

Le leurrage numérique comme complément de l'approche de cyber défense

Laurent Cordival, Fabien Thurot, Matthieu Riche, Antoine Ladune, Guillaume Meynet

Beijaflore, 11-13 Avenue du Recteur Poincaré, 75016 Paris, France
Lcordival073@beijaflore.com

Abstract.

Les entreprises développent de plus en plus leurs capacités de cyber défense pour répondre à l'accroissement des risques et menaces cyber.

Ces stratégies souvent basées sur le log management en vue de répondre aux besoins de détection et d'investigation bénéficient d'ajouts ponctuels de solutions spécialisées dites « best of breed » pour des périmètres spécifiques et potentiellement complexes. Cela tend à combler leurs faiblesses voire à adresser de nouvelles problématiques. Un premier exemple serait l'intégration du SIEM aux solutions d'orchestration appelé SOAR pour industrialiser voire automatiser les processus d'investigation ou de réponse à incident ou encore l'usage de l'EDR pour adresser les use-cases de détection techniques notamment au niveau du système et faciliter la réponse au niveau des endpoints.

Le log management n'en reste pas moins la pierre angulaire de la cyber défense de nombreuses entreprises. Cette approche présente des faiblesses dont notamment la quantité/qualité des logs, la scalabilité, la qualité de la stratégie de détection impactant notamment le pourcentage de faux positifs.

Toujours dans l'optique de renforcer voire de combler les lacunes de l'approche log management, le leurrage numérique appelé « deception tools » en anglais, peut être employé. Cette technologie qui consiste à placer des pièges ou leurres dans un Système d'Information permettrait notamment de renforcer la détection sur des cas de cyber attaques spécifiques, de faciliter la levée de doutes voire même pour les entreprises les plus matures, d'initier des processus de réponse à incident industrialisés.

Bien qu'apparu il y a plusieurs dizaines d'années sur les réseaux internet, le concept de leurrage numérique profite d'une offre en plein essor et fait l'objet ici d'une étude sur les bénéfices et les limites des différentes solutions du marché pour renforcer les capacités de détection et de réponse des entreprises actuelles.

Keywords : Leurre, Deception tools, Cyber sécurité, Big data, Right data, SOC, SIEM, Détection, Réponse, Threat Intelligence, Use cases, Vraisemblance, Interactivité.

1 Introduction

1.1 Développement de la cyber défense

Dans un contexte de cyber menace en perpétuelle évolution, la question n'est plus de savoir « Qui serait visé ? » mais bien « Quand est-ce qu'un incident se produira ? ». Il est donc essentiel de se doter de capacités de détection et de réponse adaptées aux cyber menaces toujours plus ciblées, et expertes.

Pour se faire, les entreprises ont développé leurs capacités de cyber défense sur les thématiques de détection et de réponse à incident au travers de solutions et d'outils dont notamment le SIEM, des best of breed (IDS, AV, WAF, etc.), du SOAR (Security Orchestration, Automation, and Response), de l'EDR (Endpoint Detection and Response) ou encore *via* les fonctionnalités offertes par les autres solutions ou environnements IT sur le périmètre. Concernant les équipes, les entreprises se sont dotées d'équipes de SOC interne ou externe auprès de MSSP, et de CSIRT pour renforcer les équipes IT et Sécurité dans la gestion des incidents cyber.

1.2 Le log management une pierre angulaire non sans défaut

Le log management reste souvent l'approche de détection centrale mais aussi la plus répandue et utilisée parmi les entreprises pour répondre aux enjeux de cyber défense et ceci non sans raison.

L'avantage de l'approche détection via log management

Cette approche présente plusieurs atouts majeurs :

- Aide à répondre à des obligations légales.
- Permet l'investigation et la rétention de données voire de preuves.
- S'appuie sur une approche de traitement des risques et scénarios redoutés traduite en stratégie de détection ou scénario de détection.
- Profite d'un marché mature (des acteurs reconnus, des solutions maîtrisées, etc.)
- Reste une approche connue, maîtrisée et éprouvée.

Les limites de l'approche

Cependant, cette approche présente certaines faiblesses qui pour ne citer que les plus importantes sont les suivantes :

- Grand nombre de faux positifs – très dépendant de la stratégie de détection (Notamment avec l'usage aujourd'hui plus fréquent de machine learning ajoutant en complexité et en volume d'alertes).
- Scalabilité – notamment due à la complexification du Système d'information et à l'augmentation de la surface d'attaque.
- Qualité/pertinence des logs récupérables sur le Système d'Information – qui en impacte la qualité de la stratégie de détection.

- Analyse ou levée de doute souvent nécessaires et donc vitesse de réponse dépendante de la maturité SOC/CSIRT (heure ouvrée, droit de réponse sur le scope, facilité de levée de doute, etc.).

2 Le Leurrage numérique comme complément des approches standards de centralisation de log

2.1 Introduction au leurrage numérique

Le leurrage numérique, une approche ancienne remise au goût du jour et profitant d'une offre cyber au plein essor propose le déploiement de pièges actifs sur un système d'information qui ont pour but de :

- Faire perdre du temps à l'attaquant voire même le dissuader.
- Détecter des comportements anormaux et donc de potentielles attaques cyber.
- Fournir aux équipes de sécurité des moyens d'approfondir leurs connaissances des techniques et tactiques utilisées dans le cadre de la sécurité offensive.

Le leurrage numérique peut prendre différentes formes, dont nous détaillerons les utilités et usages plus tard. Cela peut se traduire par :

- Une machine leurre se faisant passer pour un ordinateur ou un serveur. Son but étant d'inciter un attaquant à interagir avec elle afin de créer une alerte.
- Un leurre placé sur un système légitime pouvant être :
 - o Un identifiant factice dans l'AD.
 - o Un fichier en clair où sont stockées des informations paraissant confidentielles (mot de passe, instructions, etc.).

Ces leurres spécifiques sont aussi appelés miette de pain, ou *breadcrumb* en Anglais.

- Un appât, un objet leurre placé sur un hôte légitime. Son objectif est de déclencher une alerte si l'on interagit avec lui, en l'ouvrant ou en le modifiant.

Le leurrage numérique peut se déployer sous différentes formes :

- En amont du Système d'Information protégé.
- Fusionné (déployé en parallèle) au Système d'Information.
- Isolé du Système d'Information.
- Intégré directement dans le Système d'Information.

Les technologies de leurrage propriétaire actuelles sont prévues pour être déployées en amont ou fusionnées avec le Système d'Information. Ces dernières proposent des fonctionnalités pour faciliter le déploiement et l'intégration au SI dont notamment :

1. Capacité d'analyser le système d'information, soit en le scannant, soit grâce aux données d'une CMDB.

Suite à l'analyse, capacité d'établir des recommandations de déploiement notamment sur les points suivants : type d'hôte, emplacement, adresse MAC, OS ou encore nom de l'hôte. L'opérateur recevant les recommandations aura la possibilité de les accepter telles quelles ou de les adapter en fonction de ses besoins.

2. Création des leurres à la volée et intégration dans le SI sous forme de machines virtuelles potentiellement complétée par l'installation d'un agent dédié au leurrage ou lié à une suite de solution de sécurité endpoint sur le périmètre pour le déploiement des breadcrumbs.
3. Capacité à s'interfacer avec d'autres solutions du SI de tout type : Pare-feu, EDR, SIEM, SOAR, etc.

Cette intégration peut être un atout majeur pour l'entreprise en permettant une industrialisation/automatisation de la détection et de la réponse.

Les principaux usages, fonctions de la maturité du SI de l'entreprise, dont nous détaillerons ensuite les caractéristiques sont :

- La tromperie ou la désinformation de l'attaquant.
- La détection avancée via le déploiement de piège sur le Système d'Information.
- La réponse avancée au travers de la facilitation de la levée de doute voire l'automatisation de la réponse après détection mise à avant par les pièges déployés.
- Le gain d'information sur les techniques et tactiques des attaquants (« Threat Intelligence ») à destination de la Blue team.

2.2 Les différents usages du leurrage numérique

Tromperie ou désinformation de l'attaquant

Introduction

Le leurrage numérique apporte la capacité de tromper ou de désinformer l'attaquant. Cette capacité est rendue possible au travers du positionnement du leurrage. Plusieurs possibilités existent.

1. La première et la plus simple est de positionner le leurrage entre l'attaquant et la cible, il lui est possible de modifier ou de compléter l'information qui transite. Typiquement, les équipements réseaux comme les IPS, les WAF ou encore les NGFW peuvent être utilisés en ce sens pour protéger de multiples systèmes d'un réseau.
2. La deuxième possibilité serait d'utiliser un agent sur les postes cibles qui en plus de pouvoir répondre à des requêtes distantes pourraient ainsi rediriger ou répondre à des requêtes locales voire déposer sur le système de fausses informations telles que des comptes ou des fichiers. Cette technique s'avère particulièrement efficace pour contrer la phase de reconnaissance en faisant perdre du temps à l'attaquant via la complexification de l'information à analyser pour arriver à ses fins. Aussi, elle peut être utilisée pour attirer l'attaquant vers un leurre de détection déployé voire vers un environnement de sandboxing pour faciliter l'analyse de l'attaque et l'identification d'IOC. Attention toutefois à ce que le leurrage implémenté n'impacte pas des services légitimes de cartographie par exemple.

Bénéfices vis-à-vis du log management

Là où le management de log œuvre pour détecter un attaquant, la désinformation quant à elle est une approche qui entre dans le cadre de la prévention et change l'approche cyber standard.

Cette dernière complète la détection du log management vis-à-vis des cyber acteurs de niveau faible à moyen en les décourageant ou en les poussant à l'erreur via la désinformation, ou encore vis-à-vis des cyber acteurs d'un niveau supérieur et déterminé en leur faisant perdre du temps ou en les poussant à la faute pour les détecter.

Détection avancée

Introduction

La détection au travers des leurres déployés sur le Système d'Information est rendue possible grâce au fait qu'aucun accès n'est supposé avoir lieu sur ces éléments du SI. Cette méthode de détection permet de mettre en évidence à la fois les menaces externes et les menaces internes.

Cette méthode à l'initialisation nécessite de répertorier les services et usages du SI qui de manière globale et légitime pourraient accéder aux leurres tels que les outils de scan du SI, les scripts globaux, les outils d'inventaires, etc. Une bonne configuration d'une solution de leurrage doit permettre à cette dernière de ne remonter aucune alerte autre qu'une alerte légitime et avérée.

Les leurres peuvent être déployés à différents niveaux sur le Système d'Information en fonction de la stratégie de détection souhaitée. Ils peuvent faire l'objet d'un déploiement d'équipements physiques ou virtuels. Ces derniers peuvent être déployés en cœur de réseau avec possibilité de déployer des équipements au plus proche des sites voire même des agents sur les postes/serveurs. Ce déploiement permet la mise en place de pièges à plusieurs niveaux :

- Réseaux, avec la création de sous-réseaux entiers dédiés à désinformer un attaquant et à relever des alertes en cas d'accès à ces environnements.
- Systèmes – création de systèmes fictifs au plus proche du SI véritable.
- Breadcrumbs/appâts – ajout de données d'intérêts ou d'appâts pour les attaquants sur les environnements fictifs ou véritables.

Exemple de détection d'une attaque ransomware en utilisant le leurrage numérique :

- Étape 1 : Accession à un service de leurre serveur de fichier via les techniques Mitre ATT&CK : « Découverte de systèmes distants » (T1018)¹, « Exploitation d'une vulnérabilité distante » (T1210)² qui peuvent être repérées via l'accès à des réseaux, des systèmes ou des services fictifs.

¹ Découverte de systèmes distants : <https://attack.mitre.org/techniques/T1018/>

² Exploitation d'une vulnérabilité distante : <https://attack.mitre.org/techniques/T1210/>

- Étape 2 : Changement d'intégrité d'un fichier leurre à travers son chiffrement via une technique Mitre ATT&CK « Données chiffrées pour l'impact » (T1486)³ qui peut être repérée via la modification d'un appât.

Bénéfices vis-à-vis du log management

La détection de certaines tactiques du Mitre ATT&CK via le leurrage numérique peut être tout aussi, voire plus efficace, que la détection via le log management. Cela comprend notamment les tactiques suivantes :

- La reconnaissance.
- L'accès aux identifiants de connexion.
- Les mouvements latéraux.
- La collecte et l'impact sur la donnée.

Les actions de reconnaissance, telles que des scans, peuvent être détectées grâce au leurrage numérique. Un leurre implémenté dans un sous-réseau peut détecter un scan de reconnaissance lancé par un attaquant. Cela permet des détections plus précises que ce que peut faire un SIEM à travers les logs firewall, car la moindre erreur de l'attaquant sera détectée. En effet, les seuils de ces scénarios de détection SIEM doivent être suffisamment élevés pour limiter le bruit (les faux positifs), ce qui peut permettre à un attaquant discret de ne pas être détecté. En revanche, pour les leurres numériques et pour les SIEM, ce type de scénario nécessite en prérequis une bonne cartographie de son réseau, afin de pouvoir retrouver l'appareil associé à l'IP à l'origine de l'alerte et ainsi faciliter l'investigation.

Dans sa démarche de reconnaissance, l'attaquant va essayer d'obtenir des identifiants de connexion lui permettant d'accéder à des systèmes de haute importance. Le leurrage numérique peut faciliter la détection de telles activités *via* la création de faux comptes dans l'Active Directory en catégorisant toute interaction avec ces comptes comme malveillante. Cela est particulièrement efficace pour détecter des attaques type brute-force, notamment le password spraying. Ce type scénarios de détection pour les SIEM est difficile à régler, car il faut faire un compromis entre le bruit dû aux faux-positifs et la sensibilité de l'alerte. Le leurrage numérique peut également permettre de détecter des techniques plus avancées de type « pass-the-hash » ou « pass-the-ticket » via le déploiement de breadcrumbs, qui sont difficiles à détecter via un SIEM. Les SIEM restent cependant efficaces pour d'autres détection comme les attaques via keberoasting en s'intéressant à l'algorithme de chiffrement négocié.

En complément, des leurres liés à ces comptes AD factices peuvent être positionnés sous la forme de *breadcrumbs* sur un hôte légitime à un endroit potentiellement ciblé par des techniques connues. Par exemple, il est possible de déployer un identifiant dans un navigateur web ou un identifiant non sécurisé dans un fichier utilisateur. Ainsi, un attaquant ayant trouvé l'identifiant de connexion factice sur une machine compromise sera détecté s'il essaie de s'en servir pour se connecter à un service légitime.

³ Données chiffrées pour l'impact : <https://attack.mitre.org/techniques/T1486/>

La détection de mouvements latéraux peut être efficace en utilisant le leurrage numérique. En effet, toutes les utilisations de techniques de prise en main à distance (RDP, SSH, etc.) sur une machine leurre ou un compte factice seront détectées. De plus, il est possible que les identifiants de connexion obtenus précédemment par l'attaquant soient supposés authentiques par ce dernier. La connexion à distance à n'importe quelle instance en utilisant ces identifiants factices créera alors une alerte. La phase de latéralisation de l'attaque en sera complexifiée. C'est un complément efficace à l'approche de détection par le log management, qui ne peut que difficilement différencier les actions légitimes administrateurs des actions d'un attaquant réalisées grâce à un compte compromis.

Le leurrage peut aussi être un atout majeur concernant la détection de la collecte et l'impact sur des données via l'utilisation d'appâts, que nous avons présenté précédemment. Ces appâts, attirants pour un attaquant, devraient être placés à des endroits stratégiques et si possible peu fréquentés sur des hôtes légitimes. Voici quelques cas d'utilisation :

- Positionnement d'un fichier leurre nommé « Résultats 2020.pptx » sur un serveur d'échange de fichiers seulement accessible aux membres du COMEX. Dans ce cas, la population ayant accès au leurre est limitée. Il est aussi possible de sensibiliser la population voire de la mettre au courant pour assurer la qualité des remontées d'alertes.
- Positionnement d'un script « database import » sur un serveur frontal, par exemple un serveur web. Ce cas est différent du précédent mais peut être amélioré de la même façon.

Au regard de ces différents exemples, les deception tools apportent à l'approche cyber défense une plus-value pour la détection via les points suivants :

- Une réduction du volume de données nécessaires au monitoring est possible, car il y a besoin de peu de pièges pour couvrir un périmètre large (par exemple pour la détection d'actions de reconnaissance). Cette réduction du volume de données permet une diminution des coûts et une amélioration de la performance des outils type SIEM.
- Une amélioration de la pertinence des alertes à travers une réduction du bruit dû aux faux-positifs. Cela permet de réduire la charge des équipes responsables de l'analyse et de la réponse et d'augmenter le niveau de confiance dans les outils de détection. Il faut néanmoins veiller à ne pas créer de zone morte dans la détection sur le SI, que ce soit en terme de périmètre ou de scénario d'attaque non couverts.
- Un déploiement beaucoup plus rapide, car moins complexe à mettre en place qu'un système de scénario de détection dans un SIEM. Les phases de design et de tuning sont notamment grandement réduites.

Le log management reste néanmoins nécessaire pour compléter le leurrage numérique, notamment sur les points suivants :

- Avoir davantage de contexte sur les alertes remontées.
- Détecter des comportements indétectables via les outils de leurrage.
- Collecter les données nécessaires aux opérations de forensique.

Réponse avancée

Introduction

Une fois les capacités de détection déployées, les entreprises peuvent s'appuyer sur ces éléments de détection pour deux choses :

- Le renforcement et la facilitation de l'investigation ou de la levée de doute suite à une alerte.
- Le déclenchement de réponses automatiques : la mise en quarantaine de l'attaquant, le bannissement de son IP ou encore l'arrêt d'une portion du réseau. Cette automatisation de la réponse devrait être limitée aux scénarios simples et maîtrisés dans un premier temps.

Concernant la facilitation de l'investigation, l'approche est d'utiliser les informations et alertes remontées par la solution de leurrage avec d'autres informations disponibles (technique ou humaine) pour faciliter la compréhension de la situation ainsi que la levée de doutes lors de l'investigation.

La réponse automatique est quant à elle possible uniquement si un effort a été produit pour interfacier directement, ou indirectement (via solution d'orchestration en interface), la technologie de leurrage avec des technologies de « prévention » sur le Système d'Information. Cet interfaçage se ferait alors avec par exemple des pare-feux ou un EDR pour permettre le confinement d'un poste ou d'un réseau suite à la levée d'une alerte.

Exemple de réponse lors de la détection à une attaque ransomware en utilisant le leurrage numérique :

Suite à la détection des techniques suivantes : « Découverte de systèmes distants », « Exploitation d'une vulnérabilité distante » et l'accès à un fichier de leurrage, lancement d'un processus de confinement du système à l'origine des alertes via interface entre la solution de leurrage et de l'EDR.

Bénéfice vis-à-vis du log management

Les solutions de déception étant développées en vue de limiter le nombre de faux positifs, la moindre alerte d'un leurre augmente significativement la vraisemblance de toute autre alerte qui lui serait liée (source, destination, poste ou compte utilisés, etc).

Cela permet notamment de prendre de meilleures décisions, potentiellement plus rapidement, en vue de définir la posture à adopter pour répondre à l'incident. Pour des cas très spécifiques une première action de confinement pourrait être lancée automatiquement grâce à cette vraisemblance que présentent les alertes de solution de leurrage.

Ces aspects peuvent se voir renforcés en cas d'interfaçage entre la technologie de leurrage et un SIEM voire un SOAR pour les entreprises les plus matures sur le sujet.

Threat Intelligence

Introduction

Le déploiement de leurres est aussi envisageable pour permettre la récolte d'information pour mieux comprendre le déroulement d'une attaque, l'évolution des tactiques et des techniques offensives en vue de renforcer les capacités de cyber défense.

Cette solution rentre dans le cadre de la recherche et de l'innovation et doit être réservée aux entreprises matures et qui voudraient renforcer la performance de leurs services ou de leurs produits (plutôt des vendeurs de solution, des entreprises de service sécurité, MSSP, etc.).

Pour cet usage, un déploiement isolé du système d'information est préconisé pour :

- Disposer d'un environnement pour interagir librement avec l'attaquant et potentiellement le pousser à s'adapter et à se découvrir.
- Ne pas être contraint par une volonté de réduire le risque encouru sur la production ou sur le business et ainsi disposer de temps pour analyser.

Exemple de récupération d'IOCs via le déploiement d'un système d'information leurre :

- Étape 1 : Déploiement du bac à sable (système d'information leurre) isolé.
- Étape 2 : Maintien de la plateforme en condition opérationnelle et attente d'une attaque/analyse. Ou utilisation d'un payload récupéré au préalable dans un autre contexte.
- Étape 3 : Détection d'activités anormales sur la plateforme (communication interne non souhaitée, écriture sur disque, utilisation des ressources accrues, etc.). Ce point est facilité lorsque l'initialisation de la compromission est volontaire ou lorsque l'environnement est parfaitement maîtrisé car prévu à cet effet.
- Étape 4 : Analyse et suivi de l'attaque pour identifier *a minima* les points suivants :
 - o Timeline de l'attaque.
 - o Techniques et tactiques utilisées.
 - o Payloads, outils, fichiers tiers déposés.
 - o Domaines, URL, IP de livraison, de téléchargement, de communication utilisées dans le cadre de l'attaque.

- Étape 5 : Partage des IOCs à la communauté Cyber ou via son service de Threat Intelligence. Renforcement des capacités des solutions de détection via base de connaissances (Antivirus, IPS, etc.).
- Étape 6 : Utilisation de tout ou partie des IOCs récupérés pour initier une campagne de threat hunting sur son périmètre plateforme de leurre.

Bénéfice vis-à-vis du log management

Il est essentiel pour toute défense de connaître son adversaire. Cette approche le permet en fournissant un environnement se prêtant à la compréhension des tactiques et techniques de sécurité offensive.

Les principaux apports sont :

- La compréhension de l'évolution des tactiques et techniques permettant d'adapter sa cyber défense, ou encore de former sa blue team aux nouveautés.
- L'identification d'indices de compromission permettant de renforcer la détection des solutions utilisant des bases de connaissances ou d'être utilisé comme entrée ou comme hypothèse pour initier une campagne de threat hunting.

L'identification de « 0 day » bien que possible reste néanmoins peu probable car les entités ayant ce genre de capacités offensives en limite l'utilisation à des cibles très spécifiques et maîtrisées.

2.3 Limites du leurrage numérique

Outre les avantages qu'apporte le leurrage numérique à la cyber défense listés ci-dessus, cette approche présente néanmoins de réelles limites qu'il est nécessaire de comprendre pour l'utiliser :

- MCO/MCS/maintien en condition opérationnel, de sécurité, et de la furtivité de la solution développée.
- Augmentation de la surface d'attaque via l'ajout d'une nouvelle technologie voire d'un nouveau fournisseur de service sur le périmètre.
- Dépendante des solutions sur le périmètre pour agir dans le cadre de la réponse à incident de sécurité.
- Pour une solution développée en interne - Très dépendante de l'expertise cyber et informatique de l'entreprise.
- Pour une solution propriétaire - Le coût de la solution et du support voire du service tiers opérant la solution.

3 Conclusion

Le leurrage numérique peut être employé pour renforcer les capacités de cyber défense.

En fonction des besoins et de la stratégie de l'entreprise, les fonctionnalités suivantes pourront être déployées :

- Désinformation de l'attaquant.
- Détection via déploiement de leurres.
- Réponse industrialisée/automatisée suite à l'alerte remontée par la détection.
- Threat intelligence.

Les TPE et PME souffrent actuellement d'un sous-investissement en matière de cyber défense. Si un effort est réalisé sur la prévention, la réalité est tout autre sur la détection et la réponse aux incidents de sécurité. Ces entreprises pouvant être interconnectées à des grands comptes, leur maturité présente un enjeu auquel le leurrage numérique peut apporter un élément de réponse.

Au final, afin de renforcer l'usage du leurrage numérique en France et faciliter l'encadrement des risques fonctionnels, juridiques et techniques de ce type de solution, il serait utile d'intégrer ce type de solution dans la réglementation assurant la protection des infrastructures critiques (ex : Loi de programmation militaire, référentiel PDIS).

References

1. John Breeden II: How 4 deception tools deliver truer network security". CSO, Release Date: June 2017.
2. Zimmerman, C,: Ten Strategies of a World-Class Cybersecurity Operations Center, In: The MITRE Corporation (2014).
3. Deborah L. Schuh: THE CYBERSPACE ADVANTAGE: INVITING THEM IN! How Cyber Deception Enables Better Resilience, In: The MITRE Corporation (2019).