DOSSIER

L'OSINT au service de la Cyber Threat Intelligence

serenety
by xmco

Sommaire

Avant-propos.

L'EXPLOSION DES DONNÉES ET LA MULTIPLICITÉ DES CANAUX DISPONIBLES SUR INTERNET RENDENT INDISPENSABLE LA CONNAISSANCE DE VOTRE EXPOSITION SUR INTERNET.

Le renseignement est donc primordial dans l'anticipation des menaces et des planifications d'attaques.

La Cyber Threat Intelligence s'appuie sur une multitude d'informations pour déterminer si une menace est avérée et quelles sont les mesures à prendre. L'analyse est un des fondements de la Cyber Threat Intelligence, elle nous permet de traiter une grande quantité de données et de mettre en lumière les tendances d'attaques ainsi que ses attaquants.

Pour nous aider, nous utilisons le renseignement en source ouverte (l'OSINT) pour collecter les informations. Nous vous présentons dans ces quelques pages ce qu'est l'OSINT et en quoi elle peut servir vos intérêts dans une démarche globale de Cyber Threat Intelligence.

1. Méthode OSINT : mieux maîtriser son environnement et son exposition

LA CYBERSÉCURITÉ EST UNE THÉMATIQUE DE PLUS EN PLUS PRÉSENTE DANS NOS VIES QUOTIDIENNES. QU'IL S'AGISSE DES PROBLÉMATIQUES DE RANSOMWARES OU DE « BIG GAME HUNTING » (BGH) AUXQUELLES SONT CONFRONTÉES LES ENTREPRISES OU DE LA PROTECTION CONTRE LES CAMPAGNES DE PHISHING ET AUTRE INGÉNIERIE SOCIALE AUXQUELLES SONT CONFRONTÉS LES PARTICULIERS, IL EST NÉCESSAIRE POUR TOUT UN CHACUN D'ÊTRE CONSCIENT DE LA MENACE ET D'ÊTRE VIGILANT AFIN D'ÉVITER DE TOMBER DANS LES PIÈGES QUI SE PRÉSENTENT À NOUS.

Afin de connaitre son niveau d'exposition, et donc d'être en mesure d'anticiper les menaces, il convient d'identifier les informations qui nous sont liées et disponibles publiquement sur Internet (ou toutes autres sources d'information ouverte). Cela est aussi bien valable pour les personnes physiques que morales.

Cette démarche consistant à aller chercher des informations (appelées renseignement une fois qu'elles sont qualifiées et contextualisées) au sein de sources accessibles publiquement est connue sous les appellations de ROSO (Renseignement d'Origine Source Ouverte), ou pour les anglophones, d'OSINT (Open Source Intelligence).

OSINT : une méthode de recherche adaptée à de nombreux besoins

Initialement utilisée par les services de renseignements, cette technique d'investigation s'est popularisée avec l'avènement de la sécurité informatique. Elle tend désormais à être utilisée par les entreprises pour répondre à des objectifs stratégiques et économiques.

Cette méthode est également utilisée par de nombreux professionnels de la cybersécurité ou par des internautes moins scrupuleux, qui l'utilisent lors de la phase de reconnaissance de leur cible, avant la réalisation de leurs attaques (techniques ou de social engineering).

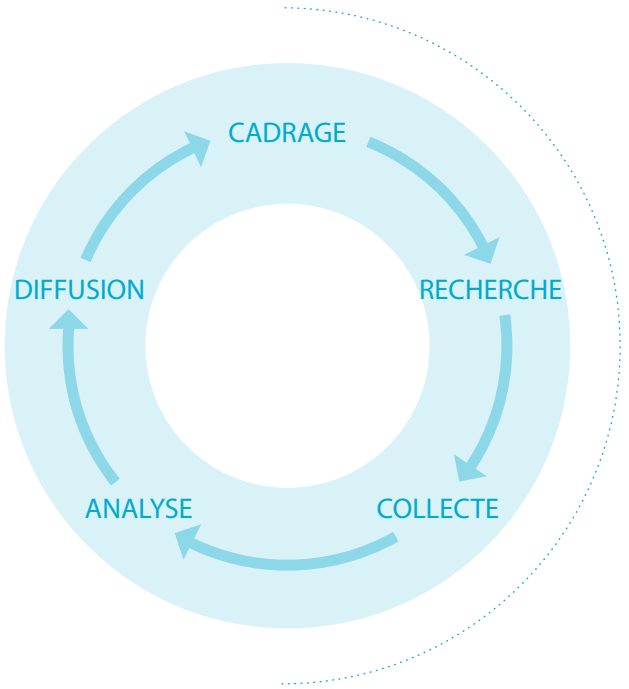
Le renseignement en sources ouvertes se définit notamment par le recueil et l'analyse des informations obtenues à partir de sources d'informations publiques. Il est principalement utilisé dans le cadre d'activités liées à la sécurité nationale, la recherche journalistique et l'intelligence économique.

Cette pratique d'investigation se base sur la recherche, la collecte et l'analyse d'informations disponibles en accès libre. L'accès à ces données n'étant pas classifié, leur acquisition est parfaitement légale et n'est pas assimilable à un vol.

Son intérêt majeur repose dans le faible niveau d'interaction avec les entités faisant l'objet de l'investigation, puisque l'analyste adopte le même comportement qu'un utilisateur légitime.

À noter, le renseignement d'origine sources ouvertes est différent de la simple recherche car il applique le processus associé au cycle du renseignement dans un but de recherche d'informations. Il a donc pour but de répondre à des besoins spécifiques ou d'accompagner la prise de décision, et non l'acquisition de connaissances.

La collecte d'information dans ce cadre n'est donc pas une finalité en soi. Les phases de collecte et d'analyse d'une démarche de type OSINT doivent répondre à une question préliminaire, et doivent donner lieu à une diffusion des résultats vers les bons interlocuteurs. Enfin, cette diffusion doit prendre en compte les besoins associés aux rôles et aux responsabilités des personnes à qui le renseignement est destiné.



L'utilisation de l'OSINT

Au-delà de son utilisation dans le domaine de l'intelligence économique, ce type de méthodologie d'investigation peut également être adaptée à d'autres cas d'usage pour répondre à d'autres besoins tout aussi importants pour les entreprises.

Ainsi dans le domaine de la cybersécurité, l'OSINT est régulièrement utilisée dans le cadre d'activités telles que la Veille Stratégique, la Sureté, ou encore de Cyber Threat Intelligence (CTI). À titre d'exemple, l'OSINT est également utilisée dans un cadre professionnel par les pentesteurs lors de la réalisation de certains types d'audit, ou par les « bounty hunters », des chercheurs en sécurité participant aux programmes de Bug Bounty.

L'OSINT peut aussi être utilisé pour identifier d'éventuelles fuites de données au travers de recherches via des moteurs de recherche type Google, d'investigations sur des sites de partage de documents ou encore sur le Dark Web.

Au-delà de la recherche en elle-même, la technique OSINT permet d'adresser des cas concrets, qui pourront répondre à des besoins spécifiques en fonction d'interlocuteurs ciblés.

L'IDENTIFICATION DES SOURCES : UNE ÉTAPE PRIMORDIALE POUR COLLECTER L'INFORMATION SOUHAITÉE

Il n'existe malheureusement pas de référentiel unique de sources pertinentes à interroger pour obtenir une information et générer du renseignement. La pertinence de ces sources dépend grandement du problème initial pour lequel cette démarche a été mise en place et de sa finalité.

Généralement, lorsque l'on parle de « sources ouvertes » on peut penser aux éléments suivants :

- [Les médias] : les journaux papier, les magazines, les radios, les chaînes de télévision accessibles dans les différents pays que l'on souhaite couvrir
- [Internet] : les publications en ligne, les blogs, les groupes de discussion, les médias citoyens, YouTube et autres réseaux sociaux
- [Les données instututionnelles] : les rapports, les budgets, les auditions, les annuaires, les conférences de presse, les sites web officiels ou encore les discours
- [Les publications professionnelles et acédémiques] : les revues académiques, les conférences, les publications et autres thèses
- [Les données propriétaires] : l'imagerie satellite, les évaluations financières et industrielles ou encore les bases de données en tout genre
- [La littérature grise] : les rapports techniques, les prépublications, les brevets, les documents de travail, les documents commerciaux, les travaux non publiés ou encore les lettres d'information

Les sources exploitées sont donc nombreuses et variées, puisque toutes les sources, de par leur nature, peuvent entrer dans le périmètre d'une démarche OSINT.

Cette démarche s'appuie également sur d'autres types de sources ou méthodes de collecte de renseignements. Dans un document de référence intitulé « NATO Open Source Intelligence Handbook » présentant la méthodologie OSINT, l'OTAN établit les liens suivants entre l'OSINT et les approches plus spécifiques telles que l'HUMINT » (renseignement d'origine humaine), le SIGINT (renseignement d'origine électromagnétique), ou encore l'IMINT (renseignement d'origine image).

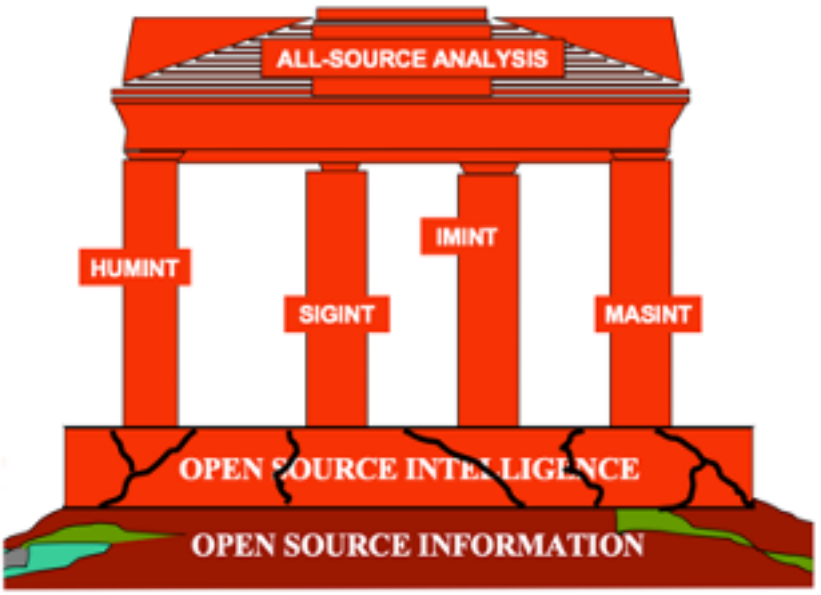


Figure 17 - Open Source - All-Source relationship

TROUVER LES BONS OUTILS EN FONCTION DE SES BESOINS DE RECHERCHE

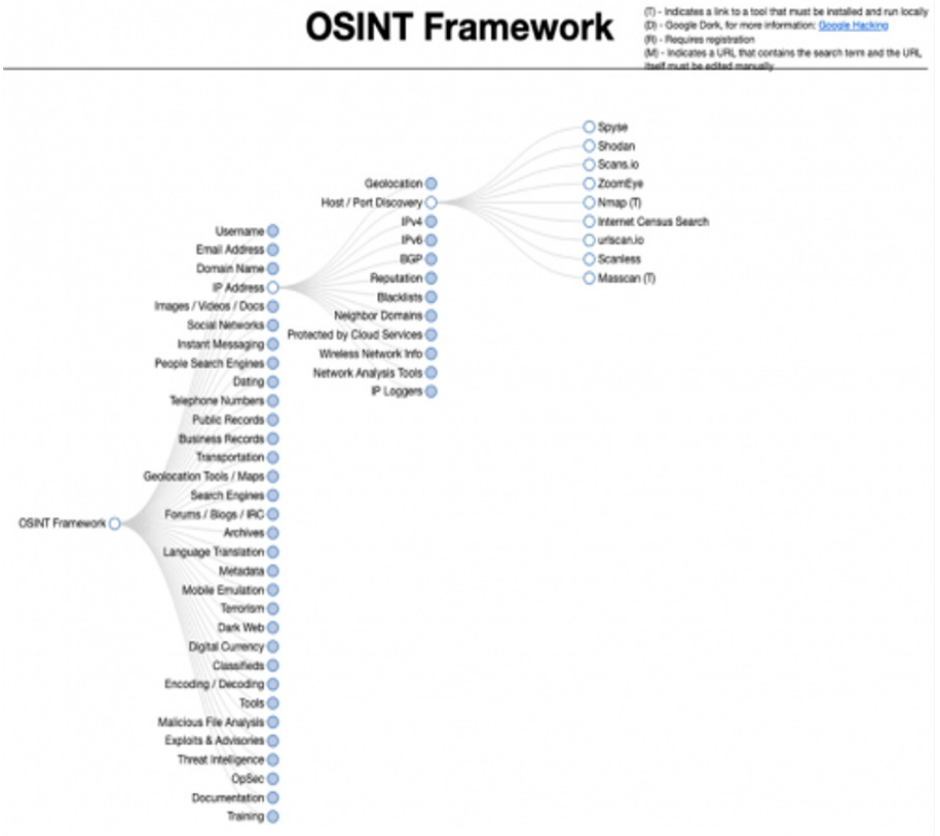
Comme le rappelle communauté Osint-FR, l'OSINT n'est pas qu'une question d'outils, mais également d'état d'esprit, de méthodologies utilisées et de réflexion.
Les éléments suivants ne sont donc volontairement pas exhaustifs.

On peut néanmoins retenir plusieurs sources intéressantes :

- **L' « OSINT Framework »** qui présente un grand nombre de sources et d'outils accessibles publiquement et pouvant être utilisés pour analyser un sujet donné sous un angle donné.

On y retrouve notamment une liste des sites utilisés pour identifier des personnes physiques ou morales ainsi que les informations en lien avec elles :
- Identification d'une personne via son adresse email
- Identification des ports ouverts sur un périmètre donné
- Identification des outils et sources permettant un suivi des médias sociaux

Parmi ces sources, réparties sur une trentaine de catégories, une grande partie est dédiée à l'information en lien avec les menaces.



– La communauté **Osint-FR** propose également une sélection d'outils "incontournables" pour la pratique de l'OSINT. En autre, des outils et sites permettant de chercher des informations en lien avec des entreprises, organisations et personnes physiques. Ce site répertorie notamment de nombreux outils développés en open source pour suivre les activités d'une cible donnée sur les réseaux sociaux.

– Enfin, et dans le même esprit, le projet **Awesome OSINT** qui référence un (très) grand nombre d'outils par cas d'usage. Plusieurs centaines d'outils sont listés et peuvent être utilisés par tous types de profils : responsable marketing, managers RH, consultant en intelligence économique ou encore journalistes.

Dans un cadre plus orienté cyber, certains permettent notamment de trouver des morceaux code via des recherches par mots-clés ou encore des outils de protection et de chiffrement de données.

Une fois le cadre posé ainsi que les ressources, outils et méthodologies identifiées, les phases de recherche, de collecte et d'analyse peuvent ensuite commencer. La spécificité de la cybersécurité nécessite cependant de s'intéresser à l'approche OSINT dans le cadre plus particulier de la CTI. Comment appliquer cette méthode pour

2. Comment l'OSINT permet-il d'enrichir sa stratégie de Cyber Threat Intelligence ?

Cadrer son besoin d'information et mettre en place une veille ciblée

Avant de se lancer dans la phase de collecte et d'analyse d'informations dans le cadre d'une investigation, il convient de définir les questions auxquelles cette démarche doit permettre de répondre.

Plusieurs questions peuvent être identifiées par un décideur dans le cas spécifique d'une stratégie OSINT appliquée au renseignement sur la menace :

ÉVALUER SON NIVEAU D'EXPOSITION

Mon entreprise expose-t-elle sur Internet des services sensibles recherchés par les pirates ?

Mon entreprise a-t-elle perdu le contrôle sur certaines informations sensibles abusivement partagées par des employés ou partenaires ?

Quelles données personnelles me concernant ont été compromises et pourraient être utilisées à mes dépend par un attaquant ?

ÉVALUER SON NIVEAU D'EXPOSITION

Mon entreprise est-elle affectée par la dernière faille du moment, massivement exploitée par des attaquants opportunistes ?

ÉVALUER SON NIVEAU D'EXPOSITION

L'identité de mon entreprise est-elle réutilisée frauduleusement par des attaquants pour tromper la vigilance de mes collaborateurs ou clients ?

Comment un utilisateur malveillant pourrait-il détourner mon produit à son avantage ?

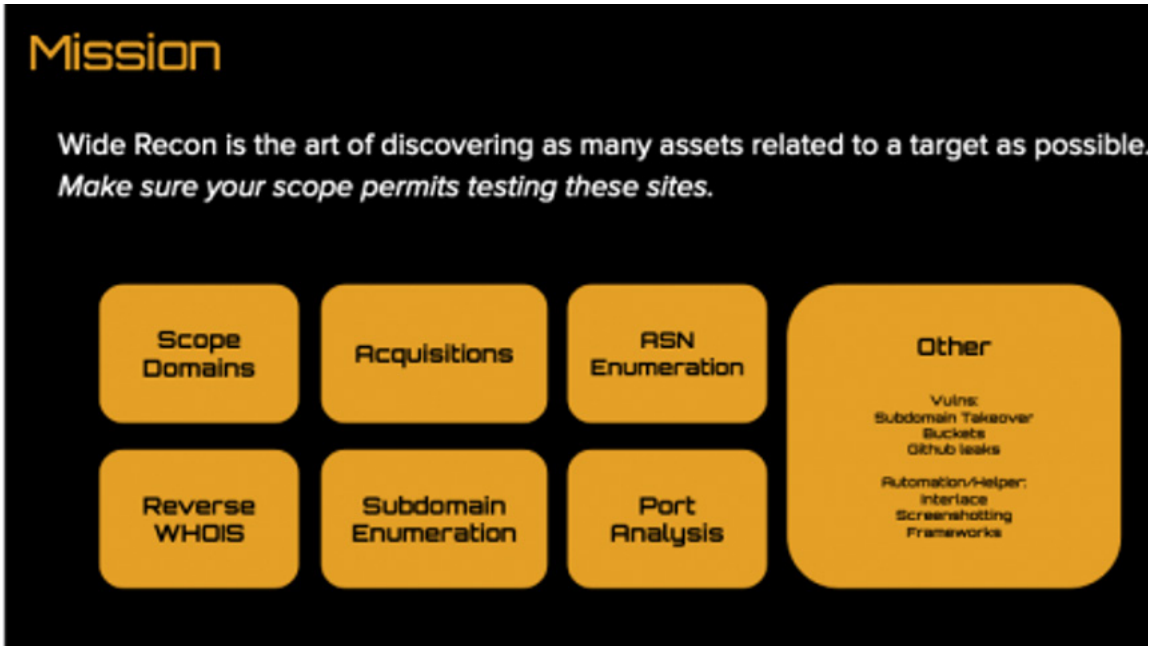
Une fois l'objectif défini, il est nécessaire d'identifier les sources et les méthodes qui pourront être utilisées pour collecter et analyser les informations recueillies.

Les matrices CTI : un outil de cadrage pour les recherches OSINT

Bien qu'il ne s'agisse que d'un exemple parmi d'autres, le chercheur Jason Haddix a publié une présentation de référence détaillant la méthodologie qu'il utilise personnellement ainsi que les sources et les outils qu'il est amené à utiliser lorsqu'il recherche des vulnérabilités dans le cadre des programmes de Bug Bounty auxquels il participe.

THE BUG HUNTER'S METHODOLOGY

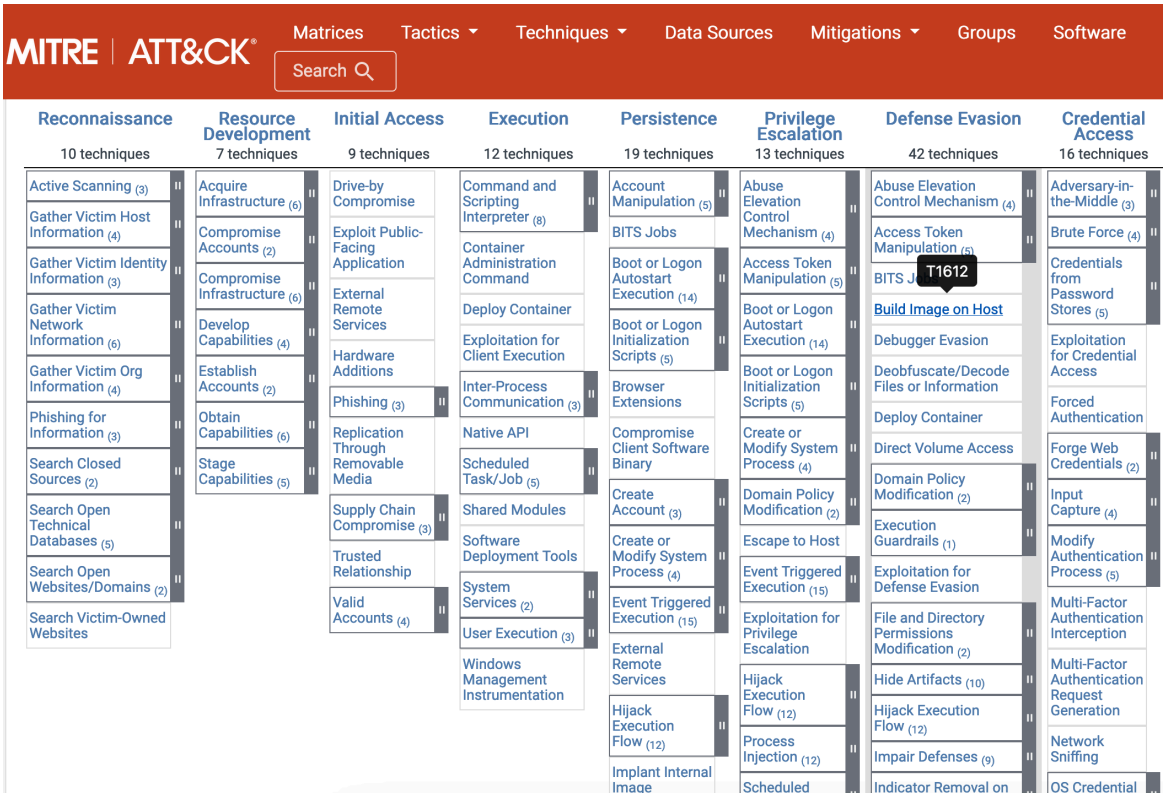
Cette présentation intitulée « **The Bug Hunter's Methodology** » illustre bien la variété des sources et la diversité des outils disponibles.



L'un des outils les plus connus et utilisés par les professionnels en matière de CTI est sans doute la matrice Mitre Att&ck. Proposée par la Mitre Corporation, une organisation à but non lucratif basée aux États-Unis, cette matrice permet de cartographier les différentes méthodes et techniques utilisées par les attaquants pour cibler des organisations. Répartie en grandes catégories, l'identification de ces techniques permet de dégager les modes opératoires des criminels ainsi que les vecteurs d'attaque qu'ils utilisent.

MITRE ATT&CK

L'un des outils les plus connus et utilisés par les professionnels en matière de CTI est sans doute la matrice Mitre Att&ck. Proposée par la Mitre Corporation, une organisation à but non lucratif basée aux États-Unis, cette matrice permet de cartographier les différentes méthodes et techniques utilisées par les attaquants pour cibler des organisations. Répartie en grandes catégories, l'identification de ces techniques permet de dégager les modes opératoires des criminels ainsi que les vecteurs d'attaque qu'ils utilisent.



Cette matrice n'est évidemment pas la seule et il convient notamment d'évoquer la Cyber Kill Chain ou encore la Diamond matrix qui figurent, toutes deux, parmi les plus connues.

Également orientée sur les techniques d'identification des cibles et des failles, la matrice PRE-ATT&CK aussi diffusée par la Mitre Corporation se focalise principalement sur les étapes préalables à l'attaque. Ces techniques, notamment utilisées par des attaquants pour collecter toutes les informations sur leurs cibles et préparer leurs actions sont réparties dans deux catégories que sont les phases de « reconnaissance » et de « développement des ressources ». Ces étapes primordiales dans le déroulement d'une attaque sont rendues exploitables par les informations disponibles en sources ouvertes sur de nombreux sites, on peut ainsi penser à certains éléments comme les adresses IP et les noms de domaine, le contenu d'un enregistrement Whois, un certificat SSL, une adresse email ou encore une adresse de wallet bitcoin.

CAS CONCRET : ANTICIPER LES FUTURES ATTAQUES GRÂCE À L'OSINT

Parmi les priorités des RSSI ou dirigeants, on peut notamment citer la maitrise de leur niveau de risque et donc d'exposition aux menaces. Afin d'avoir un regard clair sur ces niveaux, il est indispensable de disposer de données de sécurité fiables et contextualisées, qu'elles soient internes ou externes à l'organisation. L'identification des vecteurs d'attaques externes est l'un des principaux axes d'analyse permis par le renseignement sur les menaces. En disposant d'une cartographie du périmètre exposé et en surveillant son évolution, l'organisation est en capacité d'anticiper l'exploitation de ses vulnérabilités ou d'identifier celles ayant déjà été exploitées.

IDENTIFIER SON PÉRIMÈTRE EXPOSÉ

De nombreux dirigeants, RSSI et DSI n'ont qu'une vision parcellaire de leur périmètre exposé. Le shadow IT, les sites test publiés par mégarde par des sous-traitants, la démocratisation du télétravail ou encore le BYOD (Bring Your Own Device) sont autant de pratiques à risque qui peuvent exposer les actifs d'une organisation, mais qui passent souvent sous leur radar.

L'enjeu est donc d'incorporer dans l'évaluation de son niveau de risque des éléments qui n'étaient pas identifiés jusqu'alors. En scannant le web à la recherche d'informations techniques en sources ouvertes, il est possible de dresser un état des lieux de l'exposition de l'organisation.

De la même manière que ces informations pourraient être utilisées par des attaquants pour identifier un port ouvert, un serveur non sécurisé ou une interface d'administration exposant des données sensibles, elles peuvent bien sûr permettre d'anticiper des attaques en remédiant aux risques avant même que l'organisation ait été ciblée.

Une grande partie des organisations ont aujourd'hui une bonne connaissance et un bon suivi des données internes cependant une brèche se créée souvent au moment où ces données sortent de ce périmètre. Au-delà des enjeux de sécurité sur l'échange des informations, il s'agit surtout d'identifier toutes les « fissures » existantes et pouvant amener à une exposition externe de données n'ayant pas vocation à être échangées ou exposées hors du périmètre de l'organisation.

SURVEILLER SON EXPOSITION AUX MENACES

Une fois les vulnérabilités et failles identifiées, un plan d'actions est lancé afin de remédier aux risques soulevés. En plus de ce suivi ponctuel et contextualisé, une surveillance globale et continue est également nécessaire afin de maintenir son niveau d'exposition aux menaces le plus bas possible et ainsi réduire drastiquement son risque.

En plus des éléments techniques surveillés servant principalement à l'anticipation des attaques, il est impératif d'évaluer son niveau d'exposition en prenant en considération les informations et données déjà en possession des attaquants.

La surveillance des forums de criminels ou encore des comptes twitter de groupes hacktivistes permettent notamment d'identifier les leviers d'actions que les attaquants pourraient utiliser ou auraient déjà utilisé pour cibler l'organisation. La mise à disposition sur un forum de criminels d'une base de données contenant des identifiants de connexion pourrait par exemple permettre à des attaquants de s'introduire dans le système d'information de l'organisation ciblée.

Une fois attaquée et dans le meilleur des cas, l'organisation détecterait l'intrusion et pourrait y réagir. Cependant, en ayant eu accès à une notification de menace liée aux informations disponibles dans la base de données, l'organisation aurait pris des mesures correctives sans délai et aurait ainsi eu de grandes chances d'éviter l'intrusion.

Dans le cadre d'attaques par phishing ou ingénierie sociale, cette démarche permettrait par exemple de répondre à des questions telles que :

- Suis-je ciblé par la campagne d'ingénierie sociale en cours (arnaque au président, phishing, …) ?
- Des domaines frauduleux proches de mes domaines légitimes ont-ils été déposés par des pirates ?

Le renseignement sur les menaces permet donc aux organisations et experts de sécurité de mieux comprendre leur environnement de risque et d'identifier les leviers d'attaques que les criminels pourraient utiliser pour les cibler.

Ces méthodologies sont d'ailleurs récurrentes pour nos analystes du CERT-XMCO, dans le cadre des services fournis à nos clients abonnés aux services de Cyber Threat Intelligence : Serenety ou de notre service de Veille Cyber Yuno. Nous utilisons de nombreux outils : Maltego, Recon-ng, theHarvester, Shodan, Metagoofil, Searchcode, SpiderFoot ou encore Babel X.

Serenety, infiltre et collecte des données à partir de sources Darkweb. Cela permet d'avoir la connaissance de possibles fuites d'informations concernant votre organisation.

Pour anticiper les menaces qui pèsent sur votre entreprise, il est nécessaire de connaître votre degré d'exposition. C'est par cette connaissance que l'exploitation de l'OSINT participe à votre cybersécurité.

Liste de lecture #OSINT

- Un outil spécialisé sur les données françaises pour obtenir des emails, des comptes de médias sociaux, des adresses, les emplois, etc.
- Une énième méthodo d'OSINT orienté Bug Bounty
- Des API pour l'OSINT
- Un outil pour visualiser les chaines de certificats TLS
- Bibliographie sur l'OSINT
- Bellingcat's Online Investigation Toolkit
- Un tool de reconnaissance
- Partage de tips de bug hunter surtout focus sur de la recon
- Liste de petits outils très utiles pour faire de la manipulation de fichier et d'URL
- Découvrir des sous-domaine en utilisant une technique appelée RNN (Recurrent Neural Network) et ici
- Une cheat sheet OSINT
- Jason Haddix a lancé son blog
- Identifier où une image a été utilisée sur Internet

Remerciements :

Charles DAGOUAT
Charlène GREL

À propos de

serenety
By xmco

Créée en 2010, Serenety est un service de Cyber Threat Intelligence, développé par le CERT-XMCO et à destination des organisations publiques et privées. Son objectif est d'identifier la surface d'attaque et la surface d'exposition des organisations surveillées au travers d'un outil simple d'utilisation et ergonomique. Il se distingue de ses concurrents par la corrélation de ses résultats issus des analyses automatiques des sources ouvertes surveillées et des investigations manuelles de son équipe d'experts qualifiés. Cette surveillance permet d'identifier les menaces et d'anticiper les risques notamment liés aux fuites de données, aux systèmes exposés et vulnérables ou encore à la compromission de comptes.

À propos d'

xmco

Cabinet de conseil indépendant en cybersécurité, XMCO a à cœur d'accompagner ses clients, de toute taille et de tous secteurs, dans l'anticipation des vulnérabilités, la détection des failles et la réponse à incidents. XMCO est qualifié PASSI sur l'ensemble des portées, ce qui confirme le cœur de métier historique : l'audit et les tests d'intrusion.

Retrouvez-nous

Sur notre site :

www.xmco.fr

Sur les réseaux sociaux :

Envie d'échanger ?

sales@xmco.fr

01 79 35 29 30