washingtonpost.com

Cybercrooks Deliver Trouble

With Spam Filters Working Overtime, Security Experts See No Letup in '07

By Brian Krebs
washingtonpost.com staff writer
Wednesday, December 27, 2006; D01

It was the year of computing dangerously, and next year could be worse.

That is the assessment of computer security experts, who said 2006 was marked by an unprecedented spike in junk e-mail and more sophisticated Internet attacks by cybercrooks.

Few believe 2007 will be any brighter for consumers, who already are struggling to avoid the clever scams they encounter while banking, shopping or just surfing online. Experts say online criminals are growing smarter about hiding personal data they have stolen on the Internet and are using new methods for attacking computers that are harder to detect.

"Criminals have gone from trying to hit as many machines as possible to focusing on techniques that allow them to remain undetected on infected machines longer," said Vincent Weafer, director of security response at Symantec, an Internet security firm in Cuptertino, Calif.

One of the best measures of the rise in cybercrime is junk e-mail, or spam, because much of it is relayed by computers controlled by Internet criminals, experts said. More than 90 percent of all e-mail sent online in October was unsolicited junk mail, according to Postini, an e-mail security firm in San Carlos, Calif. Spam volumes monitored by Postini rose 73 percent in the past two months as spammers began embedding their messages in images to evade junk e-mail filters that search for particular words and phrases. In November, Postini's spam filters, used by many large companies, blocked 22 billion junk-mail messages, up from about 12 billion in September.

The result is putting pressure on network administrators and corporate technology departments, because junk mail laden with images typically requires three times as much storage space and Internet bandwidth as a text message, said Daniel Druker, Postini's vice president for marketing.

"We're getting an unprecedented amount of calls from people whose e-mail systems are melting down under this onslaught," Druker said.

Spam volumes are often viewed as a barometer for the relative security of the Internet community, in part because most spam is relayed via "bots," a term used to describe personal computers that online criminals have taken control of surreptitiously with computer viruses or worms. The more computers the bad guys control and link together in networks, or botnets, the greater volume of spam they can blast onto the Internet.

At any given time, between 3 million and 4 million compromised computers are active on the Internet, according to Gadi Evron, who managed Internet security for the Israeli government before joining Beyond Security, an Israeli security firm. And that estimate only counts spam bots. Evron

said millions of other hijacked computers are used to launch "distributed denial-of-service" attacks -- online shakedowns in which attackers overwhelm Web sites with useless data and demand payment to stop.

"Botnets have become the moving force behind organized crime online, with a low-risk, high-profit calculation," Evron said.

He estimated that organized criminals would earn about $2 billion this year through "phishing" scams, which involve the use of spam and fake Web sites to trick computer users into disclosing their financial and other personal data.

Another trend experts cite is the steady shift of Internet criminal activity from nights and weekends to weekdays, suggesting that online crime is evolving into a full-time profession for many.

Symantec found that the incidence of phishing scams has dropped significantly on Sundays and Mondays in the United States. The firm found a similar trend when it examined the pattern of new virus variants compiled and released by attackers.

"The bulk of the fraud attacks we're seeing now are coming in Monday through Friday, in the 9-to-5 U.S.-workday timeframe," Symantec's Weafer said. "We now have groups of attackers who are motivated by profit and willing to spend the time and effort to learn how to conduct these attacks on a regular basis. For a great many online criminals these days, this is their day job: They're working full time now."

Criminals are also becoming more sophisticated in evading anti-fraud efforts. This year saw the advent and wide deployment of Web-browser based "toolbars" with embedded technology designed to detect when users have visited a known or suspected phishing Web site. But many scam artists responded by developing new methods of hosting their fraudulent Web sites and routing traffic to them that made them harder for law enforcement and security experts to thwart.

"We've seen a pretty big evolutionary jump in tactics used by phishers over the past year, and I believe it's because some of the toolbar makers and the good guys who work to get these scam sites shut down have really done a good job at preventing them from being successful," said Dan Hubbard, vice president of research for Websense, an online security firm in San Diego.

The past 12 months also brought a steep increase in the number of software vulnerabilities discovered by researchers and actively exploited by criminals. The world's largest software maker, Microsoft, this year issued software fixes to 97 security holes that it classified as "critical," meaning hackers could use them to break into vulnerable machines without any action on the part of the user.

In contrast, Microsoft shipped just 37 critical updates in 2005. Fourteen of this year's critical flaws were known as "zero day" threats, meaning Microsoft first learned about the security holes only after criminals had already begun using them.

The year began with a zero-day hole in Microsoft's Internet Explorer, the Web browser of choice for about 80 percent of the world's online users. Criminals were able to exploit the flaw to install keystroke-recording and password-stealing software on millions of computers running Windows software.

At least 11 of those zero-day vulnerabilities were in the Microsoft Office productivity software suites, flaws that bad guys mainly used in targeted attacks against corporations, according to the SANS Internet Storm Center, a security research and training group in Bethesda. Microsoft issued patches to correct a total of 37 critical Office security flaws this year.

The year also was notable for a wave of attacks exploiting flaws in software applications that run on top of operating systems, such as media players and Web browsers. In February, attackers used a security hole in AOL's popular Winamp media player to install a hidden program when users downloaded a seemingly harmless playlist file. This month, a computer worm took advantage of a design flaw in Apple Computer's QuickTime media player to steal passwords from about 100,000 MySpace.com bloggers, accounts that were then hijacked and used for sending spam. Also this month, security experts spotted a computer worm spreading online that was powered by a six-month old hole in a corporate anti-virus product from Symantec.

Many security professionals speak highly of Microsoft's Vista, the newest version of Windows scheduled for release next month. The program includes improvements that should help users stay more secure online, such as a Web browser with new anti-fraud tools, as well as operating system changes that should make it more difficult for rogue software or viruses to make unwanted changes to key system settings and files.

But some security vulnerabilities have been identified in Vista already, including at least one in its new browser, Internet Explorer 7. Moreover, experts worry that businesses will be slow to switch to the new operating system and note that even if consumers adopt it more quickly, Microsoft will continue to battle security holes in legacy versions of its Office product.

Some software security vendors suspect that a new Trojan horse program that surfaced last month, called "Rustock.B," may serve as the template for future malicious software. The program morphs itself slightly each time it installs itself on a new machine in an effort to evade anti-virus software. In addition, it hides in the deepest recesses of the Windows operating system, creates invisible copies of itself, and refuses to work under common security analysis tools in an attempt to defy identification and analysis.

"This is about the nastiest piece of malware we've ever seen, and we're going to be seeing more of it," said Alex Eckelberry, president of the security vendor Sunbelt Software in Clearwater, Fla. "The new threats that we saw in 2006 have shown us that the malware authors are ingenious and creative in their methods."