Trend Micro

NETWORK DEFENSE

La protection contre les menaces connues, inconnues et non divulguées

Votre réseau d'entreprise fait face à de profondes mutations en matière IT, à des comportements utilisateur à risque et à des menaces toujours plus sophistiquées (ransomware, vulnérabilités zero-day, attaques ciblées). Protéger votre réseau devient ainsi plus complexe.

Les outils traditionnels de cybersécurité rencontrent leurs limites au sein de cet univers IT en mutation et les technologies de sécurité déployées de manière autonome et cloisonnées cèdent souvent face au volume important et à la diversité des menaces.

Pour faire simple, nous avons segmenté l'univers des menaces en trois profils : **les menaces connues, celles qui sont inconnues et celles connues mais non divulguées**.

Les menaces connues le sont du public et des outils de sécurité. Elles sont répertoriées dans les bases de réputation et jugulées grâce à l'application de patchs. Elles font l'objet de fichiers de signatures ou sont neutralisées par des filtres spécifiques. Mais même connues, ces menaces s'immiscent parfois sur le réseau, généralement via des logiciels non patchés. En 2015, les 10 vulnérabilités les plus exploitées étaient connues depuis plus d'un an, et 48% dataient de 5 ans et plus.* Les ressources limitées pour déployer les patchs et les systèmes en fin de vie sont les principales causes de l'absence de patchs.

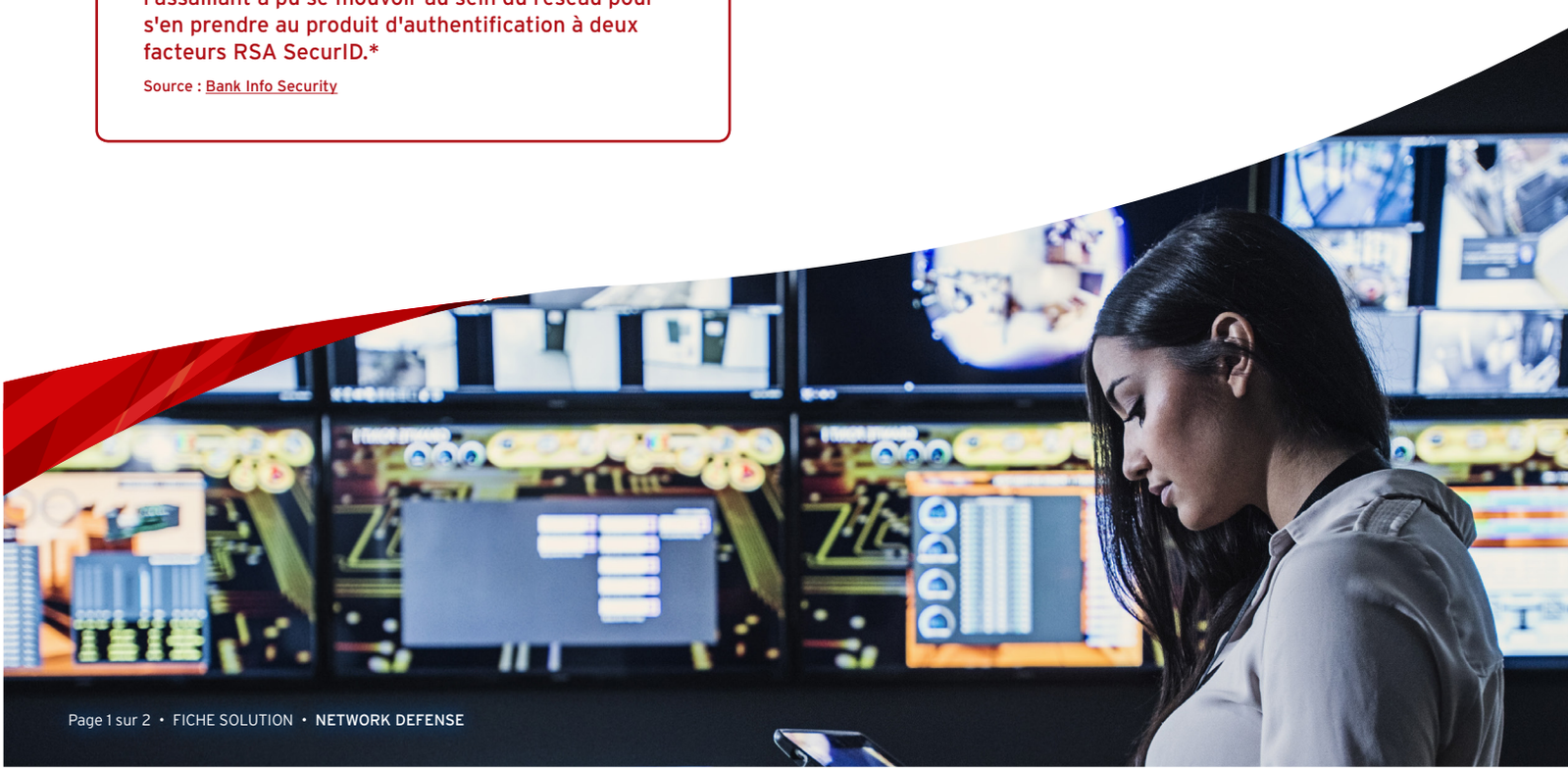
* Source : "Cyber Risk Report 2016" Hewlett Packard Enterprise, février 2016

Le ver *SQL Slammer* a exploité une vulnérabilité en janvier 2003 et infecté 75 000 victimes en 10 minutes, alors que Microsoft avait proposé un correctif six mois auparavant. Cette vulnérabilité connue s'est ainsi propagée en seulement quelques minutes, en dépit de la disponibilité d'un patch. Elle continue d'ailleurs à infecter des victimes encore aujourd'hui.

Les attaques inconnues sont souvent conçues pour cibler un seul système ou groupe restreint d'hôtes. Elles utilisent généralement de multiples vecteurs d'attaque (email, lien malveillant, téléchargement, infection d'une machine à l'autre, etc.). En 2015, un collaborateur de RSA a exécuté un fichier Excel malveillant, joint à un email indésirable. Cette action a instauré une backdoor vers Adobe Flash, et l'assaillant a pu se mouvoir au sein du réseau pour s'en prendre au produit d'authentification à deux facteurs RSA SecurID.*

Source : Bank Info Security

Les menaces inconnues sont celles qui n'ont jamais été identifiées auparavant et qui sont créées de manière spécifique pour cibler un individu ou une entreprise. Ces attaques ciblées et menaces évoluées sont personnalisées. Elles contournent les lignes de défense traditionnelles, détournent furtivement vos données sensibles ou les chiffrent avec demande de rançon à la clé.



Les vulnérabilités non divulguées sont hybrides, à la fois connues par certains chercheurs en sécurité et par l'éditeur du logiciel impacté, mais aussi inconnues du grand public. Tant que le patch logiciel n'est pas installé, les entreprises sont menacées par une exploitation potentielle de cette vulnérabilité qui offre un accès vers le réseau ou permet de mener une attaque.

L'attaque Poodle a tiré parti d'une vulnérabilité de SSL 3.0 pour pirater les réseaux d'entreprise. Cette vulnérabilité, bien qu'identifiée par une équipe de chercheurs plus de cinq mois avant d'être exploitée, restait inconnue pour la majorité des gens. Pendant cette période, ce sont de multiples réseaux d'entreprise qui étaient vulnérables.

INTÉGRER POUR MIEUX PROTÉGER

Seule une visibilité intégrale sur l'ensemble du trafic réseau permet de juguler les attaques actuelles qui exploitent les vulnérabilités du réseau pour prendre en otage ou détourner les données et communications sensibles. Trend Micro offre une prévention intégrée contre les menaces évoluées.

Trend Micro Network Defense est optimisé par la sécurité XGen™, un panel de techniques cross-générationnelles contre les menaces et de veille mondiale sur les menaces. La sécurité XGen™ protège votre réseau grâce à des technologies de sécurité **intelligentes**, **optimisées** et **interconnectées**.

Les solutions Network Defense sont **intelligentes**. Elles capitalisent sur des techniques de défense cross-générationnelles telles que l'apprentissage automatique (machine learning), le sandboxing personnalisé, l'analyse comportementale et la corrélation des contenus. Network Defense applique la technologie la plus pertinente au bon moment, activant ainsi la protection réseau la plus efficace, plutôt que de se contenter d'une approche basée sur une seule technologie. Trend Micro neutralise les menaces connues de manière rapide et accélérée, analyse et identifie les menaces inconnues et objets suspects qui entrent et sortent du réseau, ou s'y propagent en interne. Le projet Zero Day Initiative et TippingPoint Digital Vaccine® (DVLabs) offre une protection proactive contre les menaces non-déclarées, plusieurs mois en amont de leur divulgation.

Les solutions Network Defense sont **optimisées** pour fonctionner au sein des environnements clients. Elles ont été conçues pour fonctionner avec les produits de Trend Micro et avec ceux de nombreux éditeurs de sécurité positionnés sur le SIEM, la gestion des vulnérabilités, les pare-feux nouvelle-génération, le SDN, le cloud et bien d'autres.

Les solutions Network Defense font partie d'une solution **interconnectée** de défense contre les menaces, capable de partager des données de veille et disposant d'une visibilité et d'un contrôle centralisés sur les différentes couches de sécurité. Les systèmes Network Defense sont automatiquement mis à jour par les autres solutions de Trend Micro, bénéficiant ainsi d'informations à jour sur les menaces. La veille sur les menaces est alimentée par Trend Micro™ Smart Protection Network™. Smart Protection Network analyse des données en provenance du monde entier pour assurer une protection pérenne.

Trend Micro TippingPoint Next-Generation IPS (NGIPS) – Utilise un panel de technologies, comme l'inspection DPI, des services de réputation et l'apprentissage automatique pour détecter et neutraliser les menaces connues.

Trend Micro™ Deep Discovery™ – Détecte les menaces inconnues entrantes ou sortantes sur le réseau ou se déplaçant au sein de celui-ci, grâce à un monitoring de l'ensemble des ports et de plus de 100 protocoles. L'inconnu devient alors visible tandis que les informations de veille sur les menaces sont partagées avec différents outils de sécurité dont le système de prévention d'intrusion nouvelle-génération TippingPoint.

Zero Day initiative – Ce programme indépendant regroupe plus de 3 000 chercheurs en sécurité qui identifient les vulnérabilités des systèmes d'exploitation et logiciels utilisés par les entreprises ou le grand public, avant que ces vulnérabilités ne puissent être exploitées à grande échelle.

DVLabs - Offre des analyses sophistiquées sur les menaces et des filtres de sécurité contre les vulnérabilités, pour une protection évoluée contre les menaces inconnues, via un IPS nouvelle-génération.

TREND MICRO™

Securing Your Journey to the Cloud

©2018 Trend Micro Incorporated. Tous droits réservés. Trend Micro, le logo t-ball Trend Micro et Trend Micro Smart Protection Network sont des marques commerciales ou des marques déposées de Trend Micro Incorporated Les autres marques, noms de produit ou de service appartiennent à leurs propriétaires respectifs. Les informations figurant dans ce document peuvent être modifiées sans préavis. [SB01_NetworkDefense_170823FR]