MARE HW 6

dj_{dvorak}

April 26, 2020

Contents

1 Lab 9-1

1.1 How do you install?

It seems to want an argument `-in "password"` which will install itself to the System32 folder. A A registry is created along with a service, presumably for persistence.

1.2 What are the command line arguments?

Well, the main file seems to include two arguments

It looks like there are two arguments in the main. It will check for the args `-re`, then `-in`. If the `-in` is passed, it also checks for `-c` and `-cc = flags. It turns out that =-in` will install, `-re` will uninstall and `-c` will pass in 4 arguments to update the configuratino and `-cc` will print the configuration.

1.3 Can we patch to remove the password?

Sure. Since we know where the desired the function is (`0x0000402b61`), we can modify the jump at the beginning of the program to make it unconditional.

1.4 Host based-indicators

Modifies the registers in `\\SOFTWARE\Microsoft\XPS`. Also, a copy of itself in system32 folder

1.5 The Pontential Remote Actions

Through the networked commands via HTTP requests, we can

- Download
- Sleep
- Do nothing
- Upload
- Run CMD (shell scripts)

1.6 Any useful network based signatures?

Well, it sends network requests to and from `https://practicalmalwareanalysis.com`. Uses GET request with HTTP 1.0. Seems to ask for different strings each time though.

2 Lab 9-2

2.1 What strings do you statically see in the binary?

The usual KERNEL32.dll, WSAsockets, Create and Terminate Processes. But also, unexpectedly we see some function calls to what appears to be getting and setting environmental variables. Nothing special.

2.2 Run the binary?

I will not run the binary

2.3 How to run this malicious payload?

The main exe takes a file argument and loads it through `GetModuleFileName`.

2.4 Examining `0x000401133`

So this occurs near the beginning of the `main()` and it loads a bunch of what appears to be ASCII characters. It looks like `1qaz2wsx3edc\0ocl.exe`. Later on, we realize this is two different strings: one for encoding and the other is simply the name of the url.

2.5 Examining `0x00401089`

Well, this seems to be a function call that takes two args, a char* and a integer. There is a call to `strlen()` and then a loop that calls an xor function. Just guessing but it might be an encryption algorithm. Actually, the argument seems to be the array from `0x00401133`.

2.6 Domain name

This name is `practicalmalwareanalysis.com`

2.7 What encoding routine is being used?

Probably a caesar shiftp with the XOR procedure.

2.8 On `CreateProcessA` at `0x0040106E`

This calls a command prompt and allows the execution of arbitrary commands. It is probably connected to the host domain name.