaient (réussir à tenir la charge) ont concentré les efforts des analystes sur le développement de « playbooks », au point de faire perdre de vue le cœur du métier d'analyste, la capacité à investiguer.

Ensuite, si cette automatisation de l'analyse a permis d'améliorer la gestion de la charge opérationnelle, elle n'a pas permis d'amélioration réelle de la vitesse de réaction globale.

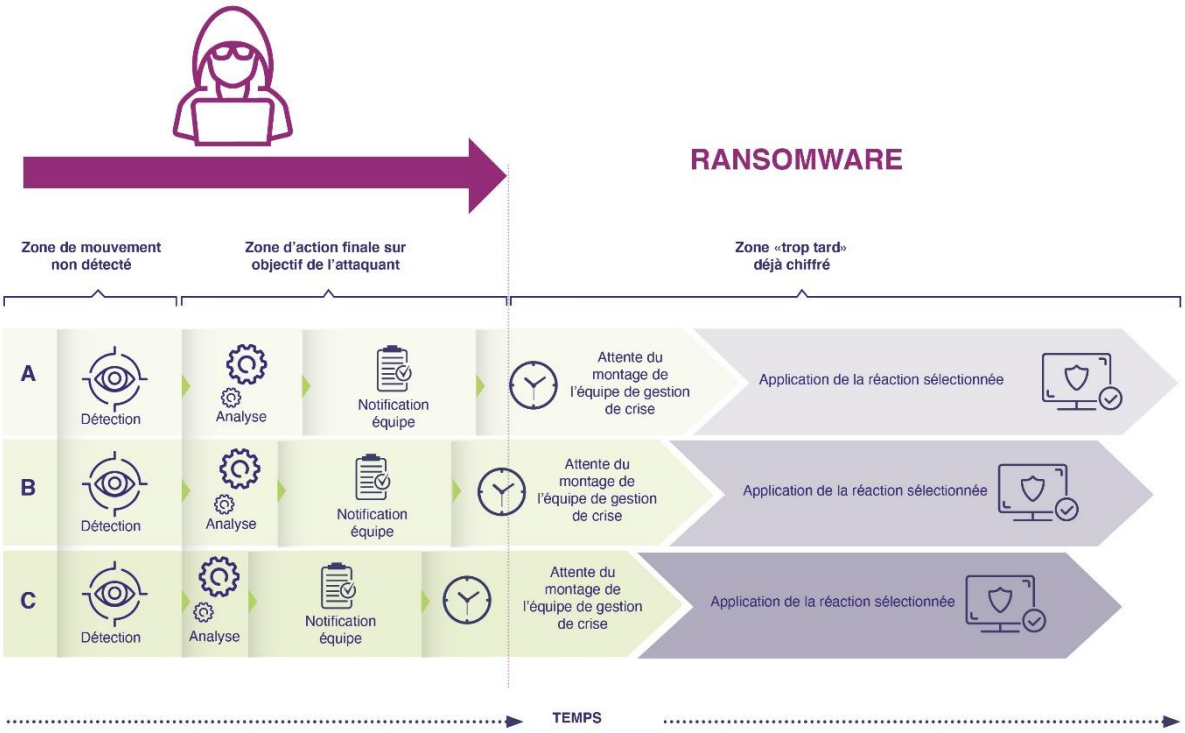

Figure 1 : Impact relatif sur le gain en durée d'analyse sur la réponse face à des attaques type rançongiciel

Le délai de réaction est lié au délai de détection, à la durée d'analyse qui suit et enfin à l'activation des actions de réponses. Les actions de réponses intègrent également les phases de décision qui nécessitent d'avoir les personnels activés. Le simple fait de gagner en temps d'analyse n'est pas suffisant pour stopper l'attaque. C'est nécessaire pour se laisser parfois quelques minutes de plus pour décider, mais c'est souvent insuffisant pour lutter contre des menaces ayant des modes opératoires rapides. Dans la figure supra, que l'activité d'analyse soit manuelle (A), semi automatique avec des techniques de classifications et d'enrichissement (B) ou totalement automatique (C), le souci reste

souvent le temps de notifier une personne qualifiée pour prendre la décision avant la phase finale de l'attaquant.

Ainsi en cas de crise, on peut se poser les questions suivantes : combien de temps avant d'avoir une cellule de crise montée, les personnels sur le pont ? En cas de crise, il faut convaincre tous les échelons de la chaîne de commandement. Cela nécessite de passer au-delà de la phase de sidération. Combien de temps avant que les gens soient en disposition de prendre des décisions, et que les équipes soient en position pour les implémenter ? Dans les faits, même après un incident type rançongiciel, il faut plusieurs heures avant déploiement, plusieurs dizaines d'heures avant les prises de décisions. Les équipes internes (administrateurs système et réseau par exemple) vont faire des choses en autonomie grâce à leur habitude de fonctionnement, et en reposant sur les niveaux d'autonomie et de responsabilité dont ils disposent habituellement. Il faudra plusieurs jours avant qu'un premier plan d'action soit conçu et commence à être implémenté.

Enfin, il faut garder à l'esprit que l'automatisation est un outil mis en appui des opérations et d'une ligne de conduite. Comme évoqué précédemment, historiquement au sein d'Airbus CyberSecurity la réflexion autour des stratégies de détection a tourné autour des menaces dites APT et de la protection des actifs « classiques » d'une organisation, au premier rang desquels Active Directory. L'idée était que les menaces APT ou étatiques étant par essence le « mieux » de ce qui se faisait, être capable de les adresser permettait d'adresser les menaces avec des profils « moins avancés ». Nous (Airbus CyberSecurity) avons également été habitués à ces réflexions par notre expérience dans le domaine de la Lutte Informatique Défensive.

C'était ignorer deux réalités : défendre contre un adversaire étatique ou APT demande des moyens conséquents. L'ennemi étatique qui cherche un effet (vol de données, sabotage, …), peut mettre des moyens importants en place et se donner un temps long pour y parvenir. Il peut par exemple se donner le temps de chercher des vulnérabilités dans votre client VPN, dans vos 2 technologies de pare-feux, … tandis qu'un groupe exploitant des rançongiciels (a fortiori encore plus pour ceux achetant le rançongiciel à d'autres groupes) cherche la rentabilité et donc l'investissement pour parvenir à ses fins est plus limité. Il aura tendance à exploiter au maximum sa recette gagnante là où elle passe facilement. La seconde réalité est celle effleurée à l'alinéa précédent. Des adversaires APT ou rançongiciel demandent des tempos opérationnels très différents, qui doivent être gérés distinctement. Ainsi, si techniquement nous avons pu développer l'usage de l'automatisation en l'optimisant à l'extrême, cela venait supporter une ligne directrice qui avait besoin d'évoluer pour suivre les menaces courantes vécues par nos clients.

Des technologies sont apparues pour compenser provisoirement cet état de fait, mais cela ne dispense pas de structurer une stratégie cohérente ne mettant pas tous ses œufs dans le panier d'une même technologie.

2.4. Développement des technologies de type EDR, premier rideau avec contremesures embarquées

« EDR » signifie « Endpoint Detection and Response », ce sont des agents déployés sur les équipements type station de travail et serveur. Cette famille d'outil propose 2 avantages, le premier la visibilité avec le « D » de détection. Ce type d'agent moderne dispose de plusieurs moteurs de détection, allant de simples listes noires, d'indicateurs de compromission (IoC), en allant jusqu'à des moteurs heuristiques ou à base d'IA pour essayer de détecter certaines menaces sous les feux de la rampe, dont les fameux rançongiciels.

Le deuxième avantage de ce type de technologie est le « R » de Response ou Réponse qui permet de prendre une posture plus ou moins automatique face à une menace. La plus courante et simple est le blocage du processus réputé malveillant. Cette réaction atomique a l'avantage de ne pas perturber le fonctionnement de l'ensemble du SI mais uniquement celui de la machine agressée en cas d'erreur de jugement. Les plus avancés de ces outils permettent également d'avertir les autres agents (via leur centre de gestion) afin d'isoler en amont le binaire responsable de l'agression. Cette manière de procéder est une sorte d'intelligence collective, où le premier qui est agressé permet de partager ses anticorps à toute sa famille si nous osions une analogie avec le corps humain. S'il s'avère être une carte dans le jeu du

défenseur, il ne faut pas oublier que toutes les technologies ont leurs limites et qu'il faut coupler leurs usages avec une notion système de défense en profondeur (en cas de perte de cette dernière).

3. Rançongiciel, la vitesse comme mode opératoire final

Le rapport M Trends 2021 de FireEye note que de 14% d'investigation en 2019 impliquant un rançongiciel, ils sont passés à 25% en 2020. Le rançongiciel est donc une menace qu'il est difficile d'ignorer de nos jours. Comprendre son anatomie permet de mieux cerner les options qui s'offrent à nous en tant que défenseur et quelles actions d'automatisation peuvent accompagner la lutte contre cette menace.

3.1. Mode opératoire d'un groupe exploitant un rançongiciel

Que se passe-t-il lors d'une attaque par rançongiciel ?

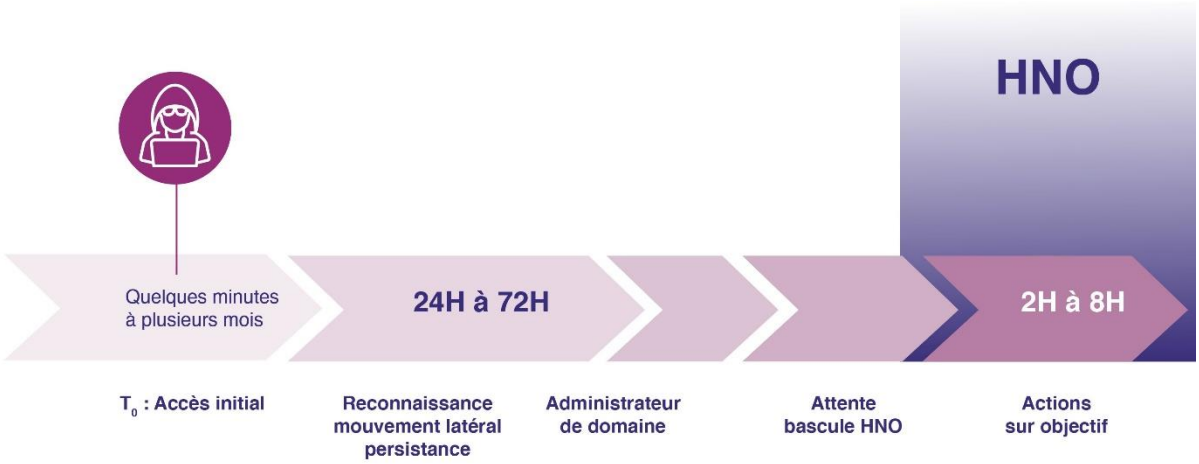

Figure 2 : Synthèse de la chronologie des attaques rançongiciel que nous avons pu déterminer lors de nos réponses à incident

Le mode opératoire observé est généralement assez simple.

En premier, l'adversaire va chercher à s'introduire au sein du système d'information. Cela peut être fait traditionnellement via un mail de phishing [2], ou par l'usage d'un exploit [2]. Ce dernier vecteur (exploit) a été l'occasion en 2020 d'une série d'intrusions par la récupération de secrets via l'exploitation de vulnérabilités non patchées sur solutions VPN [3]. Par exemple, nous avons pu constater cette technique (en post mortem) plusieurs mois avant l'attaque sur un VPN vulnérable servant à des administrateurs pour l'administration d'un sous-système. Il est à noter que cette partie de l'attaque est parfois réalisée par un premier groupe spécialisé pour obtenir des accès qui revendra ultérieurement cet accès obtenu à un autre groupe qui lui s'est spécialisé dans l'usage des rançongiciels, souvent de type « ransomware as a service ». Ensuite, votre adversaire utilise cet accès initial, soit immédiatement, soit en laissant passer un moment pour s'assurer d'être invisible, soit le temps de revendre le dit accès à un autre.

Il va alors partir à la découverte de votre système d'information. D'abord en s'assurant un accès persistant (« je compromets une machine et je déploie 5 *Remote Access Tool* (RAT) avec 3 méthodes de persistance différentes »), en se déplaçant et en itérant ces deux étapes. Ensuite en cherchant à mieux ~~vous~~ connaître votre domaine Active Directory : ses groupes et le plus court chemin vers un compte administrateur de domaine. Sauf s'il n'en a pas besoin … car les secrets de votre VPN sont déjà ceux de l'administrateur de domaine ! Mais passons sur cette erreur d'hygiène déjà rencontrée sur le terrain qui facilite la vie de l'attaquant et beaucoup moins celle du défenseur. En fonction de son mode opératoire, il va globalement chercher à établir une cartographie de votre système d'information. Cette cartographie lui sera également utile lors de la phase de chiffrement comme donnée en entrée de ses

scripts de déploiement de son rançongiciel. Après tout, lui aussi use de l'automatisation pour industrialiser son déploiement et ses actions.

Arrive le moment où il est administrateur de domaine, sur vos contrôleurs de domaine. Un contrôleur de domaine est un serveur particulièrement sensible, car c'est un élément névralgique de votre système d'information et car c'est du type chatouilleux quand on effectue des actions dessus. Et puis il y a toujours la possibilité d'avoir un administrateur qui a créé un tableau de bord pour suivre en direct les connexions. Du coup, votre adversaire va attendre patiemment que vos administrateurs rentrent chez eux.

À 2100CEST (2000Z ou UTC quand vous lirez le rapport de réponse à incident), il commencera ce qu'on appelle la phase d'« actions sur objectifs » : la compromission de vos derniers équipements critiques tels que vos serveurs de sauvegarde afin d'obtenir le contrôle définitif de votre système d'information et le chiffrement du parc. Son but est de maximiser sa couverture. Cette phase n'a rien de subtil : désinstallation des antivirus, changement des mots de passe des comptes administrateur de domaine, déploiement du rançongiciel par GPO (Group Policy Object, système permettant la gestion d'un environnement Active Directory) sont des exemples constatés sur le terrain.

3.2. Limites

La phase d'action sur objectifs s'effectue en quelques heures, souvent durant la nuit. Dans ces conditions, la vitesse de réaction est primordiale. Dans les faits, en admettant que le système soit supervisé en heures non ouvrées, si le SOC commence à détecter l'adversaire au début de la phase d'action sur objectif, il faudra probablement plusieurs heures avant d'avoir suffisamment de personnels, d'informations et de décideurs pour être en mesure de prendre des actions défensives. Si vous avez un doute, essayez dans le cadre de l'exercice à vos cellules de crises de faire revenir les personnels d'astreintes en les notifiant à 20h un vendredi soir de premier weekend de vacances pour s'assurer que les bouchons fassent partie de l'équation et lancez le compte à rebours. Ces longues minutes voire heures sont autant de temps utilisé par l'adversaire pour terminer de chiffrer le parc.

À l'heure actuelle, les actions de remédiations possibles généralement décrites et listées partout sont : la mise en quarantaine de fichiers, l'arrêt de processus, le blocage d'adresse IP, la déconnexion d'un équipement du réseau. C'est notamment l'un des arguments mis en avant par les éditeurs d'EDR. Ces actions peuvent être manuelles, semi-automatiques ou automatiques. Elles ont comme point commun d'être atomiques, donc par nature vont être limitées. Ce fonctionnement dépend ensuite de 2 choses. En premier, d'un niveau de détection et de doute suffisant pour engager une réaction. Ensuite, que l'EDR soit toujours actif sur le système. Ces agents sont généralement déployés avec les droits système. Rien de plus triste que de se faire désinstaller sur l'intégralité du parc par une GPO déployée par l'attaquant.

Dépendre de la seule capacité EDR pour défendre un système d'information revient à reproduire les raisonnements d'il y a 20 ans, avec des architectures conçues avec une unique couche de défense sur la base d'une protection périmétrique. Aussi pertinente soit-elle, une fois percée, cette défense devient inutile… « no silver bullet once again ».

Durant les premières heures d'une réponse à incident, on a généralement une vision assez floue de l'étendue de la compromission, des capacités de l'adversaire et des outils qu'il a employés. Ces points s'appliquent à l'avènement des EDR sur les parcs informatiques. Leurs capacités techniques permettent de faire un premier niveau de recherche forensique selon ce qui est fait en réponse à incident. Mais le même niveau de brouillard va subsister. Il est peu probable que le N2 d'astreinte ait les compétences et le temps disponible pour réaliser une première phase de rétro-ingénierie des logiciels malveillants identifiés ou des techniques utilisées. Il ou elle va se concentrer sur les condensats (tels que SHA256) qui auront été identifiés par les sandbox ou impliqués dans un arbre de processus suspect. Il pourra les mettre en quarantaine sur tout le parc. Si un autre RAT est toujours accessible et non détecté, ces actions n'auront ralenti l'adversaire que quelques minutes. Selon le même raisonnement, rien ne garantit que les équipements identifiés comme compromis soient les seuls. Si 15 terminaux identifiés comme compromis sont déconnectés du réseau par vos équipes et qu'un 16e subsiste, l'adversaire est averti sans (trop de) frais, sans avoir été stoppé. Il relancera sa progression depuis ce 16e terminal.

À cet endroit, il peut donc être utile de se détacher d'un raisonnement purement technique ne semblant pas comporter de réponse, pour revenir à l'échelon tactique.

3.3. Eléments d'initiative

3.3.1. L'hygiène SSI faible comme hypothèse de départ

Les « meilleures » victimes d'attaque par rançongiciel sont généralement celles ayant un SI dont l'hygiène est faible. C'est un constat régulier et répété depuis des années. Le guide d'hygiène de l'ANSSI [4] en est l'illustration. Pourtant son application est encore inégale.

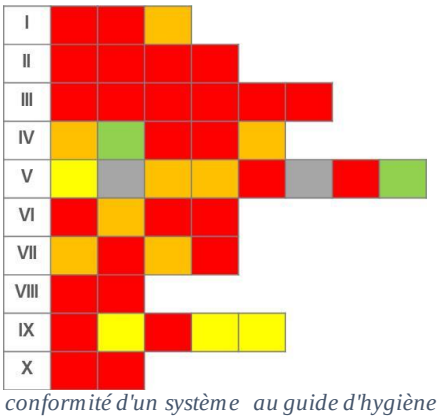

Figure 3 : exemple d'évaluation de la conformité d'un système au guide d'hygiène de l'ANSSI, avant son attaque par un rançongiciel

Certains systèmes sont peu défendables : les systèmes sans compartimentation entre les zones utilisateurs, serveurs et Active Directory ; les systèmes proposant un VPN avec (simple) authentification de comptes privilégiés ; les systèmes à plat, où les postes administrateurs ou serveurs internes sont adressables depuis n'importe où ; les systèmes sans hiérarchie ou gestion stricte des privilèges… De tels systèmes n'offrent que peu de profondeur défensive sur laquelle il est possible de capitaliser pour détecter et éventuellement absorber le choc d'une intrusion. Un adversaire franchissant le périmètre d'un tel système se retrouve sur un billard virtuel. La faille ZeroLogon [5] publiée en 2020 permettait de prendre les privilèges administrateur de domaine en quelques minutes après l'intrusion initiale. Cette faille est l'illustration et l'outil d'un tel scénario cauchemar.

Pour être capables de faire face à des attaques informatiques, ces systèmes doivent être refondus ou reconstruits. Cette démarche se heurte à plusieurs obstacles. En premier la dimension financière : cela peut représenter des coûts prohibitifs que ne peuvent se permettre certaines organisations, peu importe le risque. Ensuite, l'impact en production. Parfois les risques ou le mode dégradé temporaire qu'une telle évolution imposerait ne sont pas envisageables ou acceptés (le fameux : « ça marche, pourquoi on y toucherait ? »). Enfin, certaines équipes ne disposent pas des personnels au niveau de compétences adéquat : cela commence par la communication et la remontée d'information (« oui nous implémentons le modèle de niveau de Microsoft » - *spoiler alert*, ce n'est pas du tout le cas -) jusqu'à la phase technique : la définition d'une architecture (« nous ferons le dossier d'architecture une fois l'implémentation terminée, comme ça il sera à jour »), la planification (« ça ne sert à rien de faire un planning, de toute façon il sera faux ») et l'intégration du système.

On constate ces raisons sur le terrain de multiples façons :

- manque de moyens humains en nombre pour mener les chantiers
- difficulté d'avoir des spécialistes
- manque de priorisation de ses activités par le management
- peur d'impacter / limiter les métiers qui rapportent l'argent à la société
- manque de moyens financiers
- évolution des systèmes relativement lente (par rapport à la vitesse d'exploitation des failles par les adversaires) même pour ceux qui investissent
- …

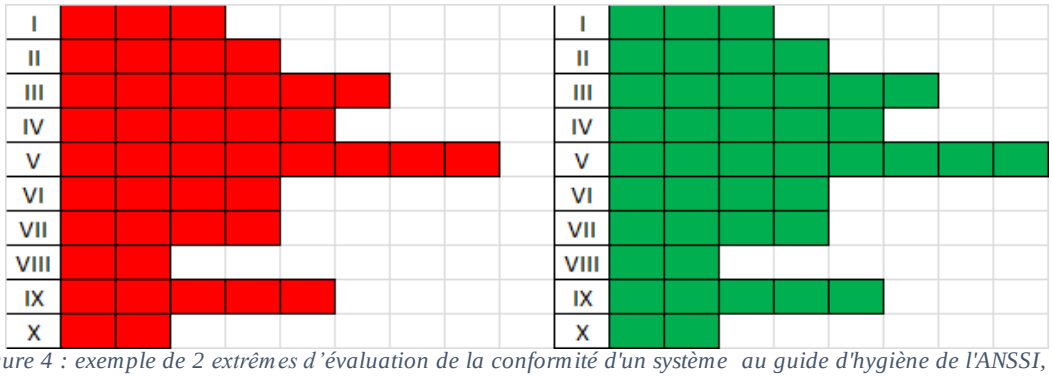

Figure 4 : exemple de 2 extrêmes d'évaluation de la conformité d'un système au guide d'hygiène de l'ANSSI,

Alors, bien évidemment, le système de gauche sera quasiment indéfendable et le système de droite se rapprochera du cas d'école souhaité. Mais gardons en tête que le guide de l'ANSSI est un guide pragmatique, qu'il est possible d'aller plus loin, mais que l'effort pour rendre intégralement vert (conforme aux recommandations) tout le SI n'est pas toujours possible (ou réellement souhaité) suivant les structures.

Si on accepte comme un état de fait que les niveaux d'hygiène de la plupart des SI resteront relativement faibles, il faut chercher ailleurs les réponses.

3.3.2. Perturber l'adversaire

Pourtant, face à ce constat et comme on l'a vu plus haut, les adversaires utilisant des rançongiciels ont généralement un mode opératoire simple basé sur la rapidité et un panel de compétences limité. C'est nécessaire pour eux afin d'avoir le meilleur rapport de rentabilité possible : il faut avoir à l'esprit le nombre de cibles qu'ils parallélisent, sachant que toutes ne vont pas générer un profit. Ils doivent garder les choses simples et efficaces.

Cela se traduit pour eux par une marge de manœuvre réduite et une séquence d'exécution s'embarrassant peu des détails. Ainsi, combien de parcs informatiques ont-ils été chiffrés, à l'exception des équipements qui n'étaient pas enregistrés dans le domaine Active Directory ? Ou de domaines épargnés car l'adversaire n'a pas eu le temps de suivre la relation d'approbation ? D'actions de reconnaissance incomplètes, ayant pour résultat des sections entières de parc qui n'ont pas eu de connexion psexec pour exécuter le rançongiciel ?

Que se passerait-il si un défenseur était en mesure d'introduire en temps réel ce genre de perturbations dans le schéma d'attaque d'un adversaire ? Vous aurez par exemple remarqué qu'étaient présentés supra deux vecteurs de communication distincts (VPN et RAT).

Perdant ses communications, sa capacité à latéraliser ou la visibilité de zones réseau complètes, un tel adversaire ne sera pas en mesure de réinventer son mode opératoire (passer par les frontaux web et remonter au « backend », sauter de VLAN, industrialiser une reconnaissance réseau active) en quelques heures. On cherche à gagner ces quelques heures, afin de permettre aux administrateurs d'arriver, et le déploiement de moyens de réponse à incident (forensic, rétro-ingénierie, renseignement) dans la foulée.

4. La stratégie du Bernard-l'hermite

Une clé de l'équation devient alors d'identifier en amont ces actions de freinage. Elles doivent être suffisamment décisives pour permettre de présenter à l'adversaire l'image d'un système apparemment gelé, tout en n'étant pas pénalisantes pour une reprise et en laissant une possibilité d'action de forensic.

En aéronautique, les systèmes d'aide au pilotage ont été développés depuis des dizaines d'années. Si le pilotage automatique, la capacité à se poser ou à ravitailler en vol de façon complètement autonome et automatique sont les aspects les plus marquants, ce sont les parties émergées d'un problème de grande complexité, où la notion de sûreté est primordiale.

Les systèmes d'assistance au pilotage sont conçus pour fonctionner selon deux niveaux de notification. Un premier niveau où le système calcule et prend les décisions de façon complètement autonome : la pompe principale d'alimentation d'un réacteur est défaillante ou est éteinte, la « standby

pump » est automatiquement activée. Cela n'impacte pas la sûreté du vol. Le sol est notifié, le problème sera réglé une fois l'appareil posé. Si un problème survient pouvant menacer la sûreté du vol, le pilote sera notifié. Certaines actions pourront être prises automatiquement par le système et notifiées au pilote, mais le pilote aura la décision sur la suite des actions.

Ce mode de fonctionnement dirigé par un très haut niveau d'exigence sur le plan de la fiabilité peut appuyer notre réflexion. On retrouve la notion de réaction autonome décidée par un agent (tel notre EDR interrompant un processus), sans contrôle instantané par l'opérateur mais avec une notification a posteriori (quelques millisecondes ou secondes plus tard) vers une console centrale. On trouve la notion de contrôle, permettant de garder l'humain dans le cycle de décision pour toutes les actions ayant un impact dimensionnant. Dans tous les cas, le facteur humain est pris en compte pour choisir la meilleure façon et le meilleur moment pour notifier l'opérateur afin d'éviter les erreurs sous facteur de stress.

Revenons au cas de notre adversaire sur le point d'interrompre le fonctionnement de votre organisation pour les 3 prochaines semaines. Au moment où l'analyste identifie de façon certaine la présence d'un adversaire actif, il peut prendre des mesures conservatoires : bloquer des comptes ou des groupes d'utilisateurs, désactiver des nœuds réseau, isoler des segments de système d'information, isoler les contrôleurs de domaine. Ces actions sont pénalisantes pour les deux parties. Ce sont néanmoins des actions de freinage qui peuvent fournir le temps nécessaire à revenir en heures ouvrées avec l'intégralité des personnels du défenseur présents sur le pont pour mener le combat.

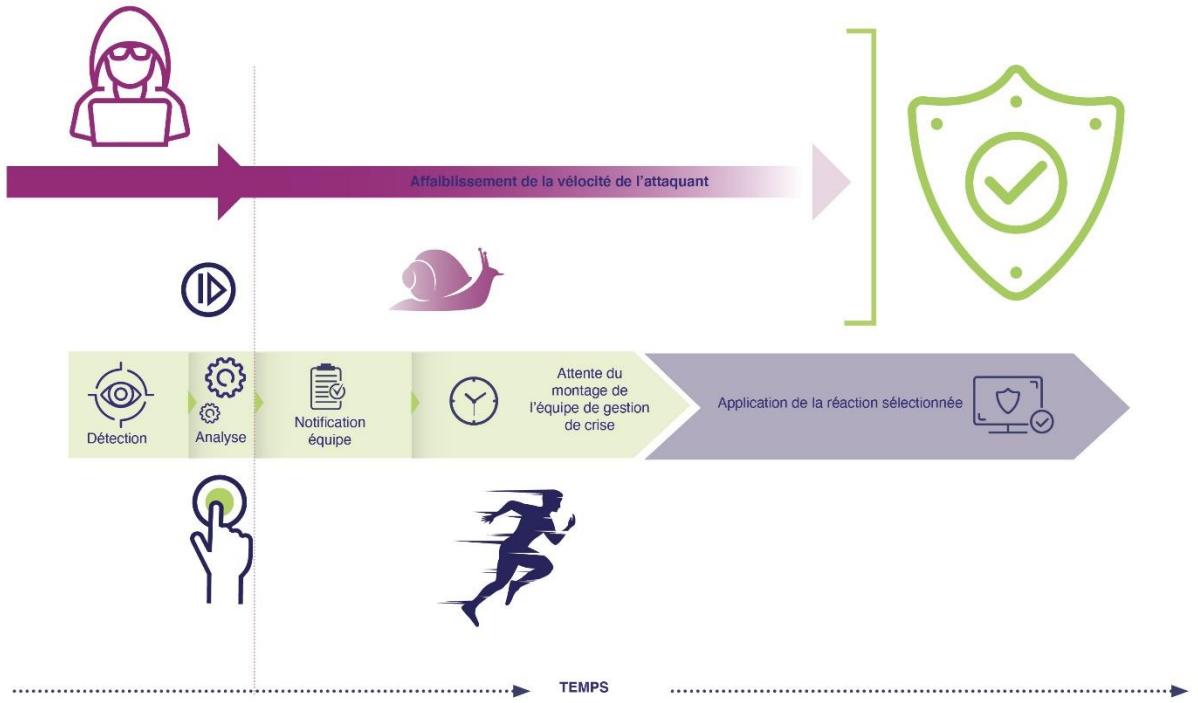

Figure 5 : Création d'une divergence temporelle suite à l'action de ralentissement

Ce stratagème a pour objectif de créer une sorte de divergence temporelle entre les deux acteurs. L'espace de l'attaquant est réduit suite à cette action de contre mesure et son temps se déroule virtuellement au ralenti, donnant le temps aux équipes du défenseur de reprendre la main.

Le système à défendre est toujours un ensemble mou, vulnérable et légèrement difforme. La proposition ici est de l'enfermer dans une coquille que l'on va clore en cas de danger. Le système à défendre est un bernard-l'hermite.

4.1. Préparation et planification

En premier, il est nécessaire de planifier le cadre d'utilisation : les actions ayant un impact sur le système, qu'il soit atomique ou dimensionnant, doivent être définies en amont. La liste de ce qui est faisable et le cadre de ce qui est faisable doit être préparé, pour réduire l'hésitation et le risque d'erreur une fois venu le moment de les utiliser. Par exemple, des checklists doivent être utilisées pour valider

que la décision est prise uniquement si tous les critères prévus sont présents. Certains critères peuvent aller jusqu'à prendre en compte l'absence de retour du commanditaire ou du métier au-delà d'une durée prévue. Au-delà, la préparation amont aura identifié que l'absence de réaction faute de retour du personnel responsable aura plus d'impact que la contre mesure définie.

Ensuite, ces actions doivent être automatisées. Le poids de la décision revient à une ou deux personnes vers 2h du matin, moins ils en ont à faire mieux ça sera (stress et fatigue amplifient le risque d'erreur [6][7][8]). À ce moment le temps de l'analyste est précieux : son travail est d'évaluer l'étendue de la compromission, de suivre les actions de l'adversaire, d'évaluer la phase à laquelle il se situe et de choisir l'action la plus adaptée pour le freiner ou le stopper puis d'informer au mieux le commanditaire de la situation pour qu'il prenne la décision ad hoc. Si la réaction est mal gérée ou étalée dans le temps, on s'expose au risque d'une réaction de l'adversaire.

Isoler des stations de travail, c'est prendre le risque de laisser accessible une station non identifiée à travers laquelle l'adversaire a toujours accès. Il a perdu quelques minutes mais son attaque continue, et il a gagné une information. Son mouvement suivant peut être de chercher à désinstaller les agents sur le parc. Ces préalables (l'appréciation de la situation et la décision d'action) sont la responsabilité de l'analyste ou du commanditaire. Pour que l'exécution de la décision se déroule normalement, il est nécessaire que les actions qui sont prises soient fiables et instantanées.

Ensuite, ces actions doivent être maîtrisées. Si en théorie le fait de se connecter à un équipement réseau pour l'éteindre ne semble pas présenter une grande complexité, seul à 3h du matin l'affaire est différente. Probablement même le temps économisé à ne pas rechercher les identifiants sera un gain salutairement utilisé pour affiner la compréhension de l'incident en cours et préserver la concentration de l'analyste. Des actions plus complexes telles qu'isoler des serveurs virtuels hébergés par un hyperviseur en déconnectant leurs *vswitchs* doivent impérativement être pré-paramétrées.

Tous ces éléments montrent que l'intégralité du raisonnement repose sur l'automatisation (ou du moins, semi automatique nécessitant l'approbation humaine avant de dérouler le plan) des actions à prendre, pour proposer aux personnels d'astreinte un choix parmi un panel d'options.

4.2. Paramètres

4.2.1. Application de ces mesures à des adversaires avancés

Le fait de couper les accès VPN ou d'éteindre des contrôleurs de domaine ne stoppera pas forcément un adversaire déterminé, notamment de niveau étatique. Si on pousse la réflexion dans cette direction, il est peu probable que ce genre de mesures fasse sens face à un adversaire de ce type, ce dernier ayant probablement déjà mis en place une autre méthode de persistance se passant de l'accès VPN.

Dans la plupart des cas, les adversaires de type APT ont tendance à s'infiltrer lentement au sein des systèmes d'information qu'ils visent. Ils peuvent faire appel à un panel d'outils et de compétences vaste et varié. De leur point de vue, un gel de quelques heures ou dizaines d'heures est insignifiant au regard des durées de compromission qu'ils peuvent rechercher.

Synthétiquement, on pourrait rencontrer 3 variantes :

- La première, l'adversaire est effectivement immobilisé et bouté hors du système
- La seconde, intermédiaire : une fois la phase de réponse à incident terminée l'adversaire a conservé un accès. Il reprend son attaque
- La dernière, scénario pire cas : il conserve un accès alors que le bernard-l'hermite est replié sur lui-même. Il décide de se « venger » ou de couvrir ses traces en sabotant le système.

4.2.2. Architecture sécurisée

Les exemples d'actions listés plus haut font appel à une multiplicité de connecteurs, avec un niveau d'accès privilégié. Cela crée une fonction de réponse orchestrée qui est une cible de choix pour l'adversaire, ou un vecteur de compromission catastrophique s'il est mal protégé. Sur ce plan, si ces réflexions vont à l'encontre de la lettre du référentiel PDIS (pas d'action depuis le SI du SOC sur le SI surveillé), on peut se référer à l'esprit de ces exigences pour implémenter une fonction SSI avec une architecture permettant une isolation adéquate. Il convient donc de protéger ces mécanismes avec le

même niveau que le reste du SI (rupture, ségrégation). Tout comme pour les accès externes VPN, une solution de type multi facteur (MFA) est recommandable pour s'assurer que l'ordre de confinement provienne exclusivement d'un utilisateur autorisé.

4.2.3. Coût de mise en place et d'utilisation

Toutes ces actions ont un coût. Leur utilisation va effectivement rendre tout ou partie d'un SI inexploitable pendant leur durée de mise en œuvre, voire peut-être pour certaines entraîner le besoin d'un ré-enclenchement. Il faut garder à l'esprit que le but n'est pas de créer plus de dégâts que l'adversaire, mais au contraire de protéger le SI le temps de pouvoir arriver à son chevet. En particulier, il pourra être utile de choisir l'autonomie de décision en fonction du coût pour l'infrastructure. Il faut ici rappeler aux amateurs du Chant du Loup qu'il n'est pas nécessaire d'avoir un deuxième sous-marin à disposition pour annuler l'ordre le cas échéant. On cherche des actions réversibles à coût raisonnable, afin d'inciter à l'initiative. Et cette annulation peut être décidée à tout moment. Le coût de l'erreur du défenseur doit être faible afin de favoriser sa prise de décision.

4.2.4. Acceptation des décideurs et des équipes techniques

Enfin, cela suppose une acceptation par les décideurs et les équipes techniques.

Pour les décideurs, le budget revêt souvent un critère prépondérant. Ils peuvent par exemple se demander si sur le cas des écoles publiques de Baltimore [9] combien ils auraient pu allouer à cette initiative pour éviter d'en arriver aux 8m$ évoqués. Les couts directs d'investigation et de remise en état étant déjà estimé à 1.2m$. Il est possible pour moins que les 1.2m d'investir dans quelques actions automatisées pour isoler ou ralentir la progression de l'attaquant.

Pour les équipes techniques, celles en charge de la sécurité sont la plupart du temps sponsors. Les équipes à convaincre sont les équipes métiers. Cette étape passe comme pour les décideurs par un processus de rapport gain / risque afin de prouver l'efficacité de la solution et identifier les lignes jaunes que les métiers ne voudront pas franchir dans un premier temps. L'argumentation budgétaire aura son sens ici, mais également l'impact d'indisponibilité qui peut être évitée ainsi que l'image de marque qui peut être sauvegardée suivant les métiers. En effet, les acteurs vendant des produits et services en ligne dans un monde concurrentiel, sont fortement sujets à perdre leurs clients en cas d'indisponibilité. Les mesures de confinement et ralentissement seront à identifier et à mettre en place avec les équipes métier.

Dans les deux cas, l'analyse de risque et les coûts des PCA / PRA (Plan de Continuité d'Activité / Plan de Reprise d'Activité) qui en résultent, sont autant d'arguments pour pousser dans cette démarche qui cherche finalement à faire des micros PCA/PRA au lieu de se lancer dans un plan qui couvre l'étendue de la société faute d'avoir réagi en amont.

5. Conclusion

Le but de cet article était de proposer des pistes de réflexions sur l'automatisation de mesures actives à opposer à un adversaire présentant une menace imminente pour la sécurité d'un système d'information en heures non ouvrées. L'idée est de compenser de façon temporaire l'absence de personnels en isolant le système ou des sous-systèmes critiques afin de les préserver.

Historiquement, notre SOC a eu comme objectif les menaces APT, et a été industrialisé en ce sens. Il est nécessaire d'évoluer pour suivre le développement des menaces à actions rapides, notamment les attaques par rançongiciel.

Des outils (comme la famille des EDR) existent pour cibler ces types de menaces et y apporter une réponse. L'histoire nous a montré plusieurs fois que malgré leurs efficacités, les nouvelles méthodes ou outils créés pour répondre à une nouvelle forme d'attaque finissaient par être contournées (ASLR, sandbox, UAC …). Il est donc utile de ne pas seulement considérer une réponse unitaire, et de garder à l'esprit les principes de défense en profondeur. Cela appelle une réponse système, afin d'éviter de reproduire les vieilles erreurs. Cela permet de gagner du temps, de limiter la casse éventuelle, et c'est utilisable contre d'autres profils d'attaques.

Ce raisonnement accepte comme donnée d'entrée qu'un nombre important de systèmes d'information ont un niveau d'hygiène faible. Le principe des mesures que nous proposons est que leur coût de mise en place est notamment beaucoup plus faible que le coût de reconstruction d'un SI, ou de sa mise à niveau technique.

Finalement, nous pouvons faire l'hypothèse que nombre de victimes d'attaque par rançongiciel auraient probablement préféré faire le choix d'une perte financière maîtrisée et planifiée en avance, plutôt que des coûts qu'ils (ou leur assurance) ont eu à supporter en conséquence.

6. Références

[1] Rapport Mandiant APT1 https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

[2] Rapport M-Trends 2021 https://content.fireeye.com/m-trends/rpt-m-trends-2021

[3] Bulletin de l'US CERT sur l'exploitation des vulnérabilités VPN https://us-cert.cisa.gov/ncas/alerts/aa20-133a

[4] Guide d'hygiène informatique de l'ANSSI https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/

[5] Article sur la faille Zerologon https://www.trendmicro.com/en_us/what-is/zerologon.html

[6] Article du Centre Canadien d'hygiène et de sécurité au travail https://www.cchst.ca/oshanswers/psychosocial/fatigue.html,

[7] Etude « Fatigue, Extended Work Hours, and Workplace Safety », Février 2017 [en anglais seulement]. Ministère du Travail de l'Alberta.

[8] Article Le stress, source d'erreur au travail ? (source sondage Indeed) https://www.preventica.com/actu-enbref-stress-source-erreur-travail-270819.php

[9] Tweet sur le cout d'une attaque d'un rançongiciel sur l'école publique de Baltimore https://twitter.com/AmySimpsonTV/status/1404887242292838412