Communiqués de presse

Sécurité informatique : Rapport X-Force IBM 2010, une année d'attaques ciblées et sophistiquées

Le rapport souligne des attaques plus ciblées (phishings, spams et mobiles), alors que la sécurité dans le cloud poursuit son évolution

Paris - 31 mars 2011: IBM dévoile aujourd'hui les résultats de son rapport X-Force 2010 sur les risques et tendances. Celui-ci révèle que les organisations publiques et privées partout dans le monde ont du faire face au cours de l'année 2010 à des menaces personnalisées de plus en plus sophistiquées. S'appuyant sur l'ensemble des informations issues des publications sur les failles de sécurité ainsi que sur celles relatives à la surveillance et à l'analyse de plus de 150 000 cas de failles par seconde chaque jour en 2010, les observations majeures fournies par l'équipe de chercheurs X-Force mettent en évidence les conclusions suivantes : • l'enregistrement par IBM de plus de 8 000 nouvelles vulnérabilités, soit une augmentation de 27% par rapport à 2009. Les rapports publics montrent également une augmentation de 21% entre 2009 et 2010. Ces données témoignent d'un environnement toujours plus menaçant dans lequel des attaques sophistiquées sont lancées contre des systèmes informatiques de plus en plus complexes • le volume de spams historiquement en hausse s'est stabilisé vers la fin de l'année. Cette tendance indiquerait que les « spammers » trouvent moins d'intérêt à accroître le volume des spams qu'à se focaliser sur le contournement des filtres de sécurité • on constate globalement une baisse sensible des attaques en mode « phishing », en revanche le « spear phishing », une technique d'attaque plus ciblée, a pris de l'importance en 2010. Une autre indication montrant que les cyber criminels sont désormais plus concentrés sur la qualité de leurs attaques que sur la quantité • pour finir, l'adoption des smartphones et autres appareils mobiles s'est accrue. Pour les départements de sécurité informatique, trouver la bonne manière d'intégrer de façon fiable ces appareils dans les réseaux d'entreprise est une bataille quotidienne. Bien que les attaques contre les dernières générations d'appareils mobiles n'aient pas crû sensiblement en 2010, les données X-Force montrent, sur ces appareils, une augmentation des failles de vulnérabilité et de leur exploitation

IBM X-Force Report: 2010 Marked a Year of Sophisticated, Targeted Security Attacks

Latest report identified more targeted phishing, spam and mobile attacks, while cloud security continued to evolve

ARMONK, N.Y., March 31, 2011 – IBM (NYSE: IBM) today released results from its annual X-Force 2010 Trend and Risk Report, highlighting that public and private organizations around the world faced increasingly sophisticated, customized IT security threats in 2010.

Based on the intelligence gathered through research of public vulnerability disclosures, and the monitoring and analysis of more than 150,000 security events per second during every day of 2010, key observations from the IBM X-Force Research team included:

· More than 8,000 new vulnerabilities were documented, a 27 percent rise from 2009. Public exploit releases were also up 21 percent from 2009 to 2010. This data points to an expanding threat landscape in

which sophisticated attacks are being launched against increasingly complex computing environments.

· The historically high growth in spam volume leveled off by the end of 2010. This indicates that spammers may be seeing less value from increasing the volume of spam, and instead are focused on making sure it is bypassing filters.

· While overall there were significantly fewer phishing attacks relative to previous years, “spear phishing,” a more targeted attack technique, grew in importance in 2010. This further indicates that cyber criminals have become more focused on quality of attacks, rather than quantity.

· As end user adoption of smartphones and other mobile devices increased, IT security departments have struggled to determine the right way to bring these devices safely into corporate networks. Although attacks against the latest generation of mobile devices were not yet widely prevalent in 2010, IBM X-Force data showed a rise in vulnerability disclosures and exploits that target these devices.

“From Stuxnet to Zeus Botnets to mobile exploits, a widening variety of attack methodologies is popping up each day,” said **Tom Cross, threat intelligence manager, IBM X-Force.** “The numerous, high profile targeted attacks in 2010 shed light on a crop of highly sophisticated cyber criminals, who may be well-funded and operating with knowledge of security vulnerabilities that no one else has. Staying ahead of these growing threats and designing software and services that are secure from the start has never been more critical.”

In conjunction with this year’s report, IBM is launching the IBM Institute for Advanced Security in Europe to combat growing security threats in the region. The IBM X-Force report stated that in 2010, nearly a quarter of all financial phishing emails targeted banks located in Europe. It also identified the UK, Germany, Ukraine and Romania among the top 10 countries sending spam in 2010. This Institute joins its predecessor in Washington, D.C., focused on U.S. clients.

A new section in the IBM X-Force Trend and Risk Report is dedicated to the security trends and best practices for the emerging technologies of mobile devices and cloud computing.

Cloud Computing -- The report highlighted a shift in perception about cloud security as adoption continued to evolve and knowledge around this emerging technology increased. Since security is still considered an inhibitor to cloud adoption, cloud providers must earn their customers' trust. This is achieved by providing an infrastructure that is secure by design with purpose-built security capabilities that meet the needs of the specific applications moving into the cloud. As more sensitive workloads move into the cloud, the security capabilities will become more sophisticated. Over time, IBM predicts the market will drive the cloud to provide access to security capabilities and expertise that is more cost effective than in-house implementations. This may turn questions about cloud security on their head by making an interest in better security a driver for cloud adoption, rather than an inhibitor.

Mobile Devices -- Organizations are increasingly concerned about the security implications of personal mobile devices used by employees. Organizations must ensure control of their data regardless of where it is, including employee-owned or business-issued smartphones. In 2010, IBM X-Force documented increases in the volume of vulnerabilities disclosed in mobile devices as well as the disclosure of exploits that target them. The desire to "jailbreak" or "root" mobile devices has motivated the distribution of mature exploit code that has been reused in malicious attacks. Nevertheless, malware is not yet common on the latest generation of mobile devices and most IT professionals view the data stored on them and how that can be misused or lost as the main security threats associated with these devices. According to the IBM X-Force Report, best practices for mobile security are evolving with enhanced password management and data encryption capabilities.

Additional trends highlighted in the report included:

The new, sophisticated face of cyber crime -- From a security standpoint, 2010 is most remembered as a year marked by some of the most high profile, targeted attacks that the industry has ever witnessed. For example, the Stuxnet worm demonstrated that the risk of attacks against highly specialized industrial control systems is not just theoretical. These types of attacks are indicative of the high level of organization and funding behind computer espionage and sabotage that continues to threaten a widening variety of public and private networks.

A significant decline in phishing -- If the IT security world is looking for a victory to chalk up in 2010, they should consider the relative decline in phishing attacks. Although phishing attacks still occurred, the peak volume of phishing emails in 2010 was less than a quarter of the peak volumes in the previous two years. This may indicate a shift toward other, more profitable, attack methodologies such as botnets and ATM skimming. Despite this decline, spear phishing, a more targeted attack technique, grew in importance in 2010, as meticulously crafted emails with malicious attachments or links became one of the hallmarks of sophisticated attacks launched against enterprise networks.

Spam volumes peaked, and then leveled off -- In 2010, spam volumes increased dramatically, reaching their highest levels in history. However, the growth in volume leveled off by the end of the year. In fact, by year's end, spammers seemed to go on vacation, with a 70 percent decline in traffic volumes occurring just before Christmas and returning early in the new year. Has the market for spam become saturated? It is possible that there are diminishing returns associated with increasing the total volume of spam, and we are starting to see spammers focus more on bypassing spam filters.

Web applications accounted for nearly half of vulnerabilities disclosed in 2010 -- Web applications continued to be the category of software affected by the largest number of vulnerability disclosures, representing 49 percent in 2010. The majority represented cross site scripting and SQL injection issues, and the IBM X-Force data showed that these vulnerabilities are being targeted by attackers. According to the report results, every summer for the past three years there has been a globally scaled SQL injection attack some time during the months of May through August. The anatomy of these attacks has been similar across the board, targeting .asp pages that are vulnerable to SQL injection.

A secure by design approach can improve security -- IBM X-Force has determined that taking proactive

steps to evaluate web application security and improve development and quality assurance processes can result in a significant improvement in the security of web application software. The report included data showing that web applications scanned for vulnerabilities often showed significant improvements upon being retested – exhibiting less than half of the number of particular classes of vulnerabilities, on average, the second time they are assessed. This encouraging information points the way toward sustained improvements in Internet security.

Nearly half of vulnerabilities remain unpatched -- To help prevent attackers from exploiting vulnerabilities, organizations must focus on shortening the window of time between vulnerability disclosure and patch installation. Forty-four percent of all security vulnerabilities had no vendor-supplied patch at the end of 2010. However, even in cases where patches are made available on the same day that a vulnerability is publicly disclosed, there may be a significant gap in time before those patches are installed on vulnerable systems. Computer criminals often privately develop exploits that target publicly disclosed security vulnerabilities, and use those exploits to launch attacks. Later, when these private exploits have ceased to be valuable as attack tools, they are publicly disclosed. The IBM X-Force report data showed that exploits are often publicly disclosed tens or hundreds of days after the vulnerabilities they target. If it is taking a long time for these exploits to surface, it may be taking a long time for networks to patch.

Continued growth of Internet botnets -- IBM X-Force saw an upward trend in Trojan botnet activity during 2010. This growth is significant because despite increasing coordinated efforts to shut down botnet activity, this threat appeared to be gaining momentum. However, IBM X-Force's data did illustrate the dramatic impact of a successful effort in early 2010 to shutdown the Waledac botnet, which resulted in an instantaneous drop off in observed command and control traffic. On the other hand, the Zeus botnet continued to evolve and constituted a significant portion of the botnet activity detected by IBM X-Force in 2010. Due to its extreme popularity with attackers, there are hundreds, or even thousands, of separate Zeus botnets active at any given time. The Zeus botnet malware is commonly used by attackers to steal banking information from infected computers.

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 over 50,000 computer security vulnerabilities, its global Web crawler and its international spam collectors, and the real-time monitoring of 13-billion security 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 (SOC), which is provided as a Managed Security Service to clients.

With more than 40 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. IBM has nine worldwide research labs innovating security technology and nine security operations centers around the world to help global clients maintain the appropriate security posture.

To access the report, visit: http://www-03.ibm.com/security/landscape.html. For more information on IBM Security Solutions, visit: www.ibm.com/security and http://www-03.ibm.com/press/us/en/presskit/33537.wss. To learn more about the IBM Institute for Advanced Security, visit: http://www.instituteforadvancedsecurity.com/.