SECURECOM
Services Conseils inc.

Cyber-espionnage industriel : la menace triple en un an

Dans le contexte mondial actuel, je trouve intéressant d'aborder le sujet du cyber-espionnage, plus spécifiquement le cyber-espionnage de nature industrielle. À la mention de cyber-espionnage, plusieurs questions sont susceptibles de nous venir naturellement à l'esprit. La forme la plus simple étant :

- **Qui** en est la cible? **Qui** en est l'auteur ? **À qui** cela rapporte-t-il ?
- Pourquoi ?
- Comment ?
- Quel est l'impact économique

Évidemment, les statistiques en cette matière peuvent s'avérer trompeuses. Après tout, la notion d'espionnage requière celle du secret en avant-plan. Il est donc assez difficile d'en connaitre le niveau d'activité avec précisions. Néanmoins en examinant les données connus (cf. sources suivantes) et en tenant compte des technologies actuelles ainsi que des motivations, il nous est possible de nous faire une idée globale et plausible de la situation.

Qui ?

Tout d'abord, je me suis intéressé au « QUI » en faisant abstraction de l'espionnage de type inter-gouvernemental. On aurait tendance à croire que les petites entreprises sont plus à l'abri de l'espionnage que les plus grandes. Hors, dans les faits, la tendance semble laisser penser que les petites entreprises sont de plus en plus visées, représentant en 2013 près de la moitié des attaques répertoriées.

Prenons comme point de départ les données du Rapport *Verizon 2014 Data breach investigation* qui contient entre autres des données sur le cyber espionnage récoltées lors d'enquêtes judiciaires à travers le monde. On peut y lire notamment que « *nos données montrent en fait que les attaques de points de vente ont eu tendance à baisser ces dernières années. Inversement, les attaques liées à l'espionnage continuent à augmenter - affectant tous les types d'entreprises, et pas uniquement les institutions gouvernementales et les organisations militaires.* »

Quelques chiffres :

Suivant le rapport Verizon, Les attaques liées à l'espionnage représentent 22% des attaques globales analysées dans le rapport, se classant au deuxième rang après les attaques applicatives web. Les attaques d'espionnage, sur un an, auraient été multipliées par trois, sur la base d'un échantillon de 511 incidents investigués pour 306 fuites de données confirmées. Selon la classification américaine (*cf.* : *https://www.census.gov/cgi-bin/sssd/naics/naicsrch?chart=2012*), les secteurs d'activités semblant être les plus touchés sont :

- Les services professionnels,
- Les transports,
- La fabrication,
- Les exploitations minières,
- Le secteur public.

Évidemment, ces données, quoiqu'éloquentes, ne représentent que la pointe de l'iceberg. Néanmoins, elles sont un indicateur important de la tendance actuelle et nous parviennent grâce à :

- les répondants aux incidents,
- les analystes du renseignement,
- Les chercheurs en virus et malware.

Donc, la taille ne semble pas être un facteur déterminant. Toutes les entreprises, PME ou grandes, sont susceptibles de faire un jour l'objet de cyber-espionnage. Mais par qui ? D'où vient la menace ?

La réponse se trouve dans la motivation de l'attaquant et du type de données recherché. Il est vrai que la description que donne Verizon s'applique souvent : « *Des agresseurs affiliés à un état compromettent une organisation, souvent via des attaques de phishing ciblées visant la propriété intellectuelle.* »

À mon sens, le terme « affiliés à un état » peut-être superflu. Bien sûr, nous pouvons tous imaginer les moyens technologiques énormes dont disposent certains pays. Il existe pourtant une certaine part des actes d'espionnage qui ne sont pas le fait d'un état mais plutôt celui du crime organisé ou encore d'un concurrent d'affaire. Bien sûr, les états possèdent le matériel, le personnel et les connaissances techniques pour se livrer à ce type d'activité. Le crime organisé aussi. Il est aujourd'hui possible, grâce entre-autres au deep web, de trouver quelqu'un de compétent qui pour une somme conséquente lancera une attaque de type « menace persistante avancé » qui consiste à attaquer la cible par tous les moyens, tant et aussi longtemps que l'attaque n'est pas réussi.

Les techniques utilisées dans le cadre d'une attaque de cyber-espionnage sont nombreuses et souvent combinées entres elles de façon à donner le meilleur résultat possible. J'énumère ici les principales :

- Ingénierie sociale,
- Phishing,
- Utilisations de malware multifonctions très avancées,
- Utilisation de faille 0 day,
- Backdoor ou C2 (cf. http://www.rapid7.com/db/modules/exploit/unix/webapp/carberp_backdoor_exec)
- Exploitation de vulnérabilités systèmes.

Les techniques privilégiées utilisées pour délivrer du code malicieux sont:

- Pièce jointe, courriel,
- Web drive-by,
- Installation directe,
- Téléchargement par malware,
- Lien courriel.

Il est important de savoir que les cybers-espions disposent d'un arsenal très perfectionné dans leur boite à outils logicielle. La plupart du temps, les malwares utilisés lors des attaques sont d'une complexité telle qu'ils ne peuvent avoir été codés que par un groupe de programmeurs chevronnés. Souvent écrit en plusieurs langages de programmation et sous forme de modules indépendants, leurs fonctions n'ont de limite que l'imagination de leurs auteurs. Les exploits de type Jour J (zero-day) sont très recherchés et se vendent à gros prix sur internet. Le passé a démontré que ce type d'exploit était souvent inclus dans les vers (Stuxnet) et logiciels espions (Gyges).

L'impact économique

Bien que difficilement mesurable, il apparait que l'impact économique associé au cyber-espionnage semble très important. Il est difficile en effet d'évaluer avec précisions le cout d'une perte de propriété intellectuelle. Par ailleurs, la plupart du temps, il n'est pas possible d'identifier avec certitude les contextes d'usage des données récupérées. Il existe néanmoins un document intéressant produit par McAfee traitant du sujet. « THE ECONOMIC IMPACT OF CYBERCRIME AND CYBER ESPIONAGE ». Les montants mentionnés sont astronomiques.

Se protéger

Il n'existe aucune solution permettant d'affirmer qu'une entreprise est à l'abri du cyber-espionnage. Néanmoins, la meilleure défense reste l'application des techniques de protection connues et qui devraient généralement être en place.

- Appliquer rapidement tous les correctifs de sécurité publiés par les différents éditeurs de logiciel. Les vulnérabilités logicielles sont souvent exploitées en première étape.
- Déployer une solution anti-virus et assurez-vous que les définitions soient constamment à jour. Beaucoup d'entreprises se font piéger par des menaces déjà connues par ces solutions.
- La formation des utilisateurs est primordiale afin qu'il puisse détecter rapidement une attaque. Des simulations d'attaque par ingénierie sociale démontrent que le niveau de vigilance des employés est grandement amélioré en les familiarisant avec les techniques d'ingénierie sociale et qu'ils connaissent bien les pièges associés au hameçonnage par courriel ou site web.
- Une solution de centralisation des journaux et des évènements est importante. Il ne suffit pas de les accumuler, il s'agit de mettre en place une routine qui inclut la surveillance de ses journaux des systèmes, du réseau et des applications de façon régulière. Cette surveillance peut permettre d'agir de façon proactive.
- Les nouveaux types d'appareils de prévention et de détection d'intrusion se veulent performants et permettent de détecter, sinon de prévenir, et d'arrêter une grande variété d'attaques. Il faut cependant s'assurer de la bonne configuration de l'appareil et être à l'affut de tout message, alerte ou trafic inhabituel, enregistrés par l'appareil. Il est peu recommandable de superposer les couches de protection en empilant les IDS/IPS. Les experts s'entendent pour dire qu'il vaut mieux un appareil performant et bien configuré que plusieurs dans lesquels peuvent se glisser des erreurs de configuration.

Dany Ouellet OSCP, MCSA security, Comptia sec+