

IBM Trusteer Apex : bloque, arrête les cyber-attaques dues aux actes malveillants

Logiciel

Posté par : JPilo

Publié le : 23/5/2014 11:30:00

IBM s'attaque aux programmes malveillants avancés grâce à un logiciel de protection étendu aux postes de travail. IBM lance un nouveau logiciel de sécurité qui permet de bloquer les menaces directement à l'endroit le plus fragile : les postes de travail, ordinateurs portables et de bureau sont des cibles vulnérables aux programmes malveillants.

Trusteer Apex est un élément clé du système de protection contre les menaces (Threat Protection System) annoncé ce mois-ci par IBM. Le logiciel Trusteer Apex associe les renseignements fournis par la sécurité intelligente avec l'analyse comportementale afin d'aller au-delà des anti-virus et pare-feux traditionnels. Il bloque les attaques et rompt la chaîne des processus d'exfiltration.

Les menaces avancées s'attaquent aux entreprises à un rythme accablant et génèrent des coûts de plus en plus élevés. Selon l'étude de l'Institut Ponemon commandée par IBM Trusteer concernant les menaces persistantes avancées, une violation de données causée par ce type de menaces représente 9,4 millions de dollars en valeur intrinsèque pour la réputation d'une marque.

La même étude indique que les attaques ciblées sont la plus grande menace et seulement 31% des répondants pensent avoir les ressources suffisantes pour les prévenir, les détecter et les contenir. Les entreprises sont confrontées à une multitude de produits qui ne fournissent pas une protection complète et posent des problèmes d'exploitabilité. Les applications Java sont particulièrement visées et comportent un risque élevé car d'ordinaire elles sont partie intégrante de l'environnement de l'entreprise.

Le logiciel de protection des postes de travail, Trusteer Apex, bloque les cybercriminels tentant d'exploiter les vulnérabilités des terminaux informatiques pour exfiltrer des données. C'est un outil d'analyse automatique des menaces, plus facile à déployer et à exploiter permettant une plus grande efficacité des équipes de sécurité informatique.

Le nouveau logiciel Trusteer Apex d'IBM bloque et éteint les attaques sur les postes de travail. Les principales fonctionnalités de ce nouveau logiciel sont les suivantes :



Utilisation de défenses multi-couches

Ces défenses utilisent différentes méthodes pour briser la chaîne d'attaques. IBM a identifié les goulots d'étranglement stratégiques sur lesquels les cybercriminels focalisent leur attention, contrôlent le poste de travail de l'utilisateur et l'infectent. Par exemple, Java est la cible de la moitié des attaques de vulnérabilités.

À

Selon le rapport du second trimestre 2014 IBM X-Force, 96% des utilisations de Java sont applicatives, permettant ainsi aux applications Java malveillantes de passer inaperçues. Apex stoppe les attaques intégrées dans le code Java et les verrouille afin d'empêcher les dommages pouvant être causés à l'entreprise. Trusteer Apex prévient l'exécution des applications Java malveillantes en évaluant la confiance en l'application, le risque lié à l'activité et interdit les applications non autorisées.

Défense contre le vol d'identifiants de l'entreprise

En dépit d'une meilleure information de l'utilisateur final, il y a encore des cas où les employés ouvrent des emails qui semblent être inoffensifs, mais qui sont en fait des attaques de phishing non identifiées comme spams. Si un e-mail de phishing est ouvert par un gardien, Trusteer Apex peut identifier les logiciels malveillants et cesser leur exécution sur le poste de travail.

Trusteer Apex empêche également les employés de réutiliser leurs identifiants d'entreprise sur les sites web qui ne respectent pas la politique de l'entreprise. Par exemple, si un nouvel employé met en place un e-mail et un mot de passe pour accéder au site de l'entreprise, et qu'il tente d'utiliser le même mot de passe sur Facebook ou un autre réseau social, Trusteer Apex l'empêche.

Réduire la charge des équipes de sécurité informatique

Les entreprises peuvent se charger de l'analyse de l'activité potentiellement suspecte via le service d'analyse IBM/Trusteer, ce qui peut les aider à identifier les activités suspectes et formuler des recommandations en matière de protection. Le service rassemble les menaces spécifiques pour une entreprise et les aide à prendre des contre-mesures.

IBM s'appuie également sur le flux d'intelligence dynamique générée par plus de 100 millions de terminaux protégés, soit une base de données qui contient plus de 70 000 vulnérabilités classifiées. Cette recherche des menaces et cette analyse intelligente se traduisent par des mises à jour de sécurité qui sont automatiquement envoyées aux terminaux protégés.

«Grâce à des recherches approfondies, IBM a identifié les étapes spécifiques de la chaîne d'attaque où les cyber-criminels ont plusieurs options pour exécuter leur contenu malveillant.», déclare Yaron Dycian, Vice-président Products and Services à Trusteer, une société IBM. «Les solutions actuelles du marché offrent des protections faibles contre les vecteurs d'attaques spécifiques et créent une importante charge de travail pour les équipes de sécurité informatique d'aujourd'hui chargées, ce qui rend difficile de parer aux menaces. Notre technologie de goulot d'étranglement stratégique offre une nouvelle approche pour briser le cycle de vie de la menace et prévenir les cyber-attaques.»

Par exemple, un acteur majeur de la santé publique a récemment déployé Trusteer Apex sur plus de 20.000 terminaux pour protéger les données sensibles des patients. Apex a détecté plus de 100 infections à haut risque, en dépit de l'existence d'une solution anti-

virus et d'un pare-feu de nouvelle génération initialement mis en place au sein de l'entreprise. Apex a réduit ces infections avec un impact opérationnel minimal, et a permis à l'équipe de sécurité informatique d'analyser les événements et de trouver une solution.

L'approche multi-couches d'IBM avec Trusteer Apex permet également :

- Interrompre la chaîne d'exploitation malveillante - Apex surveille les principales méthodes utilisées par les cybercriminels pour installer des logiciels malveillants et les bloque.
- De bloquer la communication malveillante - Pour compromettre les terminaux informatiques, prendre le contrôle et exfiltrer les données, les logiciels malveillants de pointe doivent communiquer avec le cybercriminel, Trusteer Apex empêche les canaux de communication issus d'un terminal en dehors du réseau de l'entreprise.
- D'offrir une nouvelle intégration avec IBM QRadar et IBM Endpoint Manager, permettant ainsi une gestion et une sécurité accrue du poste de travail