Communiqués de presse

Le rapport X-Force d'IBM révèle que les problèmes de sécurité sur les terminaux mobiles vont doubler en 2011

Mise en lumière et émergence de nouvelles infractions de plus en plus sophistiquées; IBM ouvre un nouvel Institut pour la Sécurité Avancée (IAS) en zone Asie/Pacifique.

Paris - 30 sept. 2011: IBM publie les résultats de son rapport semestriel *X-Force 2011 sur les tendances et les risques en matière de cybercriminalité*. Ce rapport dépeint un paysage sécuritaire très changeant, caractérisé par des attaques de plus en plus élaborées, une croissance des vulnérabilités au niveau des terminaux mobiles et des menaces plus sophistiquées comme le "Whaling". Pour aider ses clients à combattre ces dites menaces et tous les autres problèmes de sécurité qui peuvent se présenter, IBM ouvre l'*Institut pour la Sécurité Avancée* pour la zone Asie/Pacifique, qui rejoint les Instituts IBM déjà implantés en Amérique du Nord et en Europe.

Situé en première ligne dans la lutte pour la sécurité, l'équipe X-force d'IBM joue un véritable rôle de vigie pour des milliers de clients IBM en étudiant les techniques d'attaque et en travaillant à la création de défenses proactives, avant même que beaucoup de vulnérabilités ne soient révélées. Ce rapport de mi-année *sur les tendances et les risques en matière de cybercriminalité*repose sur les résultats de la recherche IBM centrée sur les failles de sécurité du domaine public ainsi que sur le contrôle et l'analyse au quotidien de 12 milliards d'événements de sécurité, et ce depuis le début de 2011.

****

IBM X-Force Report Reveals Mobile Security Exploits to Double in 2011

New High-Profile Breaches Spotlight Emerging Threats; IBM Opens New Institute for Advanced Security in Asia Pacific

ARMONK, N.Y. - 30 Sep 2011: IBM (NYSE: IBM) today released the results of its X-Force 2011 Mid-Year Trend and Risk Report, which demonstrates the rapidly changing security landscape characterized by high-profile attacks, growing mobile vulnerabilities and more sophisticated threats such as “whaling.” To help clients combat these and other security issues, IBM is opening the Institute for Advanced Security for Asia Pacific, which joins the IBM Institutes in North America and Europe

Poised at the frontline of security, the IBM X-Force team serves as the eyes and ears for thousands of IBM clients – studying security attack techniques and creating defenses before many vulnerabilities are even announced. The X-Force Mid-Year Trend and Risk Report is based on intelligence gathered through IBM’s research of public vulnerability disclosures as well as the monitoring and analysis of an average of 12 billion security events daily since the beginning of 2011.

Mobile Exploits on Track to Double

Adoption of mobile devices such as smartphones and tablets in the enterprise, including the “Bring Your Own Device” approach, which allows personal devices to access the corporate network, is raising new security concerns. IBM X-Force has documented a steady rise in the disclosure of security vulnerabilities affecting these devices. X-Force research recommends that IT teams consistently employ anti-malware and patch management software for phones in enterprise environments. Key findings include:

- X-Force is projecting that the year 2011 will see twice the number of mobile exploit releases that occurred in 2010. X-Force has observed that many mobile phone vendors do not rapidly push out security updates for their devices;
- Malicious software targeting mobile phones is often distributed through third-party app markets. Mobile phones are an increasingly attractive platform for malware developers as the sheer size of the user base is growing rapidly, and there is an easy way to monetize mobile phone infections. Malware distributors can set up premium texting (SMS messaging) services that charge users that text to a specific number. Malware then sends text messages to those premium numbers from infected phones; and
- Some mobile malware is designed to collect end user’s personal information. This data could then be used in phishing attacks or for identity theft. Mobile malware is often capable of spying on victim's personal communications as well as monitoring and tracking their physical movements via the GPS capabilities common in these phones.

"For years, observers have been wondering when malware would become a real problem for the latest generation of mobile devices," said Tom Cross, manager of Threat Intelligence and Strategy for IBM X-Force. "It appears that the wait is over."

Critical Vulnerabilities Triple in 2011

The X-Force team reports that the percentage of critical vulnerabilities has tripled thus far in 2011. X-Force is declaring 2011 the “Year of the Security Breach” due to the large number of high-profile attacks and network compromises that have occurred this year. There is a cadre of notable emerging threats from this year’s breaches:

- Teams of professional attackers motivated by a desire to collect strategic intelligence have been able to gain and maintain access to critical computer networks through a combination of stealth, sophisticated technical capabilities and careful planning. These attackers are often referred to as Advanced Persistent Threats (APTs);
- The success of APTs has raised the profile of “whaling,” a type of spear phishing which targets ”big fish,” or those positioned in high levels of an organization with access to critical data. These targeted attacks are often launched after careful study of a person’s online profiles has armed an attacker with the information needed to create a compelling phishing email that the victim will be fooled into clicking on;
- Attacks from ‘hacktivist’ groups, who targeted web sites and computer networks for political ends rather than just financial gain. Hacktivist groups have been successful in using well known, off-the-shelf attack techniques such as SQL Injection, which is one of the most common attack techniques seen in the Internet; and
- Anonymous proxies have more than quadrupled in number compared to three years earlier. Anonymous proxies are a critical type of website to track, because they allow people to hide potentially malicious intent.

“The rash of high-profile breaches this year highlights the challenges organizations often face in executing their security strategy," said Cross. "Although we understand how to defend against many of these attacks on a technical level, organizations don't always have the cross-company operational practices in place to protect themselves."

Advances in Security Highlighted

Although the X-Force team declared 2011 as a watershed in high-profile security breaches, the report also uncovered some improvements in areas of computer security that show headway in the fight against crime on the Internet.

- The first half of 2011 saw an unexpected decrease in web application vulnerabilities, from 49 percent of all vulnerability disclosures down to 37 percent. This is the first time in five years X-Force has seen a decrease;
- High and critical vulnerabilities in web browsers were also at their lowest point since 2007, despite an increasingly complex browser market. These improvements in web browser and application security are important as many attacks are targeted against those categories of software;
- As major botnet operators are taken down and off-line by law enforcement officials, the report shows a trend in the decline of spam and more traditional phishing tactics;
- After years of consistent spam growth until the middle of 2010, there has been a significant decline in spam volumes in the first half of this year; and
- In the first half of 2011, the percentage of spam that is phishing on a weekly basis was less than 0.01 percent. Traditional phishing has greatly declined from the levels X-Force was seeing prior to the middle of 2010.

Also of note, the SQL Slammer Worm has been one of the most common sources of malicious packets on the Internet since its appearance and naming by the IBM X-Force team in 2003, but it has fallen down the list after a dramatic disappearance observed in March 2011. The most recent analysis strongly suggested that the SQL Slammer Worm's disappearance is due to an unknown source or actor. The analysis showed that a time-based trigger using a Slammer's server clock was used to shut it down, proving that it was disabled by a single cause.

Traditional Vulnerabilities Still a Problem

The X-Force report uncovered numerous attacks that target traditional security vulnerabilities. According to the report, attacks on weak passwords are commonplace on the Internet, as are attacks that leverage SQL Injection vulnerabilities in web applications to compromise backend databases. Databases have become an important target for attackers. Critical data used to run organizations—including financial/ERP, customer, employee, and intellectual property information such as new product designs—is stored in relational databases. IBM researchers tested almost 700 web sites—from the Fortune 500 and other most popular sites—to uncover that 40 percent of these contain a class of security issues referred to as client-side JavaScript vulnerabilities. The existence of vulnerabilities like these in so many corporate web sites is indicative of the security blindspots in many organizations.

IBM Launches Institute for Advanced Security in Asia Pacific

To help combat security risks and to foster collaboration amongst security industry leaders, IBM is launching the IBM Institute for Advanced Security in Asia Pacific in order to combat growing security threats in the region. The IBM Mid-Year X-Force report states that top countries originating spam have shifted to Asia Pacific, with India sending out roughly 10 percent of all spam registered today, and South Korea and Indonesia also making the top five list. This Institute joins its predecessors in Brussels, Belgium and Washington, D.C., focused on European and U.S. clients respectively.

About the IBM X-Force Team and the Trend and Risk Report

This report comes from IBM's X-Force team, the premier security research organization within IBM that has catalogued, analyzed and researched more than 50,000 vulnerability disclosures since 1997. 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. It is the result of the work done in IBM's nine global Security Operations Centers, which is provided as a managed security service to clients. The report gathers facts from numerous intelligence sources, including its database of computer security vulnerabilities, global web crawler, international spam collectors, and the real-time monitoring of an average of 12 billion security events every day for nearly 4,000 clients in more than 130 countries.

With nearly 50 years of security development and innovation, IBM is the only company with the breadth and depth of research, products, services, consulting and global business partners to deliver end-to-end security.

To access the report, visit here. For more information on IBM Security Solutions,
visit: www.ibm.com/security/landscape.html