UC SANTA BARBARA
THE Current

October 26, 2010
Andrea Estrada

Technology Developed by UCSB Computer Scientist Advances Internet Security

Consider the common cold. You can take active measures to avoid catching one, but if the virus manages to invade your system, you are powerless to keep it from running its course.

Now think about your computer. You can dose it with antivirus software to make it resistant to infection, but if a virus or worm manages to slip through, you have no recourse but to wipe your hard drive clean and start over. Or do you?

Christopher Kruegel, associate professor of computer science at UC Santa Barbara and a member of the campus's Computer Security Group, has developed a new security software that can identify and neutralize viruses after they've infected a user's machine, even if that virus has no known signatures.

"Antivirus software companies focus on the end host and try to prevent malware from infecting your computer in the first place," explained Kruegel. "They have a lot of tools sitting on the host that scan files for these signatures or that try to identify programs that behave in a surprising fashion and then they block them. But the numbers show that they are not very effective."

Kruegel and his colleagues, Giovanni Vigna, professor of computer science at UCSB, and Engin Kirda, professor of computer science at Institute Eurecom in France, have taken a different approach, particularly with bots and botnets. Rather than coming between a computer and the virus, their security software comes between the infected computer and the malicious master server that has taken control of it. "The virus sitting on the machine doesn't have a negative impact," said Kruegel. "But it becomes hugely problematic when it begins to talk to that remote infrastructure and responds to commands."

They have formed a company, LastLine, Inc. –– as in "last line of defense" –– to develop the software that interferes with the communication between the infected computer and the command and control infrastructure that wants it to act in some nefarious manner –– such as stealing bank account numbers and other data, or sending spam mail to a designated group of e-mail addresses. The software works alongside existing antivirus programs and firewalls.

Antivirus software is ineffective, Kruegel explained, because the cyber-criminals create new versions of their binaries so quickly that the software companies have difficulty keeping up with them. "There are mutation engines that take a program and create many different versions so they always look different. But it's the same program," he said. "With LastLine, we give up on trying to defend the machine. But once the machine is compromised, we block the connection between the malware and its command and control server. It cannot receive commands, and it cannot send out information."

By blocking the master servers, cyber-criminals are forced to construct command and control structures elsewhere, which is far more difficult than mutating a piece of malware, Kruegel noted.

Malware can make it onto a user's computer in many ways, but the most common is a drive-by download, which happens while the user is surfing the Internet. "You go to Web sites that are malicious and they send some script that exploits your browser by downloading the malware," said Kruegel. "It can also happen through e-mail and file-sharing sites where you download a program."

Recently, Kruegel was recognized for his accomplishments in Internet security, particularly in developing software that shuts down botnets. In the current issue of Technology Review, a publication of M.I.T., Kruegel is named to the magazine's

TR35, a list published annually that recognizes 35 outstanding innovators under the age of 35. The award covers a wide range of fields, including biotechnology, materials, computer hardware, energy, transportation, and the Internet.

Related Links

Technology Review

About UC Santa Barbara

The University of California, Santa Barbara is a leading research institution that also provides a comprehensive liberal arts learning experience. Our academic community of faculty, students, and staff is characterized by a culture of interdisciplinary collaboration that is responsive to the needs of our multicultural and global society. All of this takes place within a living and learning environment like no other, as we draw inspiration from the beauty and resources of our extraordinary location at the edge of the Pacific Ocean.