Communiqués de presse

Dernier rapport IBM X-Force 2012 : des menaces accrues sur les navigateurs et les réseaux sociaux

Paris, Europe-France - 21 sept. 2012: IBM (NYSE: IBM) publie aujourd'hui les résultats de l'étude X-Force portant sur la première moitié de l'année 2012. L'étude témoigne d'une forte augmentation des problèmes liés à l'exploitation de failles dans les navigateurs. Elle s'inquiète également une nouvelle fois de la sécurité des mots de passe utilisés sur les médias sociaux et de la subsistance de grandes disparités entre les modèles de mobiles et les programmes mis en place (ou non) par les entreprises pour exploiter ce phénomène du Bring Your Own Device (BYOD).

***

IBM X-Force 2012 Mid-Year Trend and Risk Report: Browsers, Social Media Show Emerging Threat Activity

New global security operations center in Wroclaw, Poland helps clients stay ahead of threats

ARMONK, N.Y. - 21 Sep 2012: IBM (NYSE: IBM) today released the results of its X-Force 2012 Mid-Year Trend and Risk Report, which shows a sharp increase in browser related exploits, renewed concerns around social media password security, and continued disparity in mobile devices and corporate "bring your own device" (BYOD) programs.

To further protect its clients regionally from emerging threats like those reported in the IBM X-Force Mid-Year Trend and Risk Report, IBM is announcing the opening of a security operations center in Wroclaw, Poland. This newest IBM Security Operations Center is the 10th worldwide center to help clients proactively manage these threats, including real-time analysis early warning notification of security events. A principal source of information for the bi-annual X-Force report comes from IBM's security operations centers which monitor more than 15 billion security events a day on behalf of more than 3,700 clients in more than 130 countries.

"Companies are faced with a constantly evolving threat landscape, with emerging technologies making it increasingly difficult to manage and secure confidential data," said Kris Lovejoy, General Manager, IBM Security Services." A security breach--whether from an outside attacker or an insider--can impact brand reputation, shareholder value and expose confidential information. Our team of security threat analysts aggressively track and monitor emerging threats to better help our clients stay ahead of emerging threats."

New Attack Surfaces with Equal Opportunity Exploits

Since the last X-Force Trend and Risk Report, IBM’s X-Force has seen an increase in malware and malicious Web activities:

· A continuing trend for attackers is to target individuals by directing them to a trusted URL or site which has been injected with malicious code. Through browser vulnerabilities, the attackers are able to install malware on the target system. The Websites of many well-established and trustworthy organizations are still susceptible to these types of threats.

· The growth of SQL injection, a technique used by attackers to access a database through a website, is keeping pace with the increased usage of cross-site scripting and directory traversal commands.

· As the user base of the Mac operating system continues to grow worldwide, it is increasingly becoming a target of Advanced Persistent Threats (APTs) and exploits, rivaling those usually seen on Windows platforms.

“We’ve seen an increase in the amount of sophisticated and targeted attacks, specifically on Macs and social networking website passwords,” said Clinton McFadden, senior operations manager for IBM X-Force research and development. "In response, organizations must take proactive approaches to better protect their enterprises and data, because as long as these cyber-attacks remain lucrative, the attacks will keep coming."

Emerging Trends in Mobile Security

While there are reports of exotic mobile malware, most smart phone users are still most at risk of premium SMS (short message service, or texting) scams. These scams work by sending SMS messages to premium phone numbers in a variety of different countries automatically from installed applications. There are multiple scam infection approaches for this:

· An application that looks legitimate in an app store but only has malicious intent

· An application that is a clone of a real application with a different name and some malicious code

· A real application that has been wrapped by malicious code and typically presented in an alternative app store

One game-changing transformation is the legitimization of Bring Your Own Device (BYOD) programs. Many companies are still in their infancy in adapting policies for allowing employees to connect their personal laptops of smartphones to the company network. To make BYOD work within a company, a thorough and clear policy should be in place before the first employee-owned device is added to the company's infrastructure. See full IBM X-Force Mid-Year Trend and risk Report for guidance on BYOD policies.

What is a Secure Password?

The connection between websites, cloud-based services, and webmail provides a seamless experience from device to device, but users need to be cautious about how these accounts are connected, the security of their password, and what private data has been provided for password recovery or account resetting. The best recommendation is to use a lengthy password comprised of multiple words instead of an awkward combination of characters, numbers and symbols.

On the server-side, X-Force recommends encrypting passwords to the database using a hash function that is suitable for password storage. The hash function should be computationally expensive to calculate and use a salt value for each user account which limits the effectiveness of 'rainbow tables' and brute force dictionary attacks.

Improvements in Internet Security Continue

As reported in the 2011 IBM X-Force Trend and Risk Report, there is progress in certain areas of Internet security. There is a continuing decline in exploit releases, improvements from the top ten vendors on patching vulnerabilities and a significant decrease in the area of portable document format (PDF) vulnerabilities. IBM believes that this area of improvement is directly related to new technology of sandboxing provided by the Adobe Reader X release.

Sandboxing technology, a technique for security analysts to isolate an application from the rest of the system so that when an application is compromised, the attacker code running within the application is limited to what it can do or access, is proving to be a successful investment from a security perspective. In the X-Force report, there was a significant drop in Adobe PDF vulnerability disclosures during the first half of 2012. This development coincides nicely with the adoption of Adobe Reader X, the first version of Acrobat Reader released

with sandboxing technology.

IBM Expands Global Security Operations Centers

Today’s announcement of the opening of the Wroclaw, Poland IBM security operations center is part of IBM’s significant investment in growth markets. IBM is looking to tap into Poland’s highly educated workforce to attract and develop the latest security skills, which is important given the shortage of in-house skills needed to effectively guard against security threats.

The new Wroclaw security operations center has trained security analysts using the managed security service X-Force Protection System to monitor and react to various customer threats.

In addition to threat analysis, the Wroclaw center delivers a full range of services including device management and health monitoring.

"IBM is actively investing in growth markets around the world - creating new facilities and opening new branches to get us closer to the best sources of talent and revenue," said Anna Sienko, Country General Manager, IBM Poland & Baltics. "IBM is home to some of the most advanced computing skills in the world - the staff of our new security operations center in Wroclaw will join a global team of security experts with unparalleled expertise and experience at helping organizations better understand and respond to the security threats to their business."

Poland’s strategic central European position is advantageous in assisting global clients, particularly in Europe and North America. In addition to the new security operations center, IBM opened a Global Delivery Center in Wroclaw in 2010 and recently announced the opening of new branch offices in the cities of Krakow, Poznan, Wroclaw and Katowice as it extends its presence far beyond the country’s capital Warsaw.

"Like other countries, Poland is seeing increasing security threats from the adoption of new and existing technologies. Because cyber security is important to national and commercial stability, it's imperative to develop skills and resources locally to help combat this issue, said POLISH OFFICIAL. "Security research skills and insights like those that come from IBM's X-Force reports help us devise the right proactive approach to deal with emerging threats.”

IBM operates nine other global security operations centers in Atlanta, Georgia; Detroit, Michigan; Boulder, Colorado; Toronto, Canada; Brussels, Belgium; Tokyo, Japan; Brisbane, Australia; Hortolandia, Brazil, and Bangalore, India, all servicing clients from points across the globe. All of the centers are designed to ensure that mission-critical systems, electrical systems, data processing and communication links are protected from any single point of failure.

About the IBM X-Force Trend and Risk Report

The IBM X-Force Trend and Risk Report is an annual assessment of the security landscape, designed to help clients better understand the latest security risks, and stay ahead of these threats. The report gathers facts from numerous intelligence sources, including its database of more than 68,000 computer security vulnerabilities, its global Web crawler and its international spam collectors, and the real-time monitoring of 15 billion events every day for nearly 4,000 clients in more than 130 countries. These 15 billion events monitored each day – more than 150,000 per second – are a result of the work done in IBM's 10 global security operations centers, which is provided as a managed security service to clients. To view the full X-Force 2012 Mid-Year Trend and Risk Report please visit www.ibm.com/security/xforce.

About IBM Security

With nearly 50 years of security development and innovation, IBM has breadth and depth in security research, products, services and consulting. IBM has nine worldwide research labs innovating security technology and 10 security operations centers around the world to help global clients maintain an appropriate security posture. IBM Managed Security Services delivers the expertise, tools and infrastructure clients need to secure their information assets from constant Internet attacks, often at a fraction of the cost of in-house security resources. The Institute for Advanced Security is IBM’s global initiative the help organizations better understand and respond to the security threats to their business. Visit the Institute community at www.instituteforadvancedsecurity.com.

For more information on IBM Security Solutions, please visit: www.ibm.com/security.