Le nouveau rapport McAfee Labs d'Intel Security : seuls 42 % des professionnels de la sécurité partagent des renseignements sur les cyber-menaces

Le rapport révèle les résultats de l'enquête sur la perception de la valeur du partage des renseignements sur les menaces en entreprise et revient sur l'évolution du paysage de cyber-menaces au 4ème trimestre 2015

Faits saillants du rapport :

- *Seuls **42 % des professionnels de la sécurité consultés utilisent le partage de renseignements** sur les cyber-menaces ;*
- ***97 % des adeptes** du partage des renseignements estiment que l'échange des informations leur a permis de **renforcer la sécurité de leur entreprise** ;*
- *Parmi les professionnels interrogés, **91 % souhaitent recevoir des renseignements** sur les cyber-menaces dans leur domaine tandis que seuls **63 % seraient d'accord pour partager** les informations dont ils disposent ;*
- *McAfee Labs a constaté également **la progression de 26 % de nouveaux ransomwares** au 4ème trimestre 2015, par rapport au trimestre précédent*
- *Pour les mêmes périodes, les chercheurs ont noté **une augmentation de 72 % des nouveaux exemples de malwares mobiles***

Paris, le 22 mars 2016 – Le rapport ***McAfee Labs Threats Report: March 2016*** révèle les résultats de l'étude d'Intel Security sur l'adoption du partage des renseignements sur les cyber-menaces dans les entreprises. Le rapport passe également à la loupe les outils d'administration à distance (RAT) Adwind et détaille la progression des malwares, notamment celle des ransomwares et des malwares mobiles, au 4ème trimestre 2015.

Partage des renseignements sur les menaces en entreprise

En 2015, Intel Security a mené une enquête auprès de 500 professionnels de la sécurité en Europe, en Amérique du Nord et en région Asie-Pacifique, pour évaluer la sensibilisation des entreprises au partage des renseignements sur les menaces. Bien que les résultats de l'étude mettent en évidence l'intérêt des entreprises à la nouvelle tendance dans le domaine de la cybersécurité, l'enquête pointe du doigt les obstacles à l'adoption plus large :

- **Adoption et la valeur perçue.** Sur les 42 % des professionnels qui partagent des renseignements sur les menaces, 97 % estiment que cette pratique leur a permis de mieux protéger leur entreprise.

- **Renseignements spécifiques au secteur.** Avec une quasi-unanimité, 91 % des professionnels consultés s'intéressent à des renseignements sur les cyber-menaces, et notamment sur les menaces spécifiques à leur secteur. L'étude souligne que le secteur des services financiers et les opérateurs d'importance vitale (OIV) pourraient bénéficier le plus du partage des renseignements spécifiques, vu la grande spécialisation des menaces dans ces deux secteurs critiques.

- **Volonté de partager.** 63 % des professionnels consultés déclarent qu'ils pourraient apporter également les données dont ils disposent à condition que le partage se fasse sur un système privé et sécurisé.

- **Types de données à partager.** Les données les plus susceptibles d'être partagées concernent le comportement des malwares (72 %), la réputation des URL (58 %), la réputation d'adresses IP externes (54 %), la réputation de certificats (43 %) et la réputation de fichiers (37 %)

- **Les obstacles au partage des renseignements sur les menaces.** Au sein des entreprises qui n'ont pas adopté la pratique du partage des renseignements, les professionnels citent la politique de l'entreprise (54 %) ou encore les réglementations du secteur (24 %) comme obstacles principaux. Presqu'un quart de répondants (24%) se disent intéressés par les possibilités offertes par le partage des renseignements mais soulignent le manque de connaissances nécessaires sur le sujet. Plus d'un répondant sur cinq (21 %) craint que les informations partagées puissent permettre d'identifier l'entreprise, voire les individus qui partagent les renseignements. Ces témoignages suggèrent un manque d'expérience sur les diverses options possibles d'intégration du partage de renseignements sur les menaces, ainsi qu'un manque de compréhension sur les implications légales du partage des informations.

« Le partage des renseignements sur les menaces pourrait devenir un facteur important pour permettre aux spécialistes de cybersécurité de prendre une longueur d'avance sur les cybercriminels », déclare **Vincent Weafer, vice-président du groupe McAfee Labs d'Intel Security**. *« Mais afin que les entreprises puissent exploiter tout le potentiel de la cyber intelligence, elle doit surmonter les obstacles tels que la politique d'entreprise, les restrictions réglementaires, les risques juridiques et le manque de connaissance sur son implémentation. »*

Les outils d'administration à distance (RAT) Adwind

Le rapport trimestriel d'Intel Security inspecte également l'outil d'administration à distance (RAT) Adwind (un cheval de Troie de type « backdoor » en Java), qui cible diverses plates-formes compatibles avec les fichiers Java. En général, le RAT Adwind est propagé via des campagnes de spam qui utilisent des pièces jointes truffées de malwares, des pages web compromis et des téléchargements indésirables. Le rapport de McAfee Labs met en évidence une augmentation très rapide (426 %) du nombre d'exemples de fichiers .jar identifiés par ses chercheurs en tant qu'Adwin, passant de 1.388 au 1er trimestre 2015 à 7.295 au 4ème trimestre.

Statistiques pour le 4ème trimestre 2015

Après trois trimestres de recul, le nombre total de nouveaux exemples de malwares a repris sa progression au 4ème trimestre.

- **Les malwares rebondissent.** 42 millions de nouvelles signatures malveillantes ont été découvertes, soit 10 % de plus qu'au 3ème trimestre, et le deuxième record enregistré par McAfee Labs. Cette croissance au 4ème trimestre résulte en partie de celle des malwares mobiles, avec 2,3 millions de nouveaux exemples, soit 1 million de plus qu'au 3ème trimestre.

- **Le ransomware reprend sa progression.** Après un léger ralentissement en milieu d'année, le nouveau ransomware a repris une croissance rapide, avec une augmentation de 26 % au 4ème trimestre 2015. Les codes de ransomware en open source et le Ransomware-as-a-Service continuent de simplifier le lancement des attaques, les campagnes Teslacrypt et CryptoWall 3 continuent de progresser, et les campagnes de ransomware continuent d'être lucratives. Une analyse de CryptoWall 3 conduite en octobre 2015 a mis en évidence l'échelle financière de ces attaques : les chercheurs de McAfee Labs ont montré qu'une seule de ces campagnes a extorqué 325 millions de dollars aux victimes.

- **Le malware mobile décolle.** Le 4ème trimestre 2015 a vu une augmentation de 72 % des nouveaux exemples de malwares mobiles, dont la production semble avoir été plus rapide.

- **Les rootkits en chute libre.** Le nombre d'exemples de nouveaux rootkits a fortement chuté au 4ème trimestre, poursuivant une tendance de longue date pour ce type d'attaque. Ce déclin a débuté au 3ème trimestre 2011, et McAfee Labs l'attribue en partie à l'adoption de processeurs Intel® 64 bits ainsi que de Microsoft Windows 64 bits, dont des fonctions comme Kernel Patch Protection et Secure Boot améliorent la protection contre des menaces telles que les rootkits.

- **Les binaires malveillants signés sont sur le déclin.** Le nombre de nouveaux binaires malveillants a diminué chaque trimestre au cours de l'an passé, le 4ème trimestre 2015 atteignant le plus bas niveau depuis le 2ème trimestre 2013. McAfee Labs estime que ce déclin découle en partie du fait que les certificats plus anciens, notablement présents sur le marché noir, expirent ou sont révoqués car les entreprises passent à des fonctions de hachage plus fortes. En outre, des méthodes comme Smart Screen (qui fait partie de Microsoft Internet Explorer mais s'étend à d'autres parties de Windows) représentent des tests complémentaires de confiance, qui pourraient rendre la signature de binaires malveillants moins rentable pour les auteurs de malwares.

Pour consulter le rapport du McAfee Labs dans son intégralité, cliquez ici.

Pour découvrir des conseils pour mieux protéger votre entreprise des menaces décrites dans le rapport de McAfee Labs de ce trimestre, visitez Enterprise Blog.

A propos de McAfee Labs
McAfee Labs est l'entité spécialisée dans la recherche de menaces informatiques d'Intel Security. Elle est l'une des principales sources de référence à l'échelle mondiale en matière d'études et de renseignements sur les menaces, et les orientations stratégiques qu'il propose dans le domaine de la cyber-sécurité font autorité. Forte de plus de 400 chercheurs, son équipe rassemble des données provenant de millions de sondes et des principaux vecteurs de menaces : fichiers, Web, messagerie électronique et réseau. Elle exécute ensuite des analyses de corrélation des menaces entre vecteurs et procure, via son service de cloud McAfee Global Threat Intelligence, des renseignements en temps réel sur les menaces aux produits de sécurité McAfee hautement intégrés pour la protection des terminaux et du réseau. McAfee Labs met aussi au point des technologies de base pour la détection des menaces (profilage des applications, gestion des listes grises, etc.) qui sont incorporées dans la gamme de produits de sécurité la plus large sur le marché.

A propos d'Intel Security
McAfee fait désormais partie intégrante d'Intel Security. Avec sa stratégie de sécurité connectée, son approche novatrice en termes de sécurité matérielle avancée et son savoir-faire unique en termes de 'Global Threat Intelligence', Intel Security est fortement concentré sur le développement de solutions et de services de sécurité avant-gardistes en mesure de protéger les systèmes, les réseaux et les appareils mobiles à usage professionnel et personnel dans le monde d'aujourd'hui et de demain.
Intel Security associe l'expérience et l'expertise de McAfee à l'innovation et à la performance éprouvée d'Intel pour faire de la sécurité un élément essentiel de toute architecture et plate-forme informatique.
La mission d'Intel Security est de donner à chacun la confiance nécessaire pour vivre et travailler en toute sécurité dans le monde digital.

Contact presse
ComCorp
Caroline Pierron / Ksenia Kanareva
Tél. : 01 84 17 84 15 / 01 84 17 84 13
intelsecurity@comcorp.fr