A Robot Network Seeks to Enlist Your Computer

By JOHN MARKOFF
Published: October 20, 2008

REDMOND, Wash. — In a windowless room on Microsoft’s campus here, T. J. Campana, a cybercrime investigator, connects an unprotected computer running an early version of Windows XP to the Internet. In about 30 seconds the computer is “owned.”

An automated program lurking on the Internet has remotely taken over the PC and turned it into a “zombie.” That computer and other zombie machines are then assembled into systems called “botnets” — home and business PCs that are hooked together into a vast chain of cyber-robots that do the bidding of automated programs to send the majority of e-mail spam, to illegally seek financial information and to install malicious software on still more PCs.

Botnets remain an Internet scourge. Active zombie networks created by a growing criminal underground peaked last month at more than half a million computers, according to shadowserver.org, an organization that tracks botnets. Even though security experts have diminished the botnets to about 300,000 computers, that is still twice the number detected a year ago.

The actual numbers may be far larger; Microsoft investigators, who say they are tracking about 1,000 botnets at any given time, say the largest network still controls several million PCs.

“The mean time to infection is less than five minutes,” said Richie Lai, who is part of Microsoft’s Internet Safety Enforcement Team, a group of about 20 researchers and investigators. The team is tackling a menace that in the last five years has grown from a computer hacker pastime to a dark business that is threatening the commercial viability of the Internet.
Any computer connected to the Internet can be vulnerable. Computer security executives recommend that PC owners run a variety of commercial malware detection programs, like Microsoft's Malicious Software Removal Tool, to find infections of their computers. They should also protect the PCs behind a firewall and install security patches for operating systems and applications.

Even these steps are not a sure thing. Last week Secunia, a computer security firm, said it had tested a dozen leading PC security suites and found that the best one detected only 64 out of 300 software vulnerabilities that make it possible to install malware on a computer.

Botnet attacks now come with their own antivirus software, permitting the programs to take over a computer and then effectively remove other malware competitors. Mr. Campana said the Microsoft investigators were amazed recently to find a botnet that turned on the Microsoft Windows Update feature after taking over a computer, to defend its host from an invasion of competing infections.

Botnets have evolved quickly to make detection more difficult. During the last year botnets began using a technique called fast-flux, which involved generating a rapidly changing set of Internet addresses to make the botnet more difficult to locate and disrupt.

Companies have realized that the only way to combat the menace of botnets and modern computer crime is to build a global alliance that crosses corporate and national boundaries. On Tuesday, Microsoft, the world’s largest software company, will convene a gathering of the International Botnet Taskforce in Arlington, Va. At the conference, which is held twice a year, more than 175 members of government and law enforcement agencies, computer security companies and academics will discuss the latest strategies, including legal efforts.

Although the Microsoft team has filed more than 300 civil lawsuits against botnet operators, the company also relies on enforcement agencies like the FBI and Interpol-related organizations for criminal prosecution.

Last month the alliance received support from new federal legislation, which for the first time specifically criminalized the use of botnets. Many of the bots are based in other countries, however, and Mr. Campana said there were many nations with no similar laws.

“It’s really a sort of cat-and-mouse situation with the underground,” said David Dittrich, a senior security engineer at the University of Washington Applied Physics Laboratory and a member of the International Botnet Taskforce. “Now there’s profit motive, and the people doing stuff for profit are doing unique and interesting things.”

Microsoft’s botnet hunters, who have kept a low profile until now, are led by Richard Boscovich, who until six months ago served as a federal prosecutor in Miami. Mr. Boscovich, a federal prosecutor for 18 years, said he was optimistic that despite the growing number of botnets, progress was being made against computer crime. Recent successes have led to arrests.

“Every time we have a story that says bot-herders get locked up, that helps,” said Mr. Boscovich, who in 2000 helped convict Jonathan James, a teenage computer hacker who had gained access to Defense Department and National Air and Space Administration computers.
To aid in its investigations, the Microsoft team has built elaborate software tools including traps called “honeypots” that are used to detect malware and a system called the Botnet Monitoring and Analysis Tool. The software is installed in several refrigerated server rooms on the Microsoft campus that are directly connected to the open Internet, both to mask its location and to make it possible to deploy software sensors around the globe.

The door to the room simply reads “the lab.” Inside are racks of hundreds of processors and terabytes of disk drives needed to capture the digital evidence that must be logged as carefully as evidence is maintained by crime scene investigators.

Detecting and disrupting botnets is a particularly delicate challenge that Microsoft will talk about only in vague terms. Their challenge parallels the traditional one of law enforcement’s placing informers inside criminal gangs.

Just as gangs will often force a recruit to commit a crime as a test of loyalty, in cyberspace, bot-herders will test recruits in an effort to weed out spies. Microsoft investigators would not discuss their solution to this problem, but said they avoided doing anything illegal with their software.

One possible approach would be to create sensors that would fool the bot-herders by appearing to do malicious things, but in fact not perform the actions.

In 2003 and 2004 Microsoft was deeply shaken by a succession of malicious software worm programs with names like “Blaster” and “Sasser,” that raced through the Internet, sowing chaos within corporations and among home computer users. Blaster was a personal affront to the software firm that has long prided itself on its technology prowess. The program contained a hidden message mocking Microsoft’s co-founder: “billy gates why do you make this possible? Stop making money and fix your software!!”

The company maintains that its current software is less vulnerable, but even as it fixed some problems, the threat to the world’s computers has become far greater. Mr. Campana said that there had been ups and downs in the fight against a new kind of criminal who could hide virtually anywhere in the world and strike with devilish cleverness.

“I come in every morning, and I think we’re making progress,” he said. At the same time, he said, botnets are not going to go away any time soon.

“There are a lot of very smart people doing very bad things,” he said.