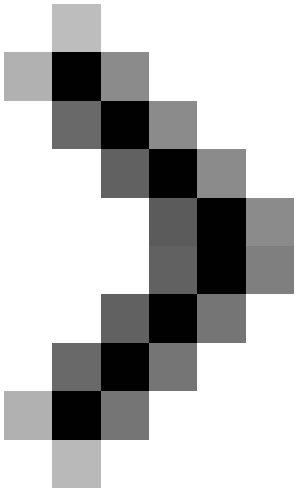
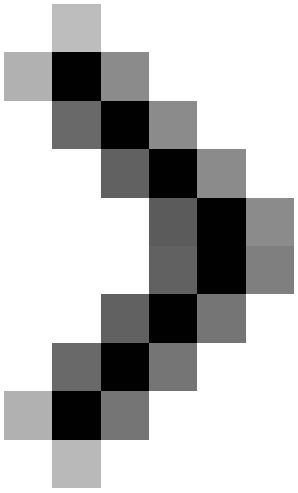
Binder and Malware (Part 3)

In the previous two sections we have configured and built the malware with binder YAB. Now will observe and execute this malware. In the perspective we will begin to implement what this executed piece of malware looks like and the behavior of n



Binder and Malware (Part 1)



Binder and Malware (Part 2)

Don Parker

In the previous two sections we have configured and built the malware with binder YAB. Now will observe and execute this malware. In the perspective we will begin to implement, what this piece of executed malware looks like and its behavior when executed by an ordinary user. Now if you recall it, we used the Pong.exe icon to represent the malware because this makes the malware look like a real program.

We will check the current installation of malware through a number of previously mentioned tools. Specifically, use Regmon and Filemon. With these two tools running in the background when executing malware, we will see what the malware does and that way will check how the malware works. If you do not install these tools on your computer, please proceed with this installation immediately to perform the test. After installation is complete, execute them and remove all running background processes. This will allow you to check the newly arising process.

How does it look?

As mentioned in the previous sections, look at this malware from the user perspective. To do this, execute it. We should acknowledge that the purpose of this article is to make the malware attack the mailbox that the user cannot detect. Take a look at the window below to see what happens when executing the malware program that has the Optix Pro trojan server and the Pong.exe program.

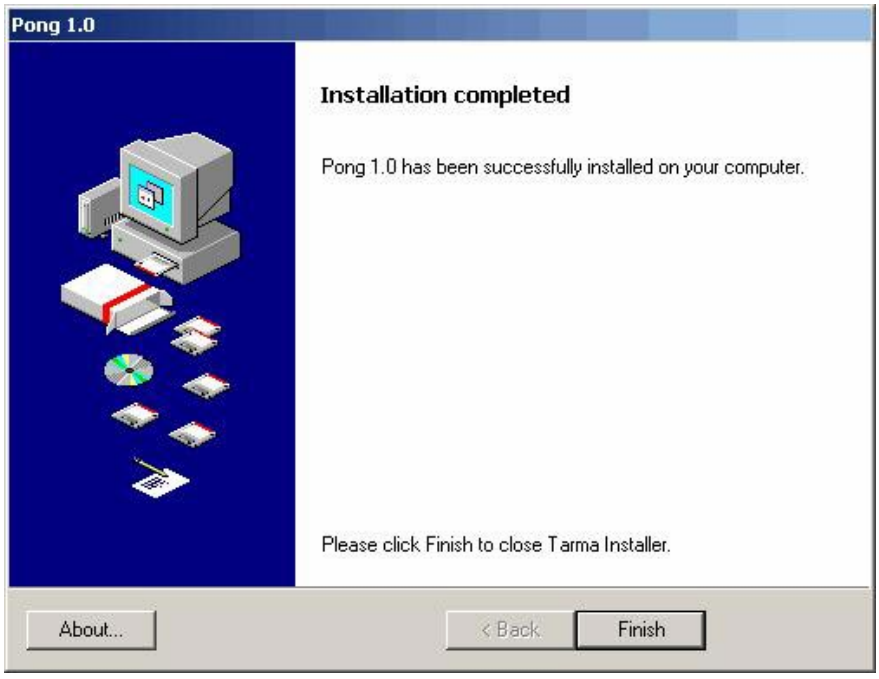


Figure 1

As expected, the installation of Pong.exe / malware is completely smooth, without any problems or warning for users. So what happens in the background? To answer that question, we used two tools Regmon and Filemon that ran in the background before executing malware. Watch Regmon see what happens.

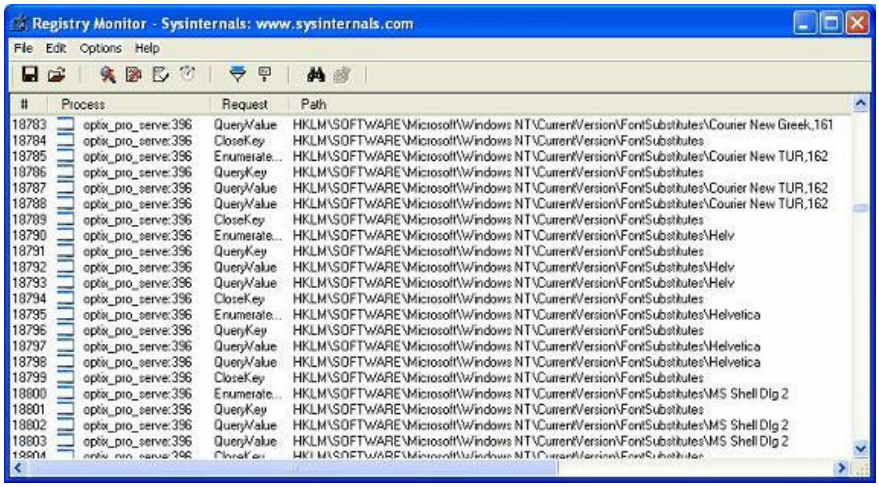


Figure 2

We have marked the output of Regmon to indicate that it is reporting the installation 'optix_pro_server' on your computer. This is all we have called the Optix Pro server when it finishes configuring it to bring it together. We will now look at what happens in Filemon during the execution of malware.

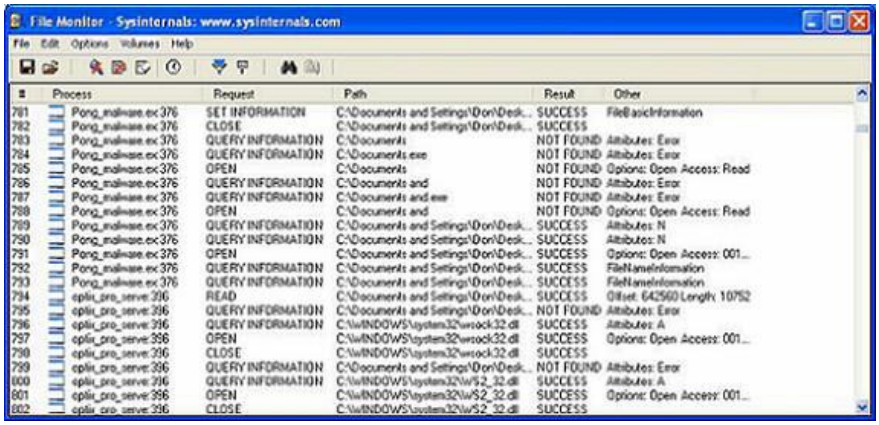


Figure 3

We see that Filemon also announced that 'optix_pro_server' was installed and made changes to the file system. Filemon also announced that the Pong.exe program (we called it Pong_malware.exe when combined with the trojan server) installed and made some file system changes. Amazingly, the Regmon and Filemon tools worked perfectly, detecting the installation of programs and changes they made with both the registry and the file system.

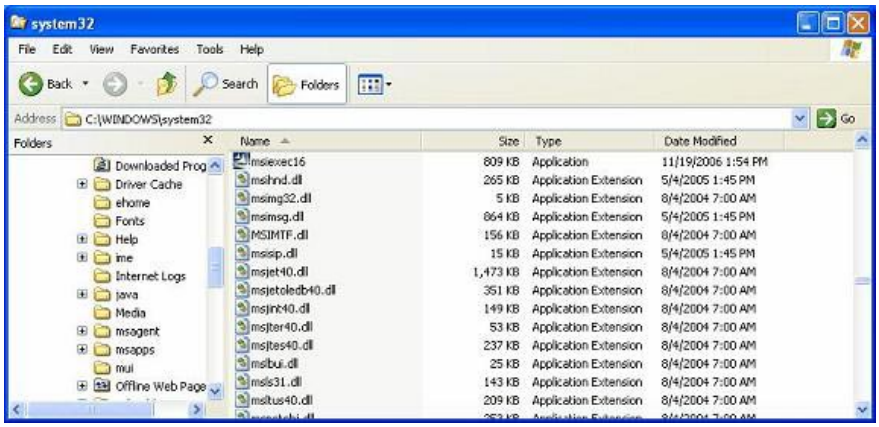


Figure 4

Looking at the figure above, we will see that there is a file called 'msiexec16' that measures 809 KB. That is indeed the Optix Pro trojan server. This 'msiexec16' is the default name that Optix Pro trojan server will come with unless you change it when configuring. Now the question is, is it really running on the computer? Let's look at the image below.

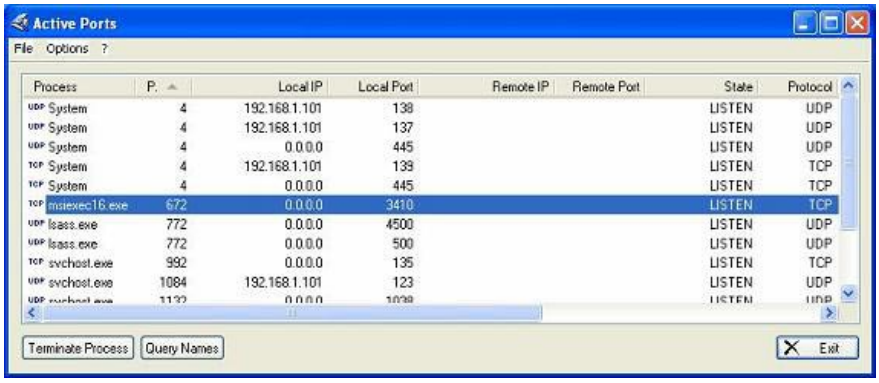


Figure 5

We look at the highlighted section in the ActivePorts program (this tool will check all TCP and UDP sockets on your computer as well as map the hard drive of the open programs), in the bookmark. This, 'msiexec16.exe' with PID is 672 indeed running. So our configuration, link and execution have been successful. We can use the Optix Pro trojan server to record keystrokes on the keyboard of the user's computer. So you can see why the entire bank account of someone is gone.

It is not difficult to understand high-level computer security concepts. This scenario is such an example. The important thing is the ability to re-create specific situations like the situation we read, which will make you understand more about this area. You can then use this knowledge to explore further dangers to user computers.

Under the crust

We have been introduced to external shapes to demonstrate the danger to computer users with malware attacks. Now is the time for us, computer security experts, to bring this knowledge to the next step. What I will talk about in the next section is what malware looks like under the helmet. This will surround how to observe it securely without executing it, and how to recognize byte-level characteristics of Microsoft Windows executables.

In the final part of this series we will look at the byte level through a hex editor for malware with the official program. Then we'll use that knowledge to learn how to recognize malware without having to wake it up. We will see the UPX encapsulation that the Optix Pro trojan server is capable of using. In addition, the UPX program will be used to open the UPX packaged trojan package. Developed we will use another program to dump the running trojan server process to see them as memory. You might think that it takes a lot of information, but doing it is important. There are many tools that can be used to analyze malware and we will mention a few tools, all of which will be addressed in the next section.

(*Also*)