Communiqués de presse

IBM s'attaque aux programmes malveillants avancés grâce à un logiciel de protection étendu aux postes de travail

Trusteer Apex permet de bloquer et d'arrêter les cyber attaques dues aux actes malveillants

Paris - 22 mai 2014: IBM (NYSE : 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 Apexest 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 s'accélérant 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 désormais 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 efficience 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 vulnérabilité. 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 mégarde, 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’en empêche.

Réduire la charge des équipes de sécurité informatique

Les entreprises peuvent se décharger 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 généré 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 déjà très 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 :

· D'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

# # #

IBM Tackles Advanced Malware with Expanded Endpoint Protection Software
Trusteer Apex Helps Block and Shut Down Cyber Attacks that Begin with Malware Exploits

ARMONK, N.Y. - 21, May 2014: IBM (NYSE: IBM <http://www.ibm.com/investor/>) announced new security software that helps stop threats at the weakest link, the endpoint, including laptops and desktops which are

most susceptible to malware. IBM's Trusteer Apex <http://securityintelligence.com/redefining-endpoint-protection-advanced-threats> software is the newest offering in the company's Threat Protection System <http://www-03.ibm.com/press/us/en/pressrelease/43824.wss> announced earlier this month, which leverages security intelligence and behavioral analytics to go beyond traditional anti-virus approaches and firewalls to disrupt attacks across the entire attack chain — from break-in to exfiltrate.

Advanced threats <http://www.ibm.com/security/threat-protection/> are attacking organizations at an alarming and ever more costly rate. Data breaches caused by such threats have cost on average $9.4 million in brand equity alone per an IBM Trusteer-commissioned Ponemon <http://securityintelligence.com/media/2014-ponemon-study-economic-impact-advanced-persistent-threats-apts/> study on Advanced Persistent Threats. The same study says targeted attacks are the greatest threat with only 31 percent of respondents believing adequate resources are available to prevent, detect and contain these threats. Organizations are faced with a myriad of point products that do not provide complete protection and also create manageability challenges. Java applications are particularly targeted and carry a high risk as a pervasive part of the corporate environment.

The **Trusteer Apex** endpoint protection software blocks attempts by cyber criminals to exploit vulnerabilities on the endpoint that lead to data breaches. It provides an easy to deploy automated threat analysis capability to prevent attacks that is less burdensome than the many, disparate point solutions in the market. Since the product is easy to manage and maintain, it helps the Chief Security Officer and the IT Security team be more resourceful and effective.

IBM's new Trusteer Apex software blocks attacks and shuts them down when they occur on the endpoint. New capabilities include:

Employing Multi-layered Defenses

These defenses combine several methods to break the attack chain. IBM has identified strategic chokepoints where cybercriminals focus their attention, take hold of a user's endpoint and infect it with malware. For example, Java is the target of half of the application vulnerability attacks. Per the IBM X-Force <http://www-03.ibm.com/security/xforce/> Q2 2014 report, 96 percent of Java exploits are applicative, meaning rogue Java applications that are not controlled.

Trusteer Apex can stop attacks that are embedded into Java applications and lock them from wreaking havoc on the enterprise. Trusteer Apex prevents malicious Java applications through assessing application trust and activity risk, and blocking untrusted apps from doing high-risk activities.

Stopping Theft of Sensitive Corporate Credentials

Despite the best end user education, there are still cases where employees open emails that appear to be legitimate but are actually spear phishing attacks that do not always go to spam folders. If a phishing email is inadvertently opened, Trusteer Apex can identify there is malware and stop it from exploiting the endpoint.

Trusteer Apex also prevents employees from re-using corporate credentials on untrusted sites that are against corporate policy. For example, a new employee sets up an email and password to access corporate sites. If the employee tries to use the same password on Facebook or other social networks, Trusteer Apex stops it.

Reducing the Ongoing Burden on IT Security Teams

Organizations can offload the analysis of potentially suspicious activity to the IBM/Trusteer threat analysis service, which can help an organization assess suspicious activities and provide protection recommendations. The service looks at an organization's specific threats and helps them take action on them.

IBM also has a dynamic intelligence feed from more than 100 million protected endpoints – a database that has more than 70,000 vulnerabilities categorized. This threat research and intelligence is translated into security updates that are automatically sent to protected endpoints.

"Through extensive research, IBM has identified specific stages of the attack chain where cyber criminals have relatively few options to execute their malicious content," said Yaron Dycian, Vice President of Marketing, Products & Services at Trusteer, an IBM company. "Current point solutions in the market offer narrow protections against specific attack vectors and create significant workload on overstretched security teams, making it difficult to manage against cyber threats. Our strategic chokepoint technology introduces a fresh approach for breaking the threat lifecycle and preempting cyber attacks."

An example of this approach is a major healthcare provider that recently deployed Trusteer Apex on more than 20,000 endpoints to protect sensitive patient data. Apex detected more than 100 high-risk infections, despite the existence of an anti-virus solution and a next-generation firewall. Apex mitigates these infections with minimal operational impact, and provides the IT Security team with event analysis and solution tuning.

The IBM Trusteer Apex multi-layered approach also:

· Disrupts the exploit chain – Attackers must gain persistency of their malware on the endpoint. Apex monitors the key methods used by attackers to install malware by exploiting vulnerabilities and blocks those methods.
· Blocks malicious communication – To compromise the endpoint, gain control and exfiltrate data, advanced malware must communicate with the attacker, often through a command and control server. Trusteer Apex prevents untrusted communication channels from the endpoint outside of the corporate network.
· Offers new integration with IBM QRadar <http://www-03.ibm.com/software/products/en/subcategory/security-intelligence> and IBM Endpoint Manager.

About IBM Security
IBM's security portfolio provides the security intelligence to help organizations holistically protect their people, data, applications and infrastructure. IBM offers solutions for identity and access management, security information and event management, database security, application development, risk management, endpoint management, next-generation intrusion protection and more. IBM operates one of the world's broadest security research and development, and delivery organizations. IBM monitors 15 billion security events per day in more than 130 countries and holds more than 3,000 security patents. For more information, please visit www.ibm.com/security<http://www.ibm.com/security>, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog <http://securityintelligence.com/> .