

Internet : APT: D tecter l espion qui est sur votre r seau

Internet

Post  par : JulieM

Publi e le : 6/6/2013 11:30:00

Que signifie le fait d tre la cible d une **Menace Persistante Avanc e** (APT ou Advanced Persistent Threat en anglais) ? Sans aucun doute, les APT sont des menaces beaucoup plus subtiles, intelligentes et dangereuses que ses pr d cesseurs qui  taient al atoires et g n ralement moins sophistiqu es.

Les menaces Internet sont beaucoup plus malveillantes aujourd hui et nous ne pouvons plus compter sur les d fenses bas es sur les signatures pour les combattre. Nous devons battre l intelligence par l intelligence.

Alors que la cybercriminalit   volue et progresse, elle peut  galement  tre vue comme r trospective dans son approche. La cybercriminalit  a aujourd hui de nombreuses similitudes avec l ge d or de l espionnage d antan   infiltrer, se cacher et extraire des informations de valeur ou sensibles sans  tre d tect . Cette approche est tr s efficace dans un monde o  les informations num riques sont de plus en plus pr cieuses.

L infiltration furtive en ligne visant   voler des informations confidentielles et de valeur est le but ultime des cybercriminels actuels. Il est clair que les organisations doivent  tre particuli rement vigilantes et pr par es pour d tecter ces nouveaux types de menaces end miques et continues. L incorporation et l ex cution r ussies de codes malveillants sur un r seau peuvent faire des ravages au sein d une organisation, le plus grand risque consistant dor navant dans le vol de propri t  intellectuelle. Avantage concurrentiel, informations d initi s, propri t  intellectuelle de valeur et cessible sont autant de donn es pr cieuses aussi bien pour les cybercriminels professionnels que pour les attaquants  mergents cautionn s (fait encore non confirm ) par les Etats.

De nouvelles fa ons de travailler comme le BYOD, o  les terminaux sont  galement utilis s   des fins non professionnels comme pour l utilisation des medias sociaux, favorisent les APT. Un simple lien sur Facebook vers une page Web infect e peut s av rer  tre le point d entr e dans le r seau d une organisation. Les cybercriminels deviennent tr s comp tents dans le ciblage des personnes avec l objectif de les inciter   leur insu   donner acc s   leurs appareils et, par cons quent, au r seau de l entreprise.

Par chance, il existe encore des moyens pour d tecter les  espions  qui tentent d infiltrer, et m me ceux qui ont eu acc s et sont sur le r seau. Ils laissent toujours des indices. Il suffit de chercher les signes et, dans le cas d un  espion  pr sum , on le pousse   commettre des erreurs qui permettront de l identifier et de le confondre.

Le sandboxing n est pas une id e nouvelle, mais il se r v le  tre de plus en plus utile dans la lutte contre les APT. Les logiciels malveillants ont toujours essay  de se dissimuler et les hackers d aujourd hui rendent leurs logiciels  conscients  de leur environnement. Le sandbox   qui peut  tre local ou en mode cloud   offre un environnement virtuel  troitement contr l  dans lequel seules les ressources de base sont fournies pour permettre aux logiciels suspects ou inconnus de s ex cuter, et o  l acc s au r seau et aux autres fonctions critiques sont restreints. Les logiciels malveillants sont dup s sur le fait qu ils ont atteint leur destination finale de sorte qu ils d voient leurs v ritables comportements alors qu ils sont observ s de pr s. Mais, comment savoir quelle partie du logiciel doit  tre

conduite dans un environnement virtuel de sandbox pour un examen plus approfondi?

Il y a cinq comportements d exfiltration et exploitations de failles qui, soit isol ment ou en tandem, peuvent indiquer une activit  de logiciels malveillants.

En les observant plus en d tails : certaines charges d APT g n rent de mani re al atoire des cha nes d adresses IP visant   faciliter leur propagation, ou elles tentent d  tablir une connexion avec un serveur de commande et de contr le dans le but d exfiltrer des donn es ou de faire appel   d autres ressources d attaques via un botnet. Si les d tails du serveur malveillant sont identifi s, c est comme si un espion pr sum  mis sous surveillance se d voile lorsqu il appelle son maitre-espion.

En outre, des cas av r s d APT ont impliqu  de nombreuses techniques pour dissimuler (obfuscating) le vrai sens et l intention du code malveillant JavaScript, et bien s r, le logiciel malveillant va certainement imiter le comportement du terminal ou de l application h te pour  viter la d tection. Par cons quent, la tendance   avoir des logiciels malveillants encrypt s au sein des charges d APT expose l ensemble du trafic encrypt    un risque  lev .

Pour une protection plus efficace et un meilleur contr le, le sandboxing devrait id alement op rer dans le cadre d une strat gie multi-couches. La premi re ligne de d fense est le moteur antivirus support  par une sandbox embarqu e en ligne op rant en temps r el. Si les menaces s av rent appropri es, les fichiers suspects peuvent  tre soumis   une sandbox bas e sur le Cloud pour davantage d analyses. Cette approche unifi e et multi-couches offre plus de contr le et de rapidit  pour contrer une attaque potentielle. Et c est n cessaire. De la m me fa on que la cybercriminalit  devient plus  volu e et multi-couches, la strat gie de s curit  de l organisation doit l  tre  galement.

Malheureusement, de nombreuses entreprises et organisations pensent que rien de tout cela ne les concerne. La forte m diatisation autour de la  cyber-guerre  d chain e entre les Etats Nations soutient cette fausse id e. Cependant, dans le cyber-espace il n y a pas de fronti res et toutes les organisations, grandes ou petites, sont une cible potentielle. Il est tr s facile pour les cybercriminels comp tents d utiliser la voie des r seaux sociaux pour acc der aux appareils et r seaux, alors, qu est ce qui les emp chent de cibler les organisations, surtout s ils partent du principe que l organisation n est pas pr par e et est vuln rable? Et avec des outils de cybercriminalit  qui deviennent plus accessibles et plus facilement disponibles, qu est ce qui arr te les concurrents de faire la m me chose ?

Face aux APT, les d fenses traditionnelles de s curit  IT sont obsol tes et dor navant inad quates. Il est de plus en plus urgent pour les organisations de reconna tre et d accepter les risques r els pos s par les APT et d adopter une approche multi-couches plus moderne et intelligente pour la d tection et la r solution des menaces. Le sandboxing est un outil cl  dans cette approche.

Christophe Auberger, Responsable Technique chez Fortinet consid re le  sandboxing  comme  tant un outil cl  dans la lutte contre les APT