

---

January 7, 2007

## Attack of the Zombie Computers Is a Growing Threat, Experts Say

By JOHN MARKOFF

In their persistent quest to breach the Internet's defenses, the bad guys are honing their weapons and increasing their firepower.

With growing sophistication, they are taking advantage of programs that secretly install themselves on thousands or even millions of personal computers, band these computers together into an unwitting army of zombies, and use the collective power of the dragooned network to commit Internet crimes.

These systems, called botnets, are being blamed for the huge spike in spam that bedeviled the Internet in recent months, as well as fraud and data theft.

Security researchers have been concerned about botnets for some time because they automate and amplify the effects of viruses and other malicious programs.

What is new is the vastly escalating scale of the problem -- and the precision with which some of the programs can scan computers for specific information, like corporate and personal data, to drain money from online bank accounts and stock brokerages.

"It's the perfect crime, both low-risk and high-profit," said Gadi Evron, a computer security researcher for an Israeli-based firm, Beyond Security, who coordinates an international volunteer effort to fight botnets. "The war to make the Internet safe was lost long ago, and we need to figure out what to do now."

Last spring, a program was discovered at a foreign coast guard agency that systematically searched for documents that had shipping schedules, then forwarded them to an e-mail address in China, according to David Rand, chief technology officer of Trend Micro, a Tokyo-based computer security firm. He declined to identify the agency because it is a customer.

Although there is a wide range of estimates of the overall infection rate, the scale and the power of the botnet programs have clearly become immense. David Dagon, a Georgia Institute of Technology researcher who is a co-founder of Damballa, a start-up company focusing on controlling botnets, said the consensus among scientists is that botnet programs are present on about 11 percent of the more than 650 million computers attached to the Internet.

Plagues of viruses and other malicious programs have periodically swept through the Internet since 1988, when there were only 60,000 computers online. Each time, computer security managers and users have cleaned up the damage and patched holes in systems.

In recent years, however, such attacks have increasingly become endemic, forcing increasingly stringent security responses. And the emergence of botnets has alarmed not just computer security experts, but also specialists who created the early Internet infrastructure.

"It represents a threat but it's one that is hard to explain," said David J. Farber, a Carnegie Mellon computer scientist who was an Internet pioneer. "It's an insidious threat, and what worries me is that the scope of the problem is still not clear to most people." Referring to Windows computers, he added, "The popular machines are so easy to penetrate, and that's scary."

So far botnets have predominantly infected Windows-based computers, although there have been scattered reports of botnet-related attacks on computers running the Linux and Macintosh operating systems. The programs are often created by small groups of code writers in Eastern Europe and elsewhere and distributed in a variety of ways, including e-mail attachments and downloads by users who do not know they are getting something malicious. They can even be present in pirated software sold on online auction sites. Once installed on Internet-connected PCs, they can be controlled using a widely available communications system called Internet Relay Chat, or I.R.C.

ShadowServer, a voluntary organization of computer security experts that monitors botnet activity, is now tracking more than 400,000 infected machines and about 1,450 separate I.R.C. control systems, which are called Command & Control servers.

The financial danger can be seen in a technical report presented last summer by a security researcher who analyzed the information contained in a 200-megabyte file that he had intercepted. The file had been generated by a botnet that was systematically harvesting stolen information and then hiding it in a secret location where the data could be retrieved by the botnet master.

The data in the file had been collected during a 30-day period, according to Rick Wesson, chief executive of Support Intelligence, a San Francisco-based company that sells information on computer security threats to corporations and federal agencies. The data came from 793 infected computers and it generated 54,926 log-in credentials and 281 credit-card numbers. The stolen information affected 1,239

companies, he said, including 35 stock brokerages, 86 bank accounts, 174 e-commerce accounts and 245 e-mail accounts.

Sensor information collected by his company is now able to identify more than 250,000 new botnet infections daily, Mr. Wesson said.

"We are losing this war badly," he said. "Even the vendors understand that we are losing the war."

According to the annual intelligence report of MessageLabs, a New York-based computer security firm, more than 80 percent of all spam now originates from botnets. Last month, for the first time ever, a single Internet service provider generated more than one billion spam e-mail messages in a 24-hour period, according to a ranking system maintained by Trend Micro, the computer security firm. That indicated that machines of the service providers' customers had been woven into a giant network, with a single control point using them to pump out spam.

The extent of the botnet threat was underscored in recent months by the emergence of a version of the stealthy program that adds computers to the botnet. The recent version of the program, which security researchers are calling "rustock," infected several hundred thousand Internet-connected computers and then began generating vast quantities of spam e-mail messages as part of a "pump and dump" stock scheme.

The author of the program, who is active on Internet technical discussion groups and claims to live in Zimbabwe, has found a way to hide the infecting agent in such a way that it leaves none of the traditional digital fingerprints that have been used to detect such programs.

Moreover, although rustock is currently being used for distributing spam, it is a more general tool that can be used with many other forms of illegal Internet activity.

"It could be used for other types of malware as well," said Joe Stewart, a researcher at SecureWorks, an Atlanta-based computer security firm. "It's just a payload delivery system with extra stealth."

Last month Mr. Stewart tracked trading around a penny stock being touted in a spam campaign. The Diamant Art Corporation was trading for 8 cents on Dec. 15 when a series of small transactions involving 11,532,726 shares raised the price of the stock to 11 cents. After the close of business that day, a Friday, a botnet began spewing out millions of spam messages, he said.

On the following Monday, the stock went first to 19 cents per share and then ultimately to 25 cents a share. He estimated that if the spammer then sold the shares purchased at the peak on Monday he would realize a \$20,000 profit. (By Dec. 20, it was down to 12 cents.)

Computer security experts warn that botnet programs are evolving faster than security firms can respond and have now come to represent a fundamental threat to the viability of the commercial Internet. The problem is being compounded, they say, because many Internet service providers are either ignoring or minimizing the problem.

"It's a huge scientific, policy, and ultimately social crisis, and no one is taking any responsibility for addressing it," said K. C. Claffy, a veteran Internet researcher at the San Diego Supercomputer Center.

The \$6 billion computer security industry offers a growing array of products and services that are targeted at network operators, corporations and individual computer users. Yet the industry has a poor track record so far in combating the plague, according to computer security researchers.

"This is a little bit like airlines advertising how infrequently they crash into mountains," said Mr. Dagon, the Georgia Tech researcher.

The malicious software is continually being refined by "black hat" programmers to defeat software that detects the malicious programs by tracking digital fingerprints.

Some botnet-installed programs have been identified that exploit features of the Windows operating system, like the ability to recognize recently viewed documents. Botnet authors assume that any personal document that a computer owner has used recently will also be of interest to a data thief, Mr. Dagon said.

Serry Winkler, a sales representative in Denver, said that she had turned off the network-security software provided by her Internet service provider because it slowed performance to a crawl on her PC, which was running Windows 98. A few months ago four sheriff's deputies pounded on her apartment door to confiscate the PC, which they said was being used to order goods from Sears with a stolen credit card. The computer, it turned out, had been commandeered by an intruder who was using it remotely.

"I'm a middle-aged single woman living here for six years," she said. "Do I sound like a terrorist?"

She is now planning to buy a more up-to-date PC, she said.