Communiqués de presse

L’équipe sécurité d’IBM ajoute la biométrie comportementale cognitive pour aider à protéger de la cybercriminalité les clients du secteur bancaire

Une nouvelle technologie Trusteer pour aider à prévenir la fraude bancaire

PARIS - 27 oct. 2016: IBM (NYSE: IBM) a annoncé aujourd’hui de nouvelles capacités d'analyse biométriques comportementales dans sa technologie de prévention de la fraude bancaire numérique, IBM Security Trusteer Pinpoint Detect, qui utilise de l’analytique et du machine learning brevetés pour la détection cognitive temps réel de la fraude. Les nouvelles capacités biométriques comportementales incluent l’utilisation du machine learning pour aider à comprendre la façon dont les utilisateurs interagissent avec les sites web des banques, en créant des modèles d’utilisation basés sur les modèles de mouvements d’une souris qui deviennent de plus en plus précis au fil du temps.

Selon IBM’s X-Force Research, les services financiers sont un des trois premiers secteurs visés par la cyber-criminalité1. En fait, près de 20 millions de données financières ont été compromisesen 20152.

Par exemple, des logiciels malveillants tels que GozNym Trojan, découvert récemment par l’équipe de recherche X-Force, utilisent des attaques de redirection dans lesquelles un client peu méfiant est détourné vers un faux site sur lequel on lui demande de saisir ses informations bancaires pour que l’attaquant puisse les voler.

Avec IBM Security Trusteer Pinpoint Detect, les banques peuvent aider à identifier qu’un utilisateur non-autorisé tente de se connecter à un compte client, à prévenir des transactions frauduleuses, et à déterminer quand des terminaux sont infectés par des logiciels malveillants très dangereux. IBM Security Trusteer Pinpoint Detect, qui utilise une technologie développée en partenariat avec le centre d’excellence en cybersécurité d’IBM de l’université de Bengurion en Israël, est conçu pour construire facilement des modèles de gestes en temps réel et confronter ces modèles de biométrie comportementale à des comportements d’utilisateurs et des schémas de fraude connus. En même temps, il rassemble des renseignements sur les menaces et adapte automatiquement la protection, fournissant aux institutions financières des niveaux de réponse personnalisables.

A propos d’IBM Security

IBM Security propose un portefeuille de solutions de sécurité pour les entreprises parmi les plus avancés et les plus intégrés. Ce portefeuille est supporté par IBM X-Force, organisation de recherche connue mondialement et

permet aux organisations de gérer efficacement les risques et de se défendre contre les menaces émergentes. IBM dispose d'une organisation de recherche et développement et de mise en œuvre parmi les plus importantes au monde, gère 35 milliards d'événements de sécurité par jour dans plus de 130 pays et possède plus de 3000 brevets de sécurité.

Pour plus d'informations : www.ibm.com/security/fr/fr

Blog US : www.securityintelligence.com

Suivez notre actualité sur Twitter @IBMSecurityFR

1 IBM Cyber Security Intelligence Index, 2016

2 IBM X-Force Interactive Security Incidents

###

IBM Security Adds Cognitive Behavioral Biometrics to Help Protect Banking Customers from Cybercrime

New Trusteer Technology to Help Prevent Bank Fraud

ARMONK, NY -- October 27, 2016 -- IBM (NYSE: IBM) today announced new behavioral biometric analysis capabilities in its digital banking fraud prevention technology, IBM Security Trusteer Pinpoint Detect, using patented analytics and machine learning for real-time cognitive fraud detection. The new behavioral biometric capabilities incorporate the use of machine learning to help understand how users interact with banking websites, creating gesture models based on patterns of mouse movements that become increasingly more accurate over time.

Through cognitive analysis of the gesture models, IBM Security Trusteer Pinpoint Detect can help determine when unauthorized users try to take over a bank account using stolen credentials by detecting anomalies from the real customer's interaction with a banking website. The technology understands the context and meaning of subtle mouse movements and clicks, and uses this information to develop increasingly more accurate gesture models through machine learning.

According to IBM's X-Force Research, financial services is one of the top three targeted industries for cybercrime.1 In fact, nearly 20 million financial records were breached in 2015.2 Cybercrime organizations continue to develop malware and social engineering techniques to target financial websites and customers, typically with the goal of obtaining credentials to take over user accounts.

For example, malware like the GozNym Trojan, recently found by IBM's X-Force Research team, uses redirection attacks where an unsuspecting customer is hijacked to a fake site where they are made to enter their banking credentials for the hacker to steal. These fake websites are set up by criminals to look precisely like the bank's site, including the correct URL and SSL certificate in the address bar. Once the criminal has those credentials, they log in as the user and attempt to move as much money as possible through fraudulent transactions.

With IBM Security Trusteer Pinpoint Detect, banks can help spot when an unauthorized user is attempting to log into a customer account, help prevent fraudulent transactions, and determine when devices are infected with high-risk malware. Using technology developed in partnership with the IBM Cyber Security Center of Excellence at Ben-Gurion University, Israel, IBM Security Trusteer Pinpoint Detect is designed to seamlessly build gesture models in real-time and analyze these behavioral biometric patterns against learned user behavior and known fraud patterns. At the same time, it gathers threat intelligence and adapts protection automatically, providing financial institutions with customizable levels of response.

The new behavioral biometric analysis features of IBM Security Trusteer Pinpoint Detect enable real-time risk assessment based on gesture modeling. When users access their online banking site, IBM Security Trusteer Pinpoint Detect is designed to collect user behavior, detect potential device spoofing, identify access with compromised credentials, and correlates various other device attributes. Through the addition of cognitive fraud detection, IBM Security Trusteer Pinpoint Detect is designed to also provide real-time evaluation of behavioral biometric indicators – with no additional costs, entitlements, or implementation requirements.

"Given enough time and resources, cybercriminals can defeat passwords and security questions," said Ravi

Srinivasan, Vice President, Strategy, IBM Security. “Behavioral biometrics is about what the user does, not what the user knows. IBM Security Trusteer Pinpoint Detect now can now better differentiate real users from fraudsters using gesture models, giving banks and other organizations the power to protect the interests of their customers, and ultimately determine the sources of financial fraud.”

IBM Security Trusteer Pinpoint Detect protects hundreds of global financial institutions and banking websites against account takeover and fraudulent transactions and helps detect end user machines infected with high risk malware. IBM intends for customers to start receiving the behavioral biometric and cognitive fraud detection capabilities at no additional charge via system updates as early as December 2016. Learn more about IBM Security Trusteer Pinpoint Detect and behavioral biometrics here.

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world’s broadest security research, development and delivery organizations, monitors 35 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, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

1 IBM Cyber Security Intelligence Index, 2016

2 IBM X-Force Interactive Security Incidents