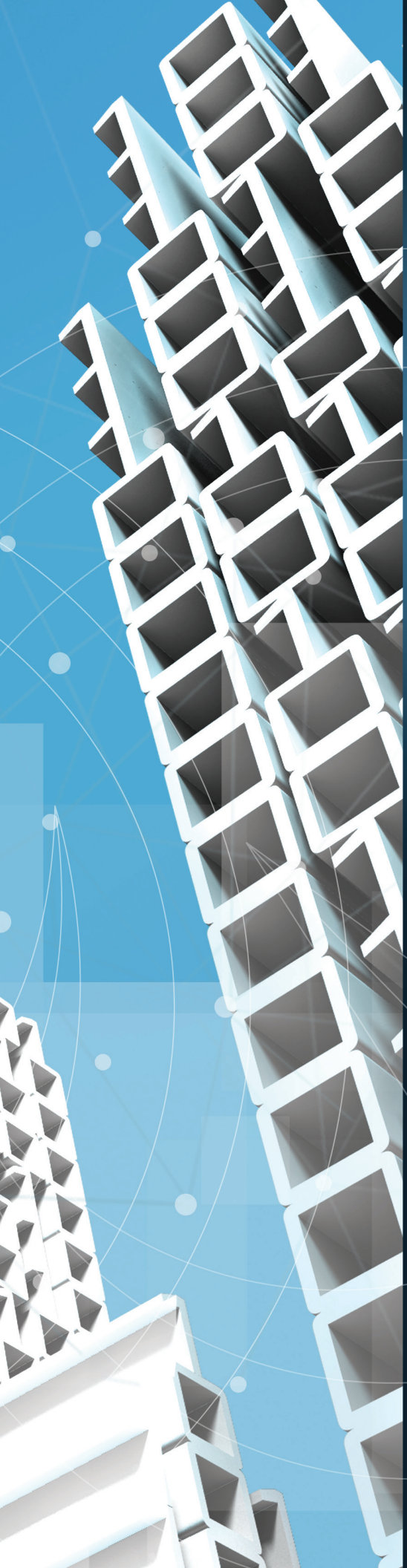

Un récapitulatif sur Websense®

Par Patrick Murray, directeur principal de la gestion des produits

MENACES PERSISTANTES AVANCÉES :

QUAND L'ÉTAT DES CRAINTES, INCERTITUDES ET DOUTES CÈDE AUX FAITS

Grâce à Websense, vous pouvez conserver une longueur d'avance sur les menaces. Depuis nos débuts en filtrage Web, nous avons analysé et classé du contenu pendant plus de 15 ans, et nous proposons aujourd'hui une solution indispensable de sécurité pour le Web, la messagerie et la DLP qui colmate les brèches laissées béantes par les logiciels de sécurité classiques.

websense®
ESSENTIAL INFORMATION PROTECTION™

« APT » (Advanced Persistent Threat, menace persistante avancée) est sur toutes les lèvres cette année, mais que signifie ce terme exactement ? Trop de battage médiatique et une certaine crainte ont voilé les faits concernant l'existence d'un réel danger pour les entreprises, quelle que soit leur taille. Les points de cet aperçu sont les suivants :

1. expliquer comment les méthodes d'APT sont appliquées aujourd'hui par les cybercriminels ordinaires,
2. analyser une attaque ciblée, et
3. offrir des solutions de défense.

Pourquoi vous devriez vous intéresser aux APT

Les grandes entreprises qui possèdent une mine d'or en matière de droits de propriété intellectuelle (comme les codes source) savent très bien qu'elles sont la cible privilégiée des cybercriminels. En revanche, les entreprises plus petites ne se font pas autant de souci : « Je suis une société de fabrication basée dans de Doubs affichant des revenus de 6 millions d'euros. Je ne pense pas que des pirates chinois ou nord-coréens vont venir frapper à ma porte. » C'est vrai, ils ne viendront pas. Mais d'autres personnes malveillantes le feront probablement.

Pour beaucoup de sociétés, les APT ne sont pas un souci majeur parce que les APT, par définition, sont habituellement utilisées par les gouvernements pour nuire aux autres gouvernements ou grands groupes. Mais les APT sont également des prototypes pour créer d'autres attaques ciblées et aujourd'hui, les entreprises de toutes sortes et de toutes tailles en sont les victimes. La réalité : la même technologie d'APT utilisée par la Chine pour pirater Google est à présent utilisée par les cybercriminels pour voler des données aux entreprises comme la vôtre.

Comment les APT s'introduisent sur le marché

Imaginez un gouvernement qui revêt un gilet pare-balles. Pour pouvoir percer ce gilet, d'autres gouvernements et agents commandités par l'état mettent en œuvre d'immenses ressources pour fabriquer des armes spécialisées qui leur permettront enfin de pénétrer l'armure. Ces armes finissent par devenir disponibles sur le marché et les criminels les utilisent pour commettre toutes sortes de crimes. La technologie des logiciels malveillants adopte ce même cycle.

Websense® Security Labs™, (laboratoire de recherche de Websense) est le leader en matière d'analyse des APT existantes et de détection des sites sur lesquels les exploits vont émerger. En savoir plus sur Security Labs.

Penchons-nous sur une APT classique, et la vitesse à laquelle ses techniques sont passées dans d'autres mains.

La durée de vie de la technologie des logiciels malveillants

Les attaques Aurora de 2009 ont été parmi les toutes premières utilisations de menaces persistantes avancées à être médiatisées. Les sociétés telles Google, Adobe et Rackspace ont été les cibles d'une APT commanditée par l'état en novembre et en décembre cette année-là. Le 12 janvier 2009, Google a annoncé qu'elle avait été attaquée. Deux jours plus tard, l'exploit « zero-day » était révélé au public. Neuf jours se sont écoulés avant que Microsoft ne corrige la vulnérabilité principale. Durant cette période, seulement 26 % des fournisseurs de logiciels anti-virus ont pu détecter l'exploit en raison de son caractère complètement nouveau. Toutefois, en l'espace d'un mois, le réseau Websense® ThreatSeeker® a détecté plus de 200 nouveaux sites Web ayant utilisé le même exploit pour délivrer d'autres logiciels malveillants. Les APT se sont propagées comme un feu de forêt, attisé par les groupes criminels organisés qui disposaient de nouvelles armes pour attaquer leurs cibles principales : les sociétés possédant des informations sur leurs clients ou des numéros de cartes de crédit, soit toutes données pouvant être rapidement utilisées pour gagner de l'argent.

Analyse d'une attaque ciblée

Comment les APT et les attaques ciblées fonctionnent-elle, au juste ? Prenons un exemple.

Avancée : les personnes malveillantes utilisent un vaste arsenal de technologies sophistiquées de collecte de l'information. L'opération débute en général des mois avant l'attaque effective contre une entreprise pour lui voler des données.

Par exemple :

- *Les personnes malveillantes s'infiltrent et s'emparent du contrôle du serveur d'une autre société (qui n'est pas la cible). Souvent cette action consiste en une injection SQL d'un ancien tableau sur une page Web qui n'est pas régulièrement actualisée, ou d'une application Web non sécurisée. Cela constituera le coup de grâce pour les données plus tard, et le chemin des données s'arrêtera là.*
- *Un morceau de code malveillant est envoyé sur le compte de messagerie personnelle d'un employé (tout en sachant que cet employé consulte son compte de messagerie personnelle au bureau). Ce logiciel malveillant va alors commencer à s'acheminer à travers le réseau et rechercher les mesures de sécurité en place. Remarque : la surveillance de la cible individuelle a débuté avant la surveillance du réseau. Souvent, la cible de ce courrier électronique est identifiée grâce à une recherche de profils sur le Web social, LinkedIn ou Facebook, à des recherches simples des cadres supérieurs sur les sites d'entreprises, etc. Dans un monde social, on trouve une pléthore d'informations disponibles concernant toute cible, ce qui rend la tâche d'ingénierie sociale bien plus aisée pour concocter un message très intéressant à envoyer à la personne intéressée dans sa langue natale, en utilisant ses goûts et ses informations pour lui donner envie d'ouvrir le message. Les personnes malveillantes sont peut-être déjà devenues « amies » et ont peut-être même conversé avec le principal intéressé sur des sites sociaux pour collecter les informations.*

Persistante : les personnes malveillantes sont tout à fait déterminées à réussir. Elles se livreront à une surveillance continue, régulière et patiente afin de déceler les vulnérabilités. Elles réitèrent leurs tentatives et changent de tactique si elles sont détectées.

- *Dans notre exemple, le logiciel malveillant a désormais identifié les informations recherchées sur le réseau et a envoyé aux personnes malveillantes des données concernant les protocoles de sécurité en place, notamment les anti-virus et l'adresse du pare-feu proxy. Les personnes malveillantes savent désormais comment s'infiltrer, et plus important encore, où se trouve probablement leur butin.*

Menace : les personnes malveillantes ont également tendance à utiliser plusieurs vecteurs d'attaque, notamment des logiciels mis au point spécifiquement et des vulnérabilités « zero-day » inconnues auparavant.

- *Dans notre exemple, nous avons déjà évoqué un morceau de code malveillant personnalisé, utilisé comme outil de surveillance. C'est maintenant au tour du code malveillant d'agir.*
- *Un nouvel e-mail est envoyé sur le compte de messagerie personnelle d'un autre employé ayant accès aux données convoitées. Il contient une grande partie de logiciel malveillant hautement sophistiqué qui sait à quels systèmes échapper, où trouver les données désirées et comment les voler sans être détecté. Le code est également polymorphe, étant capable de s'actualiser fréquemment pour ne pas être détecté par les anti-virus et autres mesures de sécurité. (Souvenez-vous que ce n'est pas un simple réseau « zombie » qui recherche des références bancaires en ligne pour vider votre compte. Ces personnes malveillantes sont plus ambitieuses. Elles veulent s'emparer des droits de propriété intellectuelle, des secrets commerciaux et d'autres données sensibles qu'elles peuvent utiliser pour vous nuire ou vous exploiter).*
- *Souvent, les données sont extirpées lentement, sans être remarquées par le personnel informatique ou l'équipe chargée de la sécurité. C'est uniquement après la survenue d'un incident séparé que les équipes chargées de la sécurité s'aperçoivent que quelque chose ne va pas dans les fichiers d'historique d'événements. C'est souvent la première fois que la connexion avec des adresses IP suspectes (vous vous rappelez de la première étape ?) est remarquée.*

Comment est-ce que Websense vous protège contre les APT et les menaces ciblées ?

Ces attaques utilisent des techniques sophistiquées et diverses qui exploitent les réseaux Web et de messagerie à la fois pour délivrer des logiciels malveillants, et se servir du même coup de ces réseaux pour en extraire des données sensibles. Souvent, le logiciel malveillant est inconnu et est conçu pour contourner tous les systèmes de défense classiques.

La solution Websense® TRITON™ unifie le Web, la messagerie et la sécurité des données pour offrir un service de sécurité diverse contre un style d'attaque diverse. Les outils d'analyse de sécurité combinés dans le Websense® Advanced Classification Engine (ACE, moteur de classification de contenu avancé), qui

constitue le cœur de la solution TRITON, passent au crible le contenu entrant et sortant d'une entreprise. La solution TRITON analyse à la fois le contexte et le contenu (y compris le code) des pages Web et des e-mails, en temps réel. Elle analyse également le contenu communiqué à l'extérieur pour s'assurer que les données sensibles ne sont pas envoyées à mauvais escient. À la différence des systèmes de défense dont le champ d'action est plus restreint, tels que les anti-virus, les filtres URL, les pare-feux, et les systèmes basés sur la réputation, la solution TRITON de sécurité diverse identifie et protège contre les menaces connues et inconnues à la fois.

Comment la solution Websense® TRITON ™ traite-t-elle mieux les APT et les menaces diverses que les autres technologies de sécurité ?

La solution de sécurité TRITON développée par Websense est la seule et véritable solution unifiée à comporter toutes les fonctions importantes suivantes :

1. **Partage d'information de sécurité :** Les outils d'analyse de sécurité diverse du Websense® Advanced Classification Engine (ACE, moteur de classification de contenu) associent une identification du logiciel malveillant et des services de protection (notamment des anti-virus de base et des filtres URL) à une inspection avancée du code, ainsi qu'à des outils d'analyse du comportement, des faits, de la réputation, ou de recherche pour traiter des menaces connues et inconnues. Ces menaces peuvent être de toutes sortes, que ce soit un virus standard, un réseau « zombie » ou un Cheval de Troie achetés, ou encore un script avancé et personnalisé qui cible une vulnérabilité dans une application ou un navigateur. ACE combine les résultats des composants de recherche individuelle (par exemple : les services de réputation, les anti-virus et l'analyse d'exploit, etc.) et prend une décision mûrie et intelligente pour savoir si le trafic doit être autorisé ou interrompu. La force du moteur ACE permet à la solution TRITON de combiner les informations à partir de nos e-mails, du Web et des technologies de sécurité pour nous aider à nous prémunir de toute intrusion par des personnes malveillantes, intrusion passant habituellement inaperçue des les systèmes de sécurité.

2. **Inspection du trafic sortant :** la plupart des technologies de sécurité classiques n'inspectent que les menaces entrantes et ignorent les communications sortantes. Toutefois, les APT et les attaques ciblées sont plus sophistiquées que des attaques classiques, et en général, réussissent mieux à pénétrer les systèmes de défense. Dans l'éventualité et au moment où ces attaques s'infiltrent dans votre réseau, il est crucial d'inspecter et de protéger les transmissions de données sortantes pour arrêter les attaques et empêcher l'extraction de vos données.

   C'est pourquoi Websense propose une surveillance du contenu sortant pour s'assurer qu'une machine infectée ne communique pas de données sensibles à l'extérieur. Websense applique une technologie de classe professionnelle de prévention contre les pertes de données (DLP) pour identifier et contrôler la communication de données sensibles sur le Web, sur votre messagerie et sur d'autres réseaux, et ce, pour garantir que ces données arrivent là où elles le doivent, et n'échouent pas entre les mains d'une personne malveillante.

La solution TRITON développée par Websense analyse également des communications cryptées, qui sont souvent utilisées dans des attaques diverses pour déguiser la transmission de données sensibles sortantes, et bloque les communications qui ne sont pas associées à des modèles SSL standards. La solution Websense® TRITON Web Security Gateway (passerelle de sécurité pour le Web) recherche également dans le trafic sortant des modèles indiquant une commande émanant de réseaux « zombie » et de centres de contrôle qui pourraient essayer de « phone home » le trafic (acte de communication illégale servant à localiser toute information ou application logicielle et à les détourner vers un autre serveur).

3. **Couverture complète, flexibilité et facilité d'utilisation :** Même si un système de sécurité propose une recherche de logiciel malveillant connu, de faits concernant un logiciel malveillant inconnu, et des contrôles de transmission des informations vers des sites hôtes pour éviter le vol des données, il subsiste toujours des failles dans le système de défense. À moins que la couverture s'étende aux dispositifs mobiles et aux succursales, ces « maillons faibles » peuvent causer une rupture de la chaîne de sécurité. À moins que la solution propose une flexibilité de déploiement (avec des solutions sur site, hébergées et/ou hybrides), il se peut qu'elle ne réponde, ne se développe ou ne s'adapte pas aux besoins d'une entreprise. Et à moins qu'elle ne soit facile à gérer, avec la précision et la simplicité d'une console de gestion unifiée, il se peut très bien qu'elle ne soit pas utilisée efficacement.

   La solution de sécurité TRITON développée par Websense est la seule et véritable solution unifiée à répondre à tous ces critères.

Conclusion : de nouvelles menaces exigent de nouvelles solutions de sécurité

Bien que les APT ne ciblent pas tout le monde, chacun doit savoir comment ces APT fonctionnent, car ces mêmes techniques sont désormais utilisées par les cybercriminels dans des attaques ciblées conçues pour voler des données sensibles aux entreprises de toutes sortes.

Pour pouvoir se défendre contre ces attaques ciblées, une nouvelle approche est nécessaire. Apprenez à vous protéger maintenant grâce aux solutions de sécurité de Websense®.