Lab 10 Report

1. Name: 林靖昀 Student ID: B12902116

2. Analyze the Lab09-01.exe

   How can you get this malware to install itself?

   Specify the “-in” flag as a command line argument.

   What are the command-line options for this program? What is the password requirement?

   1. “-in <name>”, can specify a name to use, if none specified, uses the file name.
   2. “-re <name>”, can specify a name to use, if none specified, uses the file name.
   3. “-c <a1> <a2> <a3> <a4>”, Creates and sets a registry key containing the data <a1><a2><a3><a4>.
   4. “-cc”, Prints out the registry key value.

   Password: “abcd”

   How can you use OllyDbg to permanently patch this malware, so that it doesn’t require the special command-line password?

   We can modify the password checking function (0x402510) to always return true.

   What are the host-based indicators of this malware?

   When specified with the “-in” flag, the software checks for a service name; if none exists, it creates a service on the computer.

   In the imports tab, we see lots of imports for service and registry API functions.

   What are the different actions this malware can be instructed to take via the network?

   From main -> 0x402360 -> x402020, in this function we see that it communicates with something through a socket, then depending on the received data, it can:

   1. SLEEP: Sleeps for a specified amount of time.
   2. UPLOAD: Receives data from a socket and writes it to a file.
   3. DOWNLOAD: Reads a from a file and sends it over a socket to the remote server.
   4. CMD: Executes a command.
   5. NOTHING: Does nothing, even though specified, judging from the decompiled code, it seems that any string other than the first four will do nothing.

Are there any useful network-based signatures for this malware?

1. The malware communicates with "http://www.practicalmalwareanalysis.com".
2. We see many instances of the malware communicating with sockets.

3. Analyze the Lab09-02.exe

What strings do you see statically in the binary?

We see many error messages and some .dll names, we also see a lot of import strings, among these there are several interesting import strings:

1. CreateProcessA
2. WSAStartup
3. WSASocketA
4. gethostbyname
5. closesocket
6. WSACleanup
7. htons
8. connect

What happens when you run this binary?

Nothing.

How can you get this sample to run its malicious payload?

We see that it calls GetModuleFileNameA with NULL as the hModule parameter, doing this returns the path of the executable. it then parses out the string after the last "\", which is the filename, it is then compared to "ocl.exe", if they are not the same, the program terminates, thus we just need to rename the executable to "ocl.exe".

What is happening at 0x00401133?

It is moving a lot of char values onto the stack:

"1qaz2wsx3edc" and "ocl.exe".

What arguments are being passed to subroutine 0x00401089?

At 0x004012AF, the program pushes the two arguments onto the stack, we see that the first argument is the string "1qaz2wsx3edc", the second is a pointer to [ebp-1F0] which turns out to be 0x0019FD50..

What domain name does this malware use?

After jumping to the ret in "0x00401089" and returning, we see the returned value in EAX is a pointer to the string "www.practicalmalwareanalysis.com".

What encoding routine is being used to obfuscate the domain name?

the code generates a 32 char long string by creating each char with s1[i % strlen(sq)] ^ s2[i], where s1 and s2 are the first and second arguments, and s2[i] is dereferenced as a char.

s1 46 06 16 54 42 …

s2 31 71 61 7A 32 …

w w w . p …

And so on.

What is the significance of the CreateProcessA call at 0x0040106E?

It creates a process with the command line “cmd” and with the following STARTUPINFO:

1. dwFlags = 257
2. wShowWindow = 0 (SW_HIDE)
3. hStdInput = <socket>
4. hStdError = <socket>
5. hStdOutput = <socket>

We can see that it creates a cmd process that does not display its window, and redirects all its STDIN STDOUT STDERR to the socket that the program previously connected to, thus allowing the malware owner to connect and control the host through cmd.