Le renseignement sur les cybermenaces

Le renseignement se définit comme une information récoltée soit par des moyens humains (renseignement d'origine humaine ou ROH en français, Human Intelligence en anglais ou HUMINT) ou par des moyens électroniques (renseignement d'origine électromagnétique en français ou Signal Intelligence en anglais ou SIGINT) associée à un processus cognitif qui va apporter de la valeur ajoutée. Cette information avec sa valeur ajoutée se nomme le renseignement. Le renseignement sert à prendre une décision aussi bien dans la vie politique, dans la vie économique et plus encore dans un contexte militaire. Le cyberespace ne fait pas exception au fait que le renseignement est vital aussi bien pour l'attaquant que pour la (potentielle) victime.

Une cybermenace se définit comme un danger qui peut compromettre la sécurité, l'intégrité ou la confidentialité des systèmes informatiques, des réseaux, des données ou des utilisateurs. Il en existe plusieurs types : rançons logicielles, attaque par déni de service destiné à saturer les serveurs d'un site et planter le site en question, ingénierie sociale etc. Les raisons d'une attaque sont nombreuses : l'appât du gain généralement, la vengeance, l'exploit (parfois pensant à tort, que pénétrer un réseau sans autorisation permettra d'avoir un poste), l'espionnage, la déstabilisation, le pré positionnement stratégique. Aussi, les profils sont divers : ça peut être aussi bien l'employé d'une structure sans trop de connaissances informatiques (surtout à l'heure où des « kits » de piratage peuvent s'acheter sur le dark web), que des cybercriminels plus ou moins chevronnés et organisés, que l'adolescent qui « s'amuse » ou le sommet de la chaîne alimentaire : les menaces permanentes avancées (Advanced Permanent Threats) qui sont des groupes criminels plus ou moins soutenu par les États (Russie, Corée du Nord, Iran etc).

Les enjeux sont énormes. Bien que cela soit triste, nous valons ce que valent nos données. Par conséquent, nos données, y compris personnelles valent de l'or. Par conséquent, il convient de les protéger, raison pour laquelle certains souhaitent s'en emparer. Toute attaque demande un minimum de préparatifs ; aussi chaque préparatif fait un « bruit ». Et c'est ce bruit qu'il convient de collecter, pour ensuite l'analyser et en tirer du renseignement, afin de le donner au donneur d'ordre pour enfin (dans l'idéal) recevoir un rendu…pour ensuite recommencer. Ce processus se nomme : le processus du renseignement.

Alors que le renseignement d'affaire est (relativement) plus connu que le renseignement sur les cybermenaces, et donc que les sources sont plus connues, il convient de s'interroger sur la façon dont (n'importe qui) un analyste peut faire du renseignement sur les menaces cyber afin protéger la structure à laquelle il appartient.

I L'analyse d'une cyber attaque

Robert Aaron, une des références britanniques du renseignement sur les menaces cyber a établi un modèle. Si ce modèle ne prétend pas à l'exhaustivité des paramètres à prendre en compte, il donne une bonne base pour tout analyste qui souhaite se lancer dans l'analyse d'une attaque. Ce modèle est celui du diamant où on va analyser :

- L'identité de l'adversaire : qui est-elle ? Pourquoi elle le fait ? Quel est le point d'entrée initial dans le réseau (adresse IP/adresse électronique) ? L'attribution à un acteur précis reste horriblement difficile…
- L'identité de la victime : qui est-elle ? La victime soutient -elle des positions politiques ou sociales controversées ? La victime est -elle cataloguée, à tort ou à raison, « pro Y » ou « « anti X » ? Possède-t-elle une trésorerie disponible ? La victime qui a cliqué sur le lien se retrouve-t-elle dans les bases de données violées ? Ses accès sont-ils protégés ? La victime a-t-elle besoin d'une sensibilisation en termes de sécurité pour que cela ne se reproduise pas ?
- L'infrastructure : il s'agit de la recherche de l'infrastructure utilisée. Une fois n'est pas coutume, il s'agira de déterminer à l'aide des fameuses questions « Qui ? Quand ? Quoi ? Comment ? Pourquoi ? Combien ? comment l'infrastructure utilisée a été contaminé/affecté.
- Les capacités : enfin, il est nécessaire (sachant que c'est très difficile) d'identifier l'approche utilisée par l'adversaire. Comment il a pu exploiter la victime ? Ici, il faut partir sur des hypothèses en fonction des anciennes questions du modèle et les valider.

Toutes ces questions ne sont pas exhaustives loin de là. Et selon les cas, d'autres questions seront soulevées.
Mais elles permettent de comprendre comment la cyberattaque a pu arriver.

II le cadre MITRE ATT&CK

Si on veut faire du renseignement, il est nécessaire d'employer des sources qui apporteront une connaissance, ou des pistes de réflexion pour comprendre les attaquants et anticiper leurs actions. C'est aussi vrai quand il s'agit du renseignement sur les menaces cyber. La première source à exploiter est le cadre MITRE ATT&CK[1]. Il s'agit des initiales de « Adversarial Tactics, Techniques and Common KnowledgeII ». Concrètement, c'est un outil à utiliser pour améliorer la sécurité informatique en fournissant une base de données qui concerne les tactiques et techniques utilisées par les cybercriminels tout au long du cycle de vie de l'attaque. Les informations proviennent d'une communauté effectuant de la veille, les rapports d'incidents publics, ainsi que par les recherches sur les nouvelles techniques menées par les analystes en cybersécurité et les Threat Hunters (ou chasseurs de menaces). Le cadre MITRE ATT&CK répertorie 14 tactiques :

- Reconnaissance
- Développement des ressources
- Accès initial
- Exécution
- Persistance
- Élévation des privilèges
- Contournement des défenses
- Accès aux identifiants
- Découverte
- Déplacement latéral
- Collecte
- Commande et contrôle

[1] https://attack.mitre.org

- Exfiltration
- Impact

Pourquoi cette base est elle si importante ? Car le comportement humain ne change pas. Si les outils techniques évoluent, il faut comprendre que le comportement humain ne change pas. Si le comportement humain ne change pas, la méthodologie ne changera pas. Ainsi, dans toute attaque, on trouve ces phases, bien qu'en réalité elles soient plus nombreuses :

- **Reconnaissance** : l'attaquant va lui aussi faire du renseignement sur sa cible.
- **Armement** : l'attaquant va préparer son « exploit » qu'il sera pertinent d'utiliser sur sa cible.
- **Livraison** : l'attaquant va livrer l'envoi de son « exploit » à sa cible soit par courrier électronique, clef USB ou web. C'est là que l'ingénierie sociale entre en jeu. Ex : si la recherche sur la cible a déterminé que la personne est célibataire depuis bien longtemps, il faudra préparer un exploit où il faut donner envie à la cible de cliquer sur un lien (rencontre amoureuse par exemple). Ici, les leviers psychologiques de type MICE (Monney, Interest, Contraint, Ego) ou son équivalent en français SANSOUCIS (Solitude, Argent, Nouveauté, Sexe, Orgueil, Utilité, Contrainte, Idéologie, Suffisance) seront employés.
- **Exploitation** : une fois sa charge utile livrée, l'attaquant exploite les vulnérabilités (repérées dans sa phase de reconnaissance) afin d'exécuter le code de sa cible.
- **Installation** : l'attaquant peut installer d'autres logiciels afin d'attaquer d'autres systèmes ou faire en sorte à ce que sa charge utile persiste dans le réseau de sa victime.
- **Commandement et contrôle (C2)** : l'attaquant va mettre au point un canal pour contrôler à distance le système de sa cible.
- **Actions sur les objectifs** : c'est la dernière étape où l'attaquant atteint ses objectifs initiaux : exfiltration des données, exécution de la rançon logicielle ou toute autre action.

Devant les préjudices financiers terribles des cyberattaques (2 milliards d'euros en France pour l'année 2022 sans compter les effets sociologiques, psychologiques), il

arrivera un jour où les assurances ne voudront plus assurer les risques cyber…les assurances elles-mêmes commencent à être attaquées[2]. Les entreprises françaises seraient bien inspirées se pencher sur le problème, de recruter des analystes afin d'anticiper les cyber attaques.

L'article est unique et a été rédigé par un bénévole expert de chez ADESS, ayant une grande expertise dans sa thématique de prédilection. Il a accumulé une expérience professionnelle significative et des diplômes qui lui sont associés.

ADESS n'a aucune intention d'approuver ou d'infirmer les opinions exprimées dans les publications, qui restent la propriété de leurs auteurs :

Pierre VERDIN – ID : 7319745

Source de l'article : www.adess-france.fr

[2] https://www.newsassurancespro.com/sante-un-deuxieme-operateur-de-tiers-payant-victime-de-cyber-attaque/01691586519