

Symantec Report Finds Cyber Threats Skyrocket in Volume and Sophistication

Targeted attacks, social networking threats, mobile device security and the proliferation of attack toolkits are top growing trends to watch in today's threat landscape

MOUNTAIN VIEW, Calif. – April 5, 2011 – Symantec Corp. (Nasdaq: SYMC) today announced the findings of its Internet Security Threat Report, Volume 16, which shows a massive threat volume of more than 286 million new threats last year, accompanied by several new megatrends in the threat landscape.

The report highlights dramatic increases in both the frequency and sophistication of targeted attacks on enterprises; the continued growth of social networking sites as an attack distribution platform; and a change in attackers' infection tactics, increasingly targeting vulnerabilities in Java to break into traditional computer systems. In addition, the report explores how attackers are exhibiting a notable shift in focus toward mobile devices.

2010: The Year of the Targeted Attack

Targeted attacks such as Hydraq and Stuxnet posed a growing threat to enterprises in 2010. To increase the likelihood of successful, undetected infiltration into the enterprise, an increasing number of these targeted attacks leveraged zero-day vulnerabilities to break into computer systems. As one example, Stuxnet alone exploited four different zero-day vulnerabilities to attack its targets.

In 2010, attackers launched targeted attacks against a diverse collection of publicly traded, multinational corporations and government agencies, as well as a surprising number of smaller companies. In many cases, the attackers researched key victims within each corporation and then used tailored social engineering attacks to gain entry into the victims' networks. Due to their targeted nature, many of these attacks succeeded even when victim organizations had basic security measures in place.

While the high-profile targeted attacks of 2010 attempted to steal intellectual property or cause physical damage, many targeted attacks preyed on individuals for their personal information. For example, the report found that data breaches caused by hacking resulted in an average of more than 260,000 identities exposed per breach in 2010, nearly quadruple that of any other cause.

Social Networks: A Fertile Ground for Cybercriminals

Social network platforms continue to grow in popularity and this popularity has not surprisingly attracted a large volume of malware. One of the primary attack techniques used on social networking sites involved the use of shortened URLs. Under typical,

legitimate, circumstances, these abbreviated URLs are used to efficiently share a link in an email or on a web page to an otherwise complicated web address. Last year, attackers posted millions of these shortened links on social networking sites to trick victims into both phishing and malware attacks, dramatically increasing the rate of successful infection.

The report found that attackers overwhelmingly leveraged the news-feed capabilities provided by popular social networking sites to mass-distribute attacks. In a typical scenario, the attacker logs into a compromised social networking account and posts a shortened link to a malicious website in the victim's status area. The social networking site then automatically distributes the link to news feeds of the victim's friends, spreading the link to potentially hundreds or thousands of victims in minutes. In 2010, 65 percent of malicious links in news feeds observed by Symantec used shortened URLs. Of these, 73 percent were clicked 11 times or more, with 33 percent receiving between 11 and 50 clicks.

Attack Toolkits Focus on Java

In 2010, attack toolkits, software programs that can be used by novices and experts alike to facilitate the launch of widespread attacks on networked computers, continued to see widespread use. These kits increasingly target vulnerabilities in the popular Java system, which accounted for 17 percent of all vulnerabilities affecting browser plug-ins in 2010. As a popular cross-browser, multi-platform technology, Java is an appealing target for attackers.

The Phoenix toolkit was responsible for the most Web-based attack activity in 2010. This kit, as well as many others, incorporates exploits against Java vulnerabilities. The sixth highest ranked Web-based attack during the reporting period was also an attempt to exploit Java technologies.

The number of measured Web-based attacks per day increased by 93 percent in 2010 compared to 2009. Since two-thirds of all Web-based threat activity observed by Symantec is directly attributed to attack kits, these kits are likely responsible for a large part of this increase.

Mobile Threat Landscape Comes Into View

The major mobile platforms are finally becoming ubiquitous enough to garner the attention of attackers, and as such, Symantec expects attacks on these platforms to increase. In 2010, most malware attacks against mobile devices took the form of Trojan Horse programs that pose as legitimate applications. While attackers generated some of this malware from scratch, in many cases, they infected users by inserting malicious logic into existing legitimate applications. The attacker then distributed these tainted

applications via public app stores. For example, the authors of the recent Pjapps Trojan employed this approach.

While the new security architectures employed in today's mobile devices are at least as effective as their desktop and server predecessors, attackers can often bypass these protections by attacking inherent vulnerabilities in the mobile platforms' implementations. Unfortunately, such flaws are relatively commonplace -- Symantec documented 163 vulnerabilities during 2010 that could be used by attackers to gain partial or complete control over devices running popular mobile platforms. In the first few months of 2011 attackers have already leveraged these flaws to infect hundreds of thousands of unique devices. According to findings from Mocana, it is no surprise that 47% of organizations do not believe they can adequately manage the risks introduced by mobile devices. And, that more than 45% of organizations say security concerns are one of the biggest obstacles to rolling out more smart devices.^[1]

Threat Landscape Key Facts and Figures:

- **286 million new threats** – Polymorphism and new delivery mechanisms such as Web attack toolkits continued to drive up the number of distinct malware programs. In 2010, Symantec encountered more than 286 million unique malicious programs.
- **93 percent increase in Web-based attacks** – Web attack toolkits drove the 93 percent increase in the volume of Web-based attacks in 2010. The use of shortened URLs also impacted this increase.
- **260,000 identities exposed per breach** – This is the average number of identities exposed per breach in data breaches caused by hacking during 2010.
- **14 new zero-day vulnerabilities** – Zero-day vulnerabilities played a key role in targeted attacks including Hydraq and Stuxnet. Stuxnet alone used four different zero-day vulnerabilities.
- **6,253 new vulnerabilities** – Symantec documented more vulnerabilities in 2010 than in any previous reporting period.
- **42 percent more mobile vulnerabilities** – In a sign that cybercriminals are starting to focus their efforts on the mobile space, the number of reported new mobile operating system vulnerabilities increased, from 115 in 2009 to 163 in 2010.
- **One botnet with more than a million spambots** – Rustock, the largest botnet observed in 2010, had more than one million bots under its control at one point during the year. Other botnets such as Grum and Cutwail followed with many hundreds of thousands of bots each.
- **74 percent of spam related to pharmaceuticals** – Nearly three quarters of all spam in 2010 was related to pharmaceutical products—a great deal of which was related to pharmaceutical websites and related brands.
- **\$15 per 10,000 bots** – Symantec observed an advertisement that listed the price for 10,000 bot-infected computers as \$15 on an underground forum in 2010. Bots are typically used for spam or rogueware campaigns, but are increasingly also used for DDoS attacks.

- **\$0.07 to \$100 per credit card** – The price for credit card data on underground forums ranged widely in 2010. Factors dictating prices include the rarity of the card and discounts offered for bulk purchases.

About the Symantec Internet Security Threat Report

The Internet Security Threat Report is derived from data collected by tens of millions of Internet sensors, first-hand research and active monitoring of hacker communications, and it provides a global view of the state of Internet Security. The study period for the Internet Security Threat Report Volume 16 spans January 2010 to December 2010.

About Security Technology and Response

The Security Technology and Response (STAR) organization, which includes Security Response, is a worldwide team of security engineers, threat analysts and researchers that provides the underlying functionality, content and support for all Symantec corporate and consumer security products. With Response centers located throughout the world, STAR monitors malicious code reports from more than 130 million systems across the Internet, receives data from 240,000 network sensors in more than 200 countries and tracks more than 25,000 vulnerabilities affecting more than 55,000 technologies from more than 8,000 vendors. The team uses this vast intelligence to develop and deliver the world's most comprehensive security protection.

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. More information is available at www.symantec.com.

Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.