Anti-virus Software

A false sense of security?

Microslot Purpose

- I will lead you through the process of launching a targeted attack against an organisation
- Examine how and why the attack works and how it can be prevented
- Show how vulnerable we ALL are

Disclaimer

THIS DOES NOT PROVIDE ENOUGH DETAIL TO BE AN INSTRUCTION GUIDE, AND IS NOT INTENDED TO BE AS SUCH.

Target Company Infrastructure

- 100,000 personal workstations and notebooks worldwide
- 8000 servers (web, file, SQL, Mail, Sharepoint etc…)

Company Protection Measures

- All PCs are protected by a corporate license, off the shelf antivirus solution
- Backed up by virus definition automatic update servers
- Expensive support subscriptions

The Attack!

- Targeted trojan-horse attack
- Non malicious (for testing purposes)
- With permission from network admin

How it works

- Email a .exe file to various recipients within the organisation
- Body text reads “Hey try out this office prank” (or similar, be creative!)
- The .exe runs but appears to produce an error.
- The user assumes it doesn’t work and gives up

What's Really Happening

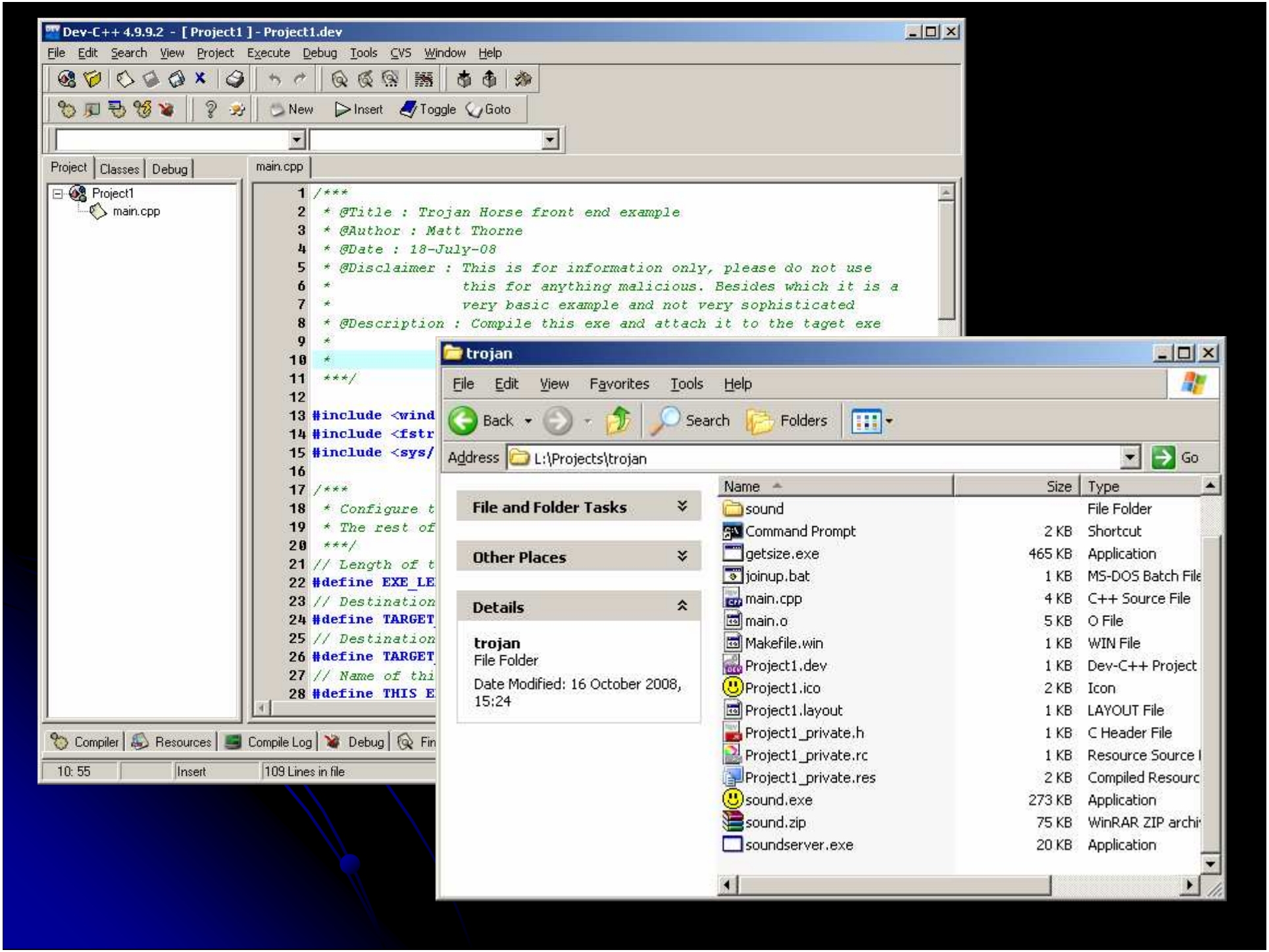
- The .exe runs and creates a new .exe in the system32 directory
- The .exe creates a new registry key to start to new executable on system start
- The exe then writes the name of the computer to a remote log
- The new exe opens a listening port on the host computer

The Tools

- 1 x C++ compiler (DevC++ ‘cos it’s free)
- 1 x Exe packer (UPX ‘cos it’s free)
- 1 x copy command (bundled with windows since 1985!)
- 2 Hours

The Method

- Use the C++ compiler to create two executables
- Exe 2 is the malicious code which you wish to run on the target
- Exe 1 is the carrier exe to distribute Exe 2


Dev-C++ 4.9.9.2 - [Project1] - Project1.dev
File Edit Search View Project Execute Debug Tools CVS Window Help
New Insert Toggle Goto
Project Classes Debug
Project1
main.cpp
main.cpp
/***
* @Title : Trojan Horse front end example
* @Author : Matt Thorne
* @Date : 18-July-08
* @Disclaimer : This is for information only, please do not use
this for anything malicious. Besides which it is a
very basic example and not very sophisticated
* @Description : Compile this exe and attach it to the taget exe
*
*
***/
#include <wind
#include <fstr
#include <sys/
/***
* Configure t
* The rest of
***/
// Length of t
#define EXE_LE
// Destination
#define TARGET_
// Destination
#define TARGET_
// Name of thi
#define THIS E
Compiler Resources Compile Log Debug Fin
10: 55 Insert 109 Lines in file
trojan
File Edit View Favorites Tools Help
Back Search Folders
Address L:\Projects\trojan
Go
File and Folder Tasks
Other Places
Details
trojan
File Folder
Date Modified: 16 October 2008, 15:24
Name Size Type
sound File Folder
Command Prompt 2 KB Shortcut
getsize.exe 465 KB Application
joinup.bat 1 KB MS-DOS Batch File
main.cpp 4 KB C++ Source File
main.o 5 KB O File
Makefile.win 1 KB WIN File
Project1.dev 1 KB Dev-C++ Project
Project1.ico 2 KB Icon
Project1.layout 1 KB LAYOUT File
Project1_private.h 1 KB C Header File
Project1_private.rc 1 KB Resource Source
Project1_private.res 2 KB Compiled Resourc
sound.exe 273 KB Application
sound.zip 75 KB WinRAR ZIP archi
soundserver.exe 20 KB Application

The Method

- Use upx to compress the two executables
- Join the two executables with the following windows command

  copy/b exe1.exe+exe2.exe Checkthisout.exe

- Send the mail!

The Results

- 17 out of 20 recipients ran the exe
- 5 recipients ran it more than once (obviously unhappy with the phoney error message!)
- 1 user ran it 5 times!

- 85% Success!

Virus protection failures

- Failed to spot two .exe headers within the one file
- Failed to prevent addition of a new run key in the registry

Virus protection failures

- Failed to notice a new port being opened and listening
- Failed to stop a new exe being created in the system32 directory

Potential Damage

- Key loggers
- Rootkits
- Data-mining
- Virus distribution
- Electronic Sabotage

Prevention

- User education/awareness