

**The Connecticut Joint Committee on Energy & Technology**

**H.B. 5816**

**Testimony by Louis Zeidman**

**Symantec Corporation**

**March 7, 2008**

Today's business environment is characterized by an unrelenting demand for real-time information from both citizens and governmental employees through the course of a typical business day. This places enormous pressure on departments and the IT organizations when you consider three variables: the compounding amount of information that governmental agencies have to store, secure and manage; the increasing infrastructure complexity within the government; and the diversity of regulations which must be strictly followed.

Given these dynamics it is not surprising that security strategies have evolved within governmental organizations to become more strategic, more expansive and more complex. Security is no longer just an IT function, but touches every part of the business – from Governor and Legislatures responsible for direction and focus; to HR, finance and legal that need to manage compliance; to Departmental leaders who drive day to day activities.

A September 2007 publication by Goldman Sachs stated that the top three drivers of enterprise security spend were IT Policy Compliance, Data Loss Prevention and Endpoint Protection. These are three significant challenges in themselves, but because they touch every aspect of the business, they are also highly interrelated.

To effectively manage these challenges and adapt to the evolving threat landscape, a security strategy must be policy driven, information centric and operationalized across a well managed infrastructure. By operationalizing security we mean standardizing and automating processes, integrating products and services, and streamlining workflows and reporting. This will not only drive down the costs of day-to-day activities but provides stakeholders with an increased understanding of overall IT risk.

We recognize that government customers are accelerating their efforts to: 1) Transform security from an inhibitor to an enabler of operational requirements, 2) Standardize and automate IT controls and security policies to improve compliance, 3) Identify and risk-rank both system and people-based vulnerabilities; and 4) Protect sensitive data and proprietary information whether it's at rest, in use, or in motion.

Today's government must have a comprehensive, integrated set of security products and services that enable the agencies to design and implement a highly effective security strategy that is risk-based and programmatic in its approach.

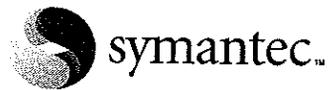
The first layer of a successful security strategy addresses IT Policy Management. All organizations have IT and security policies they need to enforce. Policies are based on internal best practices and current regulations with implementation often driven by frameworks such as ITIL, COBIT, ISO and others. Policies are critical because they provide the basis for deciding what types of information need to be protected, in what manner, at what cost, will have access to what information, and how long specific types of information should be retained. The challenge is to more effectively define and manage policy creation and distribution, as well as provide evidence of supporting processes that include technical and procedural controls.

The second layer addresses Information Risk Management to protect the information itself. Leveraging the policies established in the previous layer, Information Risk Management combines threat protection and information control enabling organizations to keep the bad things out (information security), to keep the important things in (data loss prevention), and to manage, retain and find information when needed (e-discovery).

Data Loss Prevention (DLP) is an extremely important topic to many of our largest customers. According to the IT Policy Compliance Group (ITPCG), data breach losses average \$100 per record. A publicly reported data breach can impact not only reputation, but according to the ITPCG, can cause up to an 8 percent decline in customers or share value for publicly traded companies. And while personal information record loss is the driving force behind most DLP investments today, there are other less well publicized losses - financial information, Personal Health Data, Criminal Records, etc, - that are equally impactful to businesses. In short DLP is quickly becoming a requirement to any security strategy.

The final layer of a successful security strategy relates to establishing the need for a well managed infrastructure, specifically around Endpoint Security. Proper security precautions must be put in place to protect the growing number of endpoints – from servers and PCs to laptops to mobile phones – regularly accessed and utilized by today's highly mobile workforce. As the threat landscape has evolved beyond viruses and worms, organizations now require a more comprehensive endpoint solution that combines antivirus, anti-spyware, firewall, intrusion prevention, along with device and application control in a way that is quickly and easily manageable.

We have assisted many governmental agencies around the world to refine their security models by working closely with them to develop comprehensive solutions based on their specific needs and to provide them with the needed flexibility to change with the rapidly changing threatscape. We look forward to the opportunity to do the same with the State of Connecticut.



Confidence in a connected world.

# **Symantec Government Internet Security Threat Report**

## **Trends for January–June 07**

Volume XII, Published September 2007

## Symantec Government Internet Security Threat Report

### **Government Internet Security Threat Report Overview**

The *Government Internet Security Threat Report* provides a six-month summary and analysis of trends in attacks, vulnerabilities, malicious code, phishing, and spam as they pertain to organizations in government and critical infrastructure sectors. Where possible, it will also include an overview of legislative efforts to combat these activities.

Over the past several reporting periods, Symantec has observed a shift in the threat landscape in which attackers have increasingly moved away from nuisance and destructive attacks towards targets and methods that are driven by financial motives. Today's attackers are increasingly sophisticated and organized, and have begun to adopt methods that are similar to traditional software development and business practices.

In the previous *Internet Security Threat Report*, Symantec observed that global, decentralized networks of malicious activity continued to rise and that, increasingly, regional threat patterns were beginning to emerge. Today, the threat landscape is arguably more dynamic than ever. As security measures are developed and implemented to protect the computers of end users and organizations, attackers are rapidly adapting new techniques and strategies to circumvent them. As a result, the identification, analysis and trending of these techniques and strategies must also evolve.

The ensuing changes have been evident over the first six months of 2007. Based on the data collected during that period, Symantec has observed that the current Internet security threat landscape is characterized by the following:

- Increased professionalization and commercialization of malicious activities
- Threats that are increasingly tailored for specific regions
- Increasing numbers of multistaged attacks
- Attackers targeting victims by first exploiting trusted entities
- Increased convergence of malicious activities

The *Government Internet Security Threat Report* will provide an analysis of attack activity that Symantec observed between January 1 and June 30, 2007 that targets or affects services, organizations, and/or industries of concern to government organizations around the world. For the purposes of this discussion, these government organizations include national, state/provincial, and municipal governments. Furthermore, this discussion will incorporate data and discussion that is relevant to threat activity that affects critical infrastructure industries that support or affect government and military institutions, which include:

- Aerospace
- Agriculture
- Biotech/pharmaceutical
- Government
- Financial services
- Health care
- Internet service providers

## Symantec Government Internet Security Threat Report

- Law enforcement
- Manufacturing
- Military
- Telecommunications
- Transportation
- Utilities and energy

Symantec has established some of the most comprehensive sources of Internet threat data in the world. The Symantec™ Global Intelligence Network tracks attack activity across the entire Internet. Over 40,000 sensors deployed in more than 180 countries by Symantec DeepSight™ Threat Management System and Symantec™ Managed Security Services gather this data. As well, Symantec gathers malicious code data reports from over 120 million client, server, and gateway systems that have deployed Symantec's antivirus products.

Symantec operates one of the most popular forums for the disclosure and discussion of vulnerabilities on the Internet, the BugTraq™ mailing list, which has approximately 50,000 direct subscribers who contribute, receive, and discuss vulnerability research on a daily basis.<sup>1</sup> Symantec also maintains one of the world's most comprehensive vulnerability databases, currently consisting of over 22,000 vulnerabilities (spanning more than a decade) affecting more than 50,000 technologies from over 8,000 vendors.

Finally, the Symantec Probe Network, a system of over two million decoy accounts, attracts email messages from 20 different countries around the world, allowing Symantec to gauge global spam and phishing activity. Symantec also gathers phishing information through the Symantec Phish Report Network, an extensive antifraud community of enterprises and consumers. Members of the network contribute and receive fraudulent Web site addresses for alerting and filtering across a broad range of solutions. Symantec also tracks and assesses some criminal activities using online fraud monitoring tools.

These resources give Symantec analysts unparalleled sources of data with which to identify emerging trends in malicious activity. The Symantec *Government Internet Security Threat Report* is grounded on the expert analysis of data provided by all of these sources. By publishing the analysis of Internet security activity in this report, Symantec hopes to provide enterprises and consumers in the government sector with the information they need to help effectively secure their systems now and in the future.

<sup>1</sup> The BugTraq mailing list is hosted by SecurityFocus (<http://www.securityfocus.com>). Archives are available at <http://www.securityfocus.com/archive/1>

# Symantec Government Internet Security Threat Report

## Executive Summary

The following section will offer a brief summary of the security trends that Symantec observed during the first half of 2007 based on data provided by the sources listed above. This summary includes all of the metrics that are included in the *Government Internet Security Threat Report*.

### Attack Trends Highlights

- The United States was the top country for malicious activity, accounting for 30 percent of malicious activity detected worldwide.
- Israel had the most malicious activity per Internet user, followed by Canada and the United States.
- The telecommunications sector accounted for 90 percent of all malicious activity originating from critical infrastructure sectors.
- The government sector accounted for 26 percent of data breaches that could lead to identity theft, the second most of any sector.
- The primary cause of data breaches that could facilitate identity theft was the theft or loss of a computer or other medium on which data is stored or transmitted, such as a USB key or a back-up medium.
- Hacking was responsible for 73 percent of identities exposed during this period.
- The United States was the target of the most denial of service attacks, accounting for 61 percent of all attacks during this period.
- Symantec observed an average of 52,771 active bot-infected computers per day, a 17 percent decrease from the previous reporting period.
- The lifespan of the average bot-infected computer was four days, an increase from three days in the second half of 2006.
- China had the highest number of bot-infected computers during the first half of 2007, accounting for 29 percent of the worldwide total.
- The United States had the most known command-and-control servers worldwide, accounting for 43 percent of the worldwide total.
- The United States was the top country of attack origin, accounting for 25 percent of worldwide attack activity.
- The top country of origin for attacks targeting the government sector was the United States, which accounted for 19 percent of the total.
- The most common attacks targeting government and critical infrastructure organizations were SMTP-based attacks, which accounted for 36 percent of the top ten attacks.

## Symantec Government Internet Security Threat Report

### ***Vulnerability Trends Highlights***

- Of the five operating systems tracked, Microsoft had the shortest average patch development time, at 18 days.
- Symantec documented six zero-day vulnerabilities during this period, down from 12 zero-day vulnerabilities in the second half of 2006.
- Symantec documented 90 unpatched enterprise vulnerabilities during this period.

### ***Malicious Code Trends Highlights***

- Threats to confidential information made up 65 percent of potential infections by the top 50 malicious code samples, up from 53 percent in the second half of 2006.
- Eighty-eight percent of confidential information threats had remote access capabilities, up slightly from 87 percent last period.
- Eighty-eight percent of confidential information threats had keystroke-logging capabilities, up from 76 percent in the second half of 2006.
- Of malicious code that propagated, 46 percent did so in email attachments.
- The United States had the highest number of multiple malicious code infections in the world, followed by China and Japan.
- During this period, 44 percent of Trojans were reported from North America, more than any other region.
- EMEA accounted for 43 percent of potential infections caused by worms, more than any other region.
- EMEA accounted for 45 percent of potential virus infections this period, more than any other region.
- EMEA accounted for 40 percent of all potential back door infections worldwide, more than any other region.

### ***Phishing Trends Highlights***

- Seventy-nine percent of organizations whose brands were used in phishing attacks were in the financial services sector, down from 84 percent in the second half of 2006.
- The financial services sector accounted for 72 percent of all phishing Web sites, up from 64 percent in the previous period.
- Of all known phishing Web sites, 59 percent were located in the United States, compared with 46 percent in the previous six-month period.
- Domains registered to the government of Thailand were used in 16 percent of phishing URLs hosted on government servers.
- Of the unique government domains used to host phishing Web sites, 23 percent were located in Thailand.