Abertay University

Evaluation of static, dynamic, and hybrid analysis techniques in the analysis of various malware.

Selina Fahy

CMP320: Ethical Hacking 3

BSc Ethical Hacking Year 3

2020/21

Note that Information contained in this document is for educational purposes.

.

Abstract

Malicious software, otherwise called malware, is becoming a common occurrence in the modern-day world as computerized devices are being used more and more. Viruses, spyware, adware, ransomware – these are some of the most common forms of malware that people and companies are falling victim to.

In this report, the tester goes over different types of malware and uses them to evaluate malware analysis techniques. The techniques that are discussed are Static analysis, Dynamic analysis, and Hybrid analysis.

Overall, the tester found that each technique holds their own advantages and limitations, as well as the environments that some are best used in – for example setting up a virtual machine for dynamically testing malware in order to minimize damage.

.

Contents

.

1 INTRODUCTION

1.1 BACKGROUND

Malicious software, also known as malware, is software purposefully made with the intent to do harm to a computer, network or device in order to gain access to information and do harm.

Viruses, Worms, Trojan Horses, adware and much more are some of the most common forms of malware. These programs were developed and sent across the internet in order to cause disruptions, steal information and/or to gain access to multiple devices for other intentions. With computers and the internet growing in popularity it is becoming a primary target when malicious users attempt to attain some form of information regarding other users. Such information can pertain to personal information, credit card details, or even finding way to steal user accounts to certain websites, etc. To fight these malicious programs, one needs to analyse them first. One technique of analysis is through Static analysis, which involves examining the code without executing the program.

Static analysis is considered to be the safer technique of malware analysis due to the lack of execution of said malware. However, due to the limitations of static analysis other methods needed to be considered.

Another such technique to analyse malware is through dynamic analysis. Dynamic analysis involves the actual executions of the malware to examine it's behaviour. In order to minimize damage, it is recommended that dynamic analysis occurs within a sandbox/virtual machine, as this will stop the malware from having an effect on the host PC and the network that it is connected to.

However, dynamic analysis has limitations which further provides the need to be able to examine malware a step further. This introduces the hybrid analysis technique which is a combination of static and dynamic analysis claiming to make up for the limitation in both of the mention techniques.

1.2 AIM

The aim of this report is to conduct several tests in order to evaluate the analysis techniques of malware analysers through analysing malware. By following a methodology, the tester will use each of the 3 techniques – static, dynamic and hybrid – to analyse various malware and evaluate each one in terms of how well they can determine the potential effects of the chosen malware.

This report aims to capture the process of analysis and explain the techniques while also demonstrating the techniques through analysing malware.

In order to achieve this the following objectives should be met:

- Setting up a safe environment for malware analysis.
- Prepare tools that will be used – gaining information regarding the tools used for each technique such as PEview, Dependency Walker, Wireshark, etc.
- Using methodology with each of the 3 different analysis techniques on varying types of malware.
- Reporting and evaluation – reporting all findings regarding the analysis of malware using each of the techniques supported by evidence and evaluate each technique describing their benefits and limitations.

1.3 METHODOLOGY

The tester mainly followed the guidance of the Practical Malware Analysis: A Hands-On Guide to Dissecting Malicious Software (Sikorski and Honig, 2012), which allowed the tester to follow a highly regarded malware analysis book to produce a comprehensive evaluation of malware analysis techniques.

The malware used in the report was downloaded from the practical malware analysis website under the 'labs' tab (Sikorski and Honig, 2012).

Methodology:

1. Static Analysis – a method in order to inspect malware without running it. This allows for analysis of the code and checking for signature recognition.
2. Dynamic Analysis – a method to examine malware by running it in a simulated environment (e.g. virtual machine). This allows for the analysis of the behavior of the malware.
3. Hybrid Analysis – a combination of Static and Dynamic analysis that overcomes many of the limitations of these two methods. This method allows for the analysis of signatures and observation of behaviour.

1.4 TOOLS

Here the tester will be explaining all the tools that will be used, a basic guide on how to use them, and what they do.

Some of the tools that the tester used were PEview (Radburn, 2019), PEiD (Download PEiD 0.95, 2018), Dependency Walker (Dependency Walker (depends.exe) Home Page, n.d.), Process Monitor (Wayback Machine, n.d.), Process Explorer (Russinovich, 2020), Regshot (regshot, 2008), ApateDNS (ApateDNS Download | FireEye, 2021), INetSim (Hungenberg and Eckert, 2007), Strings searching (Rissinovich, 2016), and Wireshark (Index of /download, 2012).

The first tool that will be looked at is PEview. PEview is a free and easy to use tool that is used to look at PE files, such as PE headers and PE sections. This helps in identifying imports, file size, and other file specific data.

The next tool that will be looked at is Process Monitor. Process Monitor is an advanced monitoring tool for Windows that provides a way to monitor registry, file system, network, process, and thread activity. Process Monitor uses RAM in order to log data about the system, in which can lead to the crashing of the VM, so when the tester felt that there was no need to continue monitoring, Process Monitor was turned off.

Next, there is Process Explorer, which is an application that monitors running processes and displays them through a parent-child relationships diagram.

Another tool used was Regshot – a registry snapshot tool. Regshot is an "open-source registry comparison tool" (regshot, 2008) that allowed the tester to take and compare two registry snapshots before and after the execution of malicious software. To do this the tester launches Regshot and takes a snapshot using the "1st Shot" button, runs the malware, then when the malware is presumed to have 'finished', the tester then takes a second snapshot using the "2nd Shot" button. Finally, by clicking the "Compare" button, the two snapshots are compared and returned as either a plain .TXT file or a HTML file.

ApateDNS is a free to use tool that spoofs DNS requests through listening on port 53. By connecting ApateDNS to a fake webserver that was set up on the Linux VM, it is possible to capture any requests sent along this port.

INetSim is a free software suite that can be used to simulate common Internet services. It fakes HTTP, HTTPS, FTP, IRC, DNS, SMTP, etc. connections (Sikorski and Honig, 2012).

Finally, Wireshark is an open-source sniffer or otherwise known as a packet capturing tool that intercepts and logs network traffic.

2 PROCEDURE

2.1 OVERVIEW OF PROCEDURE

Following the methodology mentioned, the tester went on to evaluate the different techniques in malware analysis. To achieve this the tester used a selection of malware from the labs located on the practical malware analysis website alongside a selection of tools to analyse the malware with.

2.2 PROCEDURE

2.2.1 Static analysis

2.2.1.1 Unpacked

The tester started with static analysis when evaluating the analysis techniques with various malware for this report. The tools that were used for this were Virus Total, Dependency Walker, PEview, and PEiD**.**

Firstly, the tester sent a malicious .EXE file through virualtotal.com to see if it was a malicious software with a signature commonly known. The results can be seen in the following figures Figure 1 and Figure 2, with all results seen in Appendix A.

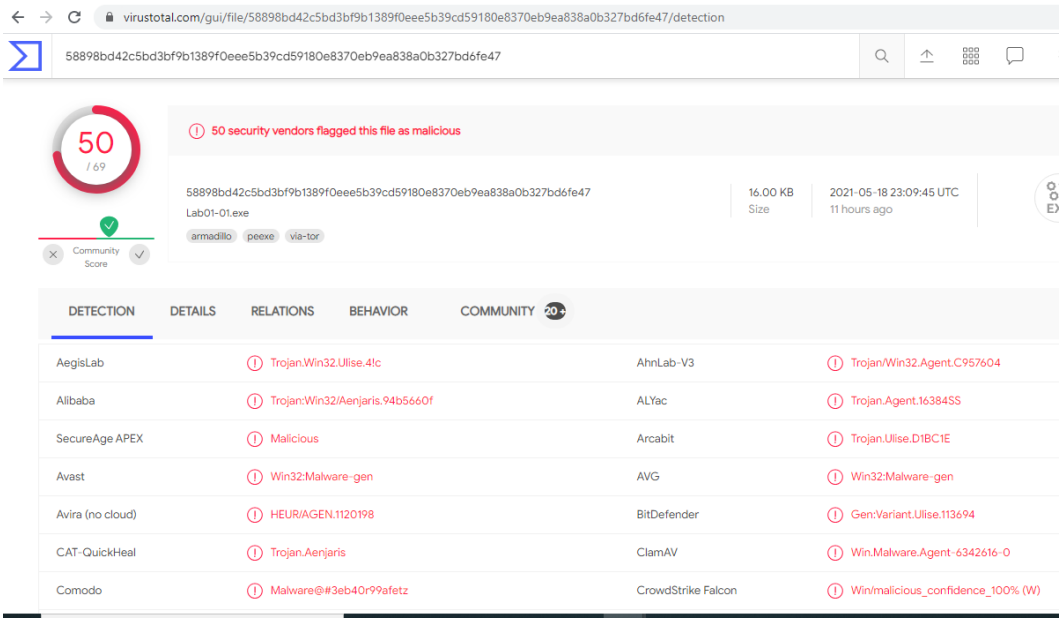


Figure 1 Virus Total – Lab01-01.exe

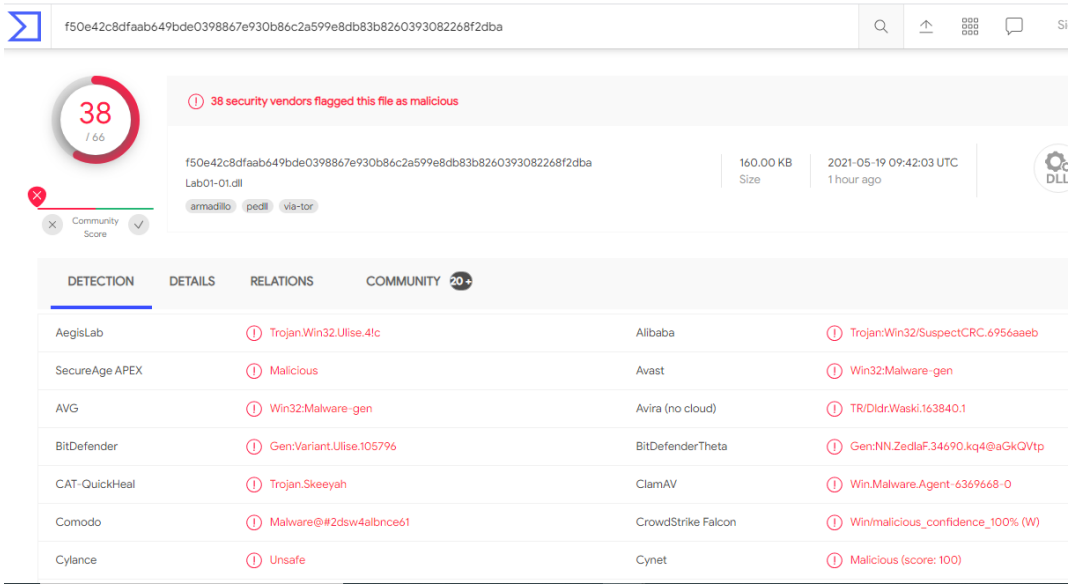


Figure 2 Virus Total – Lab01-01.dll

The above figures informed the tester that these two files are registered as malicious files on most of anti-virus scanners.

Next, the tester looked at the malware with it's corresponding .DLL file through Dependency Walker as seen in Figure 3 and Figure 4. In these figures it can be seen that there are a few imports including kernel32.dll and msvcrt.dll, each importing further functions. Screenshots pertaining to the entire Dependency Walker results can be seen in Appendix B.

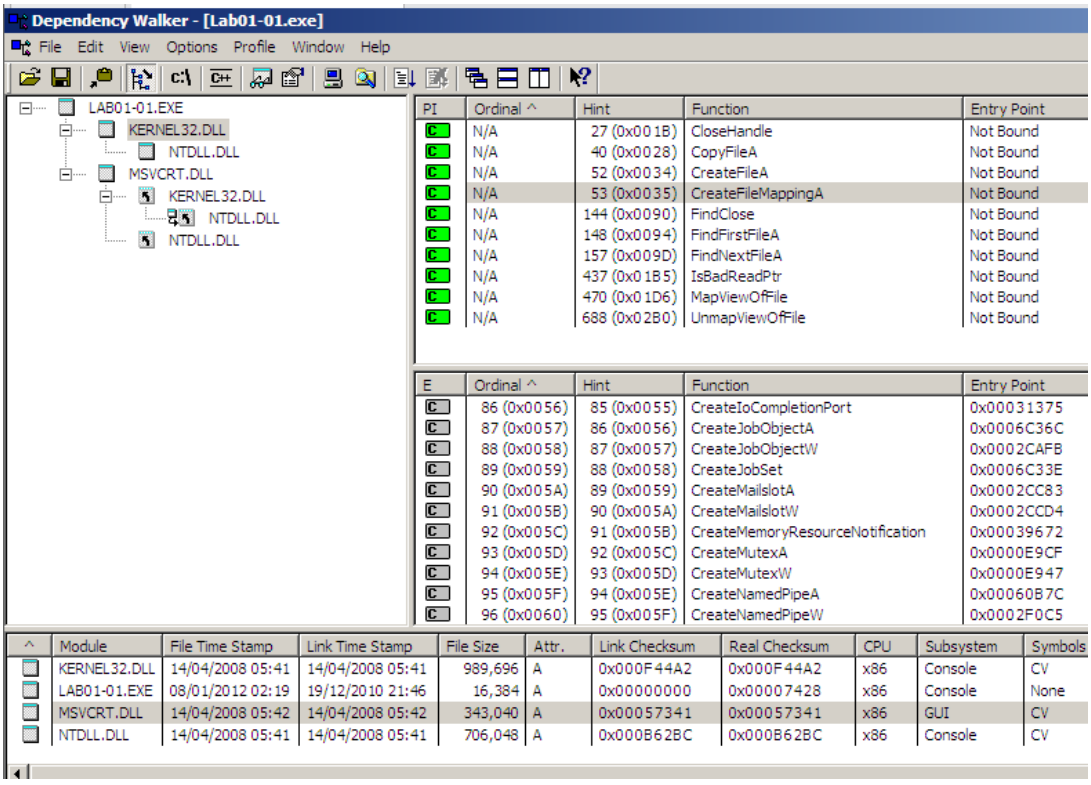


Figure 3 Static analysis of Lab01-01.exe Malware in Dependency Walker

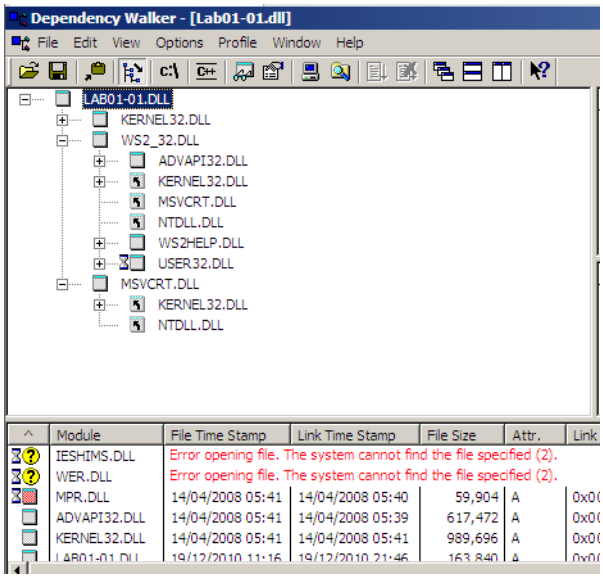


Figure 4 Static analysis of Lab01-01.dll in Dependency Walker

Kernel32.dll is a very common DLL that contains all key functions that allow for programs to do things such as have access to and manipulate memory, files, and hardware. Furthermore, the ws2_32.dll file

is library that is used to handle network connections. It relates to software processes and allows applications to communicate.

Then, the tester used the tool PEview in order to look at any chances that the malware is packed or obfuscated. This is done by looking at and comparing the Raw Data value and the Virtual Size. If the malware is not packed at most there will be little difference between the size of them, otherwise if there is a large difference between the two, this indicated that the malware had been packed. In Figure 5 it can be seen that there is very little difference between the Raw data and the Virtual Size, therefore it can be assumed that this particular malware is not packed in any way.

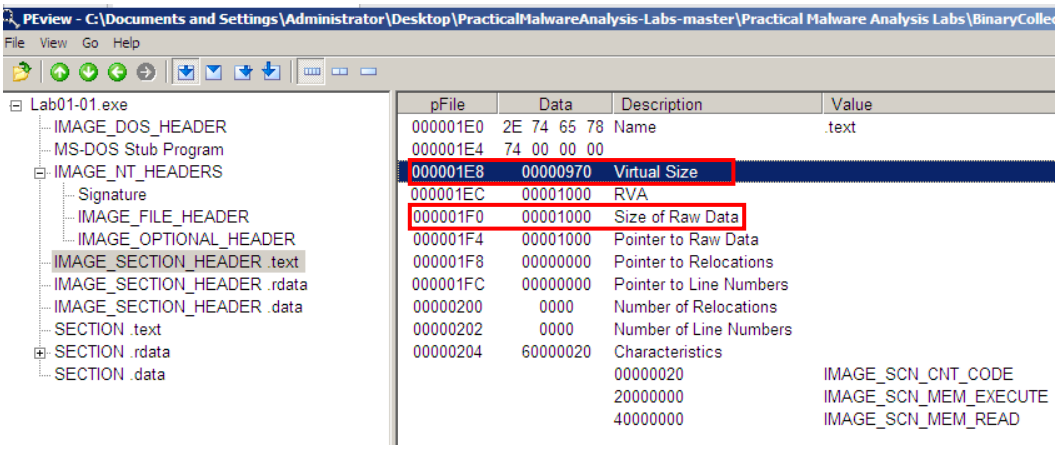


Figure 5 Static analysis of Lab01-01.exe in PEview - checking Raw Data and Virtual Size

Furthermore, the packed state is further confirmed through the use of another tool: PEiD. This tool helps in identifying if software is packed and potentially what was used to pack it. As seen in Figure 6 this particular malware is not packed and has been identified as having been compiled with Microsoft Visual Studio C++.

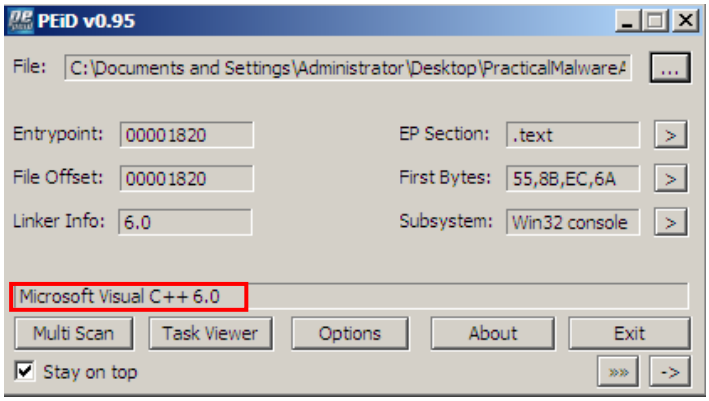


Figure 6 Static analysis of Lab01-01.exe- packed state through PEiD

After determining that the malware was not packed, the tester then moved on to see what sort of information could be gathered through string searching. To do this the tester used the Microsoft Strings program. The tester was able to find out some possible functionalities of the malware – as seen in Figure 7 and Figure 8 below, in which all information returned can be seen in Appendix C.

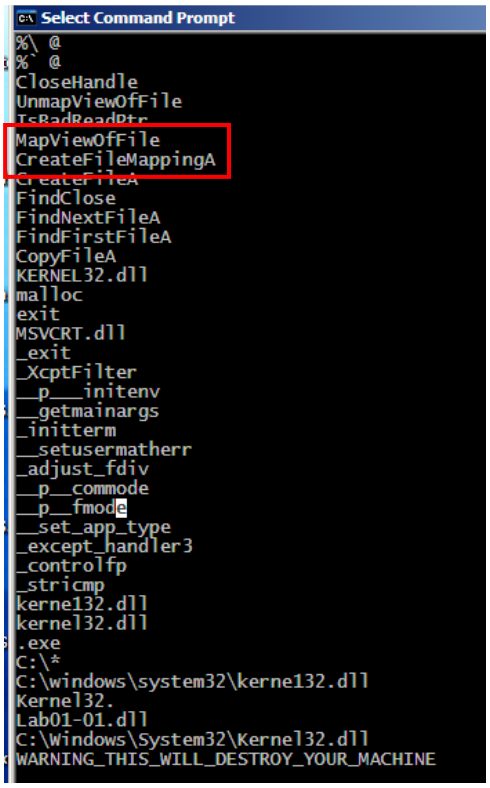


Figure 7 Static analysis of Lab01-01.exe - String search

Figure 8 Static analysis of Lab01-01.dll - String search

From Figure 7, it can be noted that some interesting functions that were being called were 'CreateFileMap', 'FindFirstFile', and 'FindNextFile'. The CreateFileMap and MapViewOfFile are both functions that allow for the software to create a 'Map' object that will allow for the software to be able to gain access to the Shared Memory – where, in simple terms, the CreateFileMap is the map object and MapViewOfFile allows the access to the memory. While the FindFirstFile and FindNextFile are functions that are used to search for specific names and files. Furthermore, there is the interesting collision of similar looking names 'Kernel32.dll' and 'Kerne123.dll', which may indicate that the malware may attempt to disguise itself as the kernel32.dll file and may contain malicious code.

Therefore, it can be presumed, from the above Figure 7, that the malware searches for .EXE files on the machine and attempts to disguise it's core malicious code as the kernel32.dll file using the name kerne123.dll.

While from Figure 8 it can be seen that there are fewer functions called, but one interesting one is 'CreateProcessA', followed by what seems to be an IP address '127.26.152.13'. 'CreateProcessA' is a function that allows for a process to be created along with a primary thread, and when used can call any process that the user wants e.g., malicious software.

It is also noted that both 'CreateProcessA' and sleep are used for backdoors, which may explain the IP address found (CreateProcessA function (processthreadsapi.h) - Win32 apps, 2018).

2.2.1.2 *Packed*

Before analysing the next malicious software, the tester uploaded Lab01-03.exe to virustotal.com in order to check if the signature was registered and a commonly known malware (Figure 9). As seen in the figure, a large majority (51 out of 69) were able to identify it as malicious.

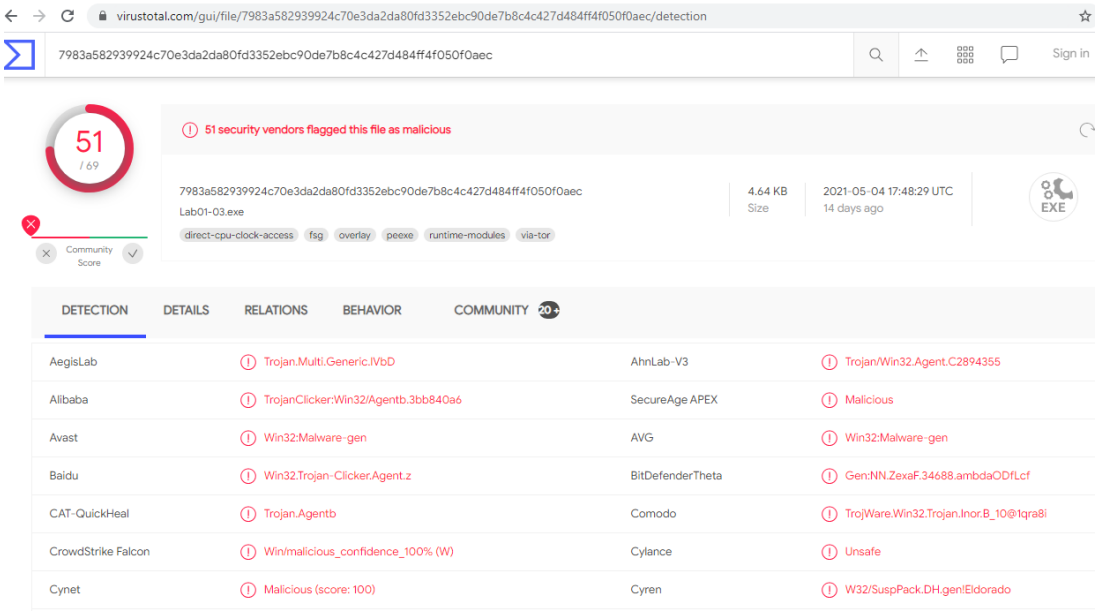


Figure 9 Virus Total - Lab01-03.exe

Next, the tester determined that this malicious file that was packed. This was determined to be packed through the lack of imports that could be found through the use of Dependency Walker as seen in Figure 10. There is only 1 import: Kernel32.dll, which is very unlikely in any software which leads it to being packed.

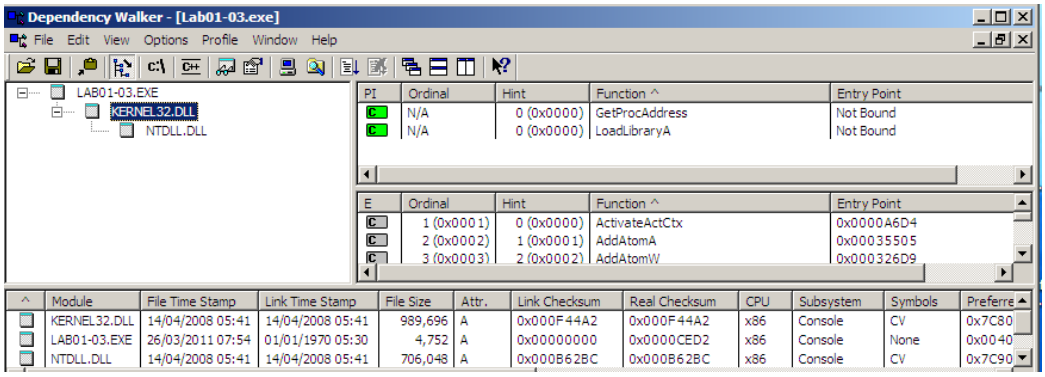


Figure 10 Static analysis of Lab01-03.exe - Dependency Walker

This is further confirmed through the use of the PEiD tool and PEview tool, in which the malware was packed using FSG (Figure 14). As can be seen in Figure 11, Figure 12 and Figure 13 the size of the Raw Data is significantly less than the Virtual Size. This would further indicate that the malware is packed.

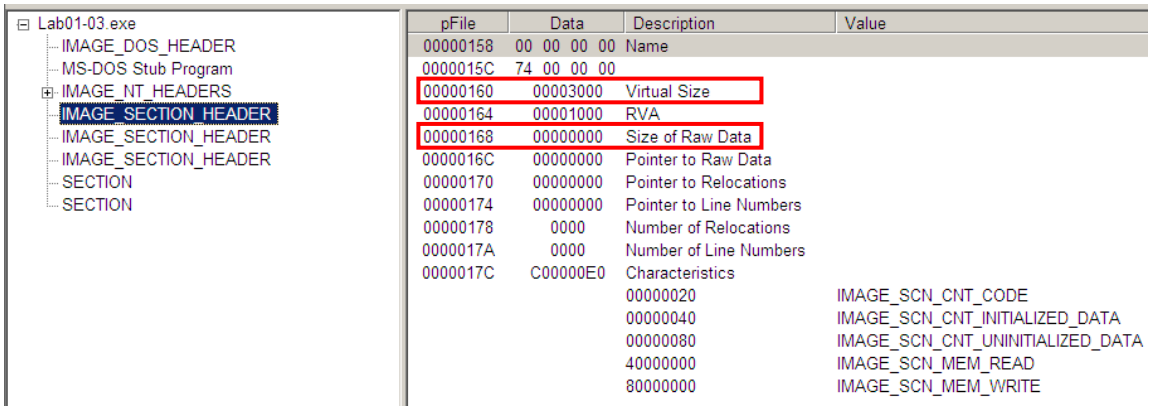


Figure 11 Static analysis of Lab01-03.exe- comparing Raw Data and Virtual Size

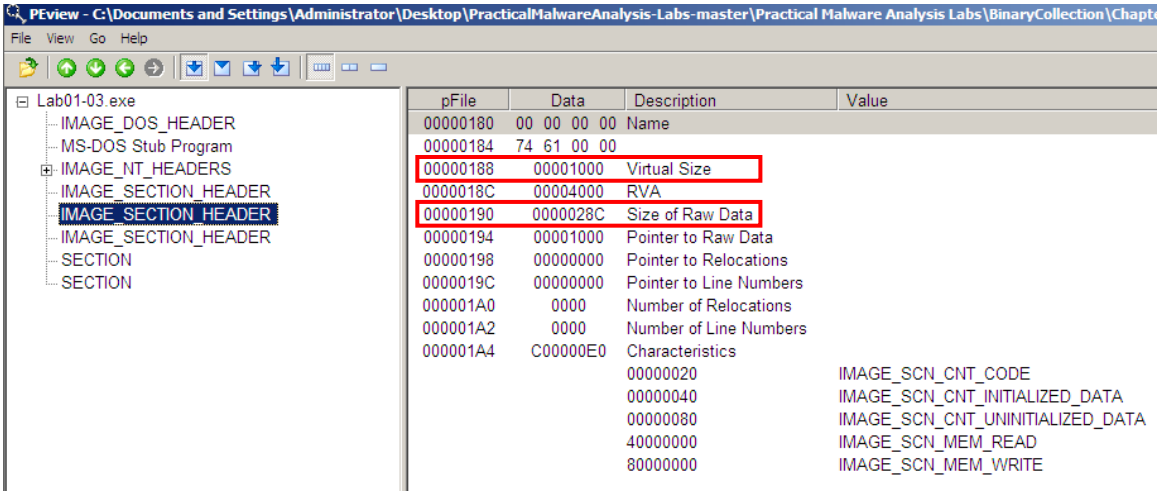


Figure 12 Static analysis of Lab01-03.exe- comparing Raw Data and Virtual Size

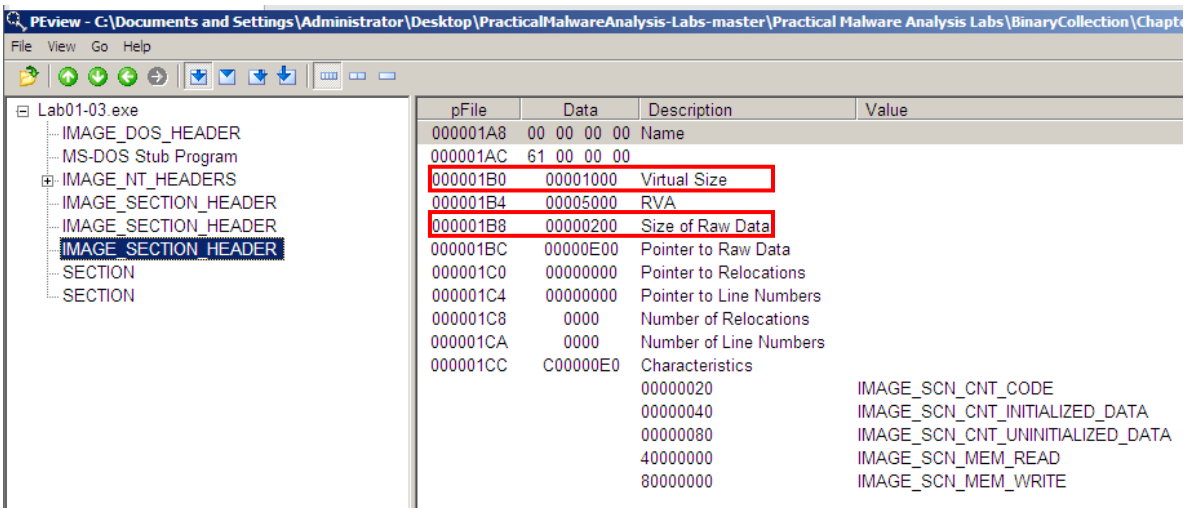


Figure 13 Static analysis of Lab01-03.exe- comparing Raw Data and Virtual Size

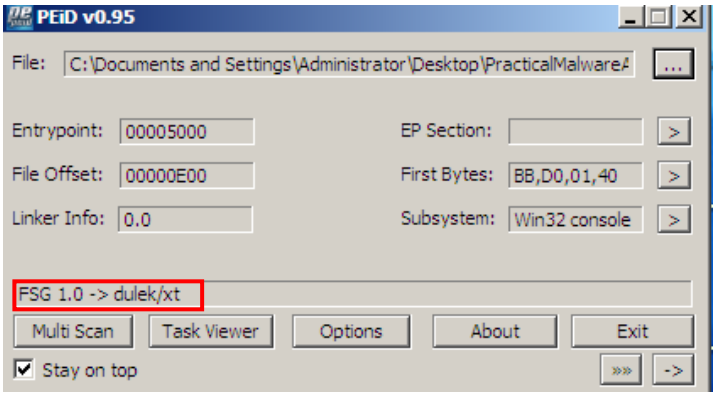


Figure 14 Static analysis of Lab01-03 packed state in PEiD

Due to the malware being packed and the tester lacking the correct knowledge for unpacking this specific malware, it was no longer possible for the tester to be able to move on in the investigation of the malware.

2.2.2 Dynamic analysis

2.2.2.1 Basic

The next technique that the tester looked at in malware analysis is dynamic analysis, where examination of the malware occurs after the execution of it. Unlike static analysis, dynamic analysis allows for the tester to be able to learn about the actual functionality of the malware, over speculation.

One could dynamically examine malware through the use of sandboxes/ Virtual Machines. Sandboxes often have the ability to analyse malware for free and are popular to use. As demonstrated in 2.2.1, the tester set up a Windows XP and a Kali Linux virtual machine for the dynamic analysis.

The tools that were used during the analysis were Process Monitor, Process Explorer, Netcat, Regshot, ApateDNS, INetSim and Wireshark. To start, Process Monitor was launched then in order to stop RAM being used up too quickly the logging was stopped and the display cleared. Following this, to save time a filter is set so that when logging is turned back on, only desired information is displayed. After, the rest of the tools are launched and set up as well such as Process Explorer, Regshot, a fake network using ApateDNS and INetSim, Netcat, and finally Wireshark.

Overall, the basic dynamic analysis method looks something like:

- Run process monitor
  - stop
  - Clear data
  - Set filter
  - Run
- Start process explorer
- Gathering a first snapshot of the registry using Regshot
  - Take a second snapshot after running malware to compare later
- Setting up VM with INetSim and ApateDNS
- Setting network traffic logging with Wireshark

The virtual network looked something like this: 2 hosts – the malware analysis Windows XP VM running ApateDNS and the Kali Linux VM running INetSim. The Linux VM is listening on many ports (80, 442, 23) while the Windows is listening for DNS (port 53) requests. The DNS server on Windows has been configured to localhost (127.0.0.1, otherwise the IP of the Linux machine). While ApateDNS is configured to redirect you to the Linux VM (IP) as seen in Figure 15.

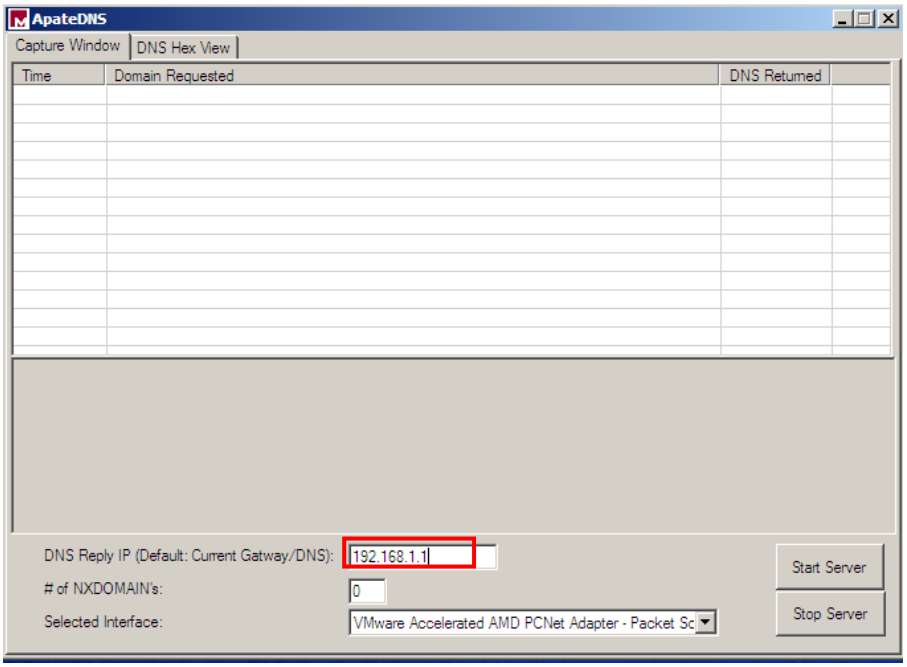


Figure 15 Set Default DNS to Linux web server

For this test, the tester looked at both a .EXE and a .DLL file.

2.2.2.1.1 EXE file

To start, the tester looked at an .EXE file. Running .EXE files are a common occurrence for both users and Windows operating system (OS), as they can be triggered by simply double-clicking them. But before running the malware, the tester did some static analysis checks through the use of Dependency Walker, to see what sort of imports there were for the malware. As seen in Figure 16 there seems to be only one import: kernel32.dll. This was most likely showing that this specific malware was packed.

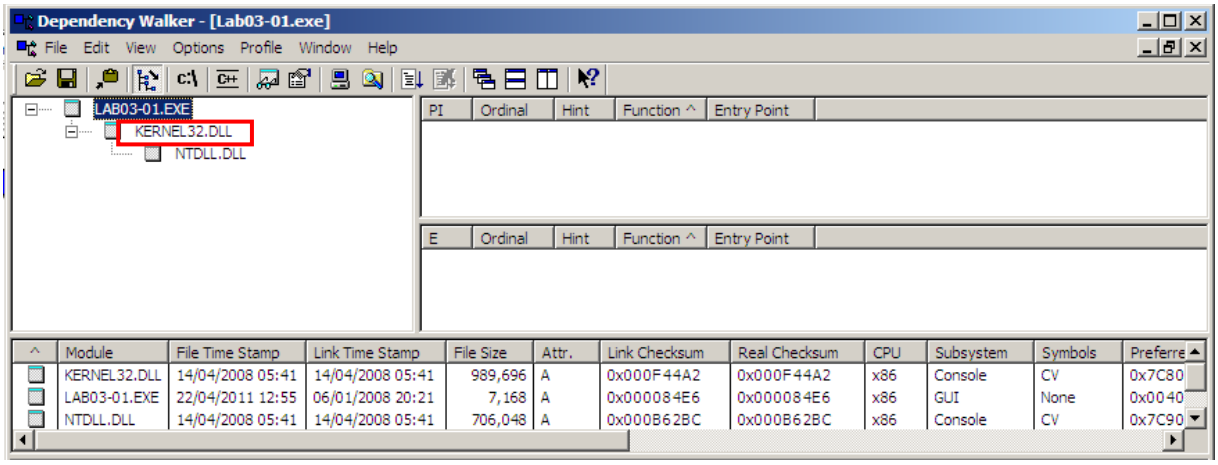


Figure 16 Lab03-01.exe - Dependency Walker

The packed state is proved through the use of both PEview and PEiD, where PEview showed a large difference between Raw Data and Virtual Size Figure 17 and Figure 18. While PEiD shows that it was packed and packed using PEncrypt 3.1 Final -> junkcode Figure 19.

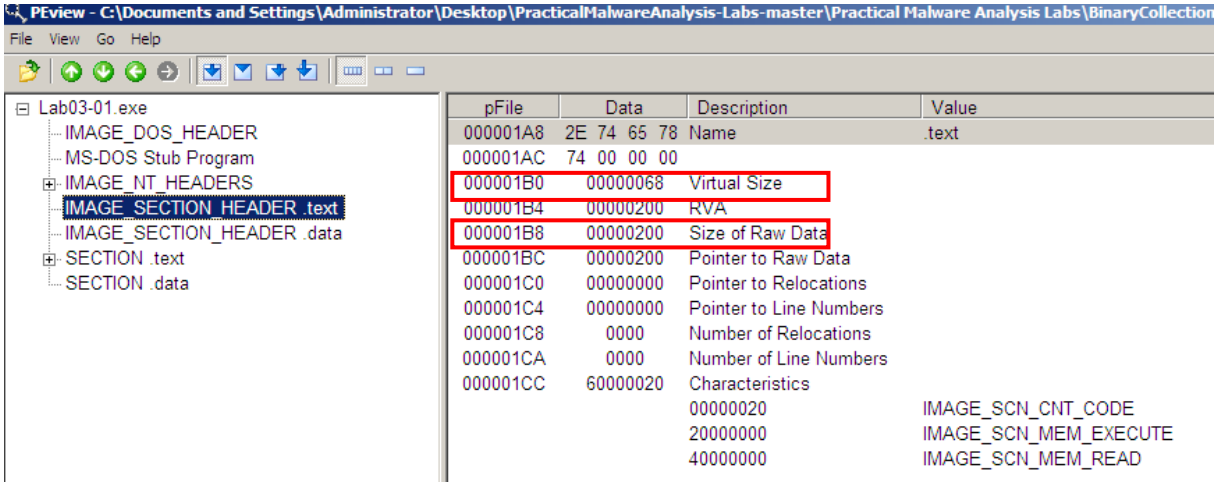


Figure 17 Comparing Raw Data to Virtual Size in Lab03-01.exe

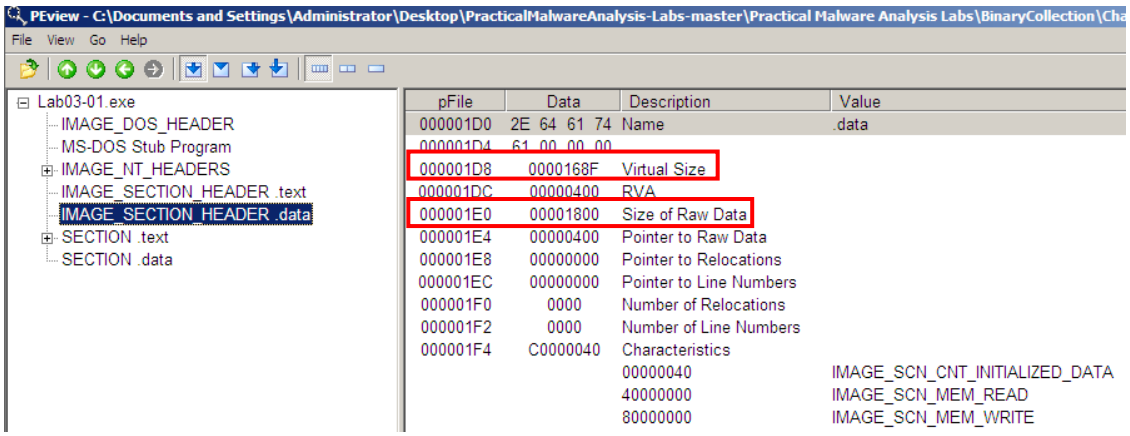


Figure 18 Comparing Raw Data to Virtual Size in Lab03-01.exe

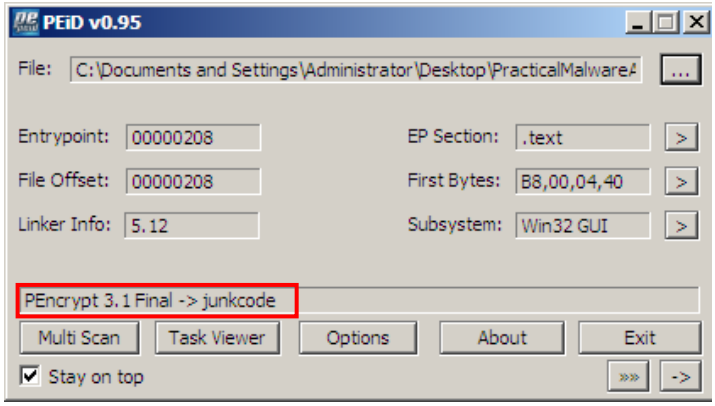


Figure 19 Lab03-01.exe is packed using PEncrypt 3.1 Final

Following this, the tester looked at any possible strings that could be recovered from the file, and what could be learned from it. This can be seen in Figure 20 and Figure 21. All returned values can be found in Appendix C.

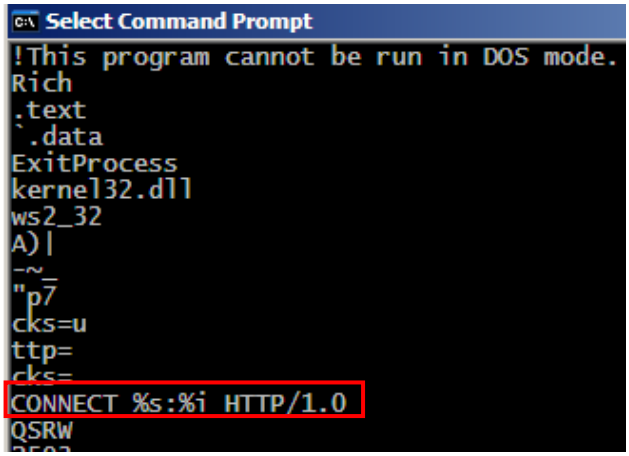


Figure 20 Strings for Lab03-01.exe

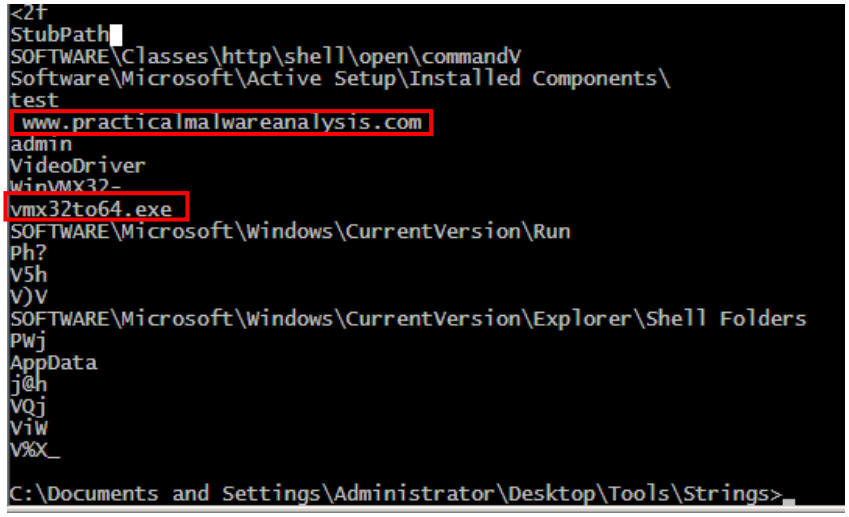


Figure 21 Strings for Lab03-01.exe

Through these figures, it is possible to discern that the malware may attempt to connect to the internet 'CONNECT HTTP/1.0' to the website 'www.practicalmalwareanalysis.com'. Furthermore, it may attempt to create and/or run a file called vmx32to64.exe, and so on.

Now, that the tester had some basic knowledge about the malware, the tester was ready to start dynamically assessing the malware.

The tester started with the Process Monitor tool. Firstly, the tester stopped the logging and cleared the display, by simply having selected the File tab and clicked the Capture events option to stop the logging of the system, then the tester goes to the Edit tab and selects the Clear Display option before starting the application to remove unnecessary information (Figure 22 and Figure 23). Then in order to start the application up again the tester clicked File Capture option in the first step again.

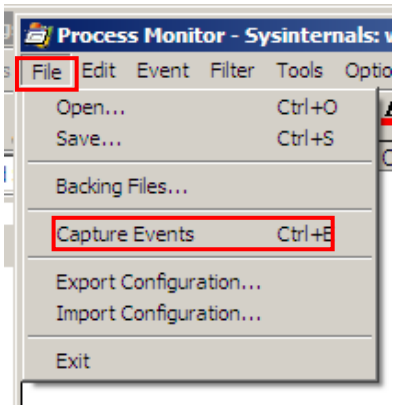


Figure 22 Stopping Process Monitor from logging

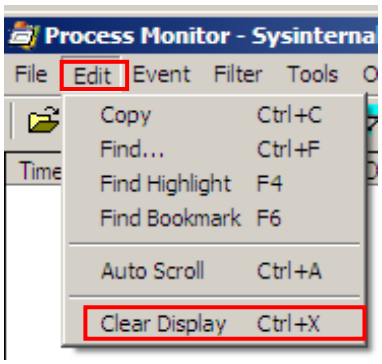


Figure 23 Clearing the display in Process Monitor

Furthermore, it was possible for the tester to be able to set Process Monitor so that it only monitored the one executable, this was through the filtering option. This is a particularly helpful tool as it reduces all the unnecessary information that appears on the display. Using this it was also possible for the tester to be able to zero in on certain system calls as well. To set the filtering option up the tester went to the Filter tab and selected the Filter option as seen in Figure 24. When the dialog pops up the tester was able to filter all the sections that the tester wanted and didn't want to show up on the screen. All processes that were shown would have a green tick next to the name while those that the tester did not want showing up had a red X by the process name (Figure 26**)**. Important filters that were considered were Process Name, Operation, and Detail, in which the tester chose from comparators such as 'Is', 'Contains', and 'Less Than'. Furthermore, some helpful filters were found within the toolbar (Figure 25**)** which can filter the Registry, File system, Process activity, and Network – in which all of them are selected by default (Figure 27).

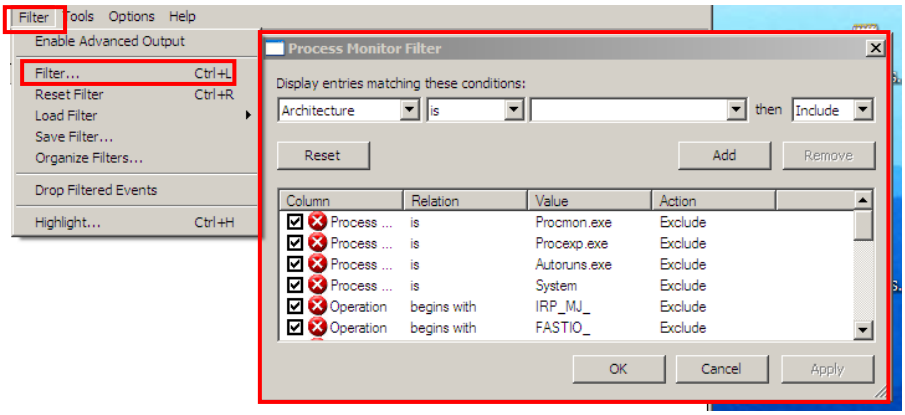


Figure 24 Filtering pop up

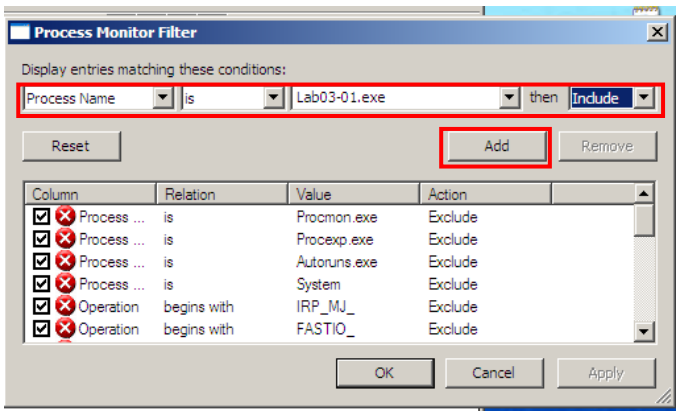


Figure 25 Entering the Process name to be filtered and shown

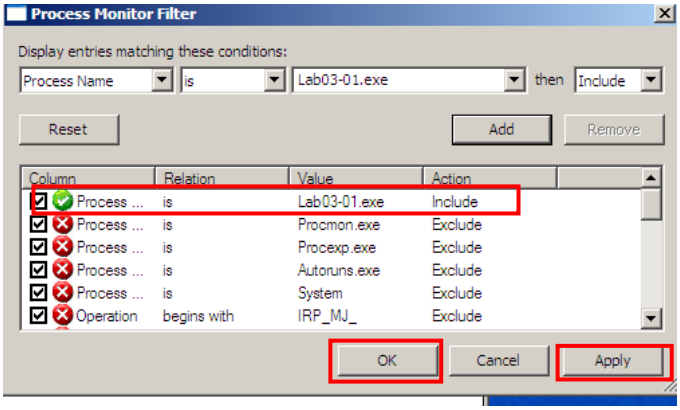


Figure 26 Green tick indicated the process will be shown in display

Figure 27 Filtering tabs

After applying the filters (Process Name, Operation WriteFile, and Operation RegSetValue) as seen in Figure 28, the tester then ran the malicious file Lab03-01.exe. After letting it run and watching Process Explorer for when the file was finished the tester turned back to Process Monitor to see what was captured during the execution of the file. Some results returned can be seen in Figure 30.

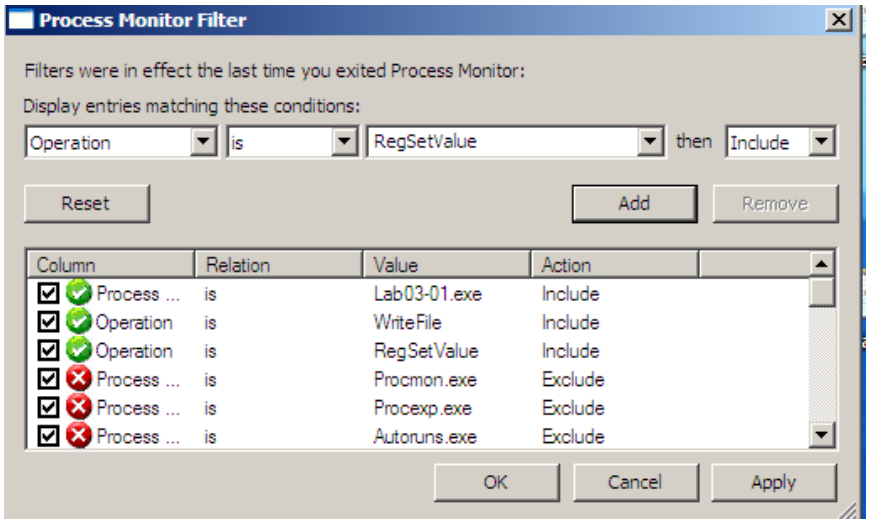


Figure 28 All the filters for Process Monitor for Lab03-01.exe

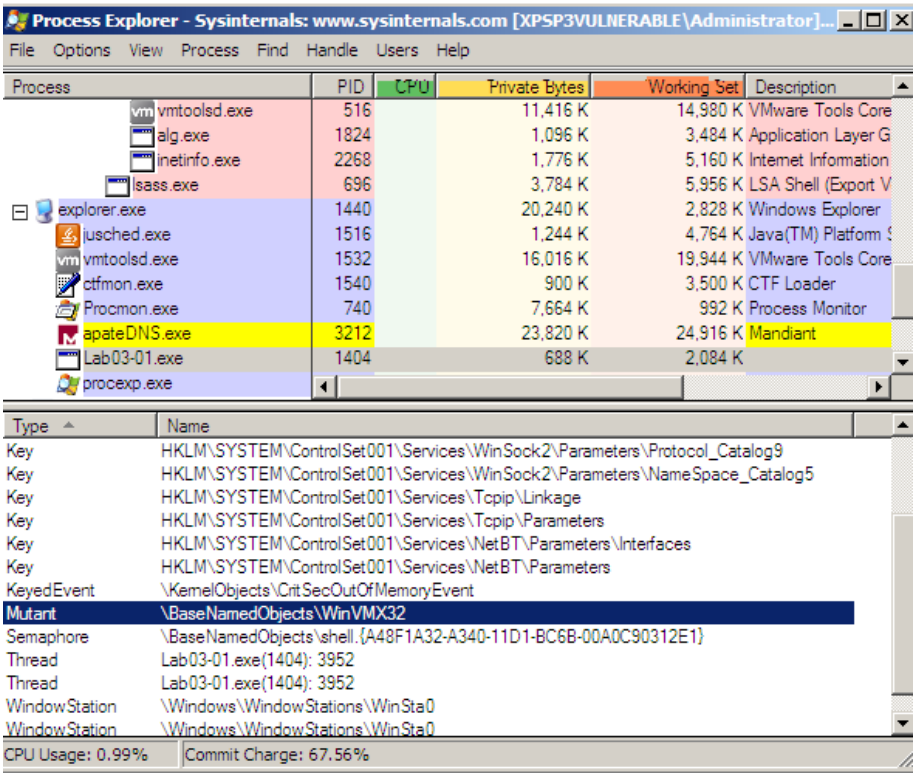


Figure 29 Mutex WinCMX32 created after running malware

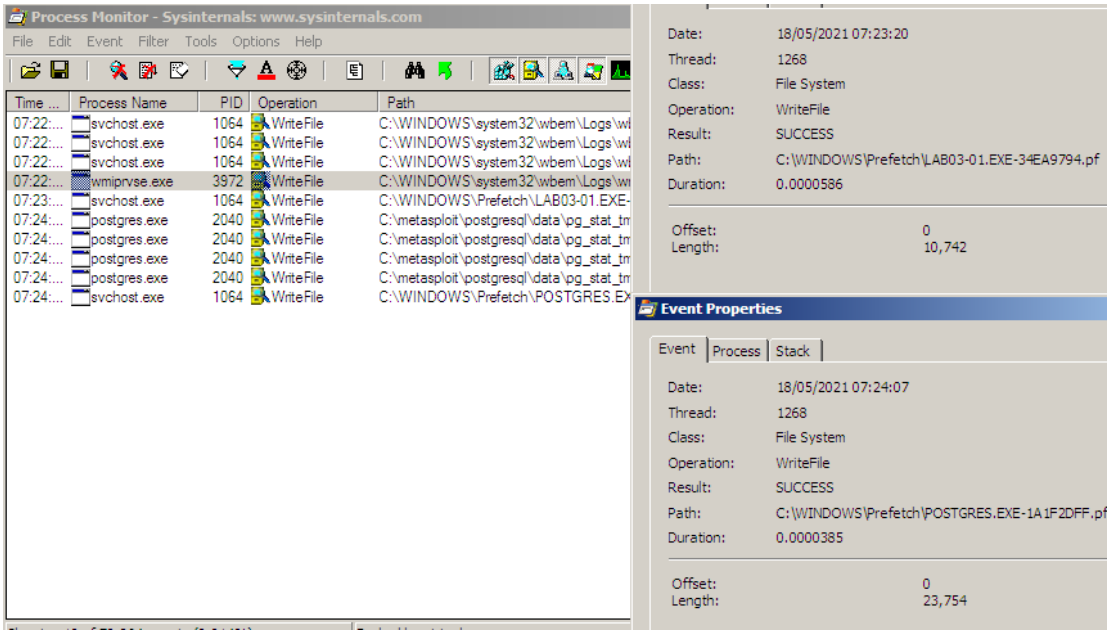


Figure 30 Returned results for WriteFile in Process Monitor for Lab03-01.exe

After confirming any possible actions that the file made to the system, the tester then turned to look at and requests logged in INetSim and captured through Wireshark. In Figure 31 it can be seen that there was a DNS request to 'www.practicalmalwareanalysis.com', as was seen and predicted in the string figures Figure 20 and Figure 21. This is further backed by the Wireshark capture of a DNS request to 'www.practicalmalwareanalysis.com' seen in Figure 32.

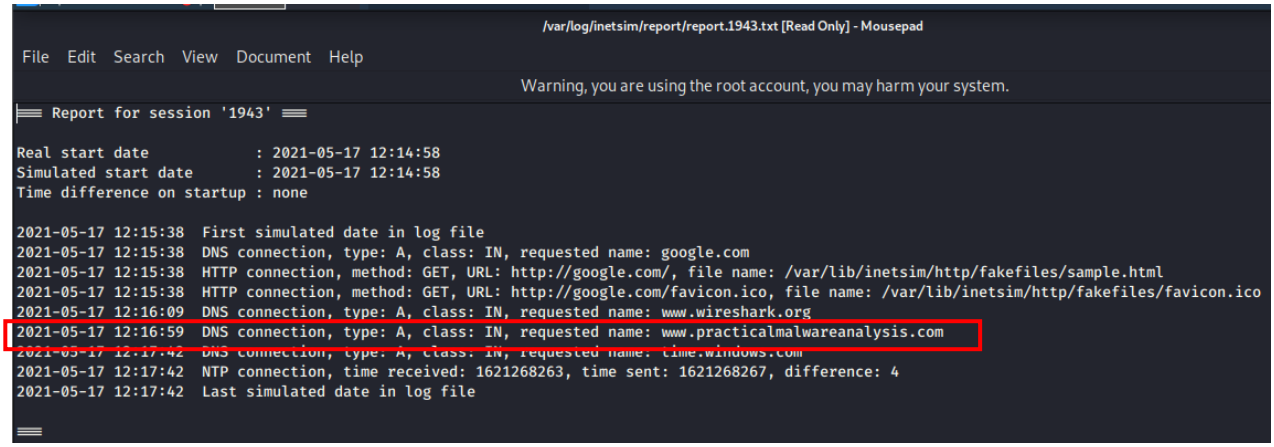


Figure 31 INetSim report

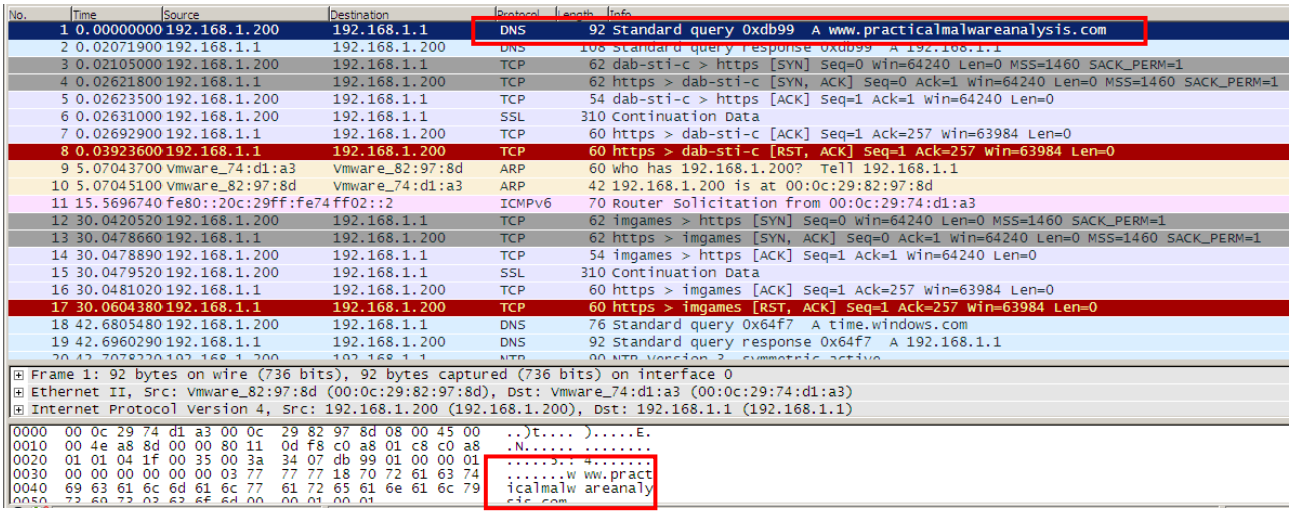


Figure 32 Wireshark capture of Lab03-01.exe

2.2.2.1.2 DLL file

Next, the tester looked at malicious a .DLL file – Lab03-02.dll. To start the tester attempted to get information about the file through the use of Dependency Walker (Figure 33 and Figure 35) as well as check if this particular malware was packed through the tool PEiD (Figure 34). This confirmed that Lab03-02.dll was not packed.

In Figure 35 a particularly interesting export was noted: ServiceMain.

ServiceMain was an indicator that this .DLL file needed to be installed as a service to run (chappell, 2021). Furthermore, by having looked at the exports table as well as the strings for the file it was believed that this malicious DLL file needed to be installed as a service using installA (Figure 35 and Figure 37).

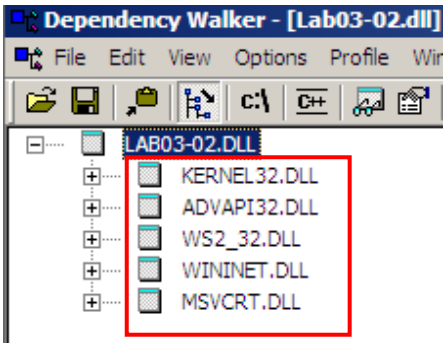


Figure 33 Dependency Walker - imports for Lab03-02.dll

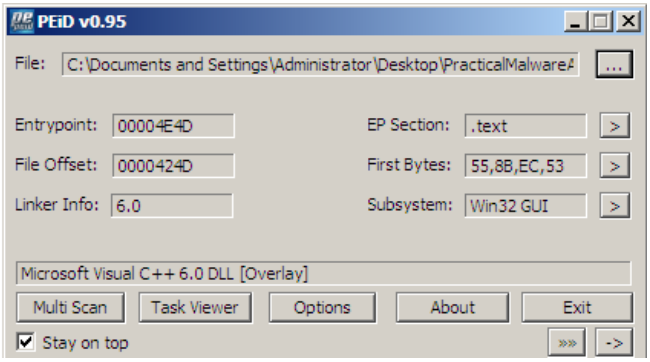
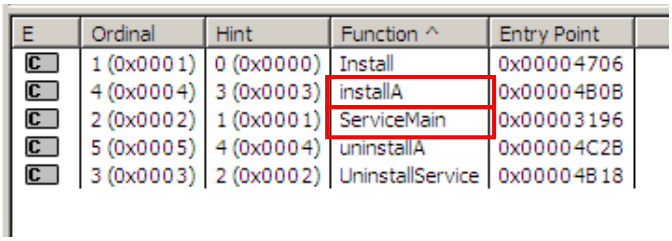


Figure 34 Using PEiD to check if Lab03-02.dll was packed



E	Ordinal	Hint	Function ^	Entry Point
C	1 (0x0001)	0 (0x0000)	Install	0x00004706
C	4 (0x0004)	3 (0x0003)	installA	0x00004B0B
C	2 (0x0002)	1 (0x0001)	ServiceMain	0x00003196
C	5 (0x0005)	4 (0x0004)	uninstallA	0x00004C2B
C	3 (0x0003)	2 (0x0002)	UninstallService	0x00004B18

Figure 35 Dependency Walker analysis for Lab03-02.dll

After learning a little about the malware through the use of Dependency Walker and PEiD, the tester then turned to see if any strings could be recovered and any potential information that could be

revealed. In the following figures – Figure 36 and Figure 37 – it can be presumed that the malware is going to make a HTTP request to 'www.practicalmalwareanalysis.com'. Furthermore, in it can be presumed that the malware has something to do with an 'Intranet Network Awareness' (Figure 38).

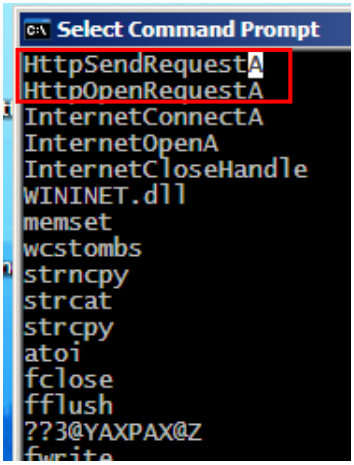


Figure 36 Strings search - HTTP Request

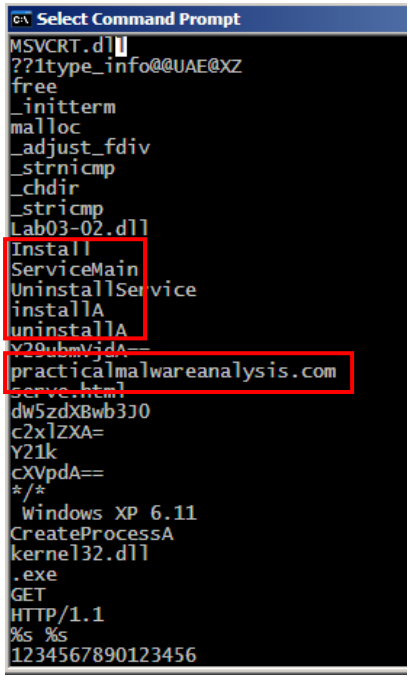


Figure 37 Strings search - export function and HTTP request Destination

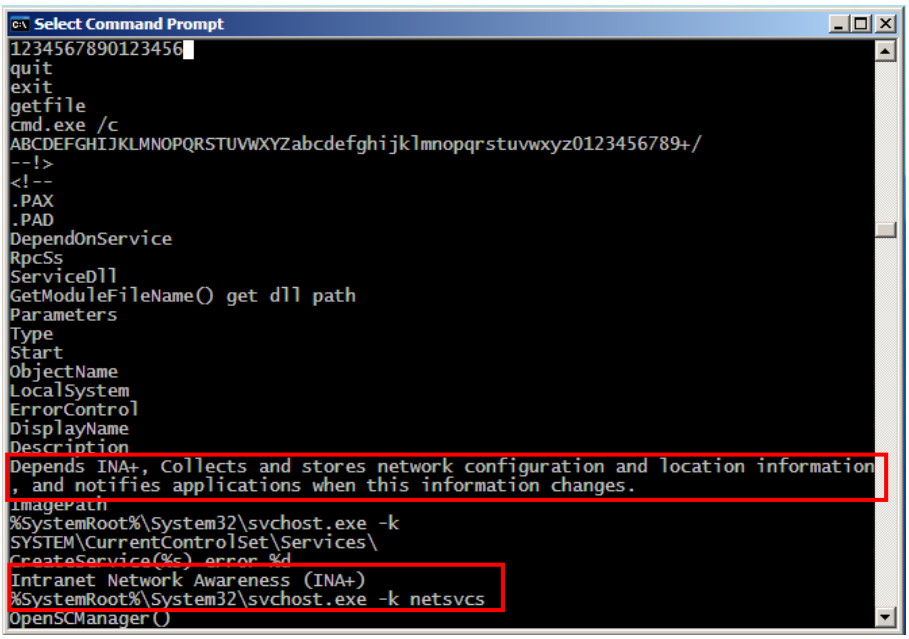


Figure 38 String search - Intranet Network Awareness

However, when considering running the malware it is key to remember that Windows does not have an automatic method of running .DLL files, unlike with .EXE files.

So, for the tester to have been able to execute this file, the tester would have needed to trigger it manually. In order to do this the tester would need to know a little about the rundll32.exe file that comes with Windows automatically and running it alongside the chosen .DLL file in the command line.

The below template code was used.

> 'rundll32.exe DLL name, Export arguments'

The 'Export arguments' value must be a function name within the .DLL file. As was demonstrated earlier through the use of the tool Dependency Walker where the tester got a list of the exported values in the Export table**.**

However, first, to track any changes that the malware might make the tester took a snapshot of the registry through the use of the tool Regshot by having clicked the "1st Shot" button, before running the malware (Figure 39). Following this the tester then set up all the tools that the tester was going to use after installing the malware, this included Process Monitor, Process Explorer, INetSim, and Wireshark.

After installing the malware (Figure 40), the tester then looked towards Process Explorer in order to ensure there are no more processes being started up or terminated that are related to the malicious .DLL file. Confirming the termination, the tester then took a second snapshot with Regshot to compare to the first shot to check if the malware installed itself within the registry. This then allows for the tester to be able to compare the two shots and have the log saved as a .TXT file (Figure 41). The entire .TXT file with comparisons for the two snapshots can be found in Appendix D.

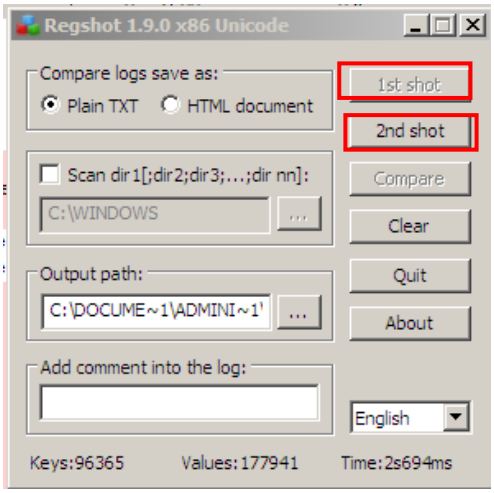


Figure 39 Regshot

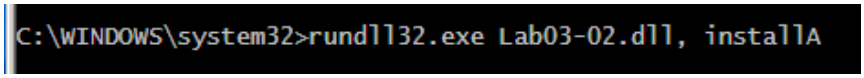


Figure 40 Running the malicious Lab03-02.dll

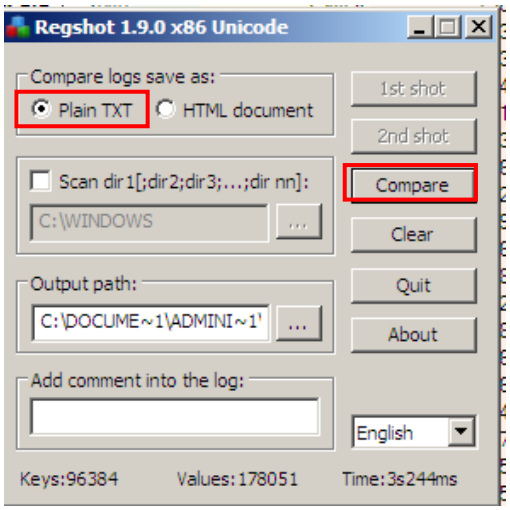


Figure 41 Compare and create a .TXT log

Also, given that the malware is installed as the IPRIP service the tester started it using the command below:

> 'net start IPRIP'

Which outputted information that was very similar to what was found in the strings search (Figure 38) can be seen in Figure 42.

```
C:\WINDOWS\system32>net start IPRIP
The Intranet Network Awareness (INA+) service is starting.
The Intranet Network Awareness (INA+) service was started successfully.
```

Figure 42 Running the service that the malware was installed under

Next, the tester filters for the .DLL file in Process Explorer looking for the process and Process ID for the malware. Following this the tester then opened the View, Lower pane view, DLLs and further confirmed the running of the malicious software (Figure 43).

Then the tester checked the rest of the tools that were set up and found that a DNS request was made that connected to a website Figure 44. And finally, in the figure there was also found that the malware made a HTTP GET request over port 80 INetSim to the same host as the DNS request.

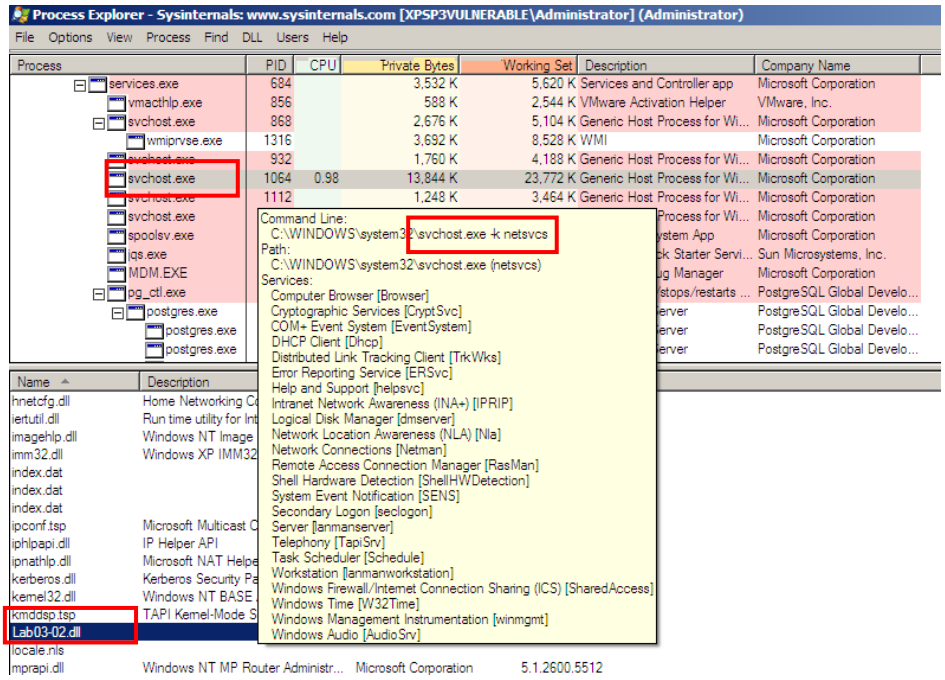


Figure 43 Process Explorer Lab03-02.dll running under svchost.exe PID 1064

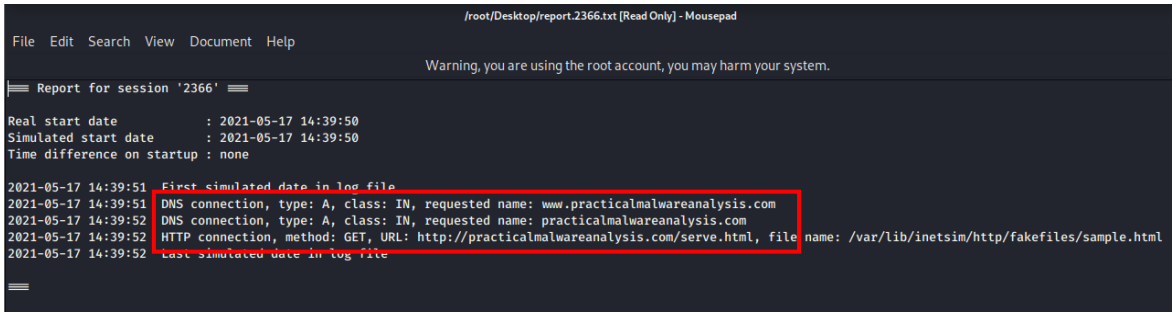


Figure 44 INetSim report on DNS and HTTP requests made

2.2.3 Hybrid analysis

With attempts to use the hybrid analysis technique to analyse malware, the tester firstly used a website called 'hybrid-analysis.com'. This website allowed a user to upload a malicious file to the website and submit it for analysis. The tester uploaded each of the files that have been used so far; Lab01-01.exe, Lab01-03.exe, Lab03-01.exe, and Lab-03-02.dll.

2.2.3.1 Lab01-01.exe

First, the tester looked at the Lab01-01.exe file. As can be seen in Figure 45, there is a simple uploading pop up where it was possible to drag and drop the malicious file for analysis. After uploading it and waiting for the analysis to complete the analysis is returned with images detailing the results of scanning the malware using various scanners (Figure 46).

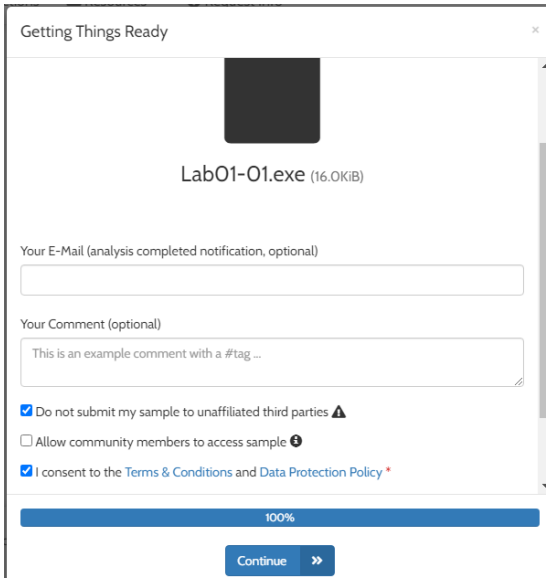


Figure 45 Uploading Lab01-01.exe to hybrid-analysis.com

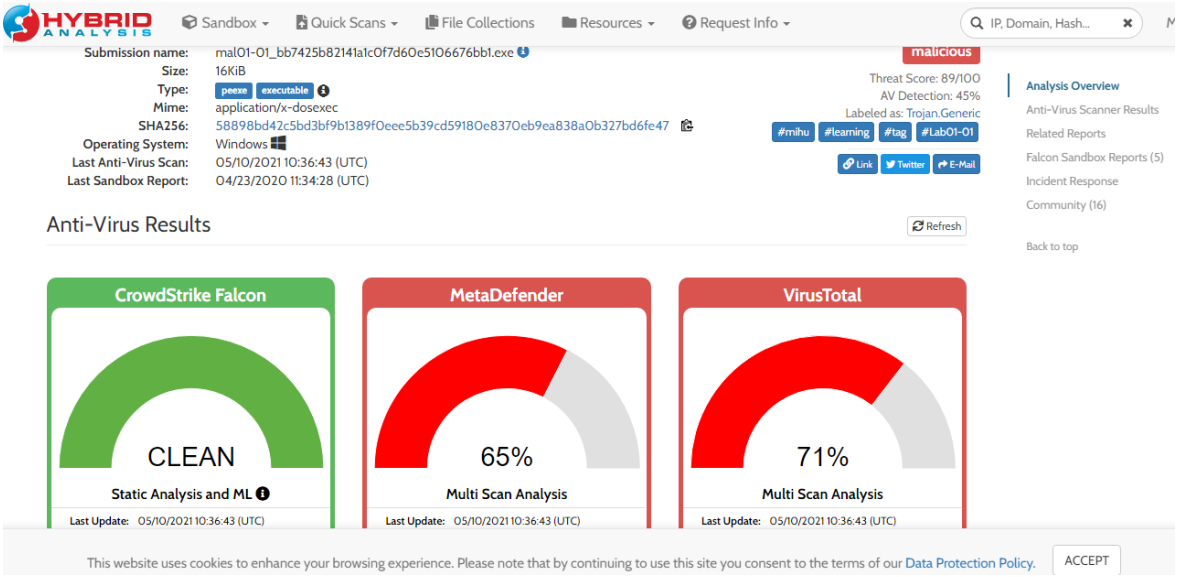


Figure 46 Report of Lab01-01.exe

2.2.3.2 Lab01-03.exe

Next the tester looked at Lab01-03.exe. After uploading the next malicous software, Lab01-03.exe (Figure 47), more results were returned. As was seen with the previous malware, there was a visual representation of the identification as malware from various scanners (Figure 48 and Figure 49). Figure 49 indicates that the malware has been identified by a large majority of the malware scanners, and is therefore classified as a threat.

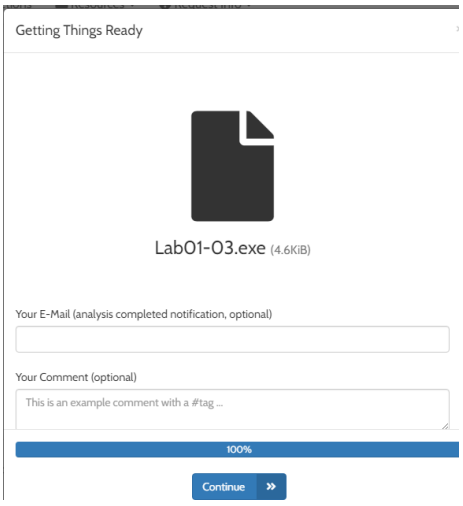


Figure 47 Uploading Lab01-03.exe to hybrid-analysis.com

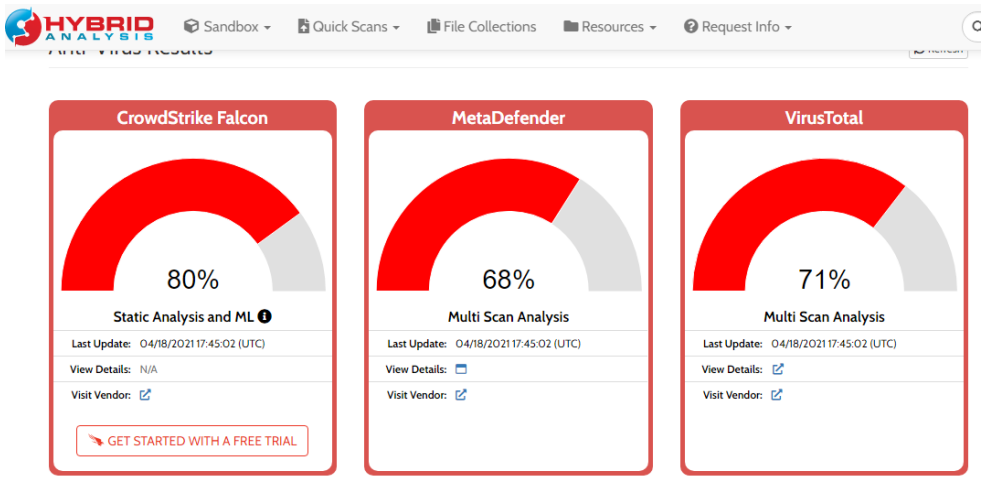


Figure 48 Report of Lab01-03.exe against various scanners

Figure 49 More information returned from the hybrid analysis - 'Malicious Indicators'

In figures Figure 50 and Figure 51 there can be seen more information regarding the malware that was uploaded. In Figure 50 it can be seen any parts of the malware that had a link to the functionalility of the malware has be indicated to be ‘suspicious’. While in Figure 51 there a more ‘informative’ peiece of information regarding the malware such as the size of the Raw Data being zero – indicating the likliness of the malware was packed as was seen in the Static analysis that occurred in section 2.2.1 part 2.2.1.2.

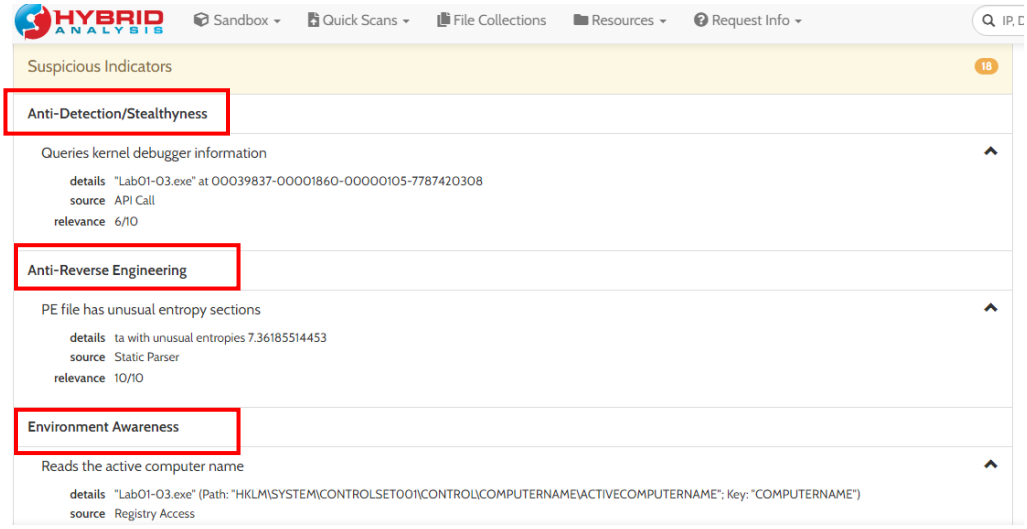


Figure 50 More information returned from the hybrid analysis - 'Suspicious Indicators'

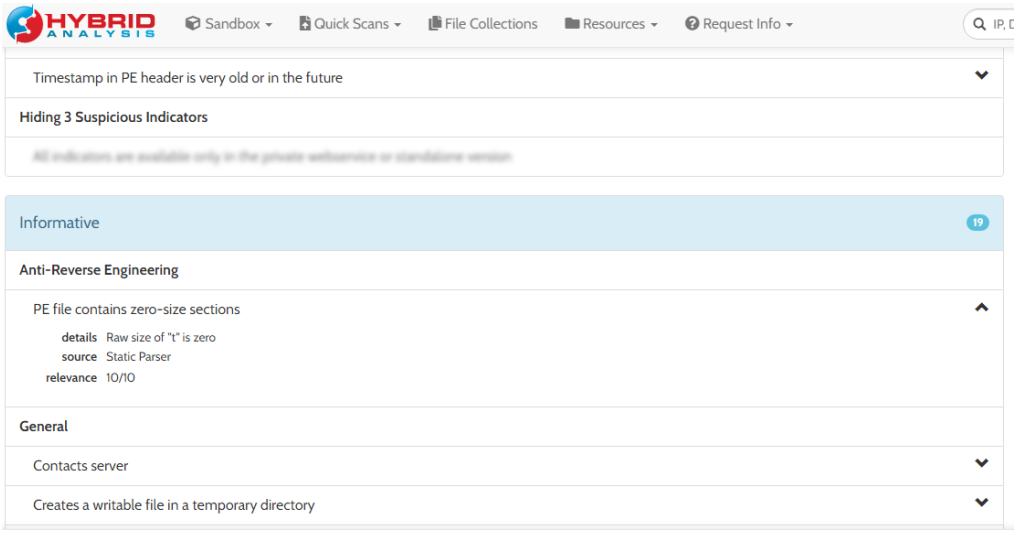


Figure 51 More information returned from the hybrid analysis - 'Informative'

2.2.3.3 Lab03-01.exe

After the completion of the of the Lab01-03.exe file, the tester then uploaded the Lab03-01.exe file (Figure 52 and Figure 53).

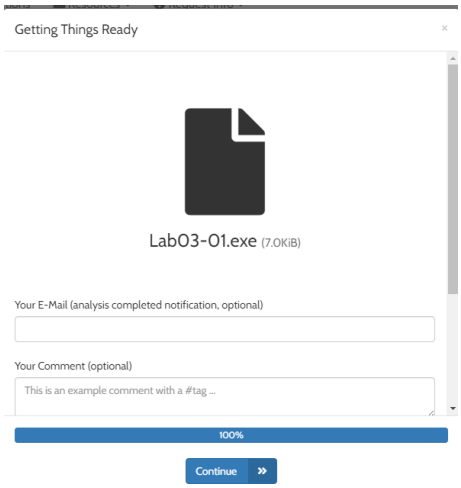


Figure 52 Uploading Lab03-01.exe

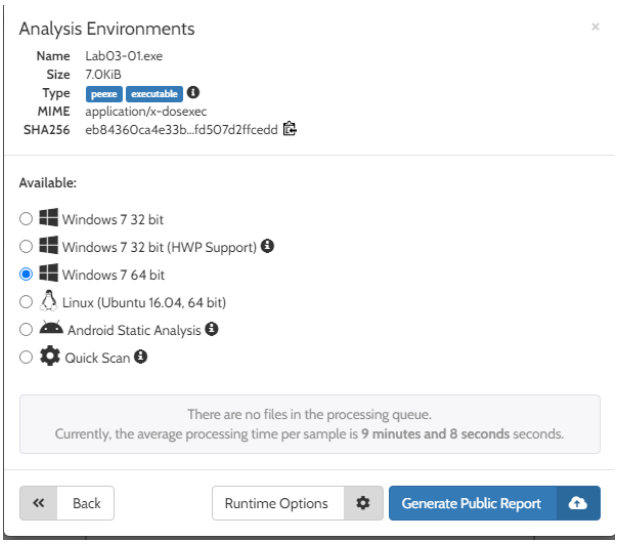


Figure 53 Uploading Lab03-01.exe

Figure 54, like the previous malware analysis, is a representation of how many scanners recognize this file as malware. Figure 55 shows results from an analysis of 'Technique Detection' where it noted interesting behaviour from the malware and catergorised it as persistent, privilege escalating, has access to Remote Desktop Protocol.

In figures Figure 56, Figure 57, and Figure 58, much like the previous malware, the report breaks down the sections of the malware into ‘Malicious Indicator’, ‘Suspicious Indicator’, and ‘Informative’.

Figure 56 is the figure representing the ‘Malicious Indicator’, which simply goes to explain that the malware was detected by a large amount of malware scanners and its relevance.

Figure 57 represents the ‘Suspicious Indicator’ section of the analysis report, which details the malware’s attempt to connect to the URL ‘www.practicalmalwareanalysis.com’ – much like what was found in the dynamic analysis of this malware.

Finally, Figure 58 shows the ‘Informative’ section of the hybrid analysis report. This shows a similar selection as to Figure 57, where the malware attempts to connect to ‘www.practicalmalwareanalysis.com’.

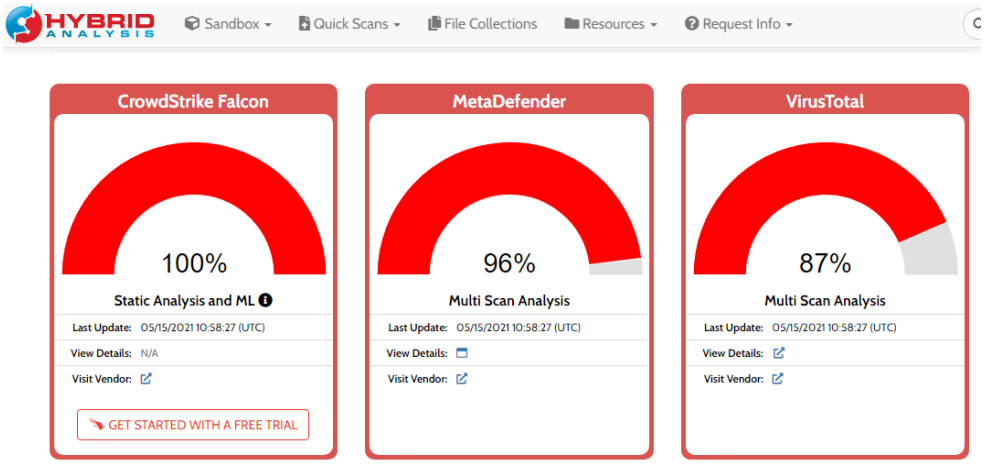


Figure 54 Report of Lab03-01.exe against various scanners

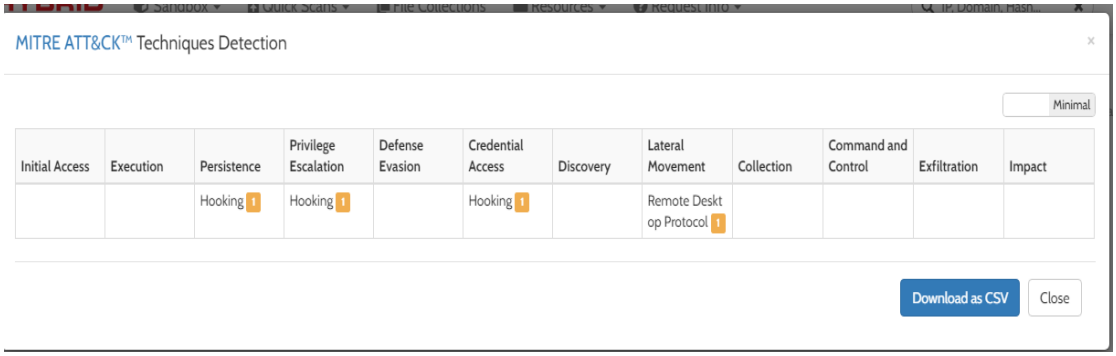


Figure 55 Technique Detection for Lab03-01.exe

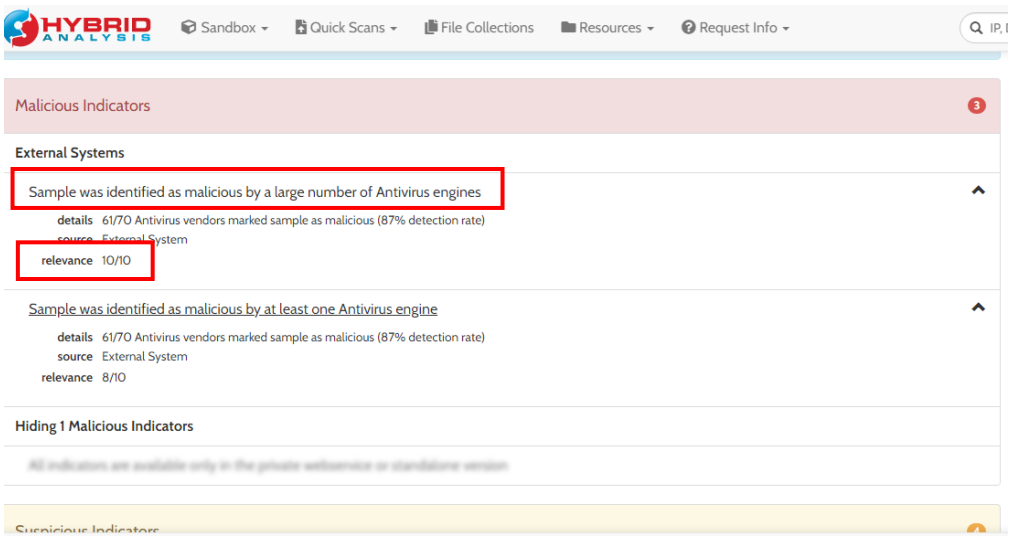


Figure 56 More information returned from the hybrid analysis for Lab03-01.exe - 'Malicious Indicators'

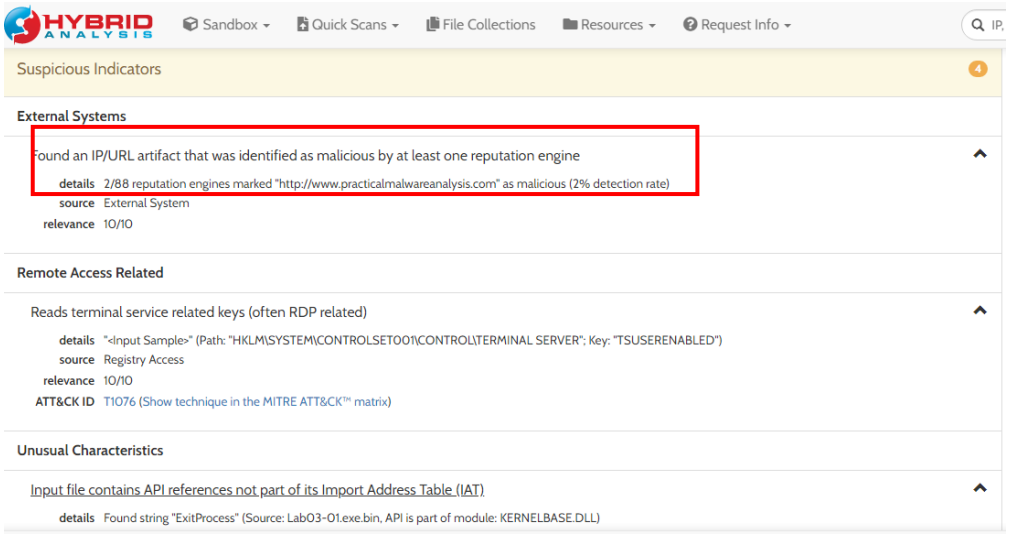


Figure 57 More information returned from the hybrid analysis for Lab03-01.exe - 'Suspicious Indicators'

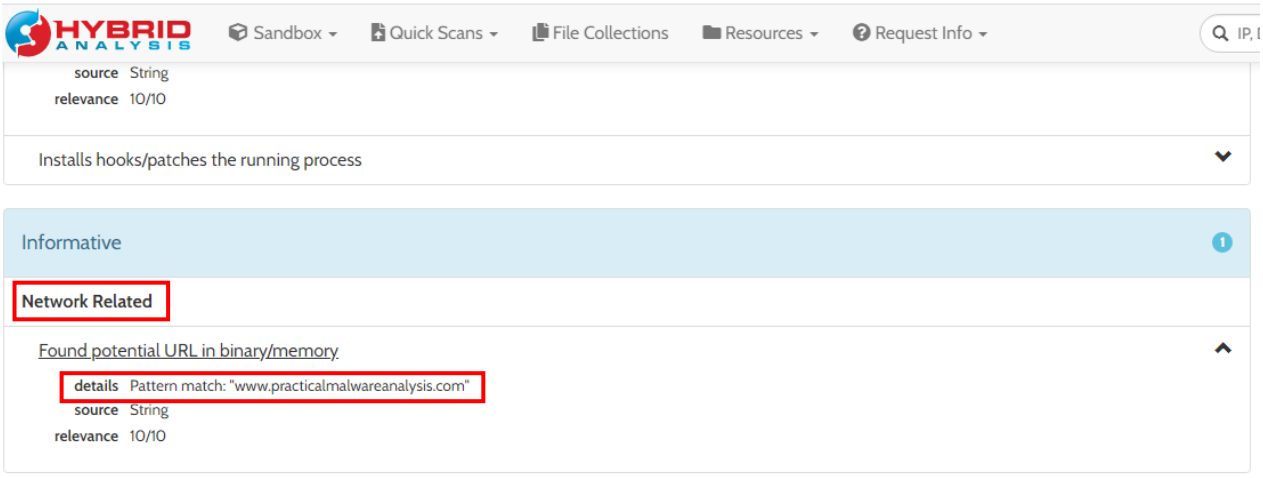


Figure 58 More information returned from the hybrid analysis for Lab03-01.exe - 'Informative'

2.2.3.4 Lab03-02.dll

Finally, the tester uploaded Lab03-02.dll onto hybrid-analysis.com (Figure 59 and Figure 60). Like the previous analysis reports Figure 61 shows the number of malware scanners to recognize this malware as a threat.

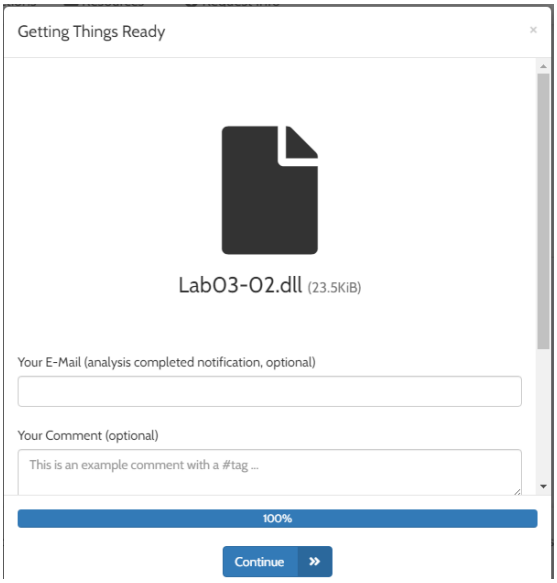


Figure 59 Uploading Lab03-02.dll

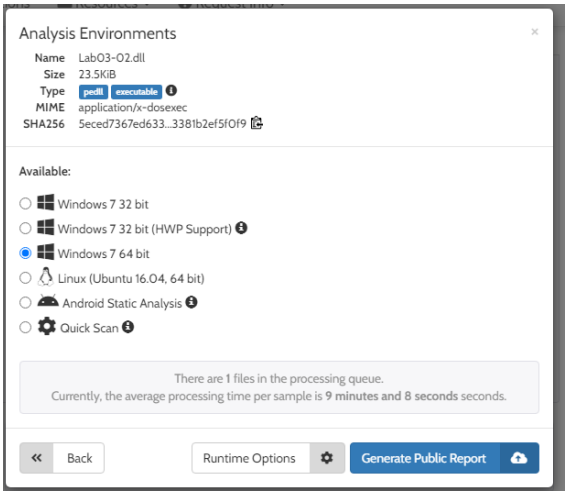


Figure 60 Uploading Lab03-02.dll

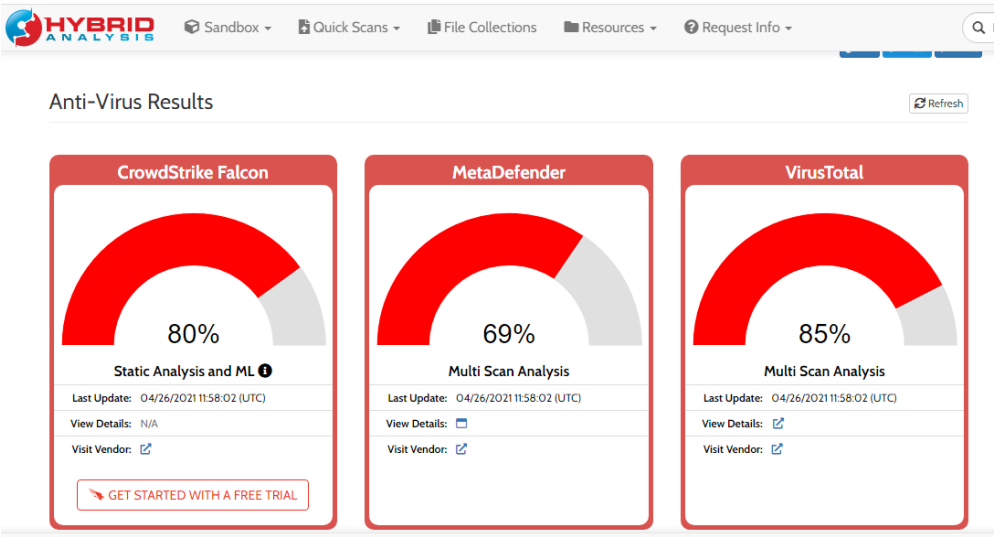


Figure 61 Report of Lab03-02.dll against various scanners

Following this, figures Figure 62 and Figure 63 show further information about the malware.

Figure 62 shows the 'Netowork Analysis' section which tells about the malware trying to make a connection to 2 IP addresses.

While Figure 63Figure 62 shows the 'Technique Detection' detailing this malware as persistent, evades defence, and so on.

These figures explains the main features if the malware by detialing that it possibly used to gain access to a device through persitance and defense evasion as well as gain access to or create any user

credentials. Then, connects to external IP addressed, to potentially pass the information back to the attacker (sender of the malware).

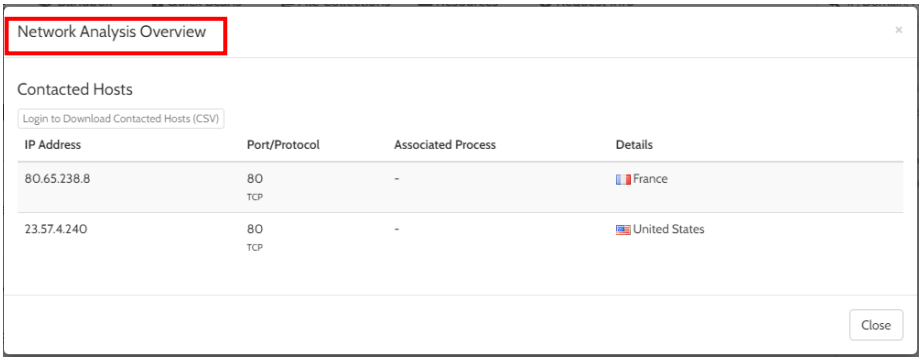


Figure 62 Further information about Lab03-02.dll – 'Network Analysis'

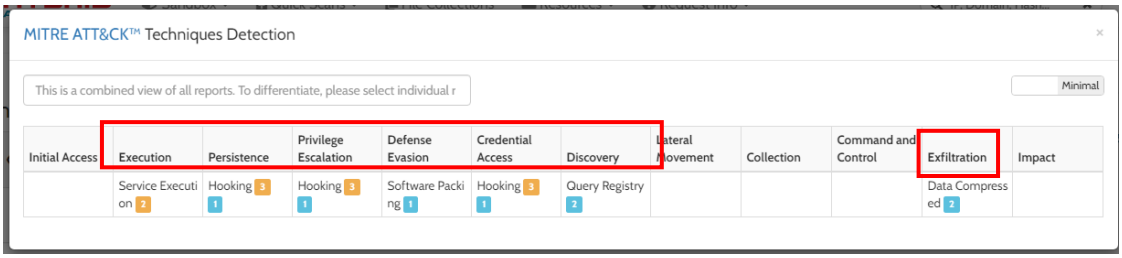


Figure 63 Further information about Lab03-02.dll – 'Technique Detection'

Following this, much like the previous few reports , there are sections details various strings and functionality of the malware (Figure 64, Figure 65, Figure 66, and Figure 67). Figure 64 show the 'Malicious Indicators' which reports that the malware is identified as a thread by a large number of antivirus scanners. While Figure 65 shows more about the potential functionality of the malware, as it details the creation of a new process after the malware is run. With the creation of a new process, there are a multitude of processes that a malicious attacker might wish to create that would allow them to be able to gain information about the machine that it has been executed as well as find a way to gain access to it. Lastly, in figures Figure 66 and Figure 67 there is information about what the malware has created, potentially after running it. This includes the creation of a mutant and new processes in Figure 66. This is finally followed by the attempt to make a connection to 'www.practicalmalwareanalysis.com' website and potential installation for persistence of the malware in Figure 67.

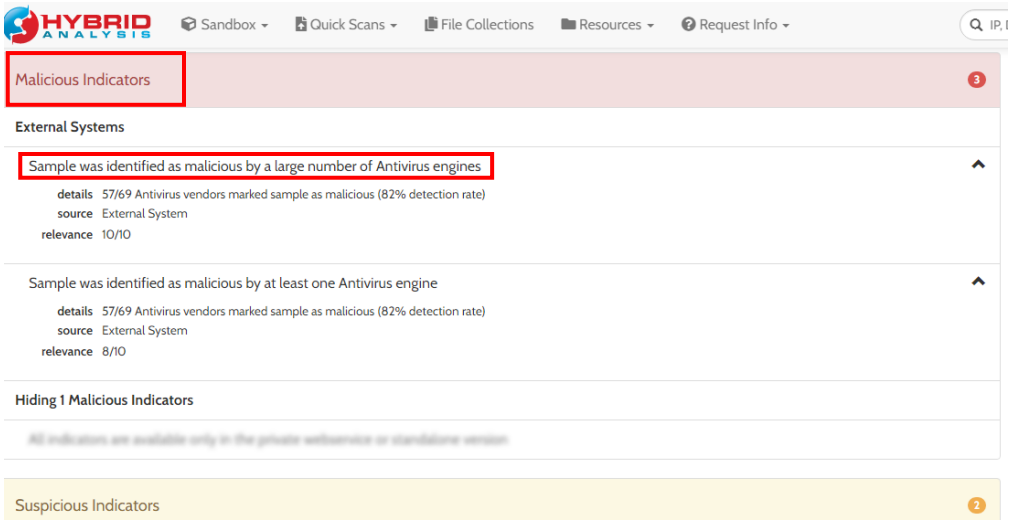


Figure 64 More information returned from the hybrid analysis for Lab03-02.dll - 'Malicious Indicator'

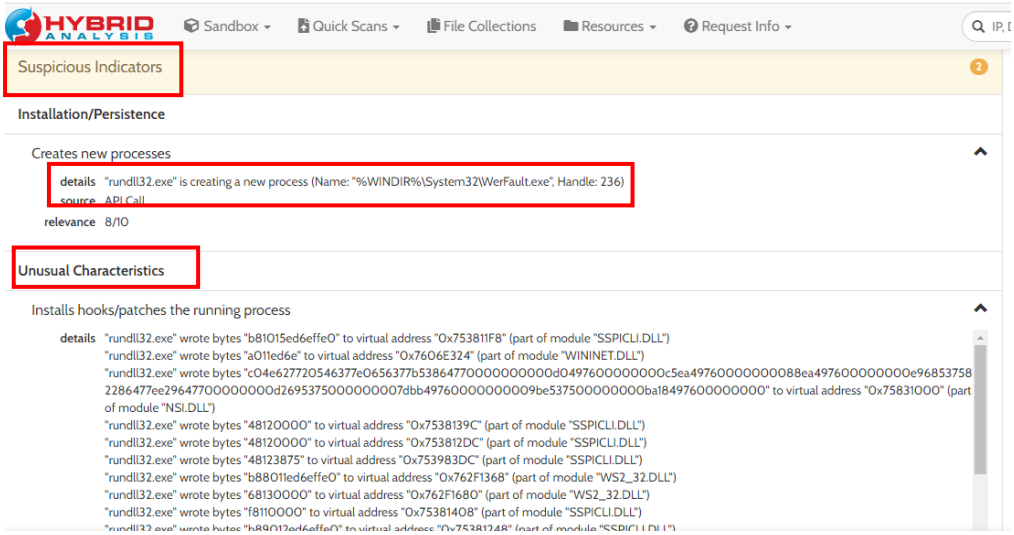


Figure 65 More information returned from the hybrid analysis for Lab03-02.dll - 'Suspicious Indicator'

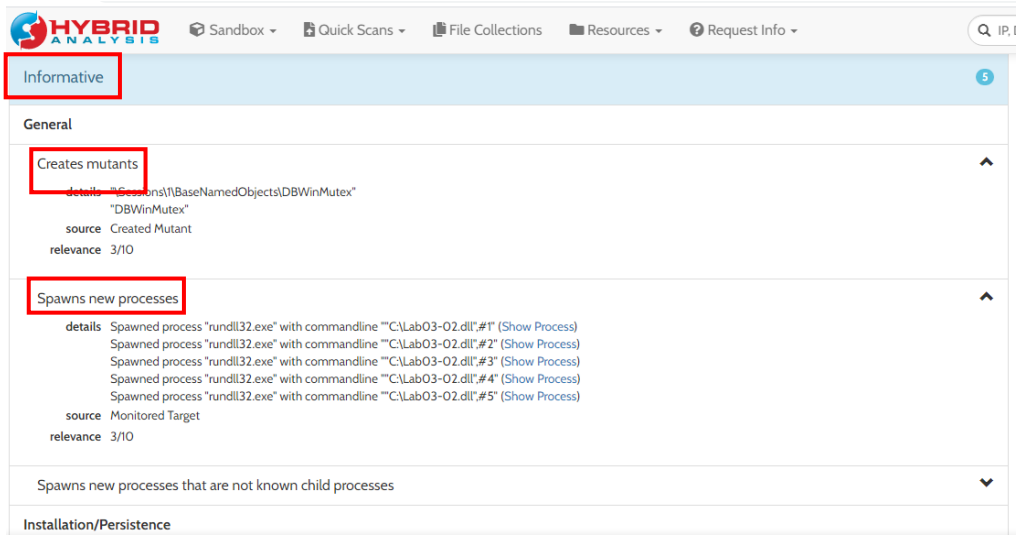


Figure 66 More information returned from the hybrid analysis for Lab03-02.dll - 'Informative'

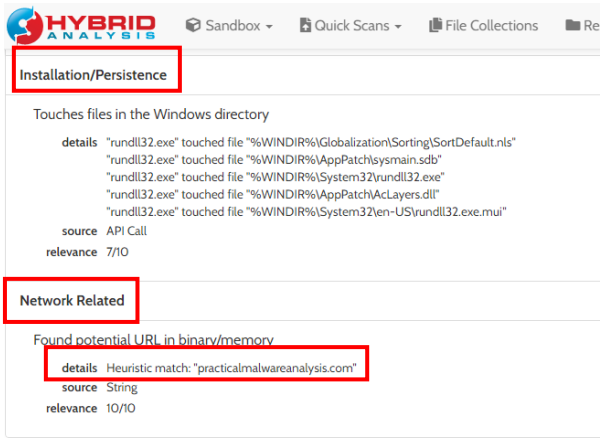


Figure 67 Install/Persist and Network related information about Lab03-02.dll

After completing the hybrid analysis using 'hybrid-analysis.com' the tester intended to use Cuckoo Sandbox, a very popular sandbox for malware analysis, however due to both technical issues and time constraints this was not achieved.

In theory, the Cuckoo Sandbox (Cuckoo Sandbox - Automated Malware Analysis, 2021) was expected to give similar results compared to 'hybrid-analysis.com' with perhaps more detailed information as well as results with a stronger demonstration of the effects of the malware, compared to the static information provided by the hybrid analysis website.

3 RESULTS

3.1 RESULTS

The aim of the analysis of malware was to evaluate the various analysis techniques that are available and mostly used: Static, Dynamic, and Hybrid analysis. These tests went to show both the advantages and limitations that each technique has, and which one may be considered to be the better technique to use.

The tester started the tests using the static analysis technique. To implement this technique the tester used tools such as VirusTotal.com, PEview, Dependency Walker, and so on. Through these, as seen in section 2.2.1 – Static analysis – the tester was able to piece together the threat level through signature, as well as potential functionality of the malware. By gathering data through these methods, it was possible for the tester to be able to evaluate the benefits and limits of static analysis. Overall, it was noted that through the use of anti-virus scanners in the browsers have the ability to identify malware that is already stored in the database through signatures, this particular method is essentially useless if one was to upload a piece of malware that is not in said database or have a signature related to it, as these can be changed by a particularly 'strong' malicious programmer. Furthermore, when using tools in order to attempt to break down the malware in strings and viewing imports etc. there is no guarantee that the malware will use each specific import and/or function used from each import. However, static analysis is a simple way to be able to gain information about a suspicious file and does not require any testing through execution and likewise does not require to set up a virtual machine/ sandbox.

Considering the limitations found in the static analysis technique, another technique was taken up – Dynamic analysis. For this analysis technique some static analysis techniques were still used, given that it provides some insight as to what the tester might expect from the malicious files that are being tested.

Following the static analysis, the tester used a Kali Linux and a Windows XP virtual machine for the execution and analysis of the malware. Through the execution of the malware, it was possible to determine, with evidence, the functionality and therefore covering one of the limitations of static analysis. Furthermore, dynamic analysis removes the limitation of the type of application that can be tested. For example, with static analysis (unless using a large number of various tools) tools will be limited to the language and/ or type of application that can be analysed. With dynamic analysis it is possible to run a much larger population of file types and capture events that have occurred.

However, this technique provides a form of false security that everything is being address and/ or recorded by the tools that are being used, even though false positives and false negatives can still occur. Furthermore, there is the consideration of the costs to have and run virtual machines/ sandboxes, which involves more knowledge in setting up and using them.

For hybrid analysis, it can be considered to be a faster alternative to both static and dynamic analysis, as well as significantly less time and labour being used. Using 'hybrid-analysis.com', suspicious files can be uploaded, and the website will do the analysis for the user, while also doing so for free. Therefore, this technique covers both static and dynamic analysis while also reducing costs and time. However, similarly

to dynamic analysis, this may give a false sense of security that everything is being tested while potential false positive and false negatives may be given. Furthermore, this technique does not eliminate the costs completely as for more advanced forms of hybrid analysis, providers may charge for the use of these systems/ sandboxes, etc.

However, a fatal limitation for all the techniques discussed is the analysis through the use of a virtual machine. Recent malwares have the ability to be able to check whether it is on a 'real' (host) machine or if it has been moved/downloaded onto a virtual machine by being able to check key parts of the machine. This can include checking the number of cores as well as checking disk size, etc., as these would be different compared to the host machine.

Moreover, through some research the validity of the hybrid analysis website that was used is not what was presumed at face value (Are hybrid-analysis reports trustworthy?, 2015). The website that was used is prone to false positives, something that is expected by the designer, in that there is a lack of a threshold for threat level that separated genuine programs from malicious ones, as genuine software can still use similar functions and imports that malicious one's use, for example creating a process. Furthermore, this could be seen in Figure 46, where Lab01-01.exe is considered as 'clean' by Crowdstrike's the Falcon sandbox, which is an unexpected outcome given that Lab01-01.exe is a malicious file. While also the lack of further information about said malware – leading to a very short report for it from the hybrid analysis website.

4 DISCUSSION

4.1 GENERAL DISCUSSION

Overall, through the various testing that was done, the tester found that each of the techniques analysed had various advantages and limitations, as was mentioned in the results section. In order of static, dynamic, and hybrid analysis the limitations of the previous are addressed and countermeasures implemented in the next technique in order to create an analysis tool that could have the potential to automate the analysis of malware completely.

Considering everything that the tester has learned about analysis techniques and of the malware, the tester believes that the technique that returned the most accurate results was the dynamic analysis technique. This technique provides a hands-on experience that allows for a user to be able to find the functionality of a piece of malware by running through a virtual machine. Even though there are some limitations to the use of this techniques, the tester finds that through practice and experience it would be possible to minimize the majority of them.

4.2 CONCLUSIONS

To conclude, there were many advantages and limitations to all the analysis techniques that were discussed in this report. As per the aim of this report each technique was used to test various malware with the intention to evaluate the technique and its efficiency with identifying malware and it's functions. Simply following the basics of this report will not provide all the detailed information that may be desired by large companies or when dealing with particularly complex malicious programs but is a strong starting point with plenty of improvements and future work to be considered.

As it is, the technique that the tester evaluated to be the better one of the three tested was the dynamic analysis technique, based on its ability to prove, more effectively through hands-on experience, the functionality and potential threat-level of malware.

4.3 FUTURE WORK

If more time were available for further analysis, the tester would look at advanced static and dynamic analysis with the use of further tools such as debuggers and disassemblers. Furthermore, this would have provided an opportunity to allow the tester to be able to get another form of hybrid analysis tool working to be able to get more results regarding this particular analysis technique. One such tool would have been the popular malware analysis sandbox 'Cuckoo'.

REFERENCES

URLs:

FireEye. 2021. *ApateDNS Download | FireEye*. [online] Available from: https://www.fireeye.com/services/freeware/apatedns-download-confirmation.html [Accessed 20 April 2021].

Dependencywalker.com. n.d. *Dependency Walker (depends.exe) Home Page*. [online] Available from: https://www.dependencywalker.com/ [Accessed 20 April 2021].

softpedia. 2018. *Download PEiD 0.95*. [online] Available from: https://www.softpedia.com/get/Programming/Packers-Crypters-Protectors/PEiD-updated.shtml#download [Accessed 20 April 2021].

Hungenberg, T. and Eckert, M., 2007. *INetSim: Internet Services Simulation Suite - Installation packages*. [online] Inetsim.org. Available from: https://www.inetsim.org/packages.html [Accessed 20 April 2021].

Wireshark.org. 2012. *Index of /download*. [online] Available from: https://www.wireshark.org/download/ [Accessed 20 April 2021].

Radburn, W., 2019. *WJR Software - PEview (PE/COFF file viewer),* [online] Wjradburn.com. Available from: http://wjradburn.com/software/ [Accessed 20 April 2021].

SourceForge. 2008. *regshot*. [online] Available from: https://sourceforge.net/projects/regshot/ [Accessed 20 April 2021].

Rissinovich, M., 2016. *Strings - Windows Sysinternals*. [online] Docs.microsoft.com. Available from: https://docs.microsoft.com/en-gb/sysinternals/downloads/strings [Accessed 20 April 2021].

Russinovich, M., 2020. *Process Explorer - Windows Sysinternals*. [online] Docs.microsoft.com. Available from: https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer [Accessed 20 April 2021].

Sikorski, M. and Honig, A., 2012. *Labs*. [online] Running the Gauntlet. Available from: https://practicalmalwareanalysis.com/labs/ [Accessed 18 April 2021].

Web.archive.org. n.d. *Wayback Machine*. [online] Available from: https://web.archive.org/web/20140627132742/http://download.sysinternals.com/files/ProcessMonitor.zip [Accessed 20 April 2021].

Docs.microsoft.com. 2018. *CreateProcessA function (processthreadsapi.h) - Win32 apps*. [online] Available from: https://docs.microsoft.com/en-us/windows/win32/api/processthreadsapi/nf-processthreadsapi-createprocessa [Accessed 5 May 2021].

Damodaran, A., Troia†, F., Corrado†, V., Austin, T. and Stamp, M., n.d. *A Comparison of Static, Dynamic, and Hybrid Analysis for Malware Detection*. [online] Available from: http://www.cs.sjsu.edu/faculty/stamp/papers/Anusha.pdf [Accessed 9 May 2021].

Doevan, J., 2018. *What is ws2_32.dll? Should I remove it?* [online] 2SpyWare. Available from: https://www.2-spyware.com/file-ws2_32-dll.html#:~:text=can%20cause%20problems-,ws2_32.,ws2_32. [Accessed 3 May 2021].

Docs.microsoft.com. 2018. *FindFirstFileA function (fileapi.h) - Win32 apps*. [online] Available from: https://docs.microsoft.com/en-us/windows/win32/api/fileapi/nf-fileapi-findfirstfilea [Accessed 2 May 2021].

Jain, S., 2018. *Malware Basic Dynamic analysis*. [online] Medium. Available from: https://medium.com/@jain.sm/malware-dynamic-analysis-338efc68a654#:~:text=Dynamic%20analysis%20is%20a%20technique,its%20behavior%20during%20run%20time.&text=Other%20way%20is%20to%20run,(no%20NAT%20to%20outside). [Accessed 4 May 2021].

Kaur, N. and Kumar, A., 2016. A Complete Dynamic Malware Analysis. *International Journal of Computer Applications*, [online] 135(4), pp.20-25. Available from: https://www.researchgate.net/publication/295256150_A_Complete_Dynamic_Malware_Analysis [Accessed 4 May 2021].

0xpat.github.io. 2020. *Malware development part 5*. [online] Available from: https://0xpat.github.io/Malware_development_part_5/ [Accessed 4 May 2021].

Mclean, B., 2018. *Using Shared Memory in a Dynamic-Link Library - Win32 apps*. [online] Docs.microsoft.com. Available from: https://docs.microsoft.com/en-us/windows/win32/dlls/using-shared-memory-in-a-dynamic-link-library [Accessed 2 May 2021].

informIT. 2010. *Windows System Programming: Process Management*. [online] Available from: https://www.informit.com/articles/article.aspx?p=1564827&seqNum=2 [Accessed 3 May 2021].

Comodo Enterprise. 2021. *Malware Analysis Methodology | Malware Analysis Tools from Comodo*. [online] Available from: https://enterprise.comodo.com/forensic-analysis/malware-analysis-methodology.php#:~:text=Malware%20Analysis%20Methodology%3A%20Dynamic%20or%20Behavioral%20Analysis&text=Examination%20of%20a%20contaminated%20file,general%20behavior%20of%20the%20file [Accessed 5 May 2021].

chappell, G., 2021. *ServiceMain*. [online] Geoffchappell.com. Available from: https://www.geoffchappell.com/studies/windows/win32/services/svchost/dll/servicemain.htm [Accessed 12 May 2021].

Cuckoosandbox.org. 2021. *Cuckoo Sandbox - Automated Malware Analysis*. [online] Available from: https://cuckoosandbox.org/ [Accessed 15 May 2021].

MalwareTips Community. 2015. *Are hybrid-analysis reports trustworthy?*. [online] Available at: <https://malwaretips.com/threads/are-hybrid-analysis-reports-trustworthy.45002/> [Accessed 16 May 2021].

JACKSON, W., 2009. *Static vs. dynamic code analysis: advantages and disadvantages -- GCN*. [online] GCN. Available from: https://gcn.com/articles/2009/02/09/static-vs-dynamic-code-analysis.aspx [Accessed 16 May 2021].

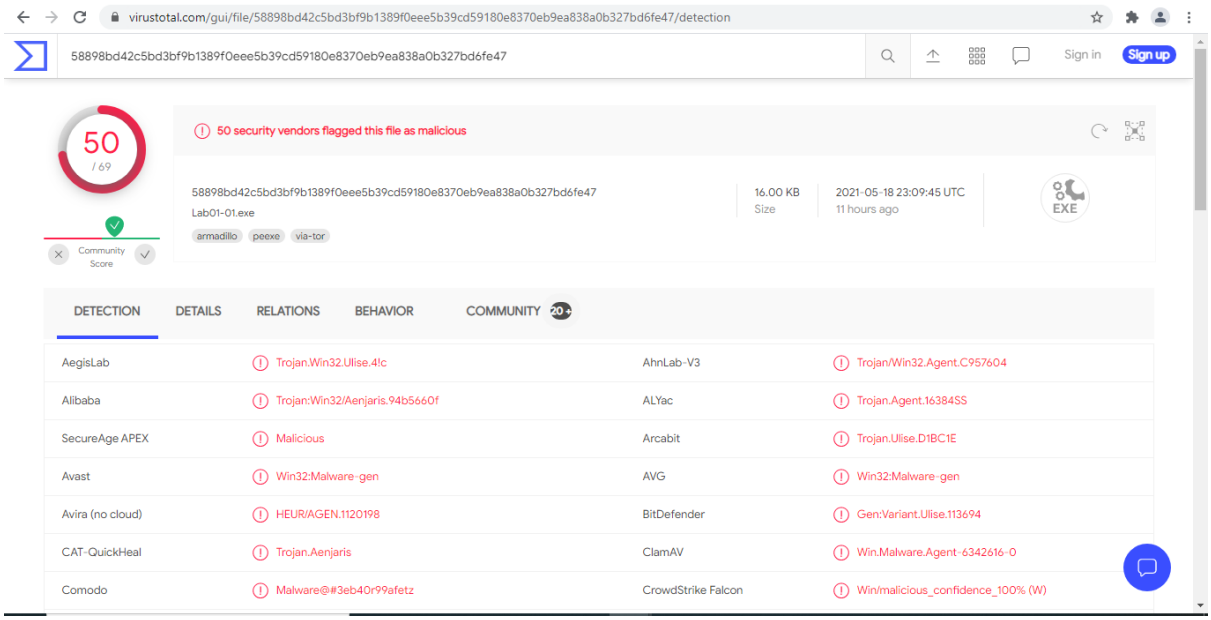
Books:

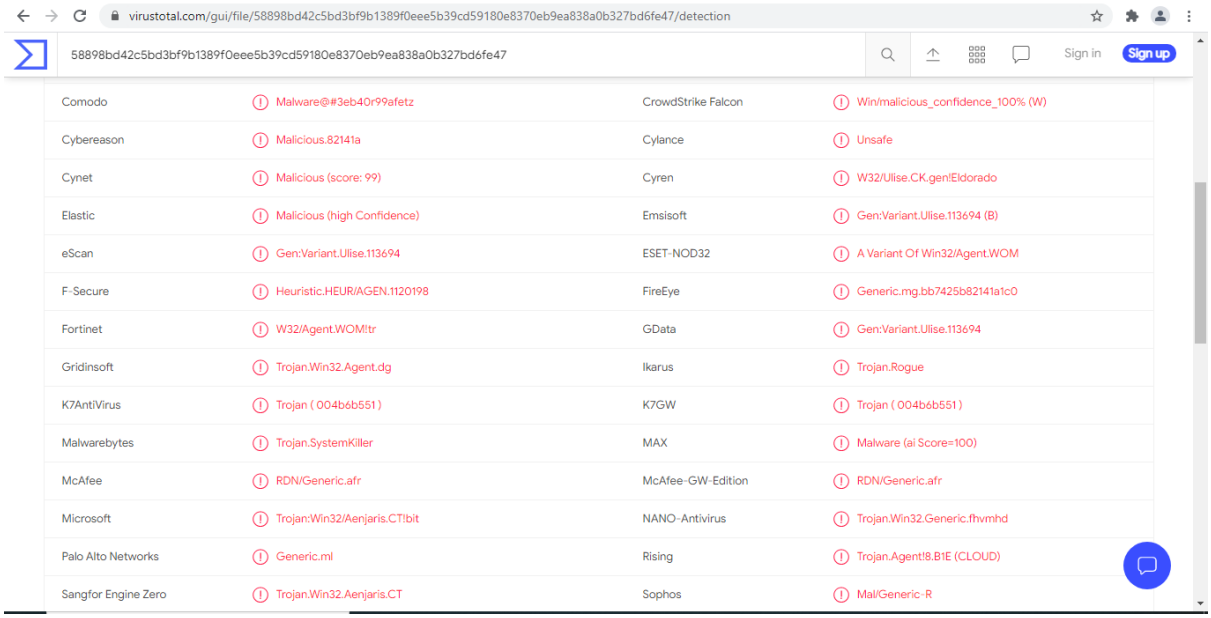
Sikorski, M. and Honig, A., 2012. *Practical Malware Analysis: A Hands-On Guide to Dissecting Malicious Software*. No Starch Press.

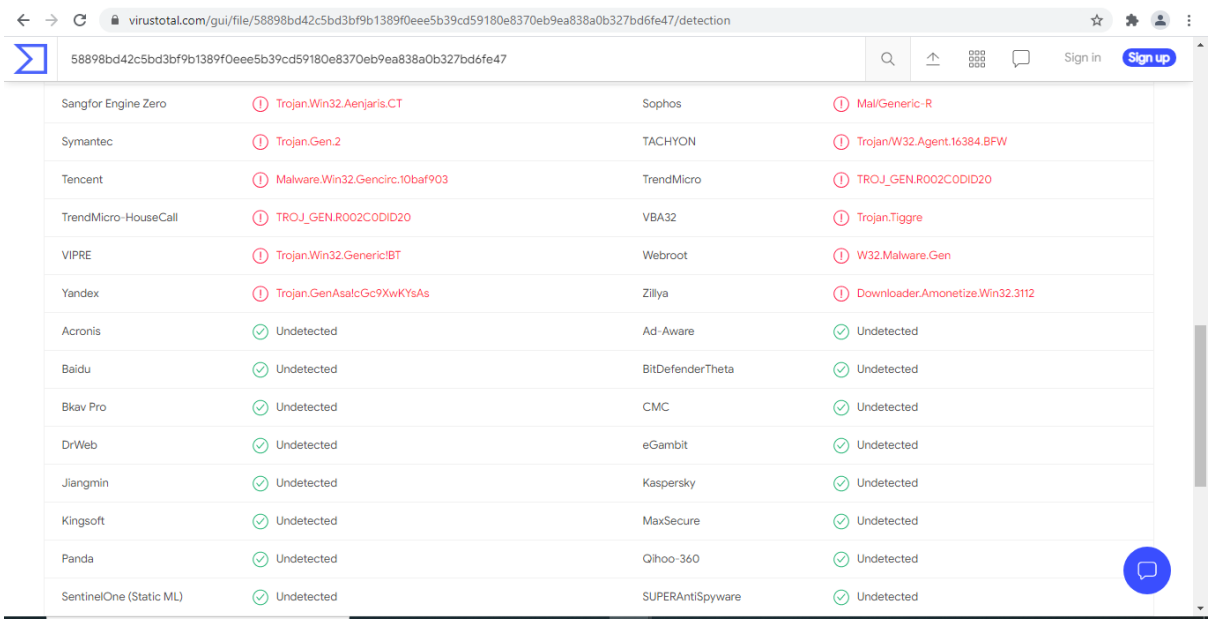
APPENDICES

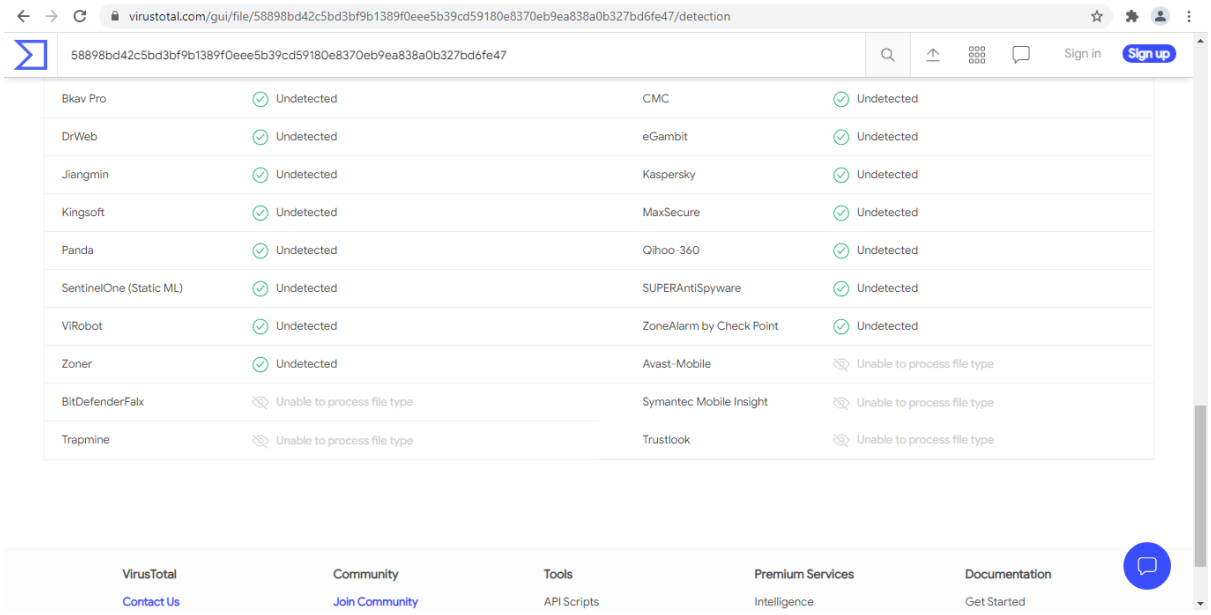
APPENDIX A – VIRUS TOTAL

1) Lab01-01
    a. Lab01-01.EXE

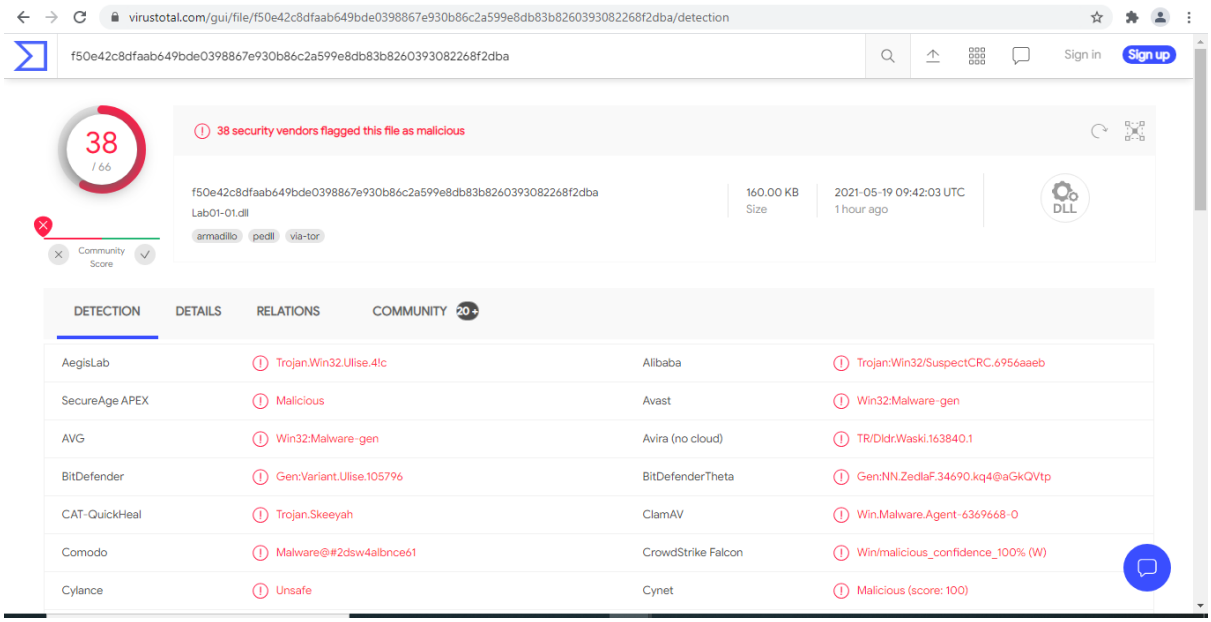


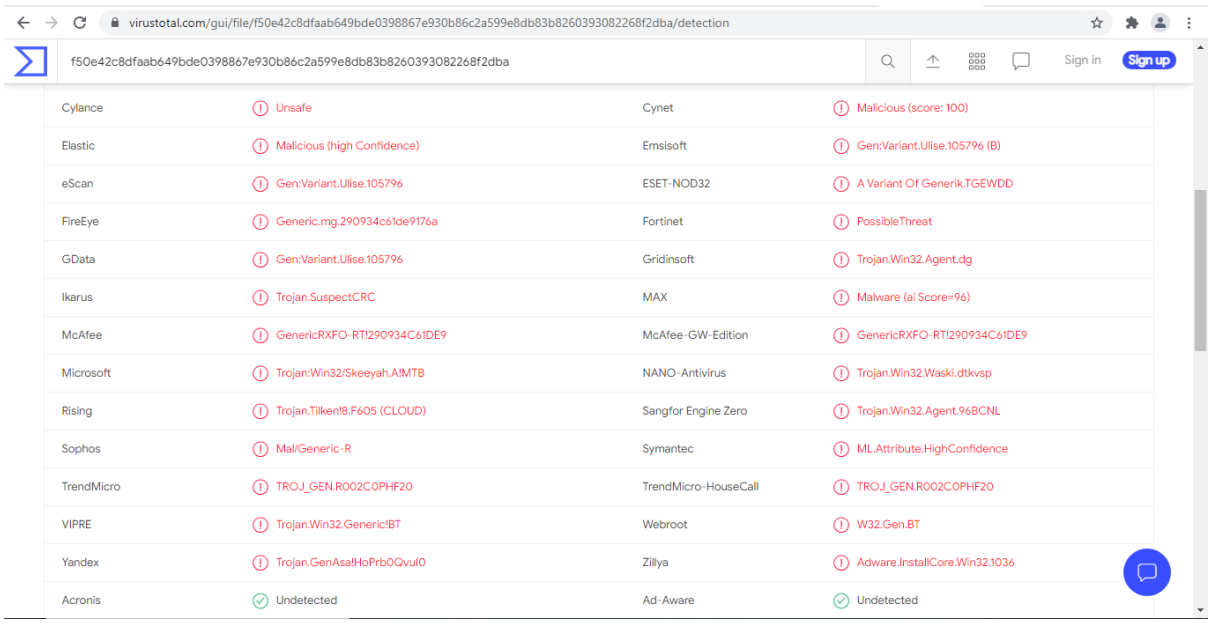

virustotal.com/gui/file/58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47/detection
58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47
Sign in
Sign up
Comodo Malware@#3eb40r99afetz
CrowdStrike Falcon Win/malicious_confidence_100% (W)
Cybereason Malicious.82141a
Cylance Unsafe
Cynet Malicious (score: 99)
Cyren W32/Ulise.CK.gen!Eldorado
Elastic Malicious (high Confidence)
Emsisoft Gen:Variant.Ulise.113694 (B)
eScan Gen:Variant.Ulise.113694
ESET-NOD32 A Variant Of Win32/Agent.WOM
F-Secure Heuristic.HEUR/AGEN.1120198
FireEye Generic.mg.bb7425b82141a1c0
Fortinet W32/Agent.WOM!tr
GData Gen:Variant.Ulise.113694
Gridinsoft Trojan.Win32.Agent.dg
Ikarus Trojan.Rogue
K7AntiVirus Trojan (004b6b551)
K7GW Trojan (004b6b551)
Malwarebytes Trojan.SystemKiller
MAX Malware (ai Score=100)
McAfee RDN/Generic.afr
McAfee-GW-Edition RDN/Generic.afr
Microsoft Trojan:Win32/Aenjaris.CT!bit
NANO-Antivirus Trojan.Win32.Generic.fhvmhd
Palo Alto Networks Generic.ml
Rising Trojan.Agent!8.B1E (CLOUD)
Sangfor Engine Zero Trojan.Win32.Aenjaris.CT
Sophos Mal/Generic-R

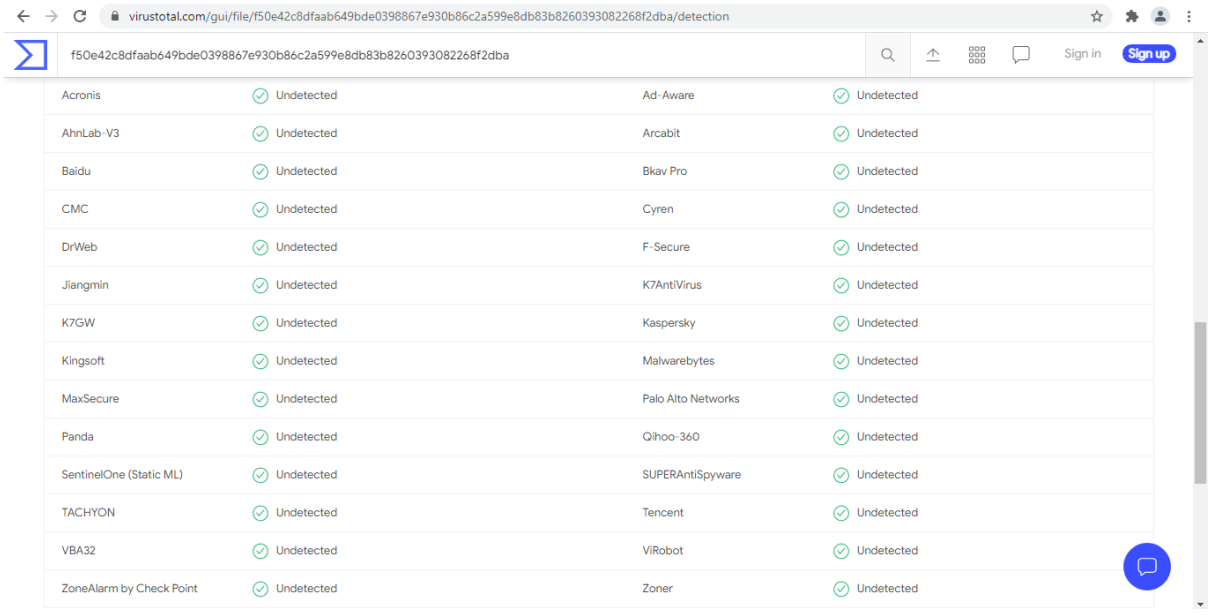

virustotal.com/gui/file/58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47/detection
58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47
Sign in
Sign up
Sangfor Engine Zero Trojan.Win32.Aenjaris.CT
Sophos Mal/Generic-R
Symantec Trojan.Gen.2
TACHYON Trojan/W32.Agent.16384.BFW
Tencent Malware.Win32.Gencirc.10baf903
TrendMicro TROJ_GEN.R002C0DID20
TrendMicro-HouseCall TROJ_GEN.R002C0DID20
VBA32 Trojan.Tiggre
VIPRE Trojan.Win32.Generic!BT
Webroot W32.Malware.Gen
Yandex Trojan.GenAsa!cGc9XwKYsAs
Zillya Downloader.Amonetize.Win32.3112
Acronis Undetected
Ad-Aware Undetected
Baidu Undetected
BitDefenderTheta Undetected
Bkav Pro Undetected
CMC Undetected
DrWeb Undetected
eGambit Undetected
Jiangmin Undetected
Kaspersky Undetected
Kingsoft Undetected
MaxSecure Undetected
Panda Undetected
Qihoo-360 Undetected
SentinelOne (Static ML) Undetected
SUPERAntiSpyware Undetected

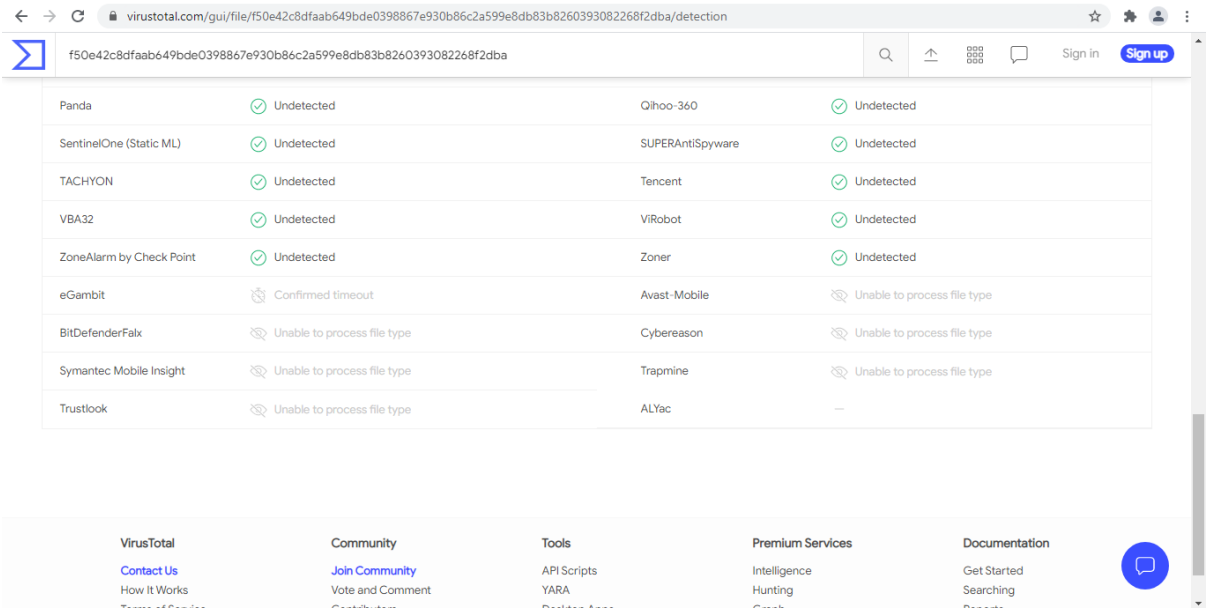


b. Lab01-01.DLL

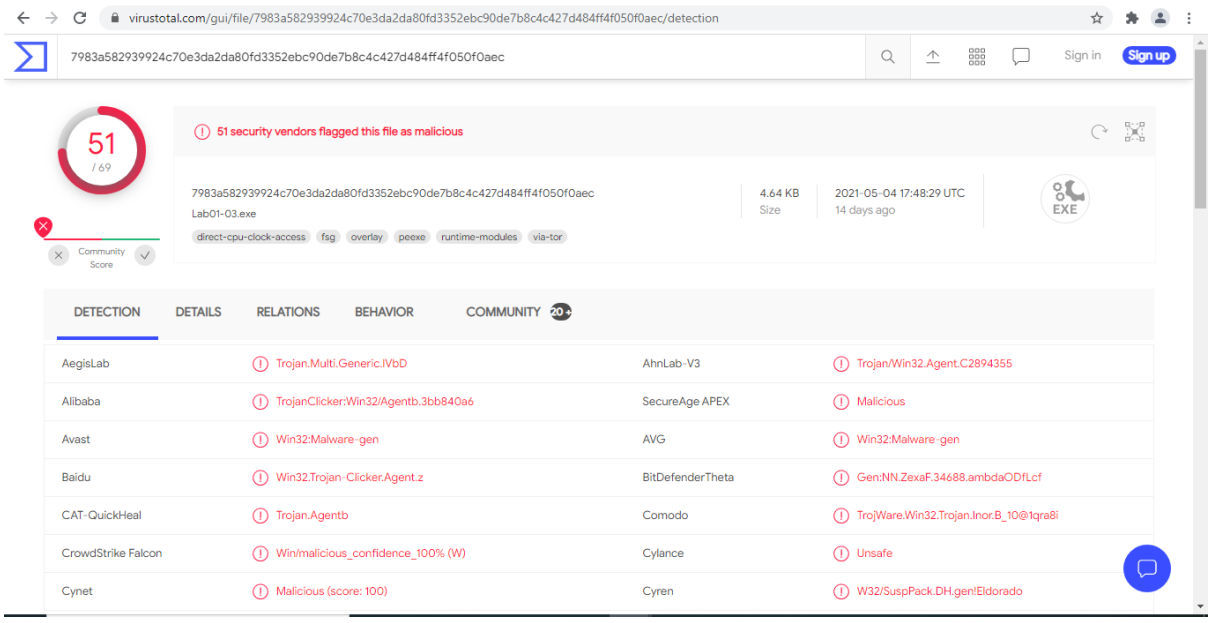


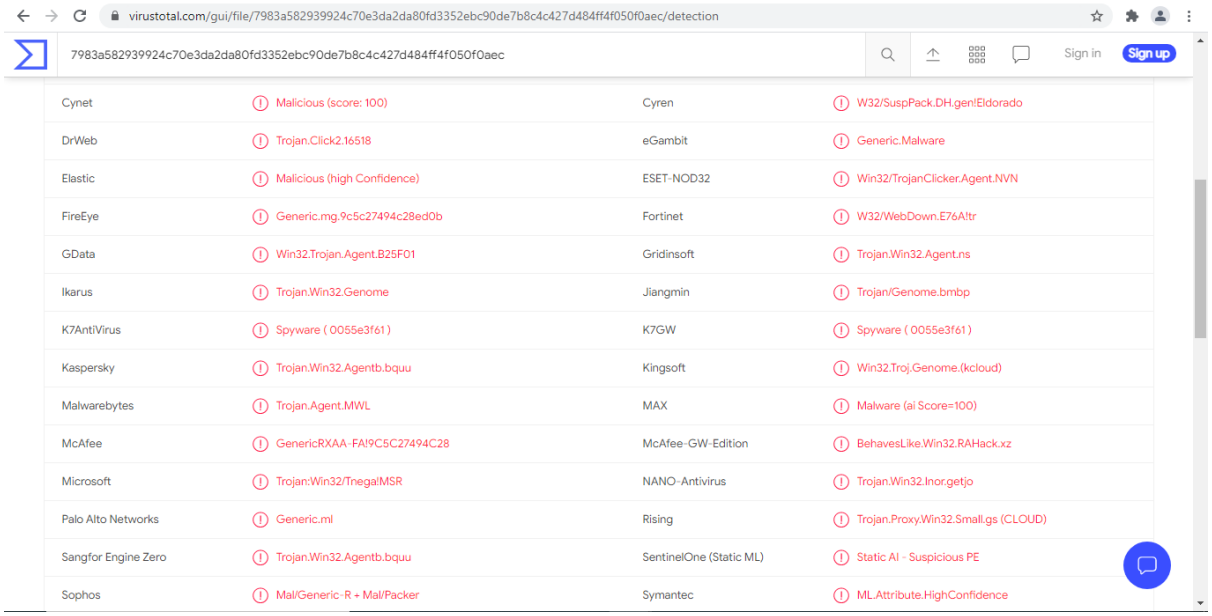

virustotal.com/gui/file/f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba/detection
f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba
Sign in
Sign up
Cylance Unsafe
Cynet Malicious (score: 100)
Elastic Malicious (high Confidence)
Emsisoft Gen:Variant.Ulise.105796 (B)
eScan Gen:Variant.Ulise.105796
ESET-NOD32 A Variant Of Generik.TGEWDD
FireEye Generic.mg.290934c61de9176a
Fortinet PossibleThreat
GData Gen:Variant.Ulise.105796
Gridinsoft Trojan.Win32.Agent.dg
Ikarus Trojan.SuspectCRC
MAX Malware (ai Score=96)
McAfee GenericRXFO-RT!290934C61DE9
McAfee-GW-Edition GenericRXFO-RT!290934C61DE9
Microsoft Trojan:Win32/Skeeyah.A!MTB
NANO-Antivirus Trojan.Win32.Waski.dtkvsp
Rising Trojan.Tilken!8.F605 (CLOUD)
Sangfor Engine Zero Trojan.Win32.Agent.96BCNL
Sophos Mal/Generic-R
Symantec ML.Attribute.HighConfidence
TrendMicro TROJ_GEN.R002C0PHF20
TrendMicro-HouseCall TROJ_GEN.R002C0PHF20
VIPRE Trojan.Win32.Generic!BT
Webroot W32.Gen.BT
Yandex Trojan.GenAsa!HoPrb0Qvul0
Zillya Adware.InstallCore.Win32.1036
Acronis Undetected
Ad-Aware Undetected

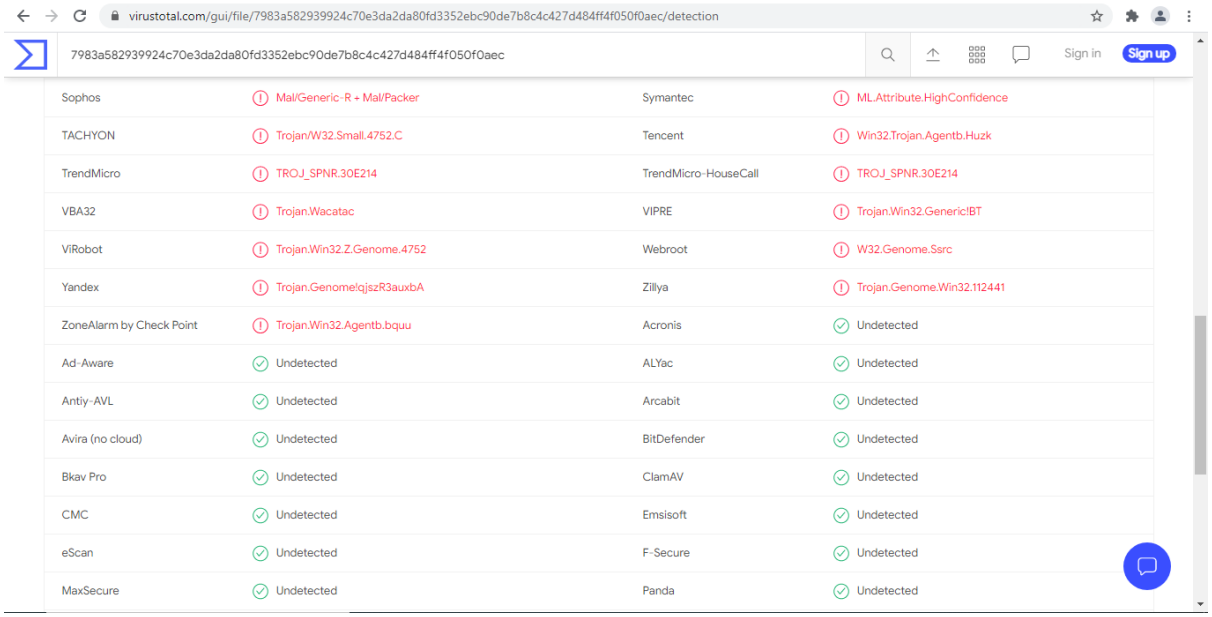

virustotal.com/gui/file/f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba/detection
f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba
Sign in
Sign up
Acronis Undetected
Ad-Aware Undetected
AhnLab-V3 Undetected
Arcabit Undetected
Baidu Undetected
Bkav Pro Undetected
CMC Undetected
Cyren Undetected
DrWeb Undetected
F-Secure Undetected
Jiangmin Undetected
K7AntiVirus Undetected
K7GW Undetected
Kaspersky Undetected
Kingsoft Undetected
Malwarebytes Undetected
MaxSecure Undetected
Palo Alto Networks Undetected
Panda Undetected
Qihoo-360 Undetected
SentinelOne (Static ML) Undetected
SUPERAntiSpyware Undetected
TACHYON Undetected
Tencent Undetected
VBA32 Undetected
ViRobot Undetected
ZoneAlarm by Check Point Undetected
Zoner Undetected

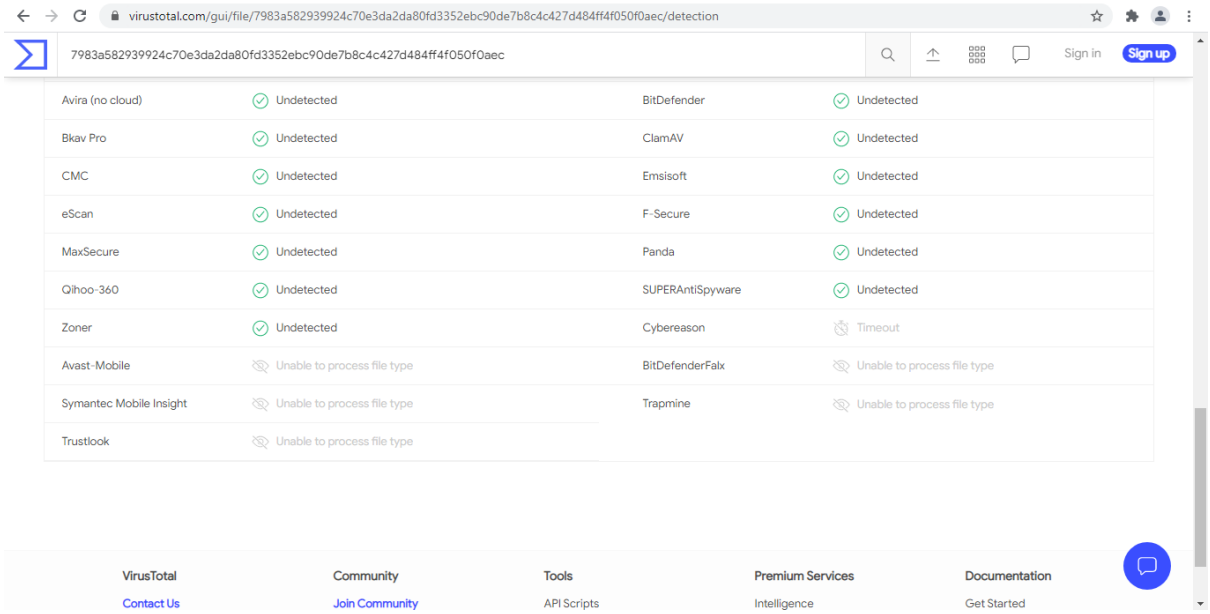


2) Lab01-03.exe




virustotal.com/gui/file/7983a582939924c70e3da2da80fd3352ebc90de7b8c4c427d484ff4f050f0aec/detection
7983a582939924c70e3da2da80fd3352ebc90de7b8c4c427d484ff4f050f0aec
Sign in
Sign up
Cynet Malicious (score: 100)
Cyren W32/SuspPack.DH.gen!Eldorado
DrWeb Trojan.Click2.16518
eGambit Generic.Malware
Elastic Malicious (high Confidence)
ESET-NOD32 Win32/TrojanClicker.Agent.NVN
FireEye Generic.mg.9c5c27494c28ed0b
Fortinet W32/WebDown.E76A!tr
GData Win32.Trojan.Agent.B25F01
Gridinsoft Trojan.Win32.Agent.ns
Ikarus Trojan.Win32.Genome
Jiangmin Trojan/Genome.bmbp
K7AntiVirus Spyware (0055e3f61)
K7GW Spyware (0055e3f61)
Kaspersky Trojan.Win32.Agentb.bquu
Kingsoft Win32.Troj.Genome.(kcloud)
Malwarebytes Trojan.Agent.MWL
MAX Malware (ai Score=100)
McAfee GenericRXAA-FA!9C5C27494C28
McAfee-GW-Edition BehavesLike.Win32.RAHack.xz
Microsoft Trojan:Win32/Tnega!MSR
NANO-Antivirus Trojan.Win32.Inor.getjo
Palo Alto Networks Generic.ml
Rising Trojan.Proxy.Win32.Small.gs (CLOUD)
Sangfor Engine Zero Trojan.Win32.Agentb.bquu
SentinelOne (Static ML) Static AI - Suspicious PE
Sophos Mal/Generic-R + Mal/Packer
Symantec ML.Attribute.HighConfidence

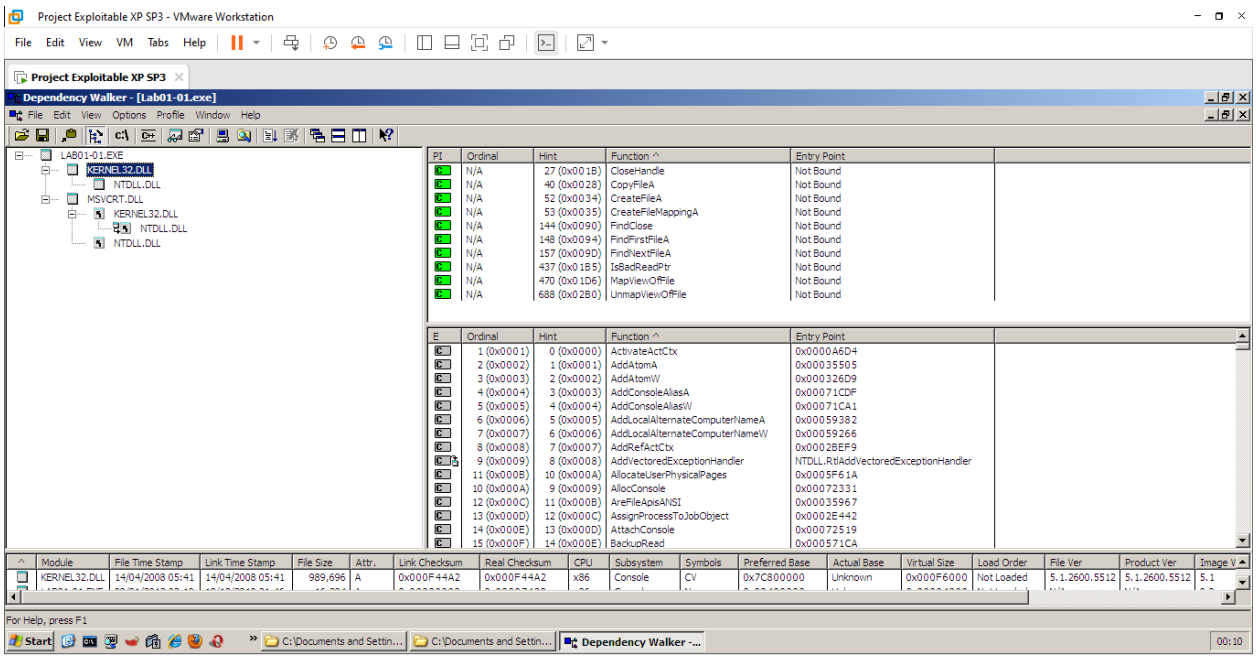

virustotal.com/gui/file/7983a582939924c70e3da2da80fd3352ebc90de7b8c4c427d484ff4f050f0aec/detection
7983a582939924c70e3da2da80fd3352ebc90de7b8c4c427d484ff4f050f0aec
Sign in
Sign up
Sophos Mal/Generic-R + Mal/Packer
Symantec ML.Attribute.HighConfidence
TACHYON Trojan/W32.Small.4752.C
Tencent Win32.Trojan.Agentb.Huzk
TrendMicro TROJ_SPNR.30E214
TrendMicro-HouseCall TROJ_SPNR.30E214
VBA32 Trojan.Wacatac
VIPRE Trojan.Win32.Generic!BT
ViRobot Trojan.Win32.Z.Genome.4752
Webroot W32.Genome.Ssrc
Yandex Trojan.Genome!qjszR3auxbA
Zillya Trojan.Genome.Win32.112441
ZoneAlarm by Check Point Trojan.Win32.Agentb.bquu
Acronis Undetected
Ad-Aware Undetected
ALYac Undetected
Antiy-AVL Undetected
Arcabit Undetected
Avira (no cloud) Undetected
BitDefender Undetected
Bkav Pro Undetected
ClamAV Undetected
CMC Undetected
Emsisoft Undetected
eScan Undetected
F-Secure Undetected
MaxSecure Undetected
Panda Undetected

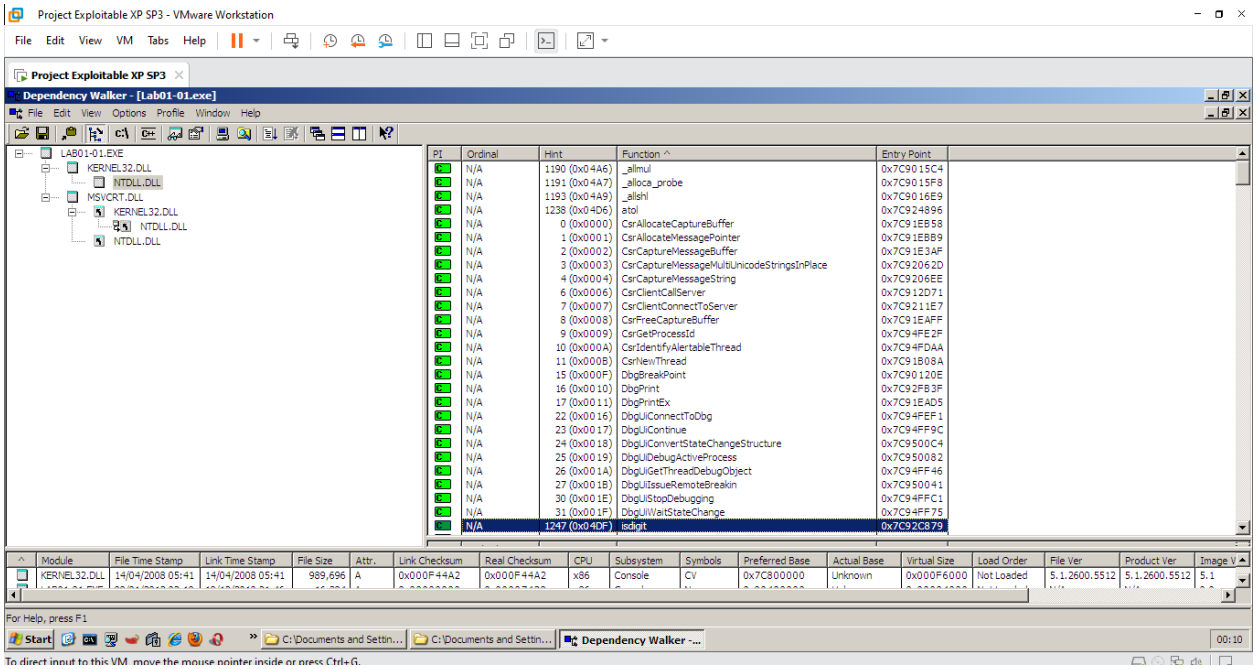

virustotal.com/gui/file/7983a582939924c70e3da2da80fd3352ebc90de7b8c4c427d484ff4f050f0aec/detection
7983a582939924c70e3da2da80fd3352ebc90de7b8c4c427d484ff4f050f0aec
Sign in
Sign up
Avira (no cloud) Undetected
BitDefender Undetected
Bkav Pro Undetected
ClamAV Undetected
CMC Undetected
Emsisoft Undetected
eScan Undetected
F-Secure Undetected
MaxSecure Undetected
Panda Undetected
Qihoo-360 Undetected
SUPERAntiSpyware Undetected
Zoner Undetected
Cybereason Timeout
Avast-Mobile Unable to process file type
BitDefenderFalx Unable to process file type
Symantec Mobile Insight Unable to process file type
Trapmine Unable to process file type
Trustlook Unable to process file type
VirusTotal
Contact Us
Community
Join Community
Tools
API Scripts
Premium Services
Intelligence
Documentation
Get Started

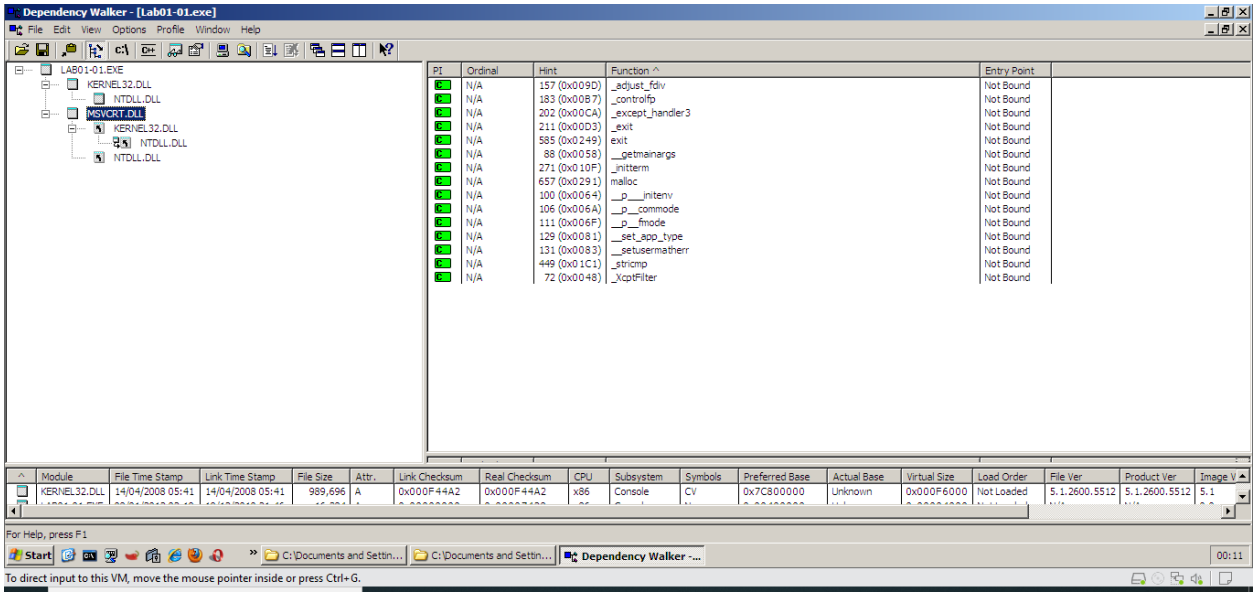
APPENDIX B – DEPENDENCY WALKER

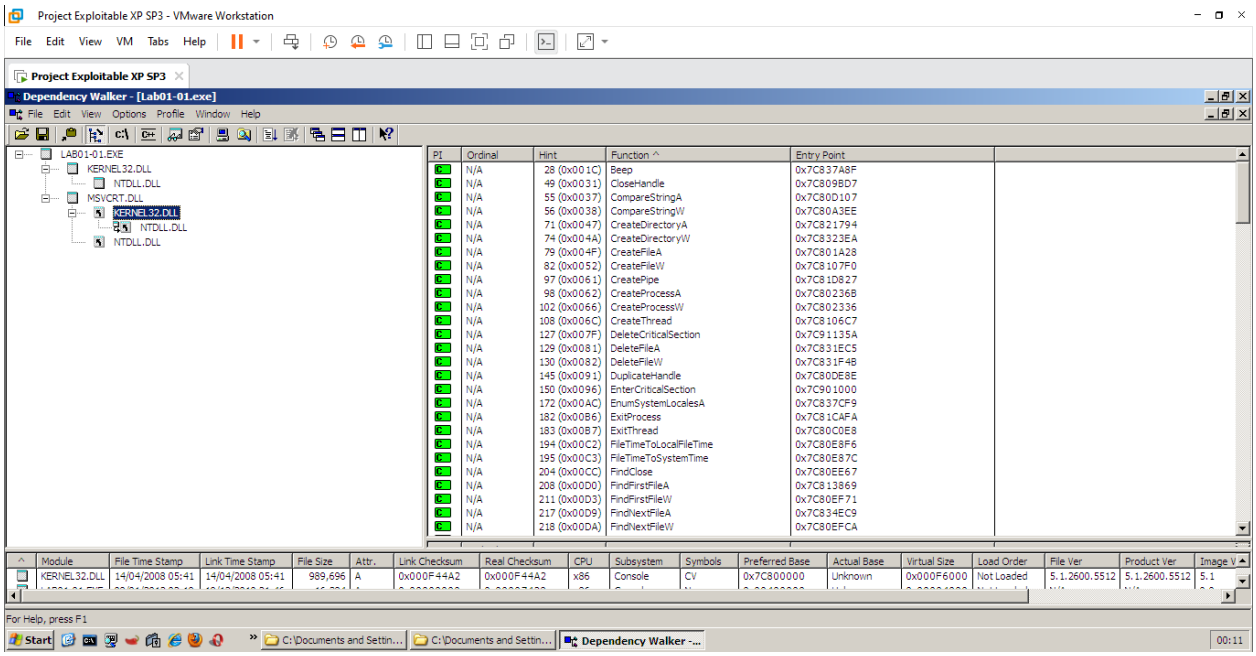
Basic Static Analysis:

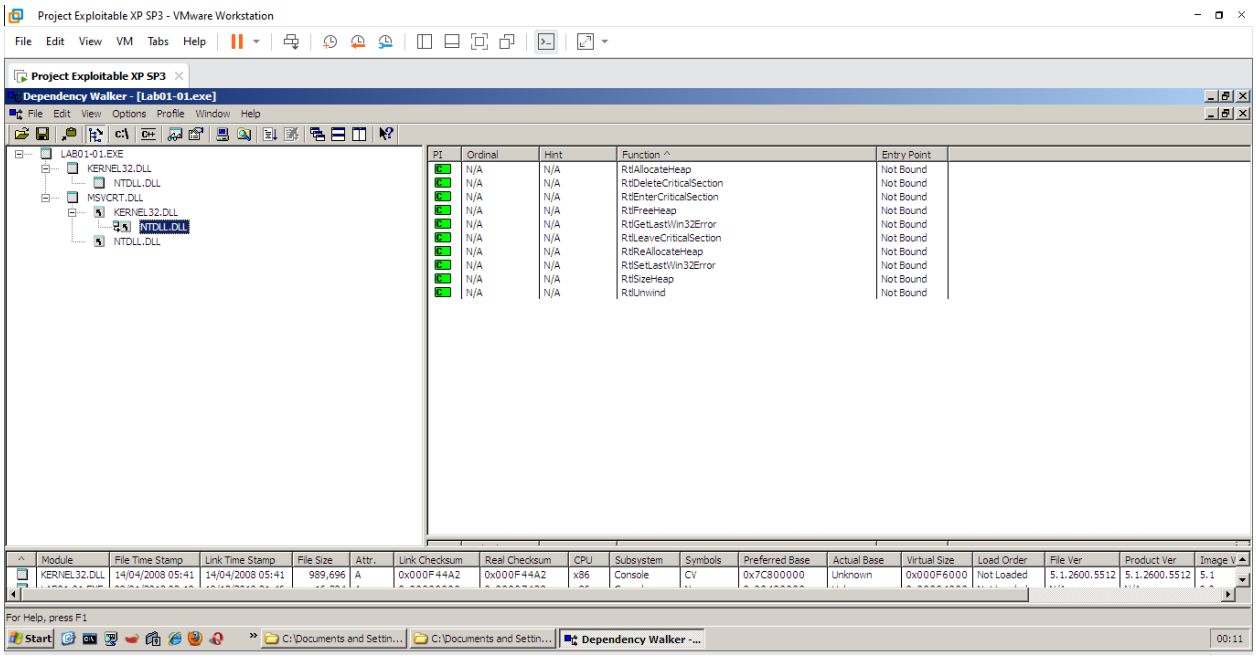
1) Lab01-01.exe

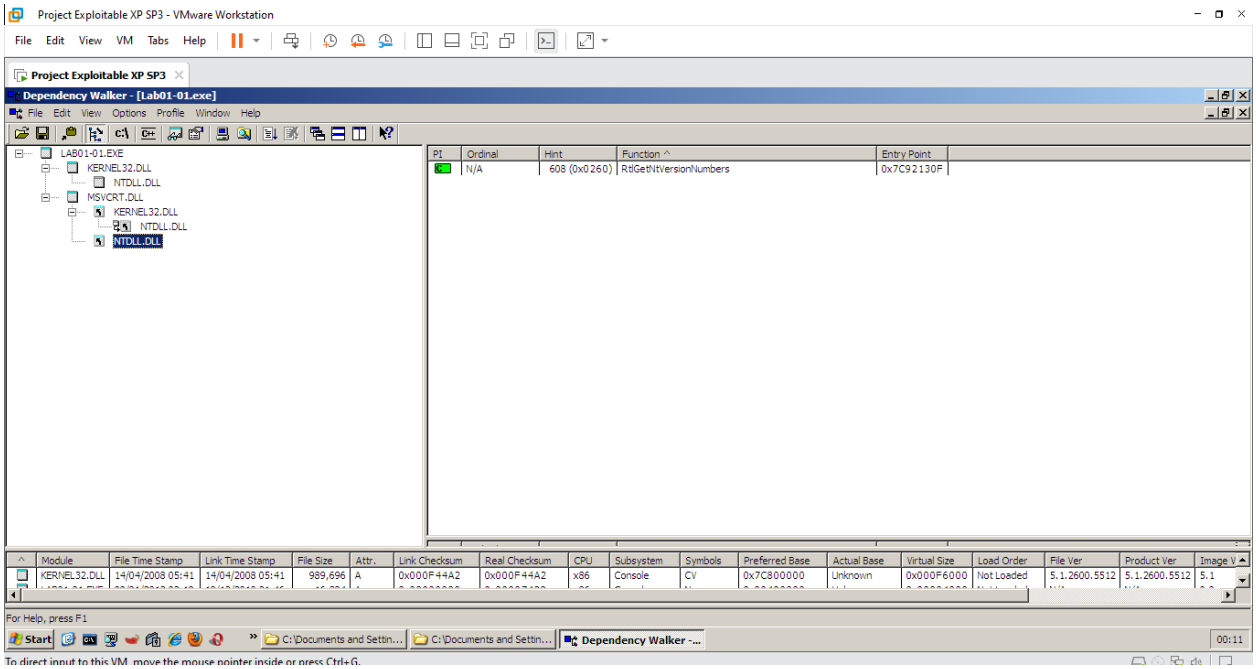





Dependency Walker - [Lab01-01.exe]
File Edit View Options Profile Window Help
LAB01-01.EXE
KERNEL32.DLL
NTDLL.DLL
MSVCRT.DLL
KERNEL32.DLL
NTDLL.DLL
NTDLL.DLL
PI Ordinal Hint Function Entry Point
N/A 157 (0x009D) _adjust_fdiv Not Bound
N/A 183 (0x00B7) _controlfp Not Bound
N/A 202 (0x00CA) _except_handler3 Not Bound
N/A 211 (0x00D3) _exit Not Bound
N/A 585 (0x0249) exit Not Bound
N/A 88 (0x0058) __getmainargs Not Bound
N/A 271 (0x010F) _initterm Not Bound
N/A 657 (0x0291) malloc Not Bound
N/A 100 (0x0064) __p___initenv Not Bound
N/A 106 (0x006A) __p___commode Not Bound
N/A 111 (0x006F) __p__fmode Not Bound
N/A 129 (0x0081) __set_app_type Not Bound
N/A 131 (0x0083) __setusermatherr Not Bound
N/A 449 (0x01C1) _stricmp Not Bound
N/A 72 (0x0048) _XcptFilter Not Bound
Module File Time Stamp Link Time Stamp File Size Attr. Link Checksum Real Checksum CPU Subsystem Symbols Preferred Base Actual Base Virtual Size Load Order File Ver Product Ver Image V
KERNEL32.DLL 14/04/2008 05:41 14/04/2008 05:41 989,696 A 0x000F44A2 0x000F44A2 x86 Console CV 0x7C800000 Unknown 0x000F6000 Not Loaded 5.1.2600.5512 5.1.2600.5512 5.1
For Help, press F1
Start
C:\Documents and Settin...
C:\Documents and Settin...
Dependency Walker -...
00:11
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Project Exploitable XP SP3 - VMware Workstation
File Edit View VM Tabs Help
Project Exploitable XP SP3
Dependency Walker - [Lab01-01.exe]
File Edit View Options Profile Window Help
LAB01-01.EXE
KERNEL32.DLL
NTDLL.DLL
MSVCRT.DLL
KERNEL32.DLL
NTDLL.DLL
NTDLL.DLL
PI Ordinal Hint Function Entry Point
N/A 28 (0x001C) Beep 0x7C837A8F
N/A 49 (0x0031) CloseHandle 0x7C809BD7
N/A 55 (0x0037) CompareStringA 0x7C80D107
N/A 56 (0x0038) CompareStringW 0x7C80A3EE
N/A 71 (0x0047) CreateDirectoryA 0x7C821794
N/A 74 (0x004A) CreateDirectoryW 0x7C8323EA
N/A 79 (0x004F) CreateFileA 0x7C801A28
N/A 82 (0x0052) CreateFileW 0x7C8107F0
N/A 97 (0x0061) CreatePipe 0x7C81D827
N/A 98 (0x0062) CreateProcessA 0x7C80236B
N/A 102 (0x0066) CreateProcessW 0x7C802336
N/A 108 (0x006C) CreateThread 0x7C8106C7
N/A 127 (0x007F) DeleteCriticalSection 0x7C91135A
N/A 129 (0x0081) DeleteFileA 0x7C831EC5
N/A 130 (0x0082) DeleteFileW 0x7C831F4B
N/A 145 (0x0091) DuplicateHandle 0x7C80DE8E
N/A 150 (0x0096) EnterCriticalSection 0x7C901000
N/A 172 (0x00AC) EnumSystemLocalesA 0x7C837CF9
N/A 182 (0x00B6) ExitProcess 0x7C81CAFA
N/A 183 (0x00B7) ExitThread 0x7C80C0E8
N/A 194 (0x00C2) FileTimeToLocalFileTime 0x7C80E8F6
N/A 195 (0x00C3) FileTimeToSystemTime 0x7C80E87C
N/A 204 (0x00CC) FindClose 0x7C80EE67
N/A 208 (0x00D0) FindFirstFileA 0x7C813869
N/A 211 (0x00D3) FindFirstFileW 0x7C80EF71
N/A 217 (0x00D9) FindNextFileA 0x7C834EC9
N/A 218 (0x00DA) FindNextFileW 0x7C80EFCA
Module File Time Stamp Link Time Stamp File Size Attr. Link Checksum Real Checksum CPU Subsystem Symbols Preferred Base Actual Base Virtual Size Load Order File Ver Product Ver Image V
KERNEL32.DLL 14/04/2008 05:41 14/04/2008 05:41 989,696 A 0x000F44A2 0x000F44A2 x86 Console CV 0x7C800000 Unknown 0x000F6000 Not Loaded 5.1.2600.5512 5.1.2600.5512 5.1
For Help, press F1
Start
C:\Documents and Settin...
C:\Documents and Settin...
Dependency Walker -...
00:11

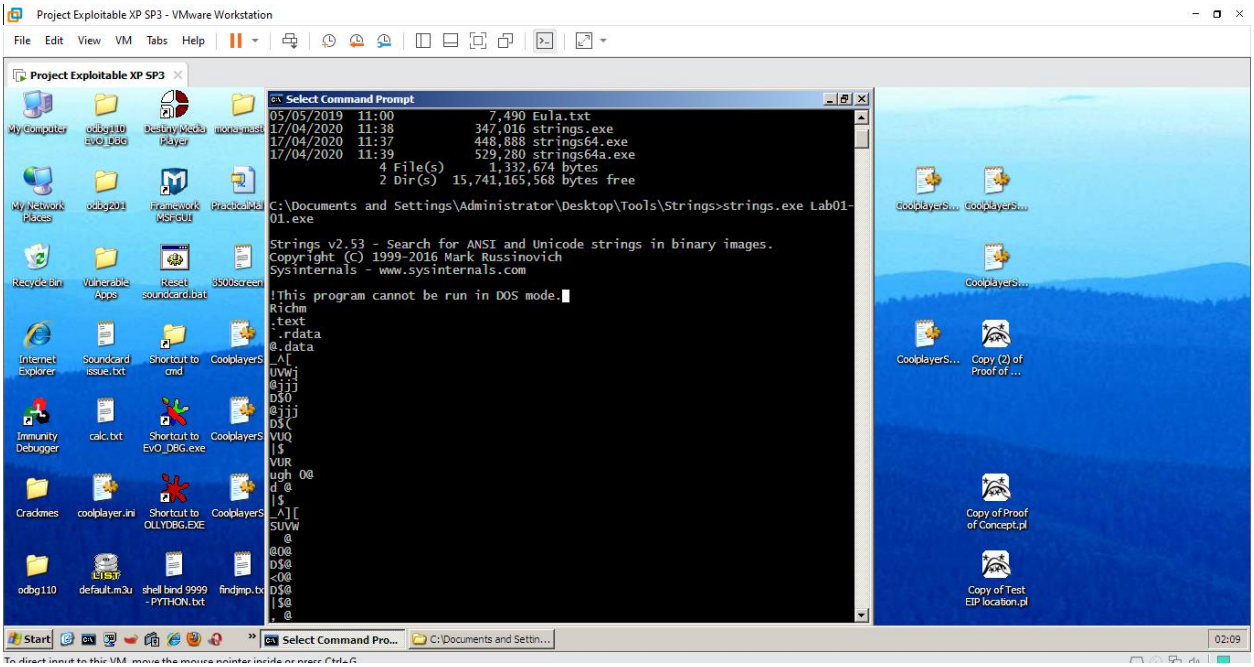

Project Exploitable XP SP3 - VMware Workstation
File Edit View VM Tabs Help
Project Exploitable XP SP3
Dependency Walker - [Lab01-01.exe]
File Edit View Options Profile Window Help
LAB01-01.EXE
KERNEL32.DLL
NTDLL.DLL
MSVCRT.DLL
KERNEL32.DLL
NTDLL.DLL
NTDLL.DLL
PI Ordinal Hint Function Entry Point
N/A N/A RtlAllocateHeap Not Bound
N/A N/A RtlDeleteCriticalSection Not Bound
N/A N/A RtlEnterCriticalSection Not Bound
N/A N/A RtlFreeHeap Not Bound
N/A N/A RtlGetLastWin32Error Not Bound
N/A N/A RtlLeaveCriticalSection Not Bound
N/A N/A RtlReAllocateHeap Not Bound
N/A N/A RtlSetLastWin32Error Not Bound
N/A N/A RtlSizeHeap Not Bound
N/A N/A RtlUnwind Not Bound
Module File Time Stamp Link Time Stamp File Size Attr. Link Checksum Real Checksum CPU Subsystem Symbols Preferred Base Actual Base Virtual Size Load Order File Ver Product Ver Image V
KERNEL32.DLL 14/04/2008 05:41 14/04/2008 05:41 989,696 A 0x000F44A2 0x000F44A2 x86 Console CV 0x7C800000 Unknown 0x000F6000 Not Loaded 5.1.2600.5512 5.1.2600.5512 5.1
For Help, press F1
Start
C:\Documents and Settin...
C:\Documents and Settin...
Dependency Walker -...
00:11

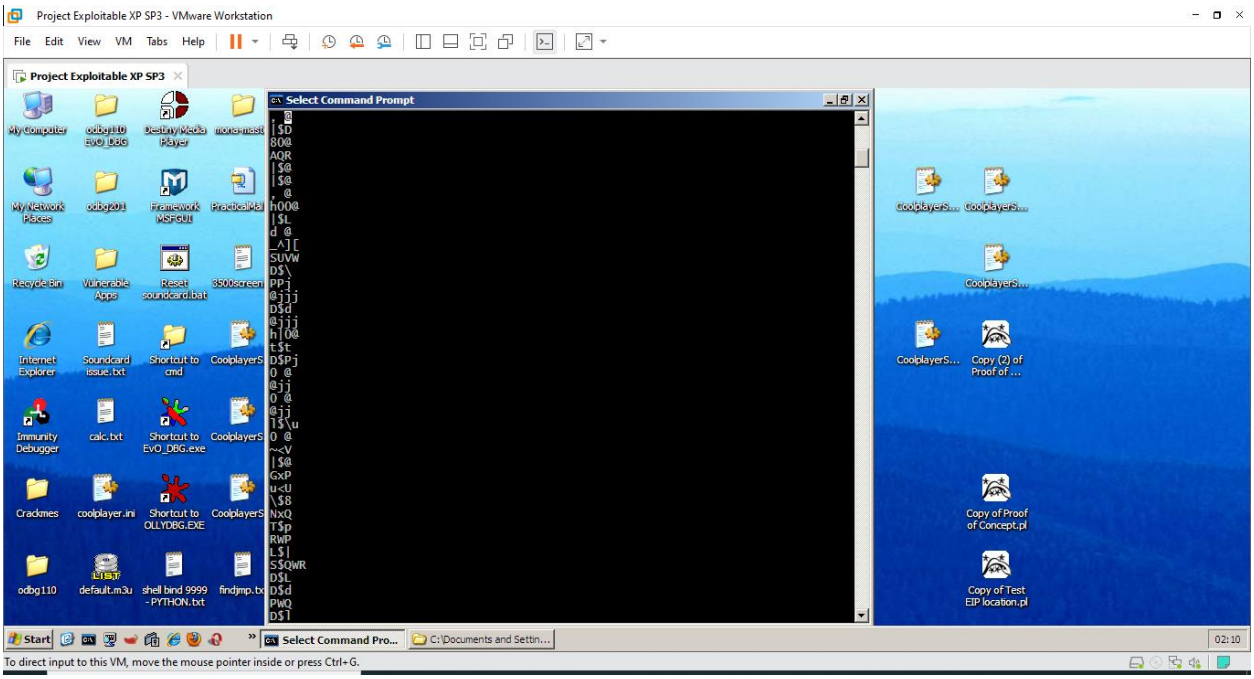

Project Exploitable XP SP3 - VMware Workstation
File Edit View VM Tabs Help
Project Exploitable XP SP3
Dependency Walker - [Lab01-01.exe]
File Edit View Options Profile Window Help
LAB01-01.EXE
KERNEL32.DLL
NTDLL.DLL
MSVCRT.DLL
KERNEL32.DLL
NTDLL.DLL
NTDLL.DLL
PI Ordinal Hint Function Entry Point
N/A 608 (0x0260) RtlGetNtVersionNumbers 0x7C92130F
Module File Time Stamp Link Time Stamp File Size Attr. Link Checksum Real Checksum CPU Subsystem Symbols Preferred Base Actual Base Virtual Size Load Order File Ver Product Ver Image V
KERNEL32.DLL 14/04/2008 05:41 14/04/2008 05:41 989,696 A 0x000F44A2 0x000F44A2 x86 Console CV 0x7C800000 Unknown 0x000F6000 Not Loaded 5.1.2600.5512 5.1.2600.5512 5.1
For Help, press F1
Start
C:\Documents and Settin...
C:\Documents and Settin...
Dependency Walker -...
00:11
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

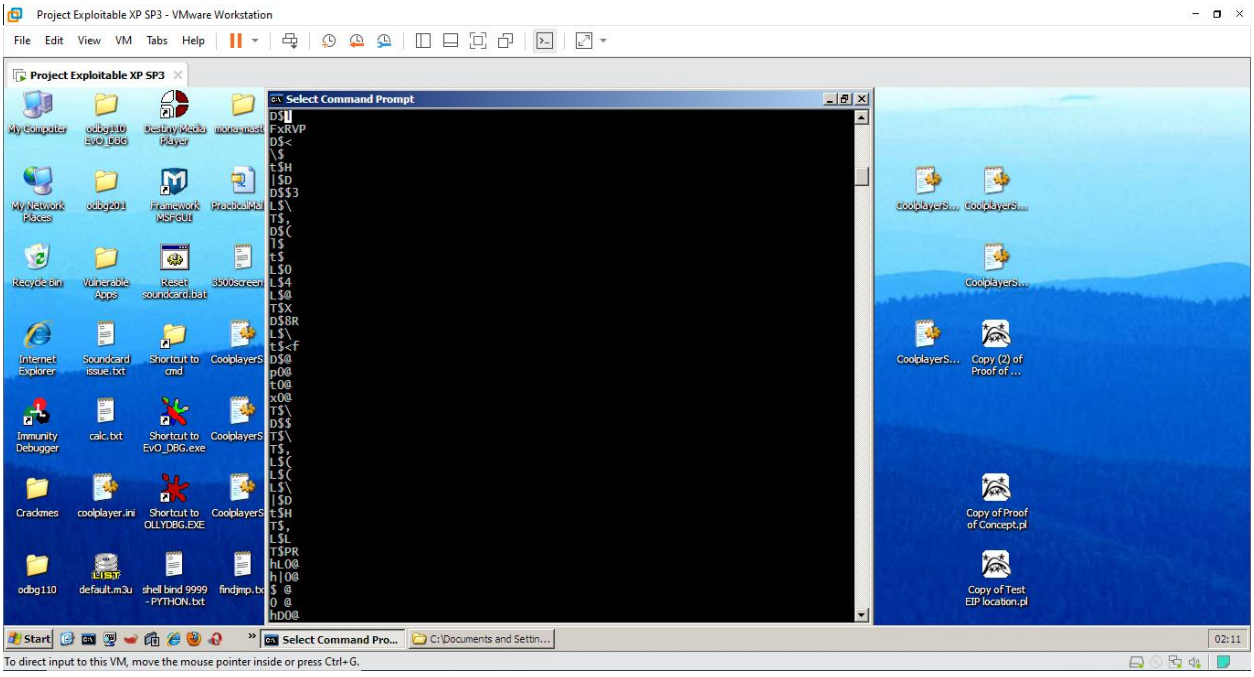
APPENDIX C - STRINGS

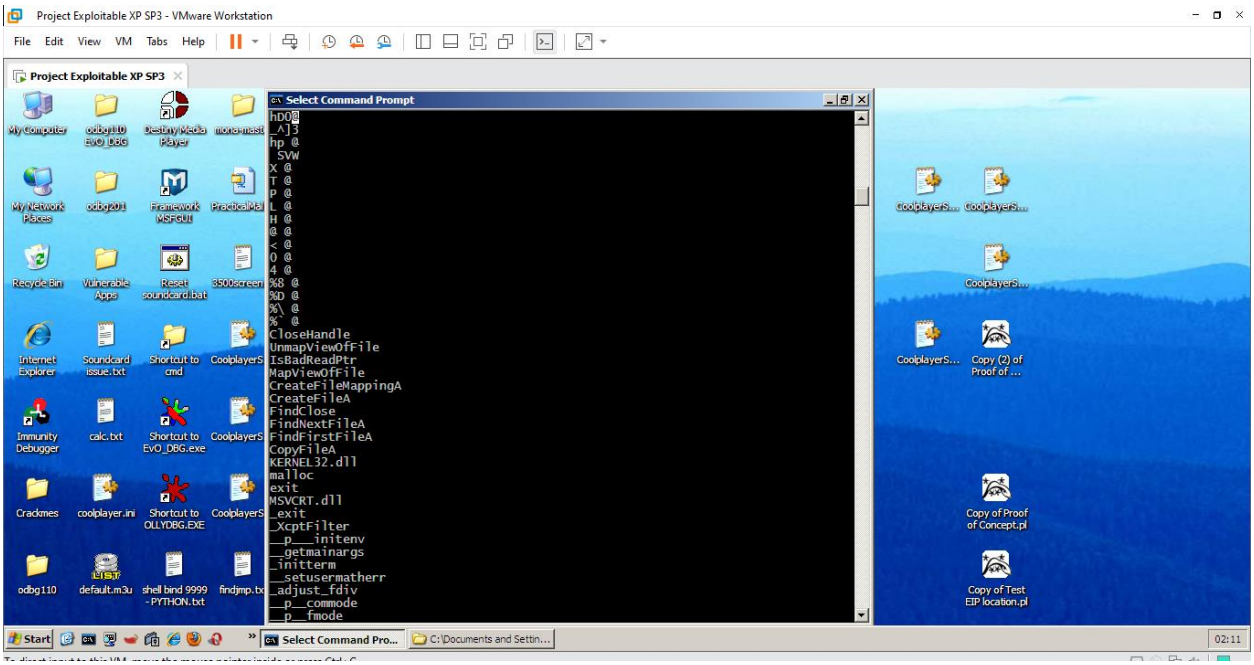
1) Static Analysis

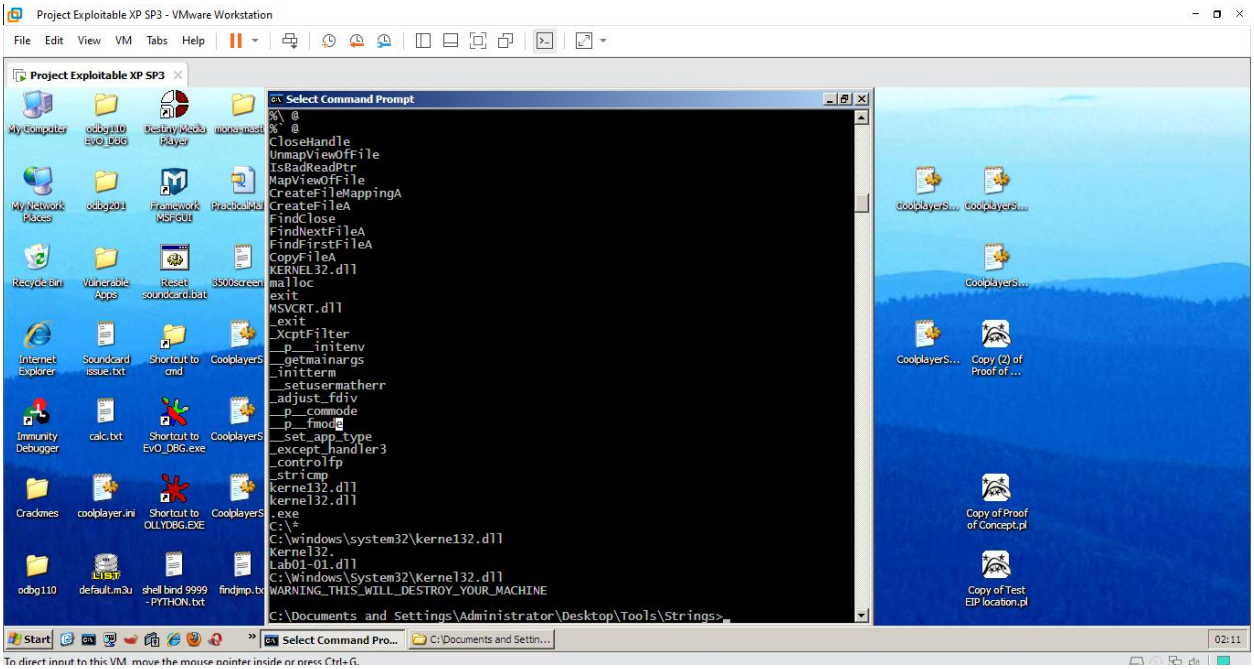
a. Lab01-01.exe



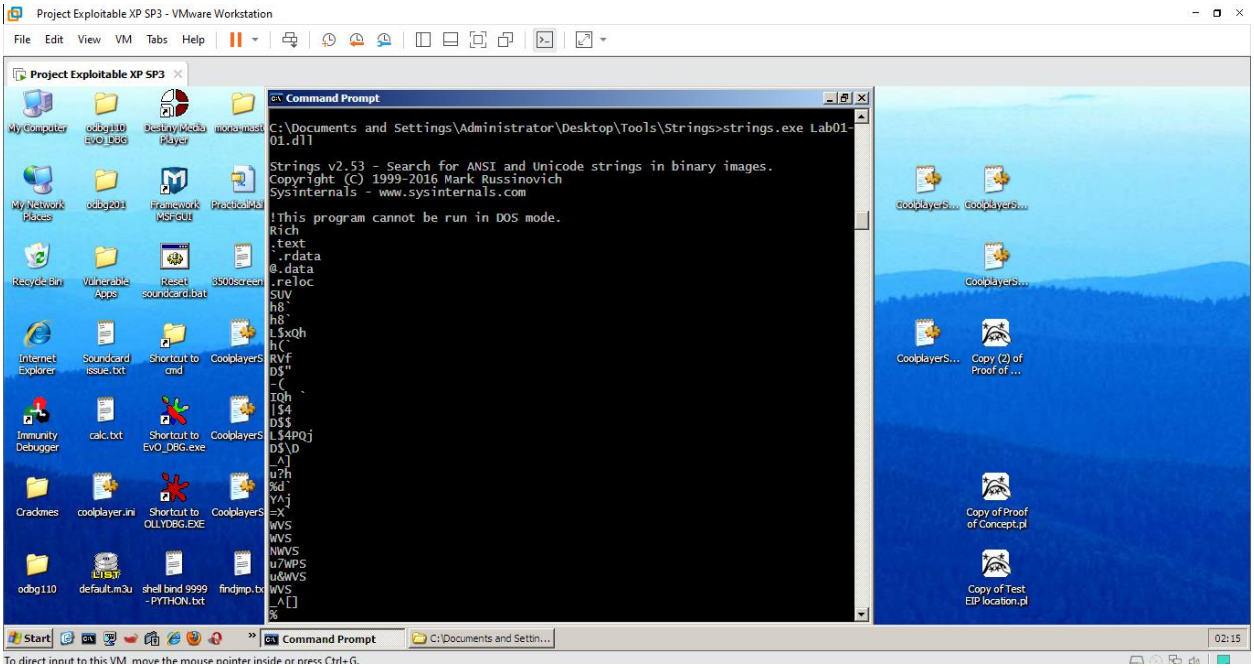

Project Exploitable XP SP3 - VMware Workstation
File Edit View VM Tabs Help
Project Exploitable XP SP3
Select Command Prompt
Start
Select Command Pro...
C:\Documents and Settin...
02:10
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

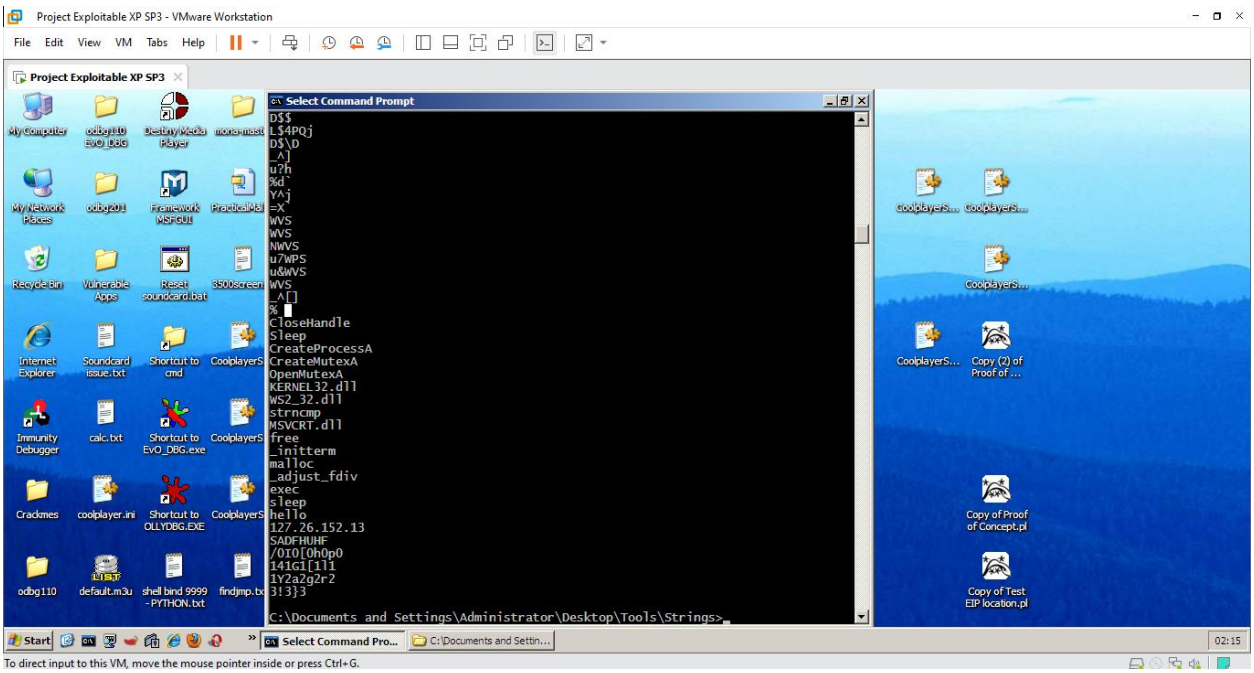

Project Exploitable XP SP3 - VMware Workstation
File Edit View VM Tabs Help
Project Exploitable XP SP3
Select Command Prompt
Start
Select Command Pro...
C:\Documents and Settin...
02:11
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Project Exploitable XP SP3 - VMware Workstation
File Edit View VM Tabs Help
Project Exploitable XP SP3
Select Command Prompt
CloseHandle
UnmapViewOfFile
IsBadReadPtr
MapViewOfFile
CreateFileMappingA
CreateFileA
FindClose
FindNextFileA
FindFirstFileA
CopyFileA
KERNEL32.dll
malloc
exit
MSVCRT.dll
_exit
_XcptFilter
__p___initenv
__getmainargs
_initterm
__setusermatherr
_adjust_fdiv
__p__commode
__p__fmode
Start
Select Command Pro...
C:\Documents and Settin...
02:11


Project Exploitable XP SP3 - VMware Workstation
File Edit View VM Tabs Help
Project Exploitable XP SP3
Select Command Prompt
CloseHandle
UnmapViewOfFile
IsBadReadPtr
MapViewOfFile
CreateFileMappingA
CreateFileA
FindClose
FindNextFileA
FindFirstFileA
CopyFileA
KERNEL32.dll
malloc
exit
MSVCRT.dll
_exit
_XcptFilter
__p___initenv
__getmainargs
_initterm
__setusermatherr
_adjust_fdiv
__p__commode
__p__fmode
__set_app_type
_except_handler3
_controlfp
_stricmp
kerne132.dll
kernel32.dll
.exe
C:*
C:\windows\system32\kerne132.dll
Kernel32.
Lab01-01.dll
C:\Windows\System32\Kernel32.dll
WARNING_THIS_WILL_DESTROY_YOUR_MACHINE
C:\Documents and Settings\Administrator\Desktop\Tools\Strings>
Start
Select Command Pro...
C:\Documents and Settin...
02:11
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

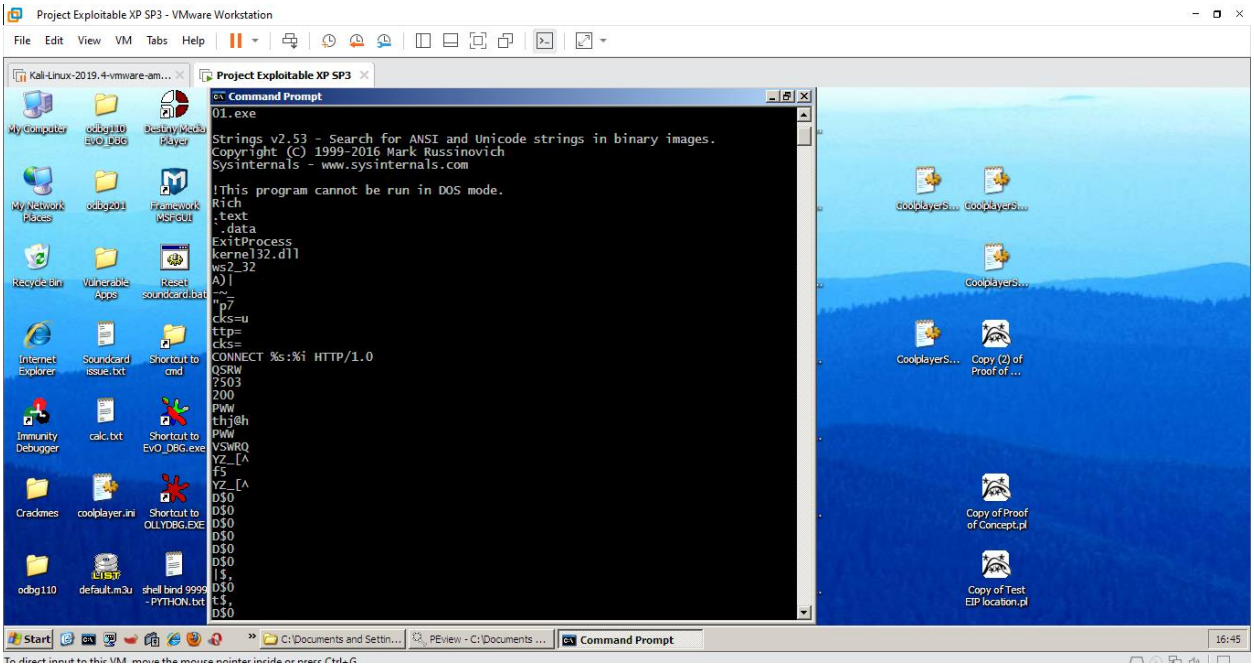
b. Lab01-01.dll

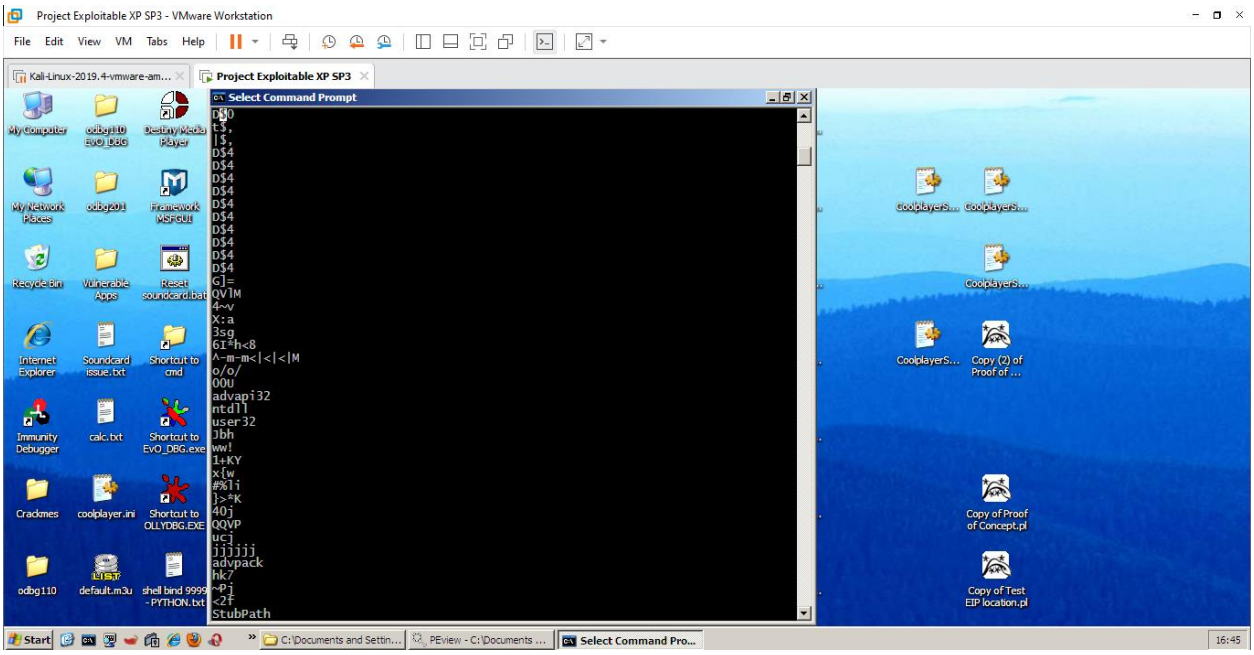


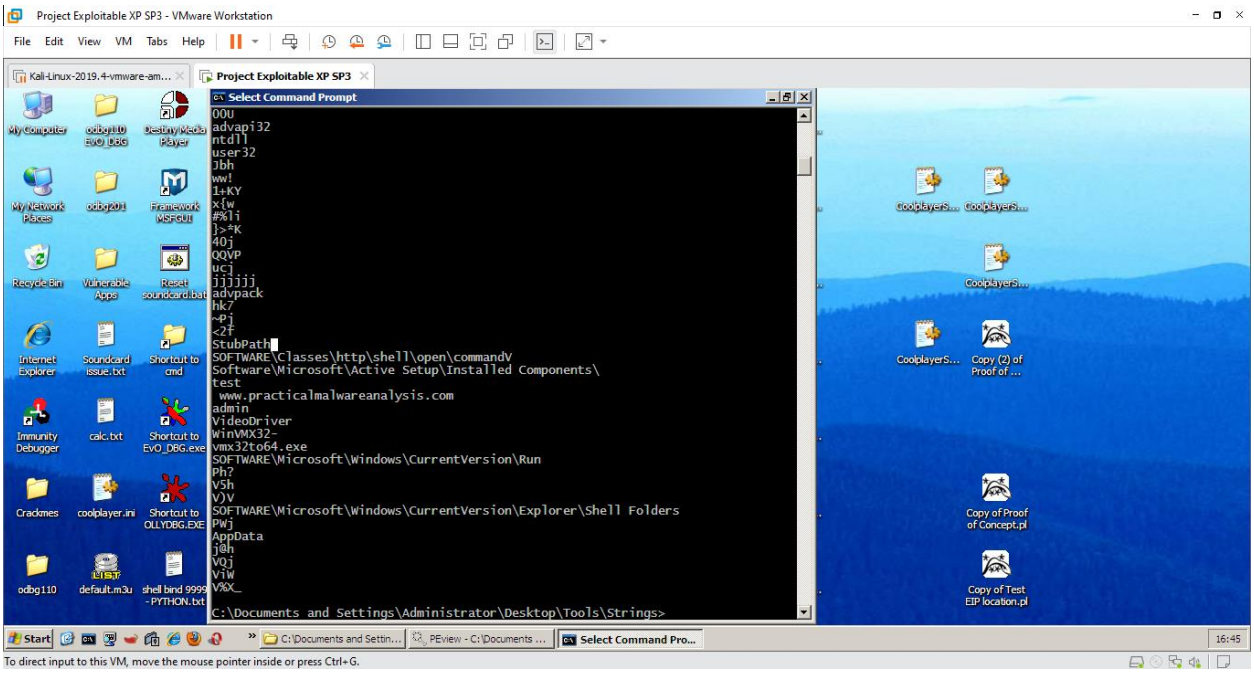


2) Dynamic analysis

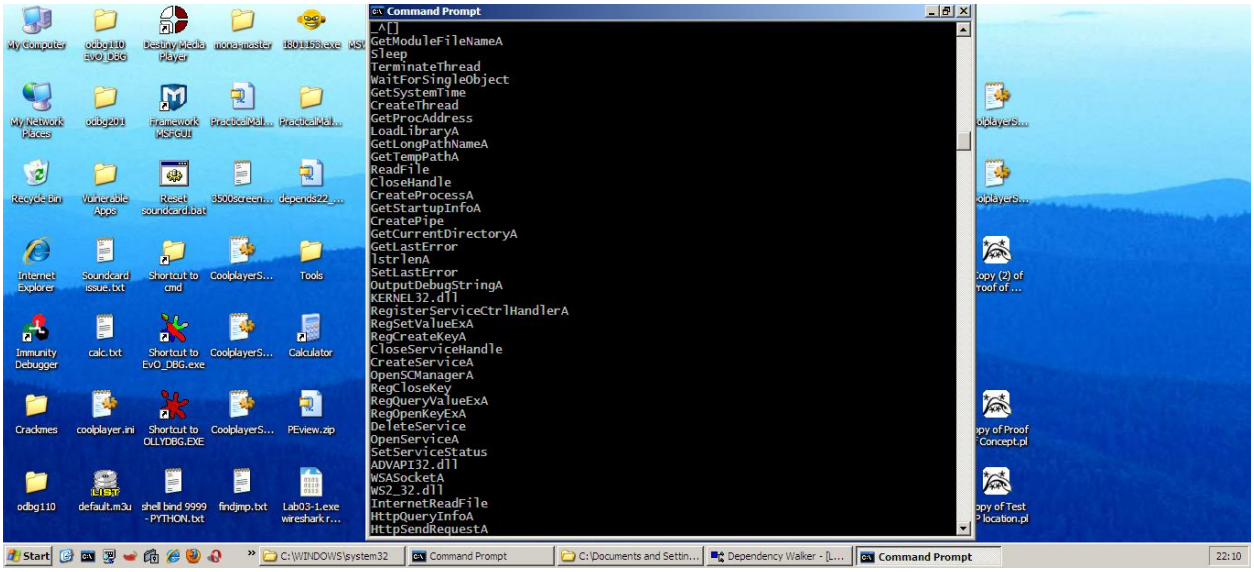
a. Lab03-01.exe

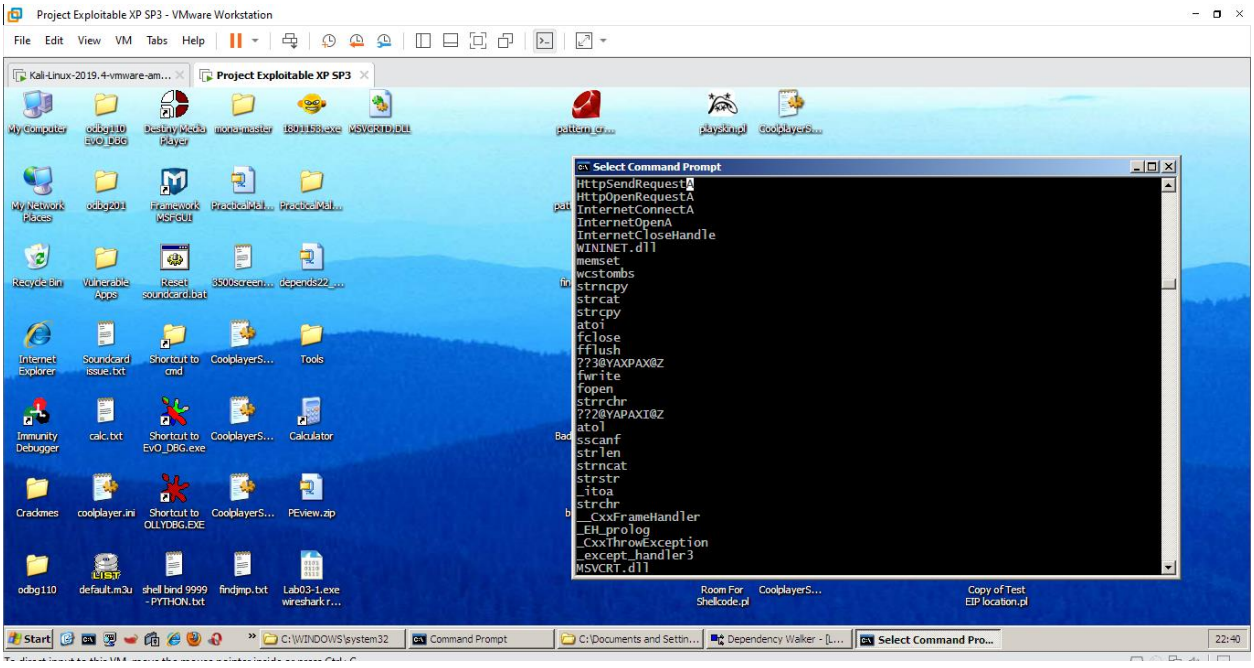


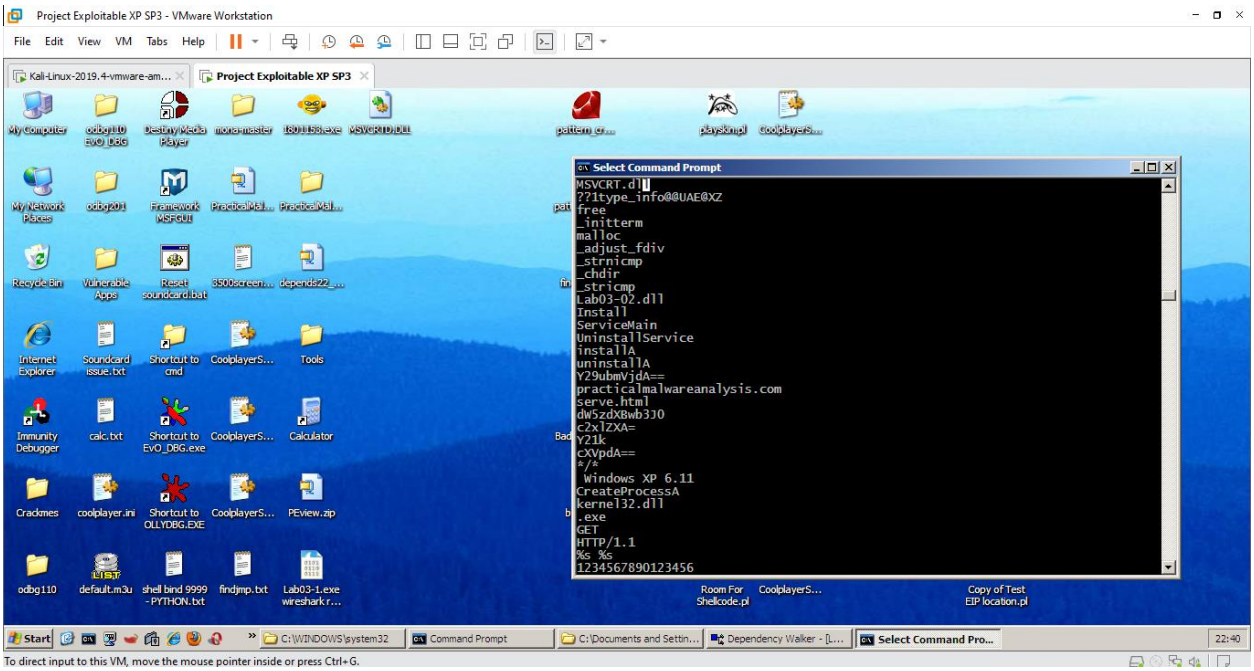


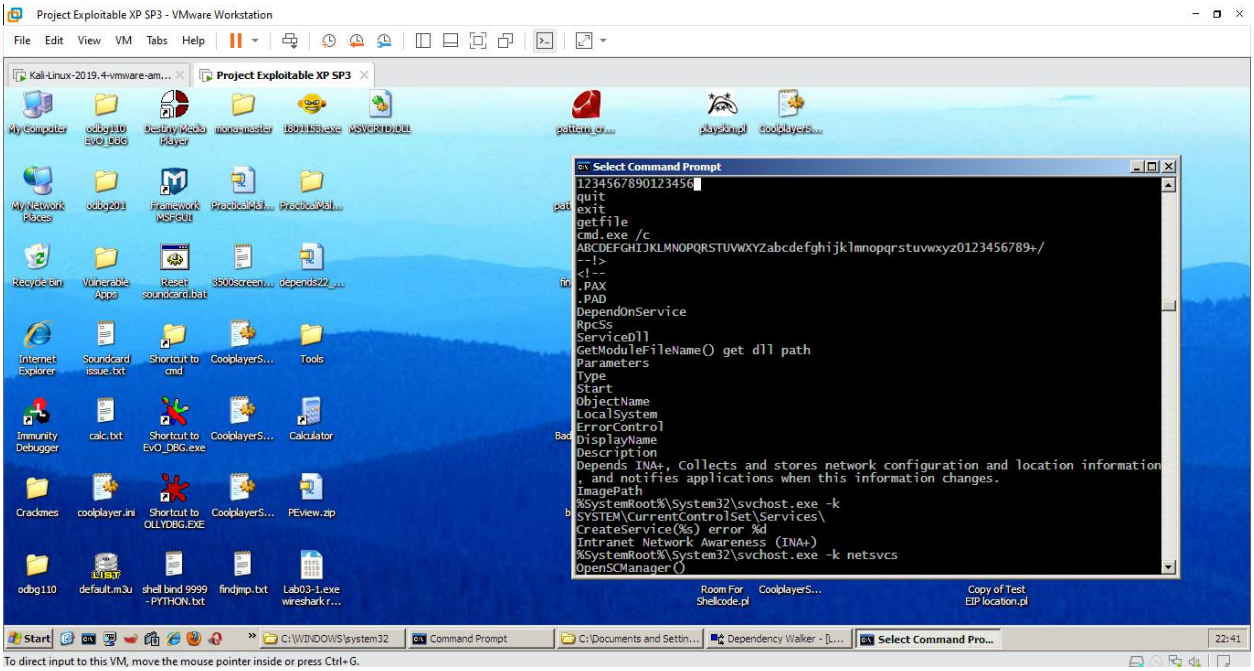

Project Exploitable XP SP3 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-2019.4-vmware-am...
Project Exploitable XP SP3
Select Command Prompt
00U
advapi32
ntdll
user32
Jbh
ww!
1+KY
xiw
#%li
]>*K
40j
QQVP
ucj
jjjjjj
advpack
hk7
~Pj
<2F
StubPath
SOFTWARE\Classes\http\shell\open\commandV
Software\Microsoft\Active Setup\Installed Components\
test
www.practicalmalwareanalysis.com
admin
VideoDriver
WinVMX32-
vmx32to64.exe
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Ph?
V5h
V)V
SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
PWj
AppData
j@h
VQj
ViW
V%X_
C:\Documents and Settings\Administrator\Desktop\Tools\Strings>
My Computer
odbg110 EvO_DBG
Destiny Media Player
My Network Places
odbg201
Framework MSFGUI
Recycle Bin
Vulnerable Apps
Reset soundcard.bat
Internet Explorer
Soundcard issue.txt
Shortcut to cmd
Immunity Debugger
calc.txt
Shortcut to EvO_DBG.exe
Crackmes
coolplayer.ini
Shortcut to OLLYDBG.EXE
odbg110
default.m3u
shell bind 9999 - PYTHON.txt
Coolplayers...
Coolplayers...
Coolplayers...
CoolplayerS...
Copy (2) of Proof of ...
Copy of Proof of Concept.pl
Copy of Test EIP location.pl
Start
C:\Documents and Settin...
PEview - C:\Documents ...
Select Command Pro...
16:45
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

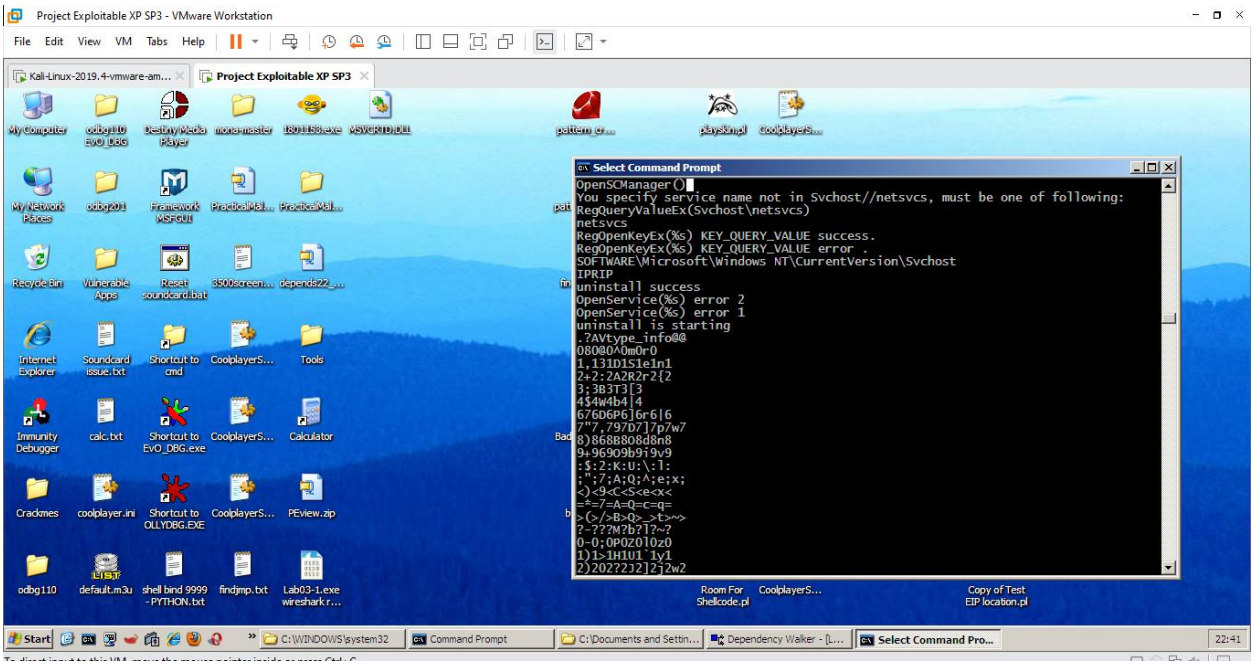
b. Lab03-02.dll



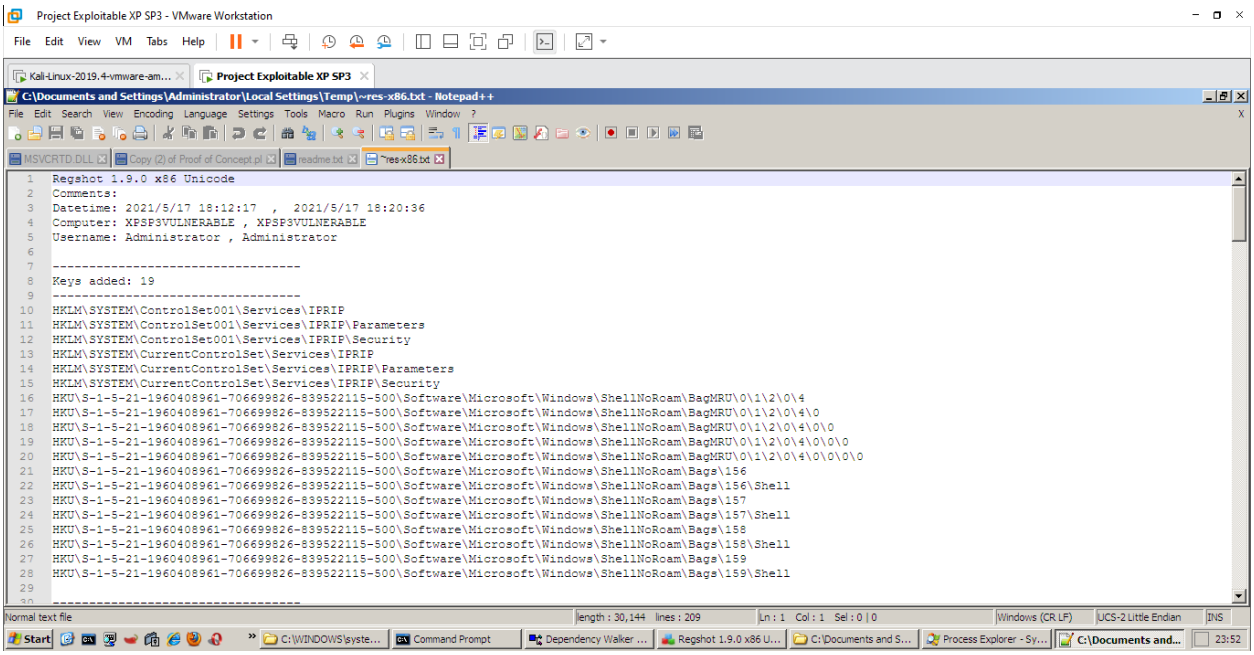


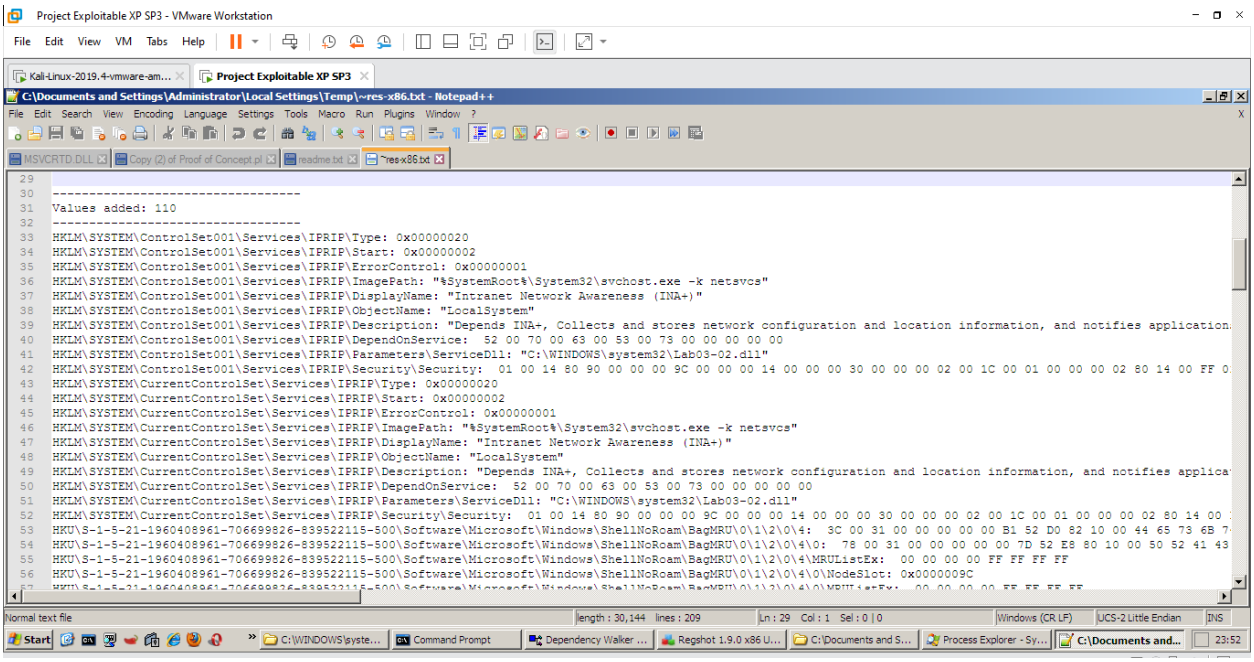

Project Exploitable XP SP3 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-2019.4-vmware-am...
Project Exploitable XP SP3
Select Command Prompt
MSVCRT.dll
??1type_info@@UAE@XZ
free
_initterm
malloc
_adjust_fdiv
_strnicmp
_chdir
_stricmp
Lab03-02.dll
Install
ServiceMain
UninstallService
installA
uninstallA
Y29ubmVjdA==
practicalmalwareanalysis.com
serve.html
dW5zdXBwb3J0
c2xlZXA=
Y21k
cXVpdA==
/
Windows XP 6.11
CreateProcessA
kernel32.dll
.exe
GET
HTTP/1.1
%s %s
1234567890123456
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

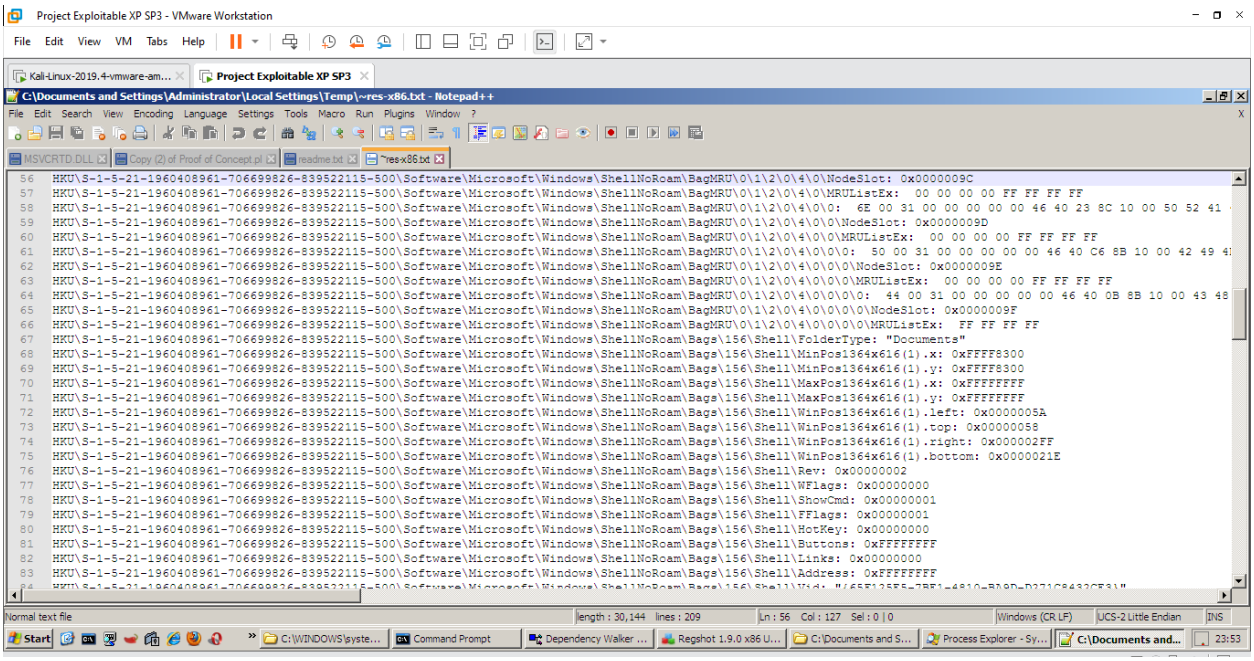

Project Exploitable XP SP3 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-2019.4-vmware-am...
Project Exploitable XP SP3
Select Command Prompt
1234567890123456
quit
exit
getfile
cmd.exe /c
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
--!>
<!--
.PAX
.PAD
DependOnService
RpcSs
ServiceDll
GetModuleFileName() get dll path
Parameters
Type
Start
ObjectName
LocalSystem
ErrorControl
DisplayName
Description
Depends INA+, Collects and stores network configuration and location information
, and notifies applications when this information changes.
ImagePath
%SystemRoot%\System32\svchost.exe -k
SYSTEM\CurrentControlSet\Services\
CreateService(%s) error %d
Intranet Network Awareness (INA+)
%SystemRoot%\System32\svchost.exe -k netsvcs
OpenSCManager()
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

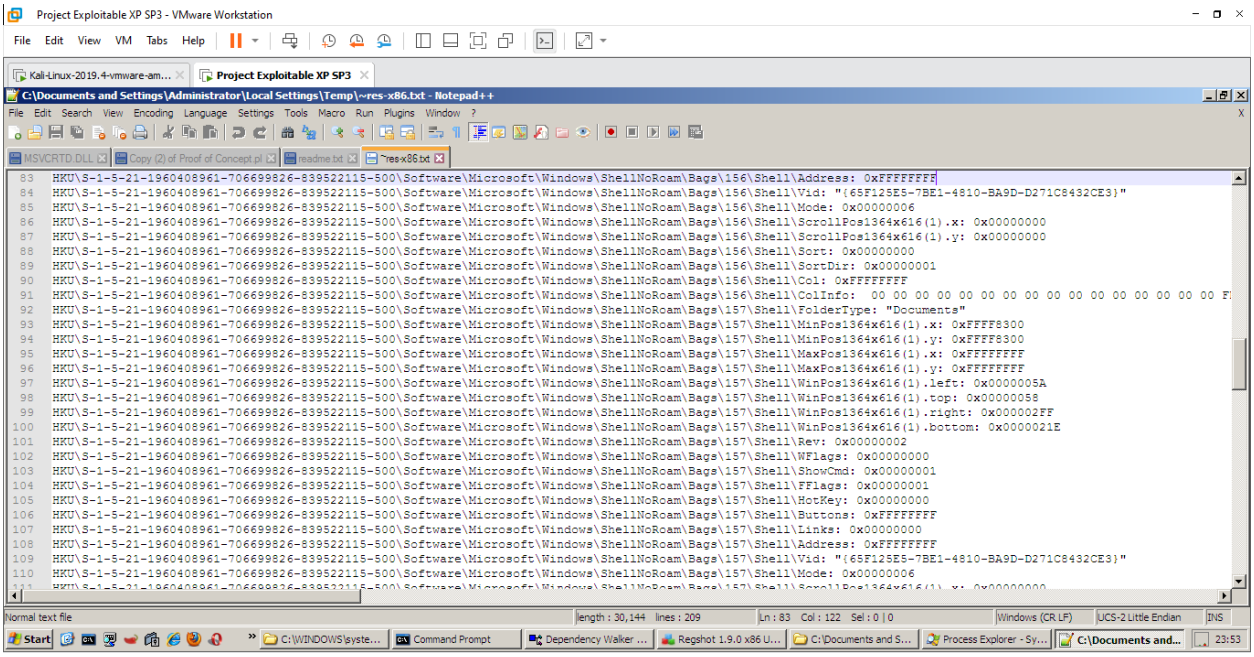


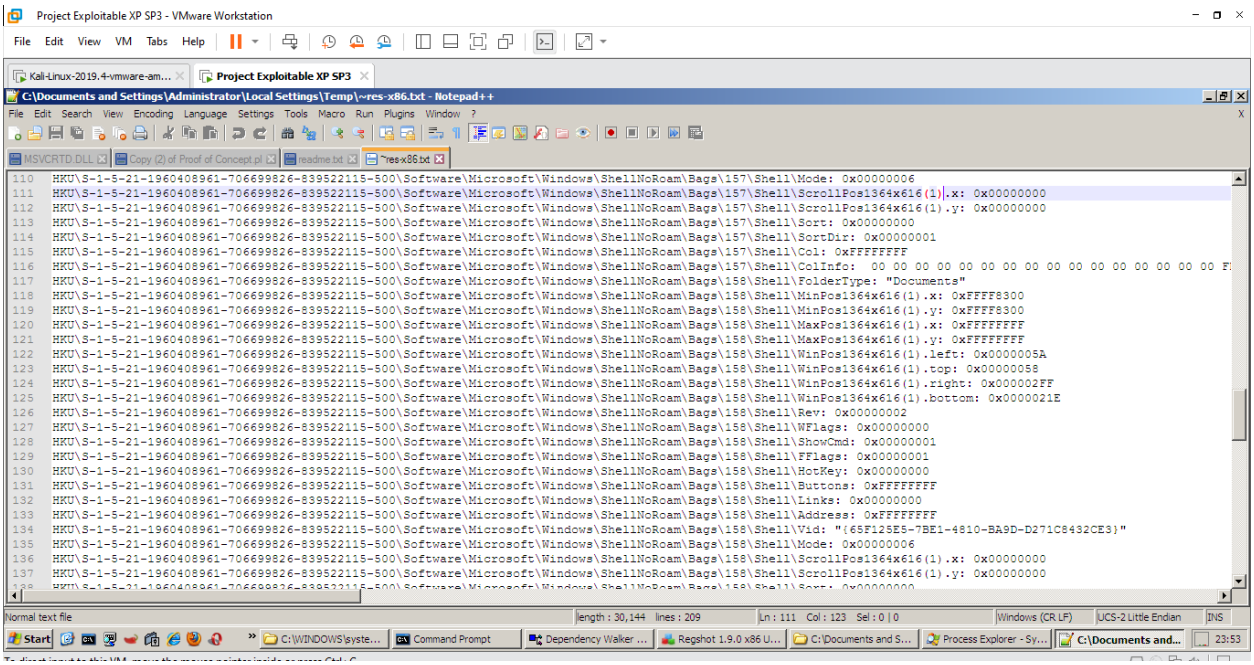
APPENDIX D – REGSHOT

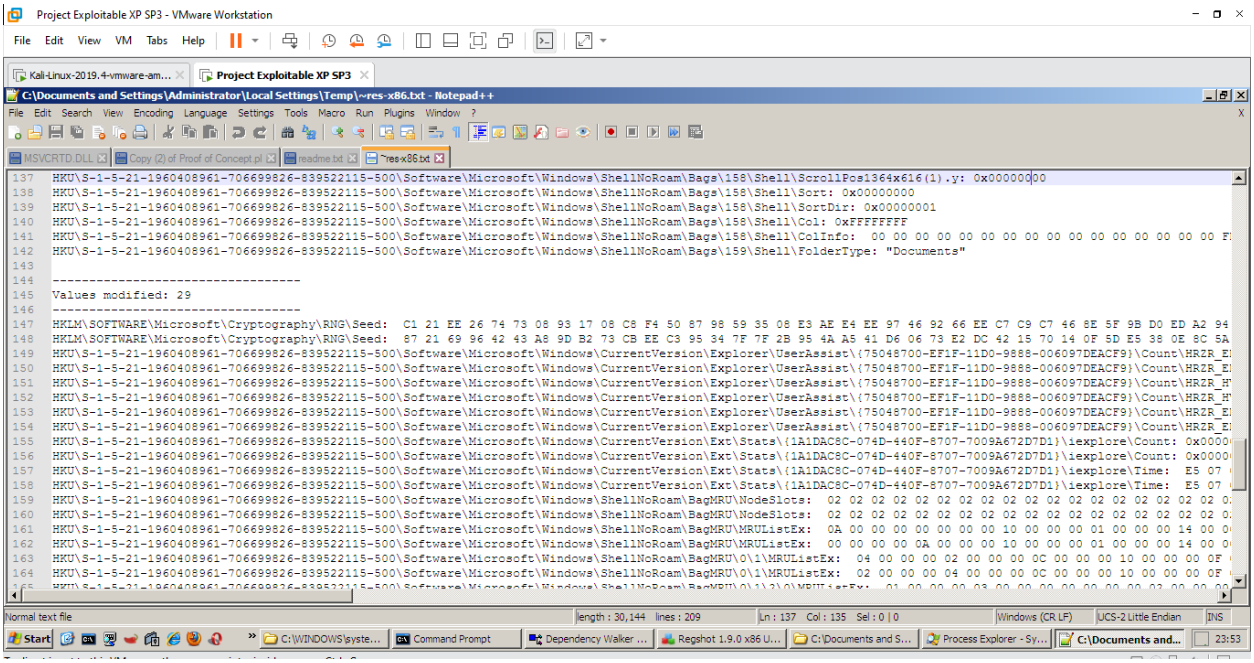

Project Exploitable XP SP3 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-2019.4-vmware-am...
Project Exploitable XP SP3
C:\Documents and Settings\Administrator\Local Settings\Temp\~res-x86.txt - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
MSVCRTD.DLL
Copy (2) of Proof of Concept.pl
readme.txt
~res-x86.txt
Regshot 1.9.0 x86 Unicode
Comments:
Datetime: 2021/5/17 18:12:17 , 2021/5/17 18:20:36
Computer: XPSP3VULNERABLE , XPSP3VULNERABLE
Username: Administrator , Administrator
Keys added: 19
HKLM\SYSTEM\ControlSet001\Services\IPRIP
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Parameters
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Security
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Parameters
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Security
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\1\2\0\4
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\1\2\0\4\0
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\1\2\0\4\0\0
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\1\2\0\4\0\0\0
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\1\2\0\4\0\0\0\0
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\159
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\159\Shell
Normal text file
length : 30,144 lines : 209
Ln : 1 Col : 1 Sel : 0 | 0
Windows (CR LF)
UCS-2 Little Endian
INS
Start
C:\WINDOWS\syste...
Command Prompt
Dependency Walker ...
Regshot 1.9.0 x86 U...
C:\Documents and S...
Process Explorer - Sy...
C:\Documents and...
23:52

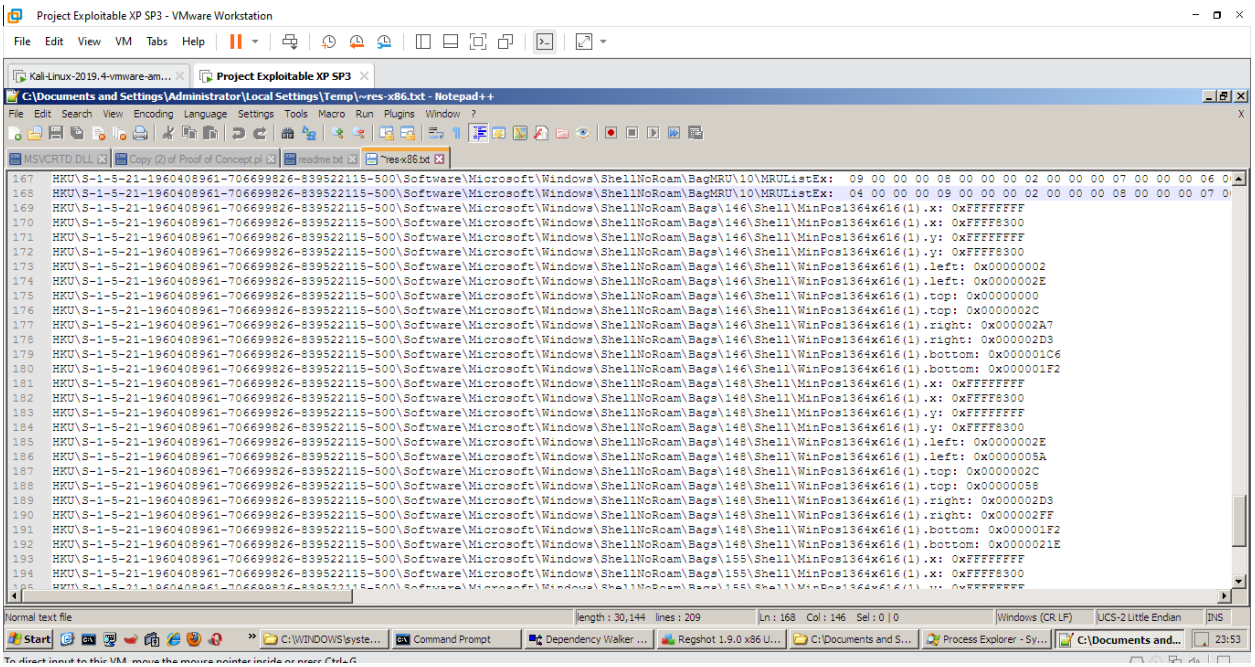

Project Exploitable XP SP3 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-2019.4-vmware-am...
Project Exploitable XP SP3
C:\Documents and Settings\Administrator\Local Settings\Temp\~res-x86.txt - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
MSVCRTD.DLL
Copy (2) of Proof of Concept.pl
readme.txt
~res-x86.txt
Values added: 110
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Type: 0x00000020
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Start: 0x00000002
HKLM\SYSTEM\ControlSet001\Services\IPRIP\ErrorControl: 0x00000001
HKLM\SYSTEM\ControlSet001\Services\IPRIP\ImagePath: "%SystemRoot%\System32\svchost.exe -k netsvcs"
HKLM\SYSTEM\ControlSet001\Services\IPRIP\DisplayName: "Intranet Network Awareness (INA+)"
HKLM\SYSTEM\ControlSet001\Services\IPRIP\ObjectName: "LocalSystem"
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Description: "Depends INA+, Collects and stores network configuration and location information, and notifies application
HKLM\SYSTEM\ControlSet001\Services\IPRIP\DependOnService: 52 00 70 00 63 00 53 00 73 00 00 00 00 00
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Parameters\ServiceDll: "C:\WINDOWS\system32\Lab03-02.dll"
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Security\Security: 01 00 14 80 90 00 00 00 9C 00 00 00 14 00 00 00 30 00 00 00 02 00 1C 00 01 00 00 00 02 80 14 00 FF 0
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Type: 0x00000020
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Start: 0x00000002
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\ErrorControl: 0x00000001
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\ImagePath: "%SystemRoot%\System32\svchost.exe -k netsvcs"
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\DisplayName: "Intranet Network Awareness (INA+)"
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\ObjectName: "LocalSystem"
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Description: "Depends INA+, Collects and stores network configuration and location information, and notifies applica
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\DependOnService: 52 00 70 00 63 00 53 00 73 00 00 00 00 00
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Parameters\ServiceDll: "C:\WINDOWS\system32\Lab03-02.dll"
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Security\Security: 01 00 14 80 90 00 00 00 9C 00 00 00 14 00 00 00 30 00 00 00 02 00 1C 00 01 00 00 00 02 80 14 00
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\1\2\0\4: 3C 00 31 00 00 00 00 00 B1 52 D0 82 10 00 44 65 73 6B 7
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\1\2\0\4\0: 78 00 31 00 00 00 00 00 7D 52 E8 80 10 00 50 52 41 43
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\1\2\0\4\MRUListEx: 00 00 00 00 FF FF FF FF
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\1\2\0\4\0\NodeSlot: 0x0000009C
Normal text file
length : 30,144 lines : 209
Ln : 29 Col : 1 Sel : 0 | 0
Windows (CR LF)
UCS-2 Little Endian
INS
Start
C:\WINDOWS\syste...
Command Prompt
Dependency Walker ...
Regshot 1.9.0 x86 U...
C:\Documents and S...
Process Explorer - Sy...
C:\Documents and...
23:52

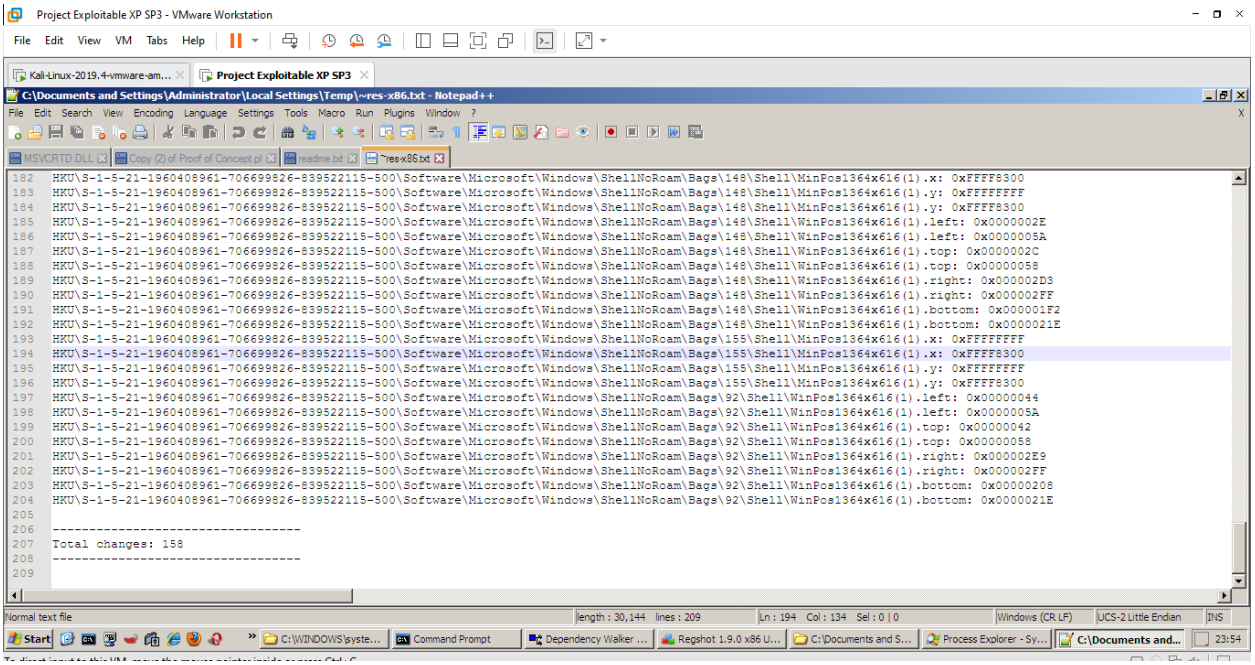

Project Exploitable XP SP3 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-2019.4-vmware-am...
Project Exploitable XP SP3
C:\Documents and Settings\Administrator\Local Settings\Temp\~res-x86.txt - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
MSVCRTD.DLL
Copy (2) of Proof of Concept.pl
readme.txt
~res-x86.txt
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\1\2\0\4\0\NodeSlot: 0x0000009C
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\1\2\0\4\0\MRUListEx: 00 00 00 00 FF FF FF FF
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\1\2\0\4\0\0: 6E 00 31 00 00 00 00 00 00 46 40 23 8C 10 00 50 52 41
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\1\2\0\4\0\0\NodeSlot: 0x0000009D
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\1\2\0\4\0\0\MRUListEx: 00 00 00 00 FF FF FF FF
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\1\2\0\4\0\0\0: 50 00 31 00 00 00 00 00 00 46 40 C6 8B 10 00 42 49
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\1\2\0\4\0\0\0\NodeSlot: 0x0000009E
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\1\2\0\4\0\0\0\MRUListEx: 00 00 00 00 FF FF FF FF
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\1\2\0\4\0\0\0\0: 44 00 31 00 00 00 00 00 00 46 40 0B 8B 10 00 43 48
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\1\2\0\4\0\0\0\0\NodeSlot: 0x0000009F
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\1\2\0\4\0\0\0\0\MRUListEx: FF FF FF FF
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\FolderType: "Documents"
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\MinPos1364x616(1).x: 0xFFFF8300
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\MinPos1364x616(1).y: 0xFFFF8300
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\MaxPos1364x616(1).x: 0xFFFFFFFF
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\MaxPos1364x616(1).y: 0xFFFFFFFF
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\WinPos1364x616(1).left: 0x0000005A
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\WinPos1364x616(1).top: 0x00000058
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\WinPos1364x616(1).right: 0x000002FF
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\WinPos1364x616(1).bottom: 0x0000021E
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\Rev: 0x00000002
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\WFlags: 0x00000000
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\ShowCmd: 0x00000001
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\FFlags: 0x00000001
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\HotKey: 0x00000000
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\Buttons: 0xFFFFFFFF
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\Links: 0x00000000
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\Address: 0xFFFFFFFF
Normal text file
length : 30,144 lines : 209
Ln : 56 Col : 127 Sel : 0 | 0
Windows (CR LF)
UCS-2 Little Endian
INS
Start
C:\WINDOWS\syste...
Command Prompt
Dependency Walker ...
Regshot 1.9.0 x86 U...
C:\Documents and S...
Process Explorer - Sy...
C:\Documents and...
23:53


Project Exploitable XP SP3 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-2019.4-vmware-am...
Project Exploitable XP SP3
C:\Documents and Settings\Administrator\Local Settings\Temp\~res-x86.txt - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
MSVCRTD.DLL
Copy (2) of Proof of Concept.pl
readme.txt
~res-x86.txt
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\Address: 0xFFFFFFFF
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\Vid: "{65F125E5-7BE1-4810-BA9D-D271C8432CE3}"
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\Mode: 0x00000006
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\ScrollPos1364x616(1).x: 0x00000000
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\ScrollPos1364x616(1).y: 0x00000000
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\Sort: 0x00000000
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\SortDir: 0x00000001
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\Col: 0xFFFFFFFF
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\ColInfo: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\FolderType: "Documents"
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\MinPos1364x616(1).x: 0xFFFF8300
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\MinPos1364x616(1).y: 0xFFFF8300
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\MaxPos1364x616(1).x: 0xFFFFFFFF
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\MaxPos1364x616(1).y: 0xFFFFFFFF
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\WinPos1364x616(1).left: 0x0000005A
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\WinPos1364x616(1).top: 0x00000058
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\WinPos1364x616(1).right: 0x000002FF
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\WinPos1364x616(1).bottom: 0x0000021E
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\Rev: 0x00000002
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\WFlags: 0x00000000
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\ShowCmd: 0x00000001
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\FFlags: 0x00000001
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\HotKey: 0x00000000
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\Buttons: 0xFFFFFFFF
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\Links: 0x00000000
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\Address: 0xFFFFFFFF
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\Vid: "{65F125E5-7BE1-4810-BA9D-D271C8432CE3}"
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\Mode: 0x00000006
Normal text file
length : 30,144 lines : 209
Ln : 83 Col : 122 Sel : 0 | 0
Windows (CR LF)
UCS-2 Little Endian
INS
Start
C:\WINDOWS\syste...
Command Prompt
Dependency Walker ...
Regshot 1.9.0 x86 U...
C:\Documents and S...
Process Explorer - Sy...
C:\Documents and...
23:53


Project Exploitable XP SP3 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-2019.4-vmware-am...
Project Exploitable XP SP3
C:\Documents and Settings\Administrator\Local Settings\Temp\~res-x86.txt - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
MSVCRTD.DLL
Copy (2) of Proof of Concept.pl
readme.txt
~res-x86.txt
110 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\Mode: 0x00000006
111 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\ScrollPos1364x616(1).x: 0x00000000
112 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\ScrollPos1364x616(1).y: 0x00000000
113 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\Sort: 0x00000000
114 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\SortDir: 0x00000001
115 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\Col: 0xFFFFFFFF
116 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\ColInfo: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F
117 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\FolderType: "Documents"
118 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\MinPos1364x616(1).x: 0xFFFF8300
119 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\MinPos1364x616(1).y: 0xFFFF8300
120 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\MaxPos1364x616(1).x: 0xFFFFFFFF
121 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\MaxPos1364x616(1).y: 0xFFFFFFFF
122 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\WinPos1364x616(1).left: 0x0000005A
123 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\WinPos1364x616(1).top: 0x00000058
124 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\WinPos1364x616(1).right: 0x000002FF
125 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\WinPos1364x616(1).bottom: 0x0000021E
126 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\Rev: 0x00000002
127 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\WFlags: 0x00000000
128 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\ShowCmd: 0x00000001
129 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\FFlags: 0x00000001
130 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\HotKey: 0x00000000
131 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\Buttons: 0xFFFFFFFF
132 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\Links: 0x00000000
133 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\Address: 0xFFFFFFFF
134 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\Vid: "{65F125E5-7BE1-4810-BA9D-D271C8432CE3}"
135 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\Mode: 0x00000006
136 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\ScrollPos1364x616(1).x: 0x00000000
137 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\ScrollPos1364x616(1).y: 0x00000000
Normal text file
length : 30,144 lines : 209
Ln : 111 Col : 123 Sel : 0 | 0
Windows (CR LF)
UCS-2 Little Endian
INS
Start
C:\WINDOWS\syste...
Command Prompt
Dependency Walker ...
Regshot 1.9.0 x86 U...
C:\Documents and S...
Process Explorer - Sy...
C:\Documents and...
23:53


Project Exploitable XP SP3 - VMware Workstation
File Edit View VM Tabs Help
Kali-Linux-2019.4-vmware-am...
Project Exploitable XP SP3
C:\Documents and Settings\Administrator\Local Settings\Temp\~res-x86.txt - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
MSVCRTD.DLL
Copy (2) of Proof of Concept.pl
readme.txt
~res-x86.txt
137 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\ScrollPos1364x616(1).y: 0x00000000
138 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\Sort: 0x00000000
139 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\SortDir: 0x00000001
140 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\Col: 0xFFFFFFFF
141 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\ColInfo: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F
142 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\159\Shell\FolderType: "Documents"
143
144 ----------
145 Values modified: 29
146 ----------
147 HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: C1 21 EE 26 74 73 08 93 17 08 C8 F4 50 87 98 59 35 08 E3 AE E4 EE 97 46 92 66 EE C7 C9 C7 46 8E 5F 9B D0 ED A2 94
148 HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: 87 21 69 96 42 43 A8 9D B2 73 CB EE C3 95 34 7F 7F 2B 95 4A A5 41 D6 06 73 E2 DC 42 15 70 14 0F 5D E5 38 0E 8C 5A
149 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_E
150 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_E
151 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_H
152 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_H
153 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_E
154 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_E
155 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{1A1DAC8C-074D-440F-8707-7009A672D7D1}\iexplore\Count: 0x0000
156 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{1A1DAC8C-074D-440F-8707-7009A672D7D1}\iexplore\Count: 0x0000
157 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{1A1DAC8C-074D-440F-8707-7009A672D7D1}\iexplore\Time: E5 07
158 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{1A1DAC8C-074D-440F-8707-7009A672D7D1}\iexplore\Time: E5 07
159 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\NodeSlots: 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 0
160 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\NodeSlots: 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 0
161 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\MRUListEx: 0A 00 00 00 00 00 00 00 10 00 00 00 01 00 00 00 14 00 0
162 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\MRUListEx: 00 00 00 00 0A 00 00 00 10 00 00 00 01 00 00 00 14 00 0
163 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\1\MRUListEx: 04 00 00 00 02 00 00 00 0C 00 00 00 10 00 00 00 0F
164 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\1\MRUListEx: 02 00 00 00 04 00 00 00 0C 00 00 00 10 00 00 00 0F
Normal text file
length : 30,144 lines : 209
Ln : 137 Col : 135 Sel : 0 | 0
Windows (CR LF)
UCS-2 Little Endian
INS
Start
C:\WINDOWS\syste...
Command Prompt
Dependency Walker ...
Regshot 1.9.0 x86 U...
C:\Documents and S...
Process Explorer - Sy...
C:\Documents and...
23:53


Project Exploitable XP SP3 - VMware Workstation
C:\Documents and Settings\Administrator\Local Settings\Temp\~res-x86.txt - Notepad++
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\10\MRUListEx: 09 00 00 00 08 00 00 00 02 00 00 00 07 00 00 00 06 0
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\10\MRUListEx: 04 00 00 00 09 00 00 00 02 00 00 00 08 00 00 00 07 0
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\146\Shell\MinPos1364x616(1).x: 0xFFFFFFFF
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\146\Shell\MinPos1364x616(1).x: 0xFFFF8300
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\146\Shell\MinPos1364x616(1).y: 0xFFFFFFFF
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\146\Shell\MinPos1364x616(1).y: 0xFFFF8300
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\146\Shell\MinPos1364x616(1).left: 0x00000002
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\146\Shell\MinPos1364x616(1).left: 0x0000002E
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\146\Shell\MinPos1364x616(1).top: 0x00000000
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\146\Shell\MinPos1364x616(1).top: 0x0000002C
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\146\Shell\MinPos1364x616(1).right: 0x000002A7
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\146\Shell\MinPos1364x616(1).right: 0x000002D3
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\146\Shell\MinPos1364x616(1).bottom: 0x000001C6
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\146\Shell\MinPos1364x616(1).bottom: 0x000001F2
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\MinPos1364x616(1).x: 0xFFFFFFFF
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\MinPos1364x616(1).x: 0xFFFF8300
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\MinPos1364x616(1).y: 0xFFFFFFFF
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\MinPos1364x616(1).y: 0xFFFF8300
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\MinPos1364x616(1).left: 0x0000002E
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\MinPos1364x616(1).left: 0x0000005A
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\MinPos1364x616(1).top: 0x0000002C
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\MinPos1364x616(1).top: 0x00000058
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\MinPos1364x616(1).right: 0x000002D3
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\MinPos1364x616(1).right: 0x000002FF
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\MinPos1364x616(1).bottom: 0x000001F2
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\MinPos1364x616(1).bottom: 0x0000021E
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\155\Shell\MinPos1364x616(1).x: 0xFFFFFFFF
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\155\Shell\MinPos1364x616(1).x: 0xFFFF8300


Project Exploitable XP SP3 - VMware Workstation
C:\Documents and Settings\Administrator\Local Settings\Temp\~res-x86.txt - Notepad++
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\MinPos1364x616(1).x: 0xFFFF8300
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\MinPos1364x616(1).y: 0xFFFFFFFF
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\MinPos1364x616(1).y: 0xFFFF8300
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\MinPos1364x616(1).left: 0x0000002E
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\MinPos1364x616(1).left: 0x0000005A
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\MinPos1364x616(1).top: 0x0000002C
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\MinPos1364x616(1).top: 0x00000058
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\MinPos1364x616(1).right: 0x000002D3
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\MinPos1364x616(1).right: 0x000002FF
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\MinPos1364x616(1).bottom: 0x000001F2
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\MinPos1364x616(1).bottom: 0x0000021E
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\155\Shell\MinPos1364x616(1).x: 0xFFFFFFFF
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\155\Shell\MinPos1364x616(1).x: 0xFFFF8300
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\155\Shell\MinPos1364x616(1).y: 0xFFFFFFFF
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\155\Shell\MinPos1364x616(1).y: 0xFFFF8300
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\92\Shell\WinPos1364x616(1).left: 0x00000044
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\92\Shell\WinPos1364x616(1).left: 0x0000005A
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\92\Shell\WinPos1364x616(1).top: 0x00000042
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\92\Shell\WinPos1364x616(1).top: 0x00000058
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\92\Shell\WinPos1364x616(1).right: 0x000002E9
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\92\Shell\WinPos1364x616(1).right: 0x000002FF
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\92\Shell\WinPos1364x616(1).bottom: 0x00000208
HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\92\Shell\WinPos1364x616(1).bottom: 0x0000021E
Total changes: 158