

Information Security: The Instructive Code "Backstop"

Robert Ing, D.Sc., D.Lit., F.A.P.Sc.

Full Article Available at www.drroberting.com

Copyright © 2004, 2005 Dr. Robert Ing, Toronto, Canada. All rights reserved.

Introduction

For the most part, computer viruses and Trojans are characterized by obvious computer malfunctions from blatant graphical on-screen representations to the computer automatically accessing the Internet, printing documents or switching on its video camera without user interaction. Most virus utility software detects and quarantines approximately 90% of those currently in distribution. As for Trojans (rogue programs that allow an unknown third party to access and control your computer), commercial virus utility software detects and quarantines approximately 60% of these, while a dedicated Trojan utility software fares better at approximately 98%.

Although these performance figures may offer a guarded level of comfort, there is a threat that even the most robust and efficient virus or Trojan utility commercially available today cannot protect you from. That threat is known as an instructive code Trojan, or as those in the cracker underworld call it, a "backstop".

The instructive code Trojan defies detection because unlike most viruses and Trojans out there, each instructive code Trojan to date has been specifically written for its victim and the targeted information it must access. While over 90% of viruses and Trojans are variations or replications of others before them, backstops are unique. Backstops or instructive code Trojans are created to obtain specific files from a targeted computer or network without detection. While it is improbable that the average computer user will encounter a backstop, the threat is very real to governments and corporate entities that routinely use or create any form of proprietary, financial or competitive data.

How it works

The instructive code searches for specific keywords or phrases.

It is delivered to its target as a hidden file attachment piggybacked to an expected attachment, embedded in the body of an e-mail, automatically loaded from a webpage the target is known to frequent, or via external media such as a floppy disk or CD. In one case, the instructive code was delivered on a music CD to an employee known to play music on her laptop. Once she connected her laptop to the network, the instructive code transferred itself to its target.

Once on the target system, the code resides in a hidden file that cannot be viewed on the system under regular default settings. The code then searches all files and folders for occurrences of the specific keywords or phrases programmed into it. When matches are found, copies of the data are made, compressed, encrypted and made into a hidden archive file. After a predetermined time, the code automatically e-mails the entire file during a routine e-mail session initiated by the target user. Once sent, the code deletes the hidden archive and invokes a self-delete procedure to remove itself, leaving all other files and programs intact. Thus, there is virtually no trace that the instructive code existed on the target system.

Users

In an age where information is a prized commodity, instructive code Trojans are the new digital tool of high level corporate espionage. From R&D data, confidential financial records to other information not meant for a wide audience, the backstop offers a potential key to gain access.

Protection

While there is no direct way to thwart a backstop being placed on your computer or network, there are measures you can take to manage the risk. Your first line of defense is a robust firewall that is properly configured to your system. Proper configuration is by no means the factory or default settings of your firewall product. Nor is it configuring your firewall once on installation and forgetting about it. The configuration of your firewall has to be reviewed every time hardware and software are upgraded, replaced or added.

Another security measure is to deploy utility software that monitors and sounds an alarm when any changes to operating system registry and configuration files are executed. In addition, audit trail and network management logging utilities should be configured to track and alert system operators whenever files of a specific size are deleted. Windows users should ensure that hidden files can be viewed by enabling the "Show All Files" option in the View>Folder Options menu. Information that is of the utmost secrecy or value should never reside on a system connected permanently or even temporarily to the outside world.

Due to the very nature and purpose of instructive code Trojans, it is unlikely that accurate victim statistics will truly reflect the real financial impact the backstop will have in the corporate sector, or on national and international security. As with any act of espionage, an average of only 3% globally ever get reported for fear of repercussions of corporate non-competence and weakened government diplomatic relations.

About the Author

Dr. Robert Ing is a digital forensics and electronic counter-intelligence specialist. He may be contacted at 416-563-6958 or by e-mail at Ring549@aol.com