

**Malware Analysis Tools and Techniques**

Year 2 (2022/23), Semester 4

## SCHOOL OF INFOCOMM TECHNOLOGY

Diploma in Information Security and Forensics

**COMMON TEST SAMPLE REVISION PAPER**

INSTRUCTIONS TO CANDIDATES:

1. Write your Student Number, Name, Module Group and Seat Number CLEARLY in the answer booklet.
2. This paper consists of 13 pages including this cover page. Check carefully to make sure your set is complete.
3. There are FOUR questions. Answer **ALL** questions.

Question 1 – 30 marks

Question 2 – 20 marks

Question 3 – 30 marks

Question 4 – 20 marks

1. This is an Open Book test.

There are FOUR questions. Answer **ALL** questions.

**Question 1 (30 marks)**

1. VirusTotal is a free online service that aggregates more than four dozen antivirus scanners made by Symantec, Kaspersky Lab, F-Secure and others. Researchers, and anyone else who finds a suspicious file on their system, can upload the file to the site to see if any of these scanners tag it as malicious.

Describe briefly any **TWO** disadvantages of VirusTotal.

(5 marks)

1. It can give conflicting results. As it uses many Avs to scan the file, there are times when the AVs will have contrasting results and if this is split near 50-50, the results can be confusing.
2. Zero-day malware, or malware that is new will not be detected by VirusTotal, as the malware signature will not be recognized by any of the AV used in VirusToltal.
3. Match the malware to the properties that best describe the malware.

|  |  |
| --- | --- |
| **Malware** | **Properties** |
| 1. Rootkit | a. replicates and spreads independently Virus |
| 2. Virus | b. tracks user activities and steals information Spyware |
| 3. Ransomware | c. hard to detect and remove Rootkit |
| 4. Adware | d. disguises itself as a harmless and useful program to  trick users to download and install malware Trojan |
| 5. Worm | e. attaches to files and cannot activate the malicious code  contained until user launches the file Worm |
| 6. Spyware | f. denies access to infected computer, locking the user out  of the system until a demanded price is paid Ransomware |
| 7. Trojan Horse | g. automatically displays advertisements Adware |

(7 marks)

1. Explain the importance of software updates with regard to malware?

(4 marks)

Software updates patch security vulnerabilities that malware might use to exploit, hence, by having software updates these vulnerabilities will cease to exist and the malware will be rendered useless.

**Question 1 Cont.**

1. What term is commonly used to describe the method or mechanism by which a piece of malware infects a system?

A. Starting Point

B. Point of Origin

C. Entry Point

D. Origination Point

(2 marks)

Ans: C

1. Which of the following system calls is most likely to be used by a keylogger?

A. GetHookAddress

B. GetKeyBoardState

C. GetSyncKeyState

D. GetAsyncKeyState

(2 marks)

Ans: D

1. Which of the following Windows registry keys is most useful for malware that aims at maintaining persistent presence on the infected system?

A. HKLM\Software\Microsoft\Windows\CurrentVersion\Run

B. HKLM\SECURITY\Microsoft\Windows\CurrentVersion\boot

C. HKLM\Boot\Microsoft\Windows\CurrentVersion\start

D. HKCU\System\CurrentControlSet\Control\ CurrentVersion\Run

(2 marks)

Ans: A

1. Which of the following is the least efficient in terms of memory management?

A. Absolute loading

B. Relocatable loading

C. Static loading

D. Dynamic run-time loading

(2 marks)

Ans: A

**Question 1 Cont.**

1. In the context of malware analysis, what does the term "patching" refer to?

A. Installing software updates that address vulnerabilities in installed

software.

B. Setting memory breakpoints by modifying access flags on memory

segments.

C. Stepping through the executable without running every instruction within

function calls.

D. Modifying a compiled executable to change its functionality without having

to recompile it.

Ans: A

(2 marks)

1. Which form of analysis involves going through lines of code but never running the file in question?
2. Basic Static Analysis
3. Basic Dynamic Analysis
4. Advanced Static Analysis
5. Advanced Dynamic Analysis

(2 marks)

Ans: A

1. Which of the following defensive measures do malware authors use to encode the original executable to protect it against code analysis?

A. Employing fast-flux DNS techniques

B. Embedding an imports table in the malicious executable

C. Targeting client-side vulnerabilities

D. Packing the malicious executable

(2 marks)

Ans: D

**Question 2 (20 marks)**

1. Figure 2a shows a list of strings extracted from the malware blinky.exe. Find **FIVE** important strings that could reveal some information and explain why these strings are useful.
2. Googlebot/2.1 (<http://www.googlebot.com/bot.hmtl>)

Indicates that there is a request made to googlebot.com which means that the malware might be trying to perform some bot attacks.

1. /download.php

Indicates that the malware is downloading something

1. /execute.php

Indicates that the malware is executing something

1. WriteFile

Indicates the malware is writing data to a file

1. 81.95.152.178

Indicates that the malware is connecting to a domain with an IP address of 81.95.152.178

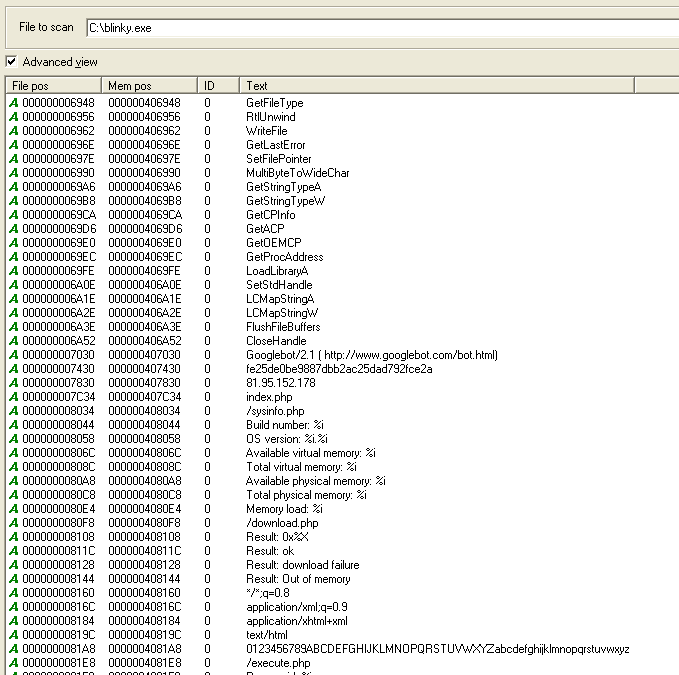


Figure 2a: List of strings from Blinky.exe

(10 marks)

**Question 2 Cont.**

1. Figure 2b shows the Import address table of the malware blinky.exe. Explain why we have two different Imports table (Import Address Table and Import name table) but they both point to same structure in disk? (I have no clue)

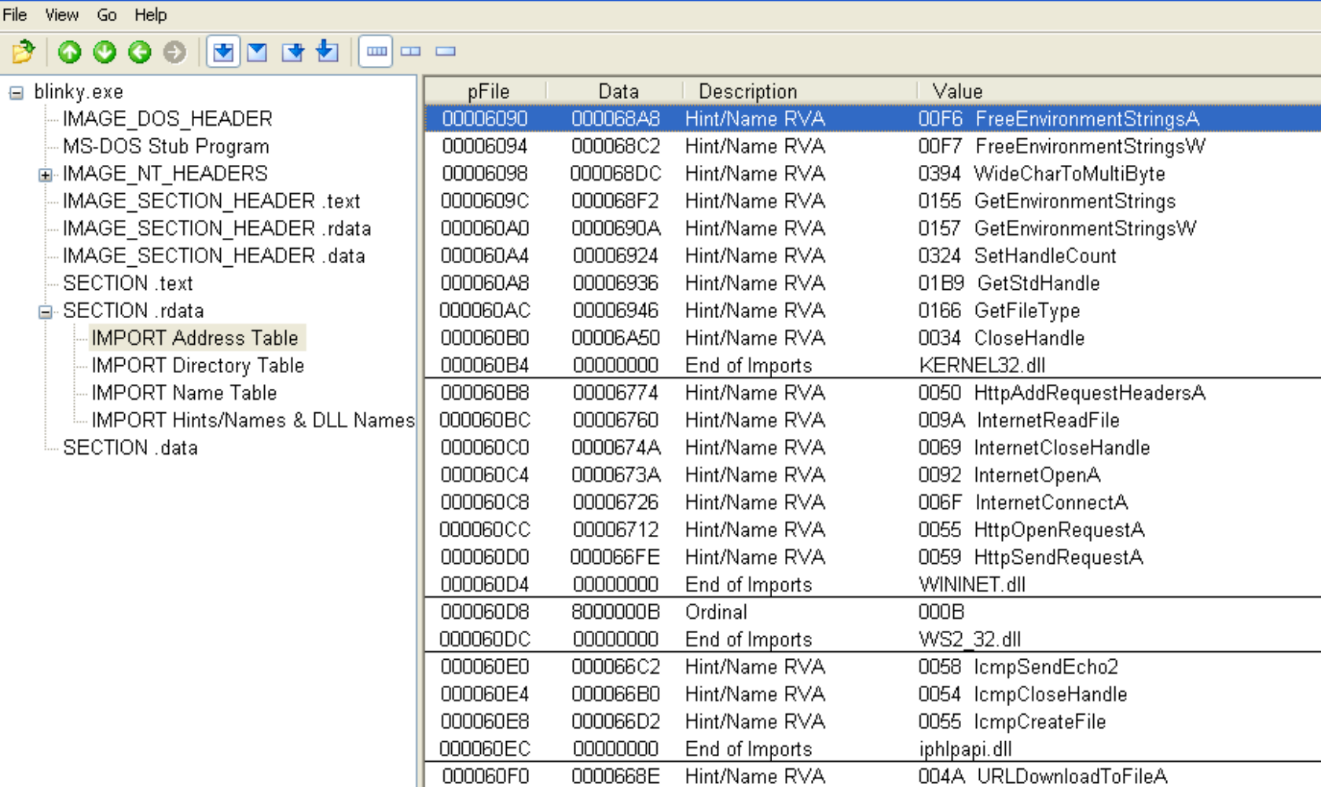


Figure 2b: Import address table of blinky.exe

(5 marks)

**Question 2 Cont.**

1. Figure 2c and 2d shows the dll’s imports and exports of the malware blinky.exe.

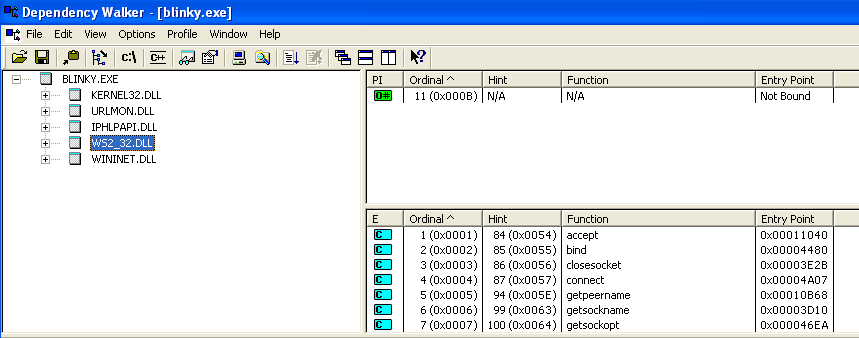


Figure 2c: Dll’s imports and exports table of blinky.exe

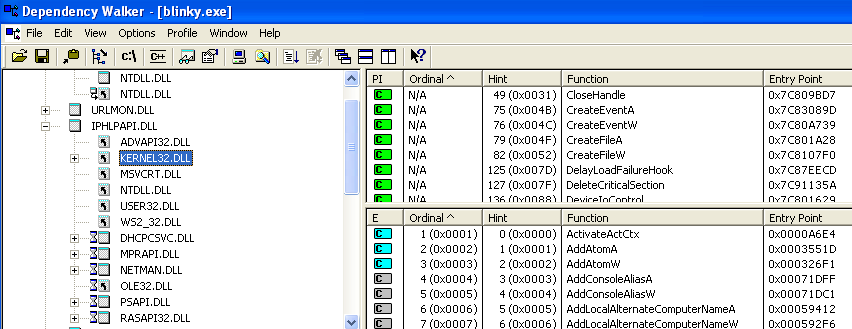


Figure 2d: Dll’s imports and exports table of blinky.exe

**Question 2(c) Cont.**

1. How many DLLs does the malware blinky.exe import?

(1 mark)

Blinky.exe imports 5 DLLs

1. What is difference between import table and export table?

(2 marks)

The import table is the table that lists the functions that the malware imports and uses. The export table is the table that lists the functions that the malware allows other DLLS and executables to import.

1. What is the purpose of ordinal value?

(2 marks)

The ordinal value is the memory address of where the function is located. So if any executable wants to use the function, it can import it using the ordinal value.

**Question 3 (30 marks)**

1. Figure 3a shows the process explorer while the malware blinky.exe is running.

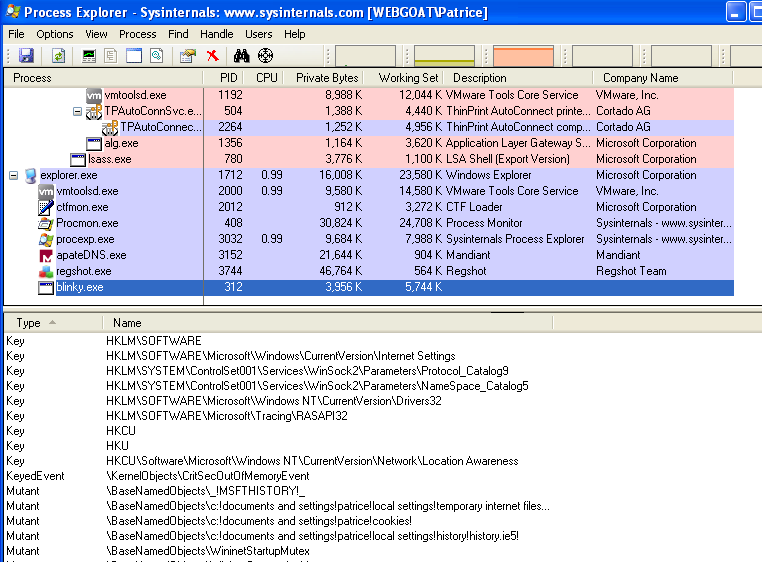


Figure 3a: Process explorer for blinky.exe

**Question 3(a) Cont.**

1. What is a mutex object? Why do malware authors create a mutex object?

(3 marks)

A mutex object is a kernel object which allows programs to synchronize events between them. Malware authors create mutex objects to prevent the malware from reinfecting an already infected system.

1. Does the malware blinky.exe create a process injection? Briefly explain process injection? (Don’t know)

(3 marks)

1. Apart from analysing for the mutex object, list any **THREE** important features which process explorer offers during malware analysis.

(6 marks)

1. Compare the strings in disk and string in memory of the malware
2. View the DLLs that the malware imported
3. View processes as well as their children processes to determine processes that are malicious.
4. Figure 3b and 3c shows the process monitor while the malware blinky.exe is running. Find **FOUR** important operations that could reveal some information and explain why these operations are useful.

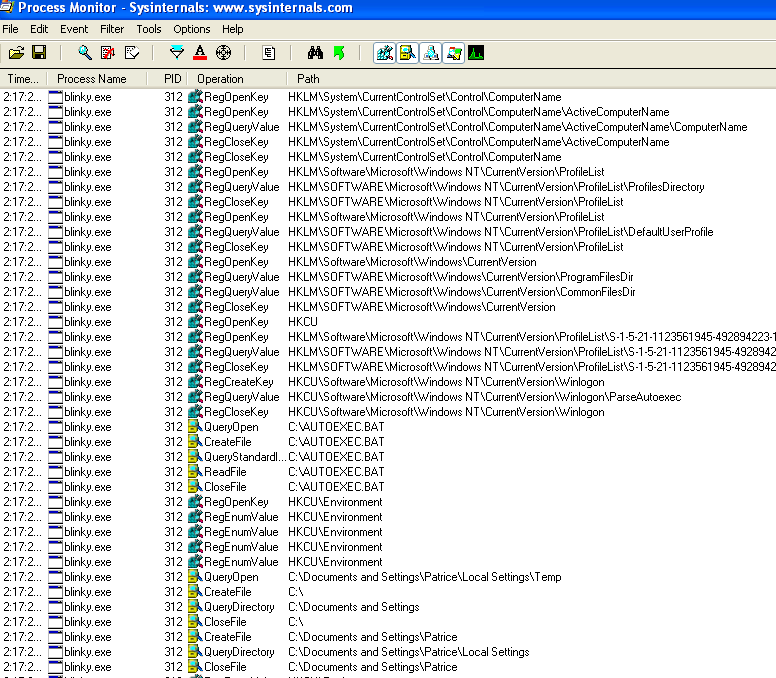


Figure 3b: Process Monitor for blinky.exe

**Question 3(b) Cont.**

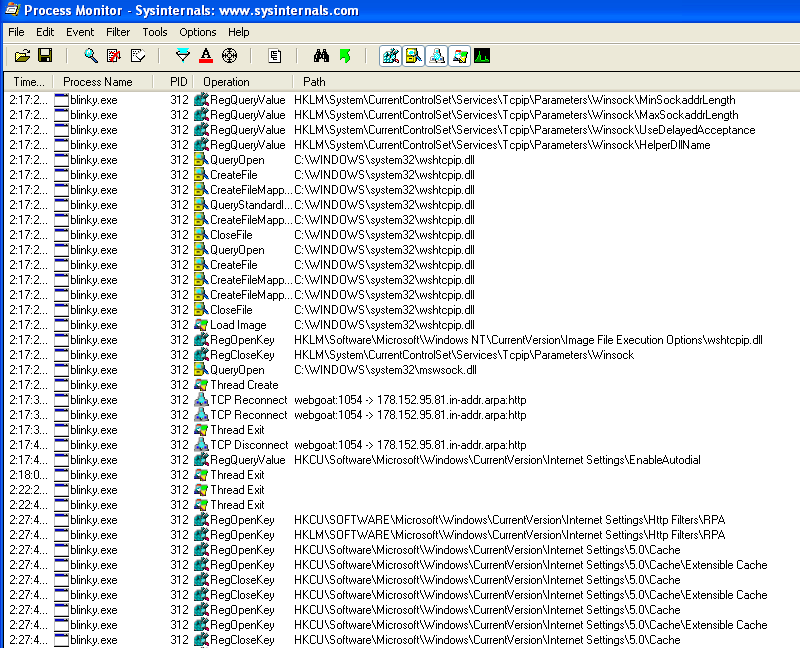


Figure 3c: Process Monitor for blinky.exe

(8 marks)

1. Describe the functionality and purpose of this malware by indicating clearly any **THREE** important host-based and network-based indicators. Note: You can refer to the basic static analysis details in Question 2.

(10 marks)

**Question 4 (20 marks) (Not Learnt)**

The number of crypto mining malware attacks used by hackers has continued rising, with total samples growing by 86% in the second quarter of 2018, according to the latest threat report by cybersecurity firm McAfee Labs released September 25, 2018.

(Source: https://cointelegraph.com/news/mcafee-labs-crypto-mining-malware-grows-by-86-in-q2-over-25-mln-new-coin-miner-samples)

1. Briefly explain why and how hackers typically launch a crypto mining malware attack.

(6 marks)

1. What are the typical warning signs observed in a victim’s PC that is infected with a crypto mining malware?

(2 marks)

1. Explain the terms Obfuscation, Hashing, and Encryption with regards to malware analysis?

(6 marks)

1. Figure 4 shows an obfuscated JavaScript code. Justify what is the code trying to achieve?

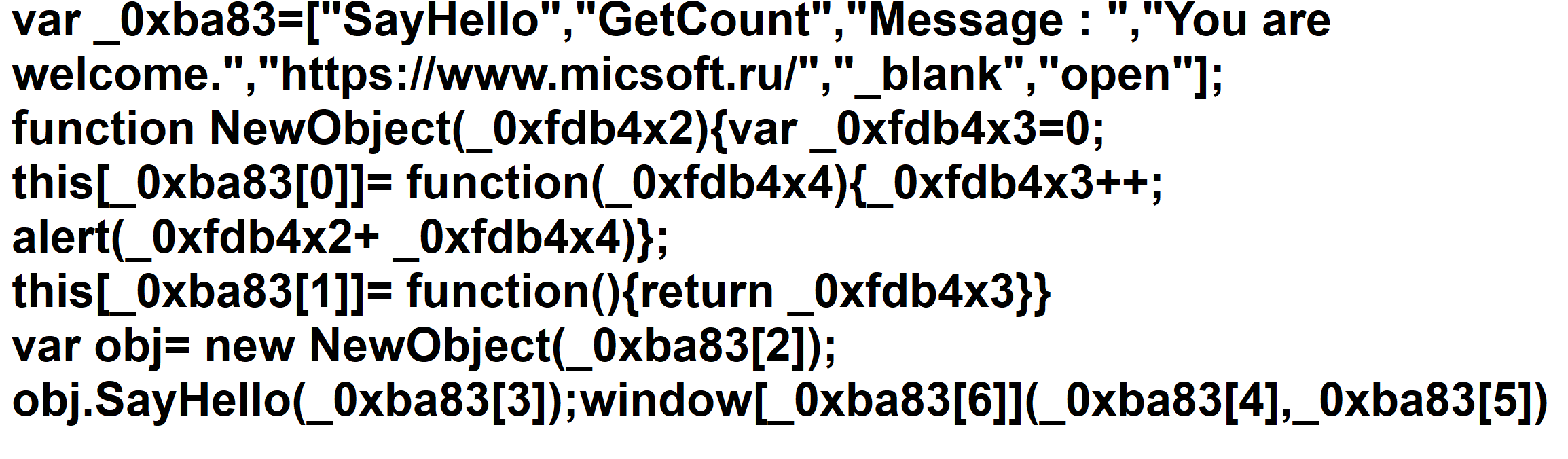


Figure 4: Obfuscated JavaScript

(6 marks)

\*\* END OF PAPER \*\*