Lumension développe les listes blanches «intelligentes» pour s'imposer sur le marché de la sécurité

Lumension annonce l'ouverture du forum IntelligentWhiteListing.com. Un site dédié au partage des connaissances autour des technologies de liste blanche, y compris avec les concurrents. *« Il vaut mieux lâcher un peu de lest pour essayer de faire passer cette approche de la sécurité que les géants du secteur ne supporteraient pas de voir arriver frontalement*, justifie Eric Naegels, dirigeant du bureau français de l'entreprise américaine. *Plus il y a de bruit autour du WhiteListing et mieux c'est pour ce marché naissant car nous ne sommes pas très nombreux. »*

Lumension a donc l'intention de jouer une carte innovante sur un marché de la sécurité qui arrive probablement à un tournant. *« Il est étonnant que les grands comptes ne se soient pas penchés plus tôt sur les technologies de liste blanche car on arrive au bout des limites de la technologie de liste noire [recherche et élimination des menaces dans le système, NDLR]. L'approche Black List est morte née car trop lourde à gérer et les risques d'infection augmentent avec les délais trop grands des mises à jour des correctifs [risques de faille 'zero day', NDLR] »*, soutient Eric Naegels.

Créé en 2007, Lumension Security construit son offre applicative autour de l'union de plusieurs technologies rachetées précédemment : SecureWave, qui se concentre sur le contrôle des applications et des périphériques, PatchLink, pour l'automatisation de la mise à jour des correctifs des éditeurs (et qui avait elle-même acquis Stat Harris (technologie de scanner réseau non intrusif utilisé par l'armée américaine) et SecuWorks qui développait des produits de gestion du risque. Au final, Lumension entend développer une offre de gestion intelligente et intégrée de sécurité de technologie sur le modèle de la liste blanche.

Deux ans de développement

Rappelons que le *white listing* consiste à ne permettre au système d'exécuter uniquement les applications validées par le responsable informatique. *« Mais si la technologie convient bien pour les postes individuels, cela devient vite ingérable sur des parcs de centaines ou milliers de machines »*, explique le dirigeant français. Le projet de Lumension consiste donc à rendre transparente la gestion de la sécurité des terminaux par liste blanche et la rendre opérationnelle. *« Nous avons travaillé pendant deux ans à intégrer plusieurs technologies et développé le concept pour rendre cette approche de White Listing possible pour toutes les organisations, des petites PME aux grands comptes »*, précise Eric Naegels.

La technologie s'appuie notamment sur le principe d'une base de données d'applications validées et signées (dans le cadre du programme Enterprise Integrated Services) sur laquelle s'appuie l'offre Lumension Intelligent Whitelisting. L'idée est de détacher cette base de Lumension pour la rendre publique et impliquer les éditeurs du marché de façon à permettre l'exécution d'au moins 80 % des applications mises à jour sur le poste de travail. *« Par exemple*, illustre le dirigeant français, *le passage d'Internet Explorer 8 à IE 9 serait accepté grâce à la présence de la signature du binaire dans la base de données publique. »* Ce qui revient à appliquer le principe des bases de signatures virales mais à

l'envers (la signature qualifie une application valide).

Cette base publique est complétée d'une base « grise » propre aux entreprises et constituée à partir des observations locales sur des applications non signées mais fréquemment utilisées. *« Sur un parc important, on retrouve des similitudes dans les exécutables, par exemple l'usage de iTunes ou Skype. La base de données intermédiaire permet à l'entreprise de faire de la corrélation entre légitimité des applications, leur pertinence et la nécessité d'arbitrer ce qui pourrait entrer dans la liste blanche ou pas. »*

Les technologies antivirales deviendront obsolètes

Lumension entend également se distinguer par la simplicité de sa solution qui se résumera à une seule offre technologique. Le contrôle des listes blanches s'effectuera depuis une même interface qui intégrera également la gestion antivirale, l'antimalware, les patches de sécurité, et le contrôle des périphériques. Cette dernière fonction passera par une technologie proche du DLP (*data leak prevention*). *« Le contrôle des périphériques est un sous domaine du DLP*, explique Eric Naegels, *il n'y a pas de notion de vérification des contenus sur le réseau. Le DLP est plus large que le contrôle de périphériques mais bien plus complexe à administrer. »* Une seule console pour tout contrôler, donc.

Reste qu'il est légitime de s'interroger sur la pertinence d'un anti virus/malware dans Lumension Intelligent Whitelisting puisque celle-ci se limite à l'exécution des applications « garanties » (et, de fait, interdira le lancement des agents malveillants). *« L'antivirus est nécessaire pour éventuellement nettoyer les systèmes avant l'installation des règles de White Listing »*, précise le responsable qui pense qu'à termes, les technologies antivirales deviendront obsolètes. *« Les grands éditeurs de sécurité cherchent à préserver leur business sur les technologies antivirales*, renchérit-il, *ils préparent la deuxième phase de leur stratégie en basculant sur des technologies plus pro-actives. La meilleure preuve est le rachat de McAfee par Intel qui vise, à long terme, à intégrer dans le chipset les technologies de liste blanche. Mais personne n'a réussi à implémenter le White Listing de manière efficace à ce jour. »*

D'où la carte qu'entend jouer Lumension sur un marché relativement vierge. L'éditeur démarrera prochainement un programme d'*early adopters* auprès de quelques comptes parmi ses 5100 clients dans le monde (avec des solutions installées sur plus de 20 millions de machines) pour valider la nouvelle approche technologique. La version finale de Intelligent WhiteListing est attendue pour avril 2011. Elle devrait être suivie, dès juin, d'une seconde version, enrichie de la notion de vérification des chemins de confiance des binaires afin d'automatiser l'intégration dans les listes blanches des applications installées depuis un site légitime (par exemple Apple.com pour iTunes). *« L'idée est vraiment de rendre transparente et opérationnelle la sécurité par liste blanche »*, résume Eric Naegels.