Back Doors (3):

RATs

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Back doors may be installed by Trojan Horse programs. For example, in July 1998, The Cult of the Dead Cow (cDc) announced Back Orifice (BO), a tool for analyzing and compromising MS-Windows security (such as it be). The author, a hacker with the L0PHT group which later became part of security firm @Stake, described the software as follows (the brackets are in the original): "The main legitimate purposes for BO are remote tech support aid, employee monitoring and remote administering [of a Windows network]." However, added the cDc press release, "Wink. Not that Back Orifice won't be used by overworked sysadmins, but hey, we're all adults here. Back Orifice is going to be made available to anyone who takes the time to download it [read, a lot of bored teenagers]." Within weeks, 15,000 copies of Back Orifice were distributed to Internet Relay Chat users by a malefactor who touted a "useful" file ("nfo.zip") that was actually a Trojan infected by Back Orifice.

BO and programs like it provide back doors for malefactors to invade a victim’s computer. Once the Bad Guy has seized control of the system, functions available include keystroke logging, real-time viewing of what’s on the monitor, screen capture, and full read/write access to all files and devices.

Today, such programs are known as RATs (Remote Administration Trojans). The PestPatrol Glossary provides this useful information [MK note: I have changed “trojan” to “Trojan” in what follows]:

>RAT: A Remote Administration Tool, or RAT, is a Trojan that when run, provides an attacker with the capability of remotely controlling a machine via a "client" in the attacker's machine, and a "server" in the victim's machine. Examples include Back Orifice, NetBus, SubSeven, and Hack’atack. What happens when a server is installed in a victim's machine depends on the capabilities of the Trojan, the interests of the attacker, and whether or not control of the server is ever gained by another attacker -- who might have entirely different interests.

Infections by remote administration Trojans on Windows machines are becoming more frequent. One common vector is through File and Print Sharing, when home users inadvertently open up their system to the rest of the world. If an attacker has access to the hard-drive, he/she can place the Trojan in the startup folder. This will run the Trojan the next time the user logs in. Another common vector is when the attacker simply e-mails the Trojan to the user along with a social engineering hack that convinces the user to run it against their better judgment.”<

RATs are frequently distributed as part of “Trojanized” applications such as WinAMP as well as in data files for (especially) pornographic pictures and MP3 sound files. Once executed or loaded, such infected files quietly install the RAT and sometimes signal a base station to inform it of the IP address of yet another victim.
There are currently over 300 RATs listed and removed by PestPatrol. For a more extensive research paper on RATs, see the PestPatrol White Paper.

***

The next article in this series will focus on preventing back doors from being included in source code.

***

References:


* PestPatrol Glossary <http://www.safersite.com/PestInfo/G/Glossary.asp>

* PestPatrol White Paper: About RATs – A look at the problem of SubSeven and “Remote Administration Trojans.” <http://www.safersite.com/Support/About/About_Rats.asp>

***


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@compuserve.com>. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at <http://www.mekabay.com/index.htm> for papers and course materials on information technology, security and management.

Copyright © 2002 M. E. Kabay. All rights reserved.

Permission is hereby granted to _Network World_ to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.