Anaisy Garcia

5734454

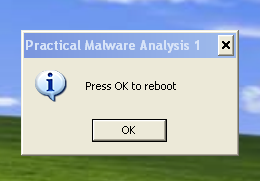
Lab 12-1

Analyze the malware found in the file Lab12-01.exe and Lab12-01.dll. Make sure that these files are in the same directory when performing the analysis.

Questions

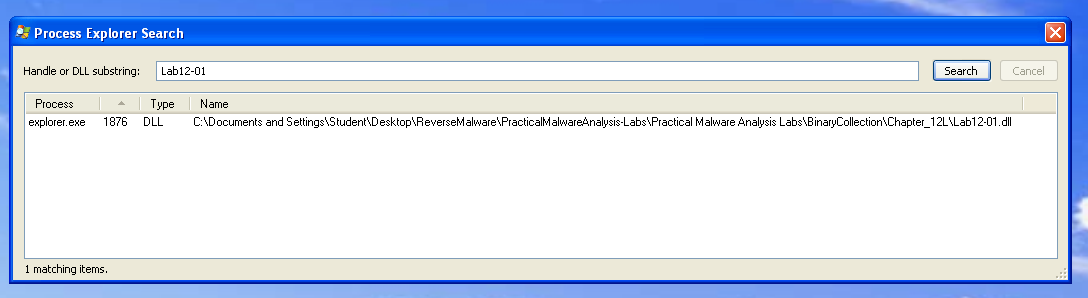
1. What happens when you run the malware executable?

Pop-ups start showing up every so often that says, “Press ok to reboot”.



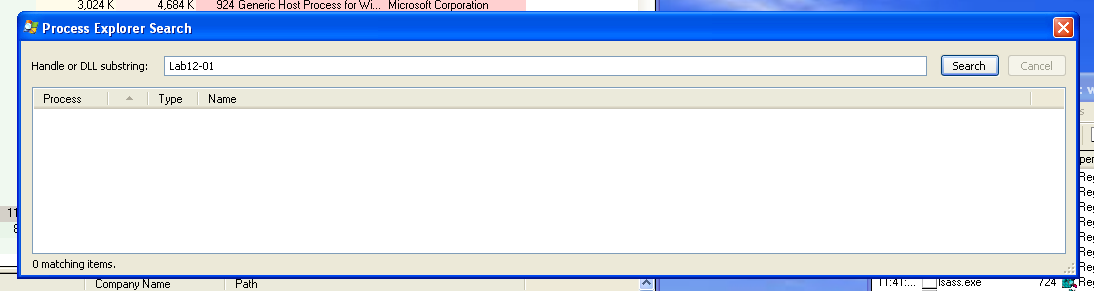
1. What process is being injected?

The process that was injected in explorer.exe.



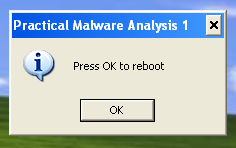
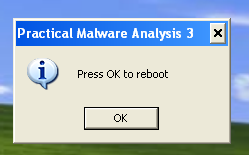
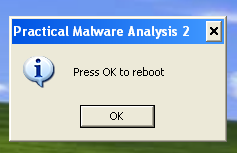
1. How can you make the malware stop the pop-ups?

Killing the explorer.exe process makes the program stop.



1. How does this malware operate?

The program injects Lab12-01.dll within explorer.exe then a random pop up comes up every now and then. The top also increments with each pop-up.



Lab 13-1

Analyze the malware found in the file Lab13-01.exe.

Questions

1. Compare the strings in the malware (from the output of the strings command) with the information available via dynamic analysis. Based on this comparison, which elements might be encoded?

Two strings, [www.practicalmalwareanalysis.com](http://www.practicalmalwareanalysis.com) and GET/aG9zdG5hbWUtZm9v, appear in beacon that cannot be found.

1. Use IDA Pro to look for potential encoding by searching for the string xor. What type of encoding do you find?

The string xor is found at 004011B8 which leads to a loop in sub\_401190.

1. What is the key used for encoding and what content does it encode?

The xor encoding uses the byte 0x3B. It decodes to www.practicalmalwareanalysis.com.

1. Use the static tools FindCrypt2, Krypto ANALyzer (KANAL), and the IDA Entropy Plugin to identify any other encoding mechanisms. What do you find?

Can only identify the use of standard Base64: ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/

1. What type of encoding is used for a portion of the network traffic sent by the malware?

Standard Base64 to create the GET request string.

1. Where is the Base64 function in the disassembly?

Starts at 0x004010B1.

1. What is the maximum length of the Base64-encoded data that is sent? What is encoded?

Max of 12 bytes from the hostname before Base64 encoding. This makes the GET request max at 16 characters.

1. In this malware, would you ever see the padding characters (= or ==) in the Base64-encoded data?

May be used if hostname length is less than 12 bytes.

1. What does this malware do?

Sends a beacon with an encoded hostname until it receives a response then terminates.