LAN Talk
Paul Merenbloom

December 2, 1996

Don't let rogue Java applets imperil network security

Every once in a while the perks of being an *InfoWorld* columnist backfire. Somebody read my column and sent me some really cool Java applications designed to manage and control routers in a secure fashion. I downloaded them recently and immediately noticed that my hard drive was acting up. Suddenly it was running as though it was out of space.

I thought it might be a Windows 95 caching issue, so I shut down the machine, rebooted in the MS-DOS mode, and headed straight for the WINDOWS\TEMP directory. Sure enough there were lots of leftover TMP files. No big deal; a simple DEL *.* ended that problem, and I went back to work.

But my troubles weren't over. I'd just gotten my browser running the Java code again -- this time without any other applications in memory -- when the hard drive went berserk. What the heck? I had a dial-up connection open because the code I was running came from a Web-based source. Bingo! A quick peek at the modem lights showed the send data light glowing solid!

The light went off, and a serial line tap installed between the modem and the computer started a capture routine. It seems that someone was using the Java code to unload my registry and select files, mainly those ending in .XLS -- spreadsheet data.

That explained the constant running of the hard drive. The code was searching through my files! Fortunately, the only .XLS files on this PC are the demos that come with Microsoft's Office Professional CD. But if there had been any real data I'd have been in big trouble.

Apparently the person showing me the new management software was completely unaware that someone had popped a bit of rogue code into the Java application.

What's interesting from a hacking perspective is that the Java applet used my e-mail code to secretly reroute the files -- definitely a good example of some miscreant playing outside the Java Sandbox.

My experience illustrates an important issue when it comes to browsers and Java. First, the mind-boggling varieties of browser code out there, each with a different flavor of Java implementation, will make integration with standard security systems very difficult. Second, Java is pretty cool and offers lots of potential, but an applet could also be hiding the next Trojan horse to enter your network.

I told a friend this story, and he suggested I check out a site called Finjan (http://www.finjan.com).

The Finjan Web site has a Java security checking system that seems very solid. You can point your Web browser there and learn just how much information an intruder can get using a simple query.

More importantly, Finjan offers a security diagnostic that will probe your browser and alert you to the status of the security implementation. It will also make recommendations as to what is at risk and how you can close any gaps. The code costs $49 per copy and can be downloaded from the Web site.

You can also send Finjan your credit card number. That's too much irony for me. If this incident proves anything, it's that there are any number of ways to get data off of your PC or LAN without either your knowledge or your permission.

I'm still a big Java fan, but I'm wiser now. Odds are good that someone will challenge your network at some point using these kinds of Java tools. Me? I'm sending Finjan my $49 via the U.S. Postal Service, and you can be sure I'll be checking our browsers.

Paul Merenbloom is vice president, technology research at Piper Jaffray in Minneapolis. Send comments to him at plmeren@mcimail.com.

Missed a column? Go back for more.

RETURN TO TOP
