CompareView Compilation and Installation Guide

December 25, 2010

1 Introduction

This document presents a tutorial on how to compile and install CompareView in Windows XP system. We describe some important files in source codes that are needed for further modification on CompareView in section 7 and virus in section 8 that are used for performance measurement.
To run experiment on CompareView, you need to comment off some code in order to produce desired results.

2 Prerequisite

In order to compile and install CompareView on Windows XP system, you need to install Windows Driver Kits(WDK) to compile the code and DebugView(DbgView) to display output from CompareView. We have a virtual machine for VirtualBox with proper environment for CompareView, contact me if you need it.

3 Compile CompareView

We host source code of CompareView in google host. Use SVN tools to check out the source code through url:`http://compare-view-vt.googlecode.com/svn/trunk/`. You need to have permission to download the code.

1. Check out source code by SVN tools in your host machine.
2. Start `WindowsDriverKits->WDKxxxx.xxx->BuildEnvironments->WindowsXP->WindowsXPx86CheckedBuildEnvironment`,if you do not want debug information, use Free Build Environment.
3. Change current directory to `yoursourcecodedirectory\tdifw\src`.

4. Compile tdifw code using command: build /ce. Modify the code until there is no errors.

5. Change current directory to `yousourcecodedirectory\passthru\`.

6. Compile passthru code using command: build /ce. Modify the code until there is no errors

4 Install CompareView

1. Copy `yoursourcecodedirectory\tdifw\src\drv\objchk_wxp_x86\i386\tdifw_drv.sys` to `C:\Windows\System32\Drivers`.

2. Copy `yoursourcecodedirectory\tdifw\src\svc\objchk_wxp_x86\i386\tdifw.exe` to `C:\Windows\System32\`.

3. Copy `yoursourcecodedirectory\passthru\objfre_wxp_x86\i386\passthru.sys` to `C:\Windows\System32\Drivers`.

4. restart Windows.

5 Compile and debug Inputlogger and InputHook

InputLogger is the user interface to key and mouse event logger. InputHook is the dll file used by InputLogger to actually record key and mouse events.

1. Download and install Microsoft Visual Studio 2008 from `http://msdn03.e-academy.com/elms/Storefront/Home.aspx?campus=rutgers_scils`.

2. Use MS VS 2008 to open `httplogger\Windows\InputLogger\InputLogger\InputLogger.vcproj`

3. Use MS VS 2008 to open `http-logger\Windows\InputHook\InputHook\InputHook.vcproj`

4. MS VS 2008 has very good compiling and debugging functions.

   Before debugging InputLogger, do not forget to copy `httplogger\Windows\InputHook\Debug\InputHook.dll` to `httplogger\Windows\InputLogger\Debug\`.

6 Check Monitor Information

1. run DgbView(DebugView)
2. use filter as 'passthru'

7 Code Description

CompareView is developed based on tdifw, an open-source firewall for Windows. We use comment *CompareView 12/17/2010* to mark the code added by us.

- *Disp_sr.c* intercepts all tcp packets from application layer to kernel layer. We add our code in *tdi_send* function to generate signature for each packet by using packet header.
- *Disp_dg.c* intercepts all udp packets from application layer to kernel layer. We add our code in *tdi_send_datagram* function to generate signature for each packet by using packet header.
- *Miniport.c* intercepts all packets from transport layer to network driver layer. We add our code in *MPSendPackets* function to verify the signature of each packet by using packet header.

8 Bypass Malware

You can find the code on the desktop of the Virual Machine(WinXP_Chehai_English.vdi). Just use installer and load the .sys file and run it. You can find in DebugView, there would be ***Not Matched*** information.

9 Others

You can find related documents or tutorials about TDI-based firewall development under *Doc* directory in the souce code.