Avis d'expert – Détecter les espions sur le réseau pour combattre les APT

Que signifie le fait d'être la cible d'une Menace Persistante Avancée (APT pour Advanced Persistent Threat) ? Sans aucun doute, les APT sont des menaces beaucoup plus subtiles, intelligentes et dangereuses que ses prédécesseurs qui étaient aléatoires et généralement moins sophistiquées. Les menaces Internet sont beaucoup plus malveillantes aujourd'hui et nous ne pouvons plus compter sur les défenses basées sur les signatures pour les combattre. Nous devons battre l'intelligence par l'intelligence.

Alors que la cybercriminalité évolue et progresse, elle peut également être vue comme rétrospective dans son approche. La cybercriminalité a aujourd'hui de nombreuses similitudes avec l'âge d'or de l'espionnage d'antan – infiltrer, se cacher et extraire des informations de valeur ou sensibles sans être détecté. Cette approche est très efficace dans un monde où les informations numériques sont de plus en plus précieuses.

L'infiltration furtive en ligne visant à voler des informations confidentielles et de valeur est le but ultime des cybercriminels actuels. Il est clair que les organisations doivent être particulièrement vigilantes et préparées pour détecter ces nouveaux types de menaces endémiques et continues. L'incorporation et l'exécution réussies de codes malveillants sur un réseau peuvent faire des ravages au sein d'une organisation, le plus grand risque consistant dorénavant dans le vol de propriété intellectuelle. Avantage concurrentiel, informations d'initiés, propriété intellectuelle de valeur et cessible sont autant de données précieuses aussi bien pour les cybercriminels professionnels que pour les attaquants émergents cautionnés (fait encore non confirmé) par les Etats.

La menace Facebook

De nouvelles façons de travailler comme le BYOD, où les terminaux sont également utilisés à des fins non professionnels comme pour l'utilisation des medias sociaux, favorisent les APT. Un simple lien sur Facebook vers une page Web infectée peut s'avérer être le point d'entrée dans le réseau d'une organisation. Les cybercriminels deviennent très compétents dans le ciblage des personnes avec l'objectif de les inciter à leur insu à donner accès à leurs appareils et, par conséquent, au réseau de l'entreprise.

Par chance, il existe encore des moyens pour détecter les 'espions' qui tentent d'infiltrer, et même ceux qui ont eu accès et sont sur le réseau. Ils laissent toujours des indices. Il suffit de chercher les signes et, dans le cas d'un 'espion' présumé, on le pousse à commettre des erreurs qui permettront de l'identifier et de le confondre.

Le *sandboxing* n'est pas une idée nouvelle, mais il se révèle être de plus en plus utile dans la lutte contre les APT. Les logiciels malveillants ont toujours essayé de se dissimuler et les hackers d'aujourd'hui rendent leurs logiciels 'conscients' de leur environnement. Le *sandbox* – qui peut être local ou en mode cloud – offre un environnement virtuel étroitement contrôlé dans lequel seules

les ressources de base sont fournies pour permettre aux logiciels suspects ou inconnus de s'exécuter, et où l'accès au réseau et aux autres fonctions critiques sont restreints. Les logiciels malveillants sont dupés sur le fait qu'ils ont atteint leur destination finale de sorte qu'ils dévoilent leurs véritables comportements alors qu'ils sont observés de près. Mais, comment savoir quelle partie du logiciel doit être conduite dans un environnement virtuel de sandbox pour un examen plus approfondi?

Exfiltration des données

Il y a cinq comportements d'exfiltration et exploitations de failles qui, soit isolément ou en tandem, peuvent indiquer une activité de logiciels malveillants.

En les observant plus en détails : certaines charges d'APT génèrent de manière aléatoire des chaines d'adresses IP visant à faciliter leur propagation, ou elles tentent d'établir une connexion avec un serveur de commande et de contrôle dans le but d'exfiltrer des données ou de faire appel à d'autres ressources d'attaques via un botnet. Si les détails du serveur malveillant sont identifiés, c'est comme si un espion présumé mis sous surveillance se dévoile lorsqu'il appelle son maitre-espion.

En outre, des cas avérés d'APT ont impliqué de nombreuses techniques pour dissimuler (obfuscating) le vrai sens et l'intention du code malveillant JavaScript, et bien sûr, le logiciel malveillant va certainement imiter le comportement du terminal ou de l'application hôte pour éviter la détection. Par conséquent, la tendance à avoir des logiciels malveillants encryptés au sein des charges d'APT expose l'ensemble du trafic encrypté à un risque élevé.

La protection par sandboxing

Pour une protection plus efficace et un meilleur contrôle, le sandboxing devrait idéalement opérer dans le cadre d'une stratégie multi-couches. La première ligne de défense est le moteur antivirus supporté par une sandbox embarquée en ligne opérant en temps réel. Si les menaces s'avèrent appropriées, les fichiers suspects peuvent être soumis à une sandbox basée sur le cloud pour davantage d'analyses. Cette approche unifiée et multi- couches offre plus de contrôle et de rapidité pour contrer une attaque potentielle. Et c'est nécessaire. De la même façon que la cybercriminalité devient plus évoluée et multi-couches, la stratégie de sécurité de l'organisation doit l'être également.

Malheureusement, de nombreuses entreprises et organisations pensent que rien de tout cela ne les concerne. La forte médiatisation autour de la 'cyber-guerre' déchainée entre les Etats nations soutient cette fausse idée. Cependant, dans le cyber-espace il n'y a pas de frontières et toutes les organisations, grandes ou petites, sont une cible potentielle. Il est très facile pour les cybercriminels compétents d'utiliser la voie des réseaux sociaux pour accéder aux appareils et réseaux, alors, qu'est ce qui les empêchent de cibler les organisations, surtout s'ils partent du principe que l'organisation n'est pas préparée et est vulnérable ? Et avec des outils de cybercriminalité qui deviennent plus accessibles et plus facilement disponibles, qu'est ce qui arrête les concurrents de faire la même chose ?

Face aux APT, les défenses traditionnelles de sécurité IT sont obsolètes et dorénavant inadéquates. Il est de plus en plus urgent pour les organisations de reconnaître et d'accepter les risques réels posés par les APT et d'adopter une approche multi-couches plus moderne et intelligente pour la détection et la résolution des menaces. Le sandboxing est un outil clé dans cette approche.

Voir aussi

Silicon.fr en direct sur les smartphones et tablettes

Silicon.fr fait peau neuve sur iOS