Communiqués de presse

Rapport X-Force : L'année 2011 montre une amélioration dans la lutte contre les menaces, mais les pirates s'adaptent !

Paris - 22 mars 2012: Aujourd'hui, IBM publie les résultats de son rapport X-Force sur les tendances et les risques 2011. Ce rapport montre des améliorations surprenantes dans de nombreux domaines de sécurité de l'Internet, telles qu'une diminution des vulnérabilités dans les applications, des codes d'exploitation ainsi que des spams.

Ainsi, le rapport indique que les criminels sont aujourd'hui contraints de repenser leur tactique pour cibler encore plus des anachronismes, ou des spécificités d'infrastructures ainsi que les technologies émergentes telles que les réseaux sociaux et les appareils mobiles.

IBM publie ce rapport X-Force chaque année pour décrire l'état global de la sécurité et les principales menaces auxquelles les clients sont confrontés. Le rapport est fondé sur le suivi et l'analyse d'une moyenne de 15 milliards d'événements de sécurité quotidiens (provenant des Services Managés de Sécurité d'IBM) en 2011, ainsi que d'autres sources.

Voici quelques-unes des principales menaces qui ont émergé en 2011 :

§ **Une augmentation de 19% dans le nombre de codes d'exploitation délivrés publiquement**, pouvant être utilisés afin de s'attaquer aux appareils mobiles - qui puisent de plus en plus dans les informations d'entreprises, du fait de la tendance du « Bring Your Own Device » (BYOD).

§ **Une hausse des tentatives de phishing, et d'usurpation d'identité sur les réseaux sociaux** ainsi que les services de courrier colis pour inciter les victimes à cliquer sur des liens menant à des pages web susceptibles d'infecter leur ordinateur par le biais de malwares.

§ **Une hausse des recherches automatisées de mots de passe**, basées sur l'emploi de mots de passe à faible degré de sécurité ou hors des politiques de sécurité, dirigées vers des serveurs de Secure Shell (SSH) au deuxième semestre 2011.

§ **Les attaques ciblant des vulnérabilités d'injection vers des Shell Command ont se sont multipliées par 2 voire 3** – alors que le nombre lié aux vulnérabilités d'Injection SQL dans les applications web publique a chuté de 46% cette année.

IBM propose ses conseils à ses clients pour lutter contre ces nouvelles menaces, mais aussi les services et solutions à utiliser pour y remédier.

Le rapport intégral est disponible ici : www.ibm.com/security/xforce.

####

IBM X-Force Report: 2011 Shows Progress Against Security Threats But Attackers Adapt

Emerging Attack Trends include Mobile Exploits, Automated Password Guessing, a Surge in Phishing and Shell Command Injection Attacks

ARMONK, N.Y. – 22 March 2012: IBM [NYSE:IBM] today released the results of its X-Force 2011 Trend and Risk Report, which shows surprising improvements in several areas of Internet security such as a reduction in application security vulnerabilities, exploit code and spam. As a result, the report suggests attackers today are being forced to rethink their tactics by targeting more niche IT loopholes and emerging technologies such as social networks and mobile devices.

The X-Force 2011 Trend and Risk Report revealed a 50 percent decline in spam email compared to 2010; more diligent patching of security vulnerabilities by software vendors, with only 36 percent of software vulnerabilities remaining unpatched in 2011 compared to 43 percent in 2010; and higher quality of software application code, as seen in web-application vulnerabilities called cross site scripting half as likely to exist in clients' software as they were four years ago.

In light of these improvements, it seems attackers are adapting their techniques. The report uncovers a rise in emerging attack trends including mobile exploits, automated password guessing, and a surge in phishing attacks. An increase in automated shell command injection attacks against web servers may be a response to successful efforts to close off other kinds of web application vulnerabilities.

The IBM X-Force 2011 Trend and Risk Report is based on intelligence gathered by one of the industry's leading security research teams through its research of public vulnerability disclosures findings from more than 4,000 clients, and the monitoring and analysis of an average of 13 billion events daily in 2011.

"In 2011, we've seen surprisingly good progress in the fight against attacks through the IT industry's efforts to improve the quality of software," said Tom Cross, manager of Threat Intelligence and Strategy for IBM X-Force. "In response, attackers continue to evolve their techniques to find new avenues into an organization. As long as attackers profit from cyber crime, organizations should remain diligent in prioritizing and addressing their vulnerabilities."

According to the report, there are positive trends as it appears companies implemented better security practices in 2011:

§ **Thirty percent decline in the availability of exploit code** – When security vulnerabilities are disclosed, exploit code is sometimes released that attackers can download and use to break into computers. Approximately 30 percent fewer exploits were released in 2011 than were seen on average over the past four years. This improvement can be attributed to architectural and procedural changes made by software developers that help make it more difficult for attackers to successfully exploit vulnerabilities.

§ **Decrease in unpatched security vulnerabilities** – When security vulnerabilities are publicly disclosed, it is important that the responsible software vendor provide a patch or fix in a timely fashion. Some security vulnerabilities are never patched, but the percentage of unpatched vulnerabilities has been decreasing steadily over the past few years. In 2011 this number was down to 36 percent from 43 percent in 2010.

§ **Fifty percent reduction in cross site scripting (XSS) vulnerabilities due to improvements in software quality** - The IBM X-Force team is seeing significant improvement in the quality of software produced by organizations that use tools like IBM AppScan OnDemand service to analyze, find, and fix vulnerabilities in their code. IBM found XSS vulnerabilities are half as likely to exist in customers' software as they were four years ago. However, XSS vulnerabilities still appear in about 40 percent of the applications IBM scans. This is still high for something well understood and able to be addressed.

§ **Decline in spam** – IBM’s global spam email monitoring network has seen about half the volume of spam email in 2011 that was seen in 2010. Some of this decline can be attributed to the take-down of several large spam botnets, which likely hindered spammers’ ability to send emails. The IBM X-Force team witnessed spam evolve through several generations over the past seven years as spam filtering technology has improved and spammers have adapted their techniques in order to successfully reach readers.

Attackers Adapt Their Techniques in 2011

Even with these improvements, there has been a rise in new attack trends and an array of significant, widely reported external network and security breaches. As malicious attackers become increasingly savvy, the IBM X-Force documented increases in three key areas of attack activity:

§ **Attacks targeting shell command injection vulnerabilities more than double -** For years, SQL injection attacks against web applications have been a popular vector for attackers of all types. SQL injection vulnerabilities allow an attacker to manipulate the database behind a website. As progress has been made to close those vulnerabilities – the number of SQL injection vulnerabilities in publicly maintained web applications dropped by 46 percent in 2011– some attackers have now started to target shell command injection vulnerabilities instead. These vulnerabilities allow the attacker to execute commands directly on a web server. Shell command injection attacks rose by two to three times over the course of 2011. Web application developers should pay close attention to this increasingly popular attack vector.

§ **Spike in automated password guessing** – Poor passwords and password policies have played a role in a number of high-profile breaches during 2011. There is also a lot of automated attack activity on the Internet in which attacks scan the net for systems with weak login passwords. IBM observed a large spike in this sort of password guessing activity directed at secure shell servers (SSH) in the later half of 2011.

§ **Increase in phishing attacks that impersonate social networking sites and mail parcel services** – The volume of email attributed to phishing was relatively small over the course of 2010 and the first half of 2011, but phishing came back with a vengeance in the second half, reaching volumes that haven't been seen since 2008. Many of these emails impersonate popular social networking sites and mail parcel services, and entice victims to click on links to web pages that may try to infect their PCs with malware. Some of this activity can also be attributed to advertising click fraud, where spammers use misleading emails to drive traffic to retail websites.

Emerging Technologies Create New Avenues for Attacks

New technologies such as mobile and cloud computing continue to create challenges for enterprise security.

§ **Publicly released mobile exploits rise 19 percent in 2011** – This year's IBM X-Force report focused on a number of emerging trends and best practices to manage the growing trend of "Bring your Own Device," or BYOD, in the enterprise. IBM X-Force reported a 19 percent increase over the prior year in the number of exploits publicly released that can be used to target mobile devices. There are many mobile devices in consumers' hands that have unpatched vulnerabilities to publicly released exploits, creating an opportunity for attackers. IT managers should be prepared to address this growing risk.

§ **Attacks increasingly relate to social media** - With the widespread adoption of social media platforms and social technologies, this area has become a target of attacker activity. IBM X-Force observed a surge in

phishing emails impersonating social media sites. More sophisticated attackers have also taken notice. The amount of information people are offering in social networks about their personal and professional lives has begun to play a role in pre-attack intelligence gathering for the infiltration of public and private sector computing networks.

§ **Cloud computing presents new challenges** - Cloud computing is moving rapidly from emerging to mainstream technology, and rapid growth is anticipated through the end of 2013. In 2011, there were many high profile cloud breaches affecting well-known organizations and large populations of their customers. IT security staff should carefully consider which workloads are sent to third-party cloud providers and what should be kept in-house due to the sensitivity of data. Cloud security requires foresight on the part of the customer as well as flexibility and skills on the part of the cloud provider. The IBM X-Force report notes that the most effective means for managing security in the cloud may be through Service Level Agreements (SLAs) because of the limited impact that an organization can realistically exercise over the cloud computing service. Therefore, careful consideration should be given to ownership, access management, governance and termination when crafting SLAs. The IBM X-Force report encourages cloud customers to take a lifecycle view of the cloud deployment and fully consider the impact to their overall information security posture.

"Many cloud customers using a service worry about the security of the technology. Depending upon the type of cloud deployment, most, if not all, of the technology is outside of the customer's control," said Ryan Berg, IBM Security Cloud Strategist. "They should focus on information security requirements of the data destined for the cloud, and through due diligence, make certain their cloud provider has the capability to adequately secure the workload."

IBM continues to work with its clients to step up security to address these new areas. Recommendations for helping clients improve the security of their IT department in light of these new threats include: performing regular security assessments; segmenting sensitive systems and information; training end users about phishing and spear phishing and secure computing principals in general, as well as examining the policies of business partners.

To view the full X-Force 2011 Trend and Risk Report and watch a highlight video please visit www.ibm.com/security/xforce

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 50,000 computer security vulnerabilities, its global Web crawler and its international spam collectors, and the real-time monitoring of 13 billion events every day for nearly 4,000 clients in more than 130 countries. These 13-billion events monitored each day – more than 150,000 per second – are a result of the work done in IBM's nine global Security Operations Centers, which is provided as a managed security service to clients.

About IBM Security

With more than 40 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 nine 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