Trojan horse technology exploits Internet Explorer

By Kim Zetter, PC World.com
AUGUST 06, 2002

LAS VEGAS -- A new technology could let a Trojan horse disguise itself as the Internet Explorer browser and allow hackers to steal data from PCs by fooling firewalls into thinking it's a trusted Microsoft Corp. application, say three security consultants.

The trio of South African researchers demonstrated the technique for breaching firewalls at Def Con, the annual security conference that draws hackers, security professionals and cybercrime investigators.

Security professionals have been warning for two years that a Trojan horse bypassing firewall detection is the inevitable next step in hacking technology. At Def Con, it appeared in the form of Setiri, a demo Trojan horse that can operate without a user or firewall detecting its actions. The researchers say they won't release Setiri into the wild for hackers to use, but they called on Microsoft to change the IE features that permit it to operate.

The Trojan horse gets loaded onto a victim's PC in the same manner as other Trojan horses -- either embedded in an e-mail attachment or downloaded file, or installed physically onto a PC via a disk.

But Setiri differs from other Trojan horses in that it doesn't contain executable commands that can cause its malicious actions to be blocked by the firewall.

Instead, the program launches an invisible window in Internet Explorer to connect stealthily to a Web server through an anonymous proxy site called Anonymizer.com. The site is intended to enable anonymous surfing, but Setiri uses it to execute commands on your PC without your knowledge. Such commands can include downloading a keystroke-logging program to your system or uploading files or passwords to a remote PC. Because the stolen data is passed back through the Anonymizer proxy, you can't trace the location of the remote computer.

The Trojan horse exploits a standard feature in Internet Explorer that lets invisible browser windows open and connect to the Internet. The browser windows open in the background and don't appear on the desktop, so you can't see what they're doing. If you look for evidence of an open window in your Windows Task Manager, the window will be listed as iexplore.exe, just like a regular Internet Explorer window.

Internet Explorer uses invisible windows for many legitimate purposes, such as sending registration info to the Net. The e-mail program Eudora makes use of invisible browser windows to download pictures in e-mail.

One possible way to thwart the Trojan horse would be for Microsoft to turn off the invisible window function, said researcher Roelof Temmingh. But doing so would hinder some Internet Explorer operations.

Temmingh said that the only way to prevent Setiri from going to the Web site where its commands are stored is to configure a firewall to deny access to the Anonymizer site.

But Haroon Meer, Temmingh's colleague, said this wouldn't stop other variations of the Trojan horse, which might use a different proxy Web site or even use a trusted Web site, where a hacker could conceivably embed malicious code.

A Microsoft programmer in attendance said the company will look for ways to restrict invisible browsers to certain actions, the researchers said. A Microsoft spokesperson would say only that the company is committed to keeping customer information safe and that the vendor is evaluating the scenario presented in the Setiri demonstration.

Users can, of course, help protect themselves from getting the Trojan horse in the first place, the researchers noted. Security experts routinely warn users to not open e-mail attachments from unknown sources and to be careful about the sites from which they download programs.

Temmingh, Meer, and colleague Charl van der Walt, consultants at SensePost Information Security, said they demonstrated the Trojan horse not to scare users and systems administrators, but to raise awareness about what may already be in the wild. They said they wanted to promote discussion of what must be done to protect systems from such programs. "We are three guys who work full-time jobs, and we came up with this program just in our spare time," said Temmingh. "So imagine what guys with a lot of time on their hands have already come up with."

After the Def Con presentation, a hacker in the audience told Temmingh that he and friends have already devised a Trojan horse that does what Temmingh's test Trojan horse does. "This stuff could be happening on your machine right now. It's out there, and you must think about the problems with this now," Temmingh said.

Van der Walt urged a closer look at firewalls and invisible programs.

"The idea is to look at this mechanism that's trusted by firewalls and see how such

a Trojan horse can abuse that trust," he said. "We need to look at what methods should be allowed for invisible programs to operate."

Meer said the three hope Microsoft will soon deal with the invisible window function. But he acknowledged that this will be difficult, since "it will take some functionality away from IE if Microsoft tries to limit the invisible browser."

The researchers also said their demonstration should prompt firewall developers to reexamine how they handle Net access and designate trustworthy applications.

"The message is, don't think you're safe because you have the usual defenses, such as a firewall," Meer said.

VIRUSES, WORMS AND SECURITY HOLES

Recent Headlines

- CERT: Security flaw in Sun library could affect Kerberos
- Trojan horse technology exploits Internet Explorer
- Trojan horse found in OpenSSH
- Hole in PHP could give attacker server control

Additional Coverage

- View our Viruses, Worms and Security Holes special coverage page
  Coverage of the latest news in computer viruses, Trojan horses, worms and security holes.

Source: Computerworld

About Us Contacts Editorial Calendar Help Desk Advertise Privacy Policy