

Pour se protéger des fuites de données orchestrées via des logiciels de vols d'informations, il faut avant tout comprendre le mode opératoire des pirates et connaître les différentes formes de surveillance des données.

Par **Justin Peltier**

Le pirate informatique et le braqueur de banque ont beaucoup en commun. Tous deux commencent par une reconnaissance de la cible potentielle. Pour le braqueur, il s'agira de se rendre sur place pour se faire une idée précise des lieux.

Le pirate, quant à lui, emploie

différentes techniques de collecte de données, telles que le piratage Google, en vue de pénétrer dans un ordinateur. Il effectue ensuite un scan des ports à distance afin de cerner les divers points d'accès possibles à l'ordinateur.

Une fois que les ports ont été identifiés, l'étape suivante consiste à chercher les failles des applications

ouvertes découvertes par le scan de ports. Le pirate, alors paré pour l'assaut, lance un exploit contre un système vulnérable.

L'idéal, évidemment, serait un système ne présentant pas la moindre faille. Mais à l'échelle d'une entreprise, déceler chaque faille relève de l'impossible.

Trend Micro LeakProof



Fournisseur Trend Micro
Contact www.trendmicro.com

Le produit proposé par Trend Micro est une appliance tout-en-un munie d'un éventail d'options complet. La seule chose que l'administrateur ait à faire est de configurer le dispositif. Pour

la configuration initiale, il suffit de raccorder un câble d'alimentation, un clavier avec port PS/2 et un câble VGA au dispositif.

Le système d'exploitation sous-jacent est un système Linux mais la configuration s'effectue entièrement par l'intermédiaire de menus, sans lignes de commandes à saisir. Une fois l'installation initiale terminée, la machine dispose d'une adresse IP propre et vous pouvez configurer le dispositif à l'aide d'un protocole http, https ou ssh.

Dans la plupart des environnements, un ingénieur participe

à l'installation de LeakProof. L'ingénieur a pour rôle principal d'aider l'entreprise à définir précisément les informations sensibles et les sources éventuelles de danger. Des modèles prédéfinis de stratégies sont disponibles, pour les lois américaines SOX et GLBA, par exemple. Ces règles peuvent être personnalisées ou établies à l'aide d'une interface d'assistance.

Le logiciel côté client est très bien conçu et fonctionne sans icône dans la barre d'état système.

Il est possible de supprimer ou de désactiver le client à l'aide d'une technologie anti-rootkit, mais la console d'administration signale immédiatement que le système est hors ligne et notifie l'administrateur système.

La principale difficulté avec cette solution consiste à envoyer le client sur chaque ordinateur client. Le programme peut être converti en fichier msi et distribué à l'aide de SMS sur Zenworks ou tout autre package de déploiement de logiciels grand public.

LeakProof offre plusieurs moyens de protéger les données, dont une fonctionnalité pour les documents sensibles.

Plutôt que de joindre une signature numérique, ce programme de prévention des fuites de données utilise des regroupements de lettres en plusieurs points du document pour créer l'empreinte digitale, ce qui accélère le traitement de la sécurité.

LeakProof est capable de bloquer les activités suspectes et d'avertir

les utilisateurs. Il peut également rediriger les utilisateurs vers le site de l'entreprise relatif à l'utilisation d'Internet. Enfin, la solution offre une fenêtre permettant aux utilisateurs de justifier les actions qu'ils entreprennent.

La documentation se présente sous la forme d'un fichier PDF composé de sous-sections facilitant la consultation. L'assistance est offerte gratuitement la première année suivant l'acquisition du produit et peut être prolongée, voire complétée par d'autres options comme l'assistance 24 h/24, 7 j/7, moyennant supplément.

LA NOTE SC MAGAZINE

Caractéristiques	★★★★★
Performances	★★★★★
Simplicité d'utilisation	★★★★★
Documentation	★★★☆☆
Assistance	★★★★☆
Rapport qualité/prix	★★★★★
NOTE GÉNÉRALE	★★★★★

Point fort Un produit simple d'utilisation, extrêmement efficace, aux fonctions tellement nombreuses qu'elles ne peuvent pas toutes être présentées ici

Point faible Un déploiement du logiciel client ardu, nécessitant une planification méticuleuse

Verdict Un produit solide avec un logiciel côté client très bien conçu pour un prix très attractif. Notre conseil d'achat



Un produit solide avec un logiciel côté client très bien conçu pour un prix très attractif.

Justin Peltier



Contact :