Assignment 3 (IDA) summary - Daniel Ayzenshteyn

**** A detailed analysis and answers to all questions could be found in pdf files under the corresponding directories - this file is the summary of the key points in the assignment**

Question 1

The task included patching a number of bugs found in the sample - at the end I was able to make the program functional, working as “strings” program:

```
C:\Users\user\Desktop\hw3-samples2\samples>q1.exe test.txt 1 100
Hello
there
I'm
daniel
the
reverser!

C:\Users\user\Desktop\hw3-samples2\samples>
```

```
C:\Users\user\Desktop\hw3-samples2\samples>q1.exe ..\..\hw3-samples\samples\q1.exe 0 1000
MZÉ
=!╕L=!This
program
cannot
be
run
in
DOS
mode.
$
╥]g╫╠╥]g╧╠╥]g╙╠╥ji╧╠
╥┌┐>╥ª┌╥╠╥ª┌4┐╥ª┌╔╠╥Rich╥
```

Question 2

This is an Injector program, which injects a payload into other process memory and executes a thread which runs the payload. The payload itself is used to collect information about the other process running times in different modes (kernel/user) and implements a 64 bit division that could not be supported on the hardware. However the results of this injection not appear to be returned to the injector process and could not be collected.

Question 3

The 3 functions are: Caesar Cipher (key=3), Reverse (string) and XOR encryption (with 75).

Question 4 - Sample 4

The malware gains persistence via the registry under the name “PHIME2008”. It then downloads and runs msupd.exe. Enumerates the system with custom functions that get the local time, local ip and some other api calls to get computer name, user name and local info. This collected data is sent to a C2 server via HTTP GET request to a hard coded ip 125.206.117.59 on port 80. Then it runs 100 threads which execute the same function “scan_network” (sub_401870) indefinitely. The “scan network” function scans the network with randomly generated non-private ip addresses and searches for machines which have port 445 open. If such a machine is found the whole subnet /24 is scanned for more targets with open port 445 (SMB). On each found SMB share an enumeration is done to identify the users on the share. This list of users is then combined with a pre-made wordlist to make a

dictionary attack on the open IPC$ share. If the login attempts succeed with any credentials the malware tries to exploit the target via uploading a payload to the remote share and scheduling a task to run the payload remotely. Overall - this sample persists on the infected machine, downloads additional payload (dropper), exfiltrates data (espionage) and tries to exploit and infect other machines on the network (worm) via the IPC$ share.

Question 4 - Sample 5

The analyzed malware demonstrates sophisticated techniques for stealth and persistence (Registry & Services), including user impersonation (Impersonate), dynamic resolution of system calls (GetProcAddress), and manipulation of Windows services. It has capabilities for lateral movement through network and service exploitation, potentially allowing the malware to spread within and across networks - Via remote services and registry. The malware employs various evasion tactics, such as obfuscation and encryption and such as disabling file system redirection and cleaning up after execution to minimize detection. It interacts with the Windows Registry and uses the Service Control Manager to modify system configurations and service properties, possibly for deploying malicious payloads or sabotaging system operations. In the resources there are 3 noised pictures that are probably decryption keys or other steganography.
It also includes a copyright string that is used for disguise.

Thanks for reading!

**** A detailed analysis and answers to all questions could be found in pdf files under the corresponding directories - this file is the summary of the key points in the assignment**