Security
April 13, 2009 10:23 PM PDT

Symantec: Security holes, malware spike in 2008

by Elinor Mills

If you worry that the Internet is a scary place full of digital pickpockets and online identity thieves, your fears will be bolstered by the latest **Symantec Internet Security Threat Report** released Tuesday.

The report finds huge increases in the number of security holes in software and the number of Internet threats, particularly attacks in which browsers are hijacked and forced to download malicious programs as people surf the Web.

Even visiting trusted Web sites isn't always safe. Most Web-based attacks target visitors to legitimate Web sites that have been compromised and that either serve up malicious content to the visitor or embed a malicious and invisible iframe on the page that surreptitiously redirects the user's browser to another Web server under an attacker's control, according to the report.

Attacks are traded in underground channels, with people buying and selling software that automates attacks or even entire botnets of infected computers that serve as spam armies, the report says. Stolen data is then marketed and offered up with price lists and guarantees. Oddly, the price of stolen data remained the same in 2008 despite the fact that the economy took a nose dive, said Zulfikar Ramzan, a technical director at Symantec Security Response.

The top Web-based attack in 2008 exploited the Microsoft IE ADODB.Stream Object File Installation Weakness vulnerability, while the top attacked vulnerabilty was the Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability, according to the report.

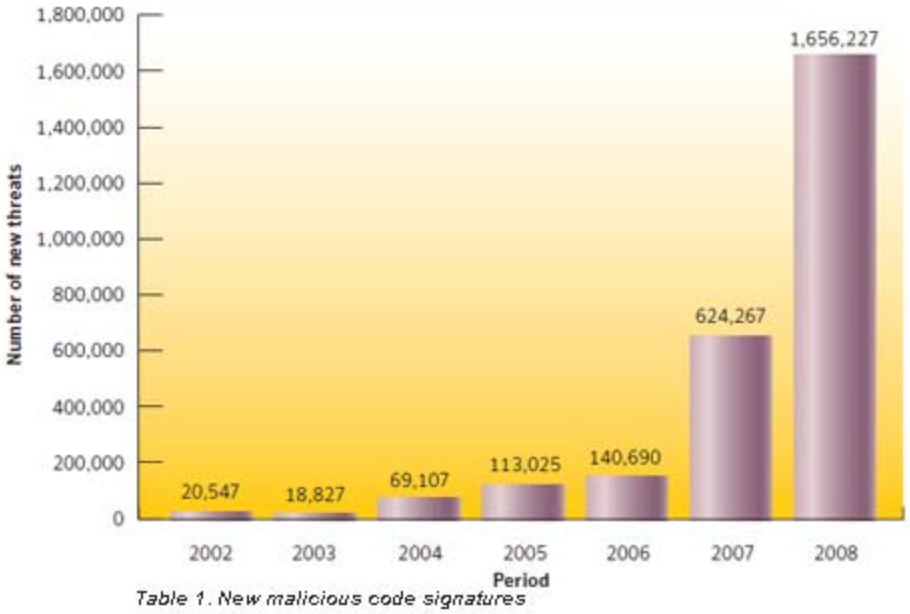

Table 1. New malicious code signatures

Symantec detected nearly 1.66 malicious code threats, which represent 60 percent of the 2.6 million total malware threats Symantec has detected since it has been tracking this. The number of new malicious code signatures grew by 265 percent from 2007.
(Credit: Symantec)

Here are other highlights for 2008 from Symantec's report:

Conficker

Infections of Conficker, also known as Downadup, have been particularly strong in Asia Pacific and Latin America, areas with some of the highest rates of software piracy. Pirated versions of software can not be automatically updates to receive security patches. The worm, **which has infected millions of Windows-based PCs that are not patched**, is now communicating with other infected machines via peer-to-peer, dropping a mystery payload and installing malware that masquerades as anti-virus software.

Identity fraud

Nearly 80 percent of confidential information threats exposed user data and 76 percent used used keystroke-logging to steal data like banking account credentials. Seventy-six of the phishing attacks attempted to lure victims to specific financial sector brands and one group--the Russian Business Network--is believed to be responsible for about half of the phishing incidents that occurred worldwide last year.

Twelve percent of all data breaches exposed credit card information, which is the most popular item for sale in the underground economy. Credit card data can range in price from 6 cents to $30, while bank account credentials range from $10 to $1,000 and e-mail accounts from 10 cents to $100. Most of the stolen credit card data for sale is from the U.S.

Most data breaches that could lead to identity fraud were in the education sector, while the financial sector was the top industry for identities exposed. Theft or loss of equipment accounted for nearly half of data breaches that could lead to identity fraud and for 66 percent of identities exposed.

Spam

The most common type of spam detected was related to Internet- or computer-related goods and service. Spam volumes rose nearly 200 percent in 2008 to nearly 350 billion messages in 2008. Botnets were responsible for distributing about 90 percent of all spam e-mail.

Malware spikes

Symantec detected nearly 1.66 million malicious code threats, which represent 60 percent of the 2.6 million total malware threats Symantec has detected since it has been tracking this. The number of new malicious code signatures grew by 265 percent from 2007. Trojans make up nearly 70 percent of the volume of the top 50 malicious code samples.

Vulnerabilities up

Symantec documented nearly 5,500 vulnerabilities in 2008, up nearly 20 percent over 2007 and 80 percent of documented vulnerabilities were classified as easily exploitable.

Safari had the longest window of exposure between when the exploit code was released for a vulnerability and when a vendor released a patch, with a nine day average, while Mozilla had the shortest with a less than one day average. Mozilla browsers were affected by 99 new vulnerabilities in 2008, followed by 47 in IE, 40 in Safari, 35 in Opera and 11 in Google Chrome. There were 424 browser plug-in vulnerabilities and ActiveX accounted for most of those.

Geographies

Most attacks originated in the U.S. and the U.S. was the country most frequently targeted by denial-of-service attacks. China had the most bot-infected computers and Buenos Aires was the city with the most bot-infected computers.

Critical infrastructure

Telecommunications was the top critical infrastructure sector for malicious activity, accounting for 97 percent of the total, and the most common type of attack was denial-of-service. The top country of origin for attacks targeting the government sector in the U.S. was China. Symantec documented 6 public SCADA vulnerabilities in 2008.

Elinor Mills covers Internet security and privacy. She joined CNET News in 2005 after working as a foreign correspondent for Reuters in Portugal and writing for The Industry Standard, the IDG News Service, and the Associated Press. E-mail Elinor.

Topics: **News**, **Privacy & data protection**, **Vulnerabilities & attacks**

Tags: **Symantec**, **malware**, **vulnerabilities**, **threat report**

Related

From CNET

Microsoft: Scareware, PDF exploits rise

Pentagon spends over $100 million on cyberattack cleanup

The marriage of identity yin and security yang

From around the web

Microsoft Outlines Rogue Anti-virus, Dat... eWeek

Torture Watch Washington Post - White House ...

More related posts powered by Sphere