

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	Intro	oduction	1						
	1.1	Background	1						
	1.2	Aim	2						
	1.3	Methodology	2						
	1.4	Tools	3						
2	Proc	cedure	4						
	2.1	Overview of Procedure	4						
	2.2	Procedure	4						
	2.2.3	1 Static analysis	4						
	2.2.2	2 Dynamic analysis	12						
	2.2.3	3 Hybrid analysis	27						
3	Resu	ults	39						
	3.1	Results	39						
4	Disc	cussion	41						
	4.1	General Discussion	41						
	4.2	Conclusions	41						
	4.3	Future Work	41						
Re	eferenc	ces	42						
A	Appendices								
	Appen	ndix A – Virus Total	45						
	Appen	ndix B – Dependency Walker	52						
	Appen	ndix C - Strings	55						
	Appen	ndix D – Regshot	63						

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.

\leftrightarrow	C invirustot	al.com/gui/file/58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b3	27bd6fe47/detection									
Σ	58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47 Q 🛧 🎬 🖵											
	50	① 50 security vendors flagged this file as malicious										
	169 × Community √ Score √	58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47 Lab01-01.exe (armadilio) (peexe) (via-tor	16.00 KB Size	2021-05-18 23:09:45 UTC 11 hours ago								
	DETECTION	DETAILS RELATIONS BEHAVIOR COMMUNITY										
	AegisLab	Trojan.Win32.Ulise.4!c	AhnLab-V3	Trojan/Win32.Agent.C957604								
	Alibaba	() Trojan:Win32/Aenjaris.94b5660f	ALYac	() Trojan.Agent.16384SS								
	SecureAge APEX	() Malicious	Arcabit	() Trojan.Ulise.D1BC1E								
	Avast	() Win32:Malware-gen	AVG	() Win32:Malware-gen								
	Avira (no cloud)	() HEUR/AGEN.1120198	BitDefender	() Gen:Variant.Ulise.113694								
	CAT-QuickHeal	() Trojan.Aenjaris	ClamAV	() Win.Malware.Agent-6342616-0								
	Comodo	() Malware@#3eb40r99afetz	CrowdStrike Falcon	Win/malicious_confidence_100% (W)								

Figure 1 Virus Total – Lab01-01.exe

Σ	f50e42c8dfaab64	9bde0398867e930b86c2a599e8db83b8260393082268f2dba		Si					
	38	() 38 security vendors flagged this file as malicious							
8	166 × Community √ Score	f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba Lab01-01.dll armadilio pedit via-tor	160.00 KB Size	2021-05-19 09:42:03 UTC 1 hour ago	Oc DLL				
	DETECTION	DETAILS RELATIONS COMMUNITY							
	AegisLab	Trojan.Win32.Ulise.4!c	Alibaba	() Trojan:Win32/SuspectCl	RC.6956aaeb				
	SecureAge APEX	() Malicious	Avast	() Win32:Malware-gen					
	AVG	() Win32:Malware-gen	Avira (no cloud)	() TR/Dldr.Waski.163840.1					
	BitDefender	() Gen:Variant.Ulise.105796	BitDefenderTheta	() Gen:NN.ZedlaF.34690.k	:q4@aGkQVtp				
	CAT-QuickHeal	() Trojan.Skeeyah	ClamAV	() Win.Malware.Agent-636	() Win.Malware.Agent-6369668-0				
	Comodo	Malware@#2dsw4albnce61	CrowdStrike Falcon	() Win/malicious_confiden	() Win/malicious_confidence_100% (W)				
	Cylance	① Unsafe	Cynet	() Malicious (score: 100)	() Malicious (score: 100)				

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.

C De	pendency Walk	er - [Lab01-01.e	ke]										
📑 🖧 Fi	le Edit View C	Options Profile V	Vindow Help										
	🖬 🔎 🔛 (c:\ 📴 📮 🖆	' 🔜 🔍 🗉		۵.		?						
_	LAB01-01.EX	E		PI	Ordinal	^	Hint	Fund	tion			Entry Po	oint
1	E KERNE	L32.DLL		C	N/A		27 (0x001B)	Close	eHandle			Not Bou	nd
I .	🔟 N	VTDLL.DLL		C	N/A		40 (0x0028)	Copy	CopyFileA			Not Bou	nd
I .	🗄 🔤 MSVCR	T.DLL		C	N/A		52 (0x0034)	CreateFileA				Not Bou	nd
I .	Ė 🛐 K	KERNEL32.DLL		C	N/A		53 (0x0035)	Crea	iteFileMappingA			Not Bou	nd
I .		NTDLL.DLL		C	N/A		144 (0x0090)	Find	Close			Not Bou	nd
I .	🐻 N	NTDLL.DLL		C	N/A		148 (0x0094)	FindF	FirstFileA			Not Bou	nd
I .				C	N/A		157 (0x009D)	Find	VextFileA			Not Bou	nd
I .				C	N/A		437 (0x0 1B 5)	IsBa	dReadPtr			Not Bou	nd
I .				C	N/A		470 (0x0 1D6)	Map	ViewOfFile			Not Bou	nd
I .				C	N/A		688 (0x02B0)	Unm	apViewOfFile			Not Bou	nd
1				E	Ordinal	^	Hint	Fund	tion			Entry Po	pint
1				C	86 (0x	0056)	85 (0x0055)	Crea	teIoCompletionPort			0x0003	1375
1				С	87 (0x	0057)	86 (0x0056) CreateJobObjectA					0x0006C36C	
I .				88 (0x0058)			87 (0x0057)	Crea	teJobObjectW			0x0002CAFB	
I .				C	89 (0x	0059)	88 (0x0058)	CreateJobSet				0x0006C33E	
1				C	90 (0x	005A)	89 (0x0059)	CreateMailslotA				0x0002CC83	
1				C	91 (Ox	005B)	90 (0x005A)	CreateMailslotW				0x0002	CCD4
1				С	92 (0x	005C)	91 (0x005B)	Crea	teMemoryResourcel	Votificatio	n	0x0003	9672
1				C	93 (0x	005D)	92 (0x005C)	Crea	iteMutexA			0x0000	E9CF
1				<u>c</u>	94 (0x	005E)	93 (0x005D)	Crea	teMutexW			0x0000	E947
1				C	95 (0x	005F)	94 (0x005E)	Crea	teNamedPipeA			0x0006	0B7C
				C	96 (0x	0060)	95 (0x005F)	Crea	teNamedPipeW			0x0002	F0C5
~	Module F	File Time Stamp	Link Time Stamp	Fi	le Size	Attr.	Link Checksu	ım	Real Checksum	CPU	Subsy	/stem	Symbols
	KERNEL32.DLL 1	14/04/2008 05:41	14/04/2008 05:4	11	989,696	A	0x000F44A	2	0x000F44A2	x86	Conso	ole	CV
	LAB01-01.EXE 0	08/01/2012 02:19	19/12/2010 21:4	16	16,384	A	0x0000000	0	0x00007428	x86	Conso	ole	None
	MSVCRT.DLL 1	14/04/2008 05:42	14/04/2008 05:4	12	343,040	А	0x0005734	1	0x00057341	x86	GUI		CV
	NTDLL.DLL 1	14/04/2008 05:41	14/04/2008 05:4	11	706,048	A	0x000B62B	С	0x000B62BC	x86	Conso	ole	CV
				•		•	•			•			

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

C De	pendency Walk	er - [Lab01-01	.dll]							
📑 🖧 Fi	le Edit View C	Options Profile	Window	Help						
2	🖬 🔎 🖹 🖓	c:\ <u>c+</u> 💭	8 3	Q E.	1					
Ē	LAB01-01.DL	L								
	🗄 ···· 🔲 KERNE	L32.DLL								
	🚊 🔲 WS2_3	32.DLL								
DVAPI32.DLL										
	÷… 🛐 I	KERNEL32.DLL								
	🛐 1	MSVCRT.DLL								
	····· 🛐 I	NTDLL.DLL						_		
	I WS2HELP.DLL I USER32.DLL									
	HI MSVCR	RT.DLL						_		
	+···· 5	KERNEL32.DLL						_		
	····· 🖪 I	NTDLL.DLL						_		
	4	1								
^	Module	File Time Stamp	o Link	Time Stamp	File S	lize	Attr.	Link		
33	IESHIMS.DLL Error opening file. The system cannot find the file specified (2).									
WER.DLL Error opening file. The system cannot find the file specified (2							tified (2).			
3	MPR.DLL	14/04/2008 05	:41 14/0	4/2008 05:	40	59,904	A	0x0		
	ADVAPI32.DLL	14/04/2008 05	:41 14/0	4/2008 05:	39 6	17,472	A	0x0		
	KERNEL32.DLL	14/04/2008 05	:41 14/0	4/2008 05:	41 9	39,696	A	0x0		
	LLAB01-01 DU	19/12/2010 11	·16 19/1	2/2010-21+	46 I 1	53,840	Δ	1.0v0i		

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.

C PEview - C:\Documents and Settings\Administrator\I	Desktop\Pract	icalMalwareAnal	ysis-Labs-master\Practical I	1alware Analysis Labs\BinaryCollec
File View Go Help				
🔌 🔾 😋 😂 💌 💌 🛨 📖 🚥 🗕				
E Lab01-01.exe	pFile	Data	Description	Value
IMAGE_DOS_HEADER	000001E0	2E 74 65 78	Name	.text
MS-DOS Stub Program	000001E4	74 00 00 00		
HAGE_NT_HEADERS	000001E8	00000970	Virtual Size	
- Signature	000001EC	00001000	RVA	
IMAGE_FILE_HEADER	000001F0	00001000	Size of Raw Data	
MAGE_OPTIONAL_HEADER	000001F4	00001000	Pointer to Raw Data	
IMAGE_SECTION_HEADER .text	000001F8	00000000	Pointer to Relocations	
IMAGE_SECTION_HEADER .rdata	000001FC	00000000	Pointer to Line Numbers	
IMAGE_SECTION_HEADER .data	00000200	0000	Number of Relocations	
- SECTION .text	00000202	0000	Number of Line Numbers	
	00000204	60000020	Characteristics	
SECTION .data			0000020	IMAGE SCN CNT CODE
			2000000	IMAGE SCN MEM EXECUTE
			4000000	IMAGE_SCN_MEM_READ

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++.

<u> P</u> EiD v0.	95									
File: C:\D	ocuments and Settings\Administrat	tor\Desktop\PracticalMalwareA								
Entrypoint:	00001820	EP Section: .text >								
File Offset:	00001820	First Bytes: 55,8B,EC,6A >								
Linker Info:	6.0	Subsystem: Win32 console >								
Microsoft V	isual C++ 6.0									
Multi Scan Task Viewer Options About Exit										
🔽 Stay on	top	»» ->								

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 kernel23.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.

← →	C 🔒 virustota	al.com/gui/file/798	3a582939924	c70e3da2da80fd3	3352ebc90de7b8	3c4c427d484ff4f0	0f0aec/detection							☆
Σ	7983a582939924c70e3da2da80fd3352ebc90de7b8c4c427d484ff4f050f0aec											000	\square	Sign in
	51	() 51 security	vendors flagge	ed this file as malic	cious									C
8	Community	7983a582939924 Lab01-03.exe direct-cpu-clock-	4c70e3da2da8 -access (fsg)	f4f050f0aec via-tor		4.64 KB Size	2021-(14 day	05-04 17 rs ago	:48:29 UT	c		exe		
	DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 🚳					тү								
	AegisLab	()	Trojan.Multi.G	eneric.IVbD			AhnLab-V3			Trojan/Win32.Agent.C2894355				
	Alibaba	0	TrojanClicker:	Win32/Agentb.3bb	840a6		SecureAge APEX (() Malicious				
	Avast	0	Win32:Malwar	e-gen			AVG		() W	/in32:Mal	ware-ge	n		
	Baidu ① Win32.Trojan-Clicker.Agent.z CAT-QuickHeal ① Trojan.Agentb					BitDefenderTheta	() G	en:NN.Ze	exaF.346	38.ambda	aODfLcf			
						Comodo (Cylance (TrojWare.Win32.Trojan.Inor.B_10@1qra8i					
	CrowdStrike Falcon () Win/malicious_confidence_100% (W)				① Unsafe									
	Cynet ① Malicious (score: 100)					Cyren		() W	32/Suspl	Pack.DH.	gen!Eldo	rado		

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.

Cependency Walker - [Lab	1-03.exe]										
📲 File Edit View Options P	ofile Window Help										_ 8 ×
□····· 🔲 LAB01-03.EXE		PI	Ordinal		Hint	Funct	ion ^		Entry P	oint	
🖃 🔤 KERNEL32.DLL		C	N/A		0 (0x0000)	GetPro	ocAddress		Not Bou	ind	
NTDLL.DLL			N/A		0 (0x0000)	LoadLi	ibraryA		Not Bou	ind	
x									F		
		Е	E Ordinal Hint Function ^ E			Entry P	oint				
		C	C 1 (0x0001) 0 (0x0000) ActivateActCtx 0x			0x000	Dx0000A6D4				
		C	2 (0x	0002)	1 (0x0001)	AddAt	tomA		0x000	35505	
		C	3 (0x)	0003) I	2 (0x0002)	AddAt	tomW		0x000	326D9	
^ Module File Time S	amp Link Time Stam	p F	File Size	Attr.	Link Checksu	m	Real Checksum	CPU	Subsystem	Symbols	Preferre 🔺
KERNEL32.DLL 14/04/2004	05:41 14/04/2008 05	:41	989,696	Α	0x000F44A	2	0x000F44A2	x86	Console	CV	0x7C80
						۰ L	0-0000000000	202	Concelo	None	0-0040
LAB01-03.EXE 26/03/201	07:54 01/01/1970 05	:30	4,752	A	000000000	• I'	0X0000CLD2	X00	Console	None	0,0040

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.

🖂 Lab01-03.exe	pFile	Data	Description	Value
IMAGE_DOS_HEADER	00000158	00 00 00 00	Name	
MS-DOS Stub Program	0000015C	74 00 00 00	1	
IMAGE_NT_HEADERS	00000160	00003000	Virtual Size	
MAGE_SECTION_HEADER	00000164	00001000	RVA	
IMAGE_SECTION_HEADER	00000168	00000000	Size of Raw Data	
IMAGE_SECTION_HEADER	0000016C	00000000	Pointer to Raw Data	
SECTION	00000170	00000000	Pointer to Relocations	
SECTION	00000174	00000000	Pointer to Line Numbers	
	00000178	0000	Number of Relocations	
	0000017A	0000	Number of Line Numbers	
	0000017C	C00000E0	Characteristics	
			0000020	IMAGE_SCN_CNT_CODE
			00000040	IMAGE_SCN_CNT_INITIALIZED_DATA
			00000080	IMAGE_SCN_CNT_UNINITIALIZED_DATA
			4000000	IMAGE_SCN_MEM_READ
			8000000	IMAGE_SCN_MEM_WRITE

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

C, PEview - C:\Documents and Settings\Administrator\	Desktop\Pract	icalMalwareAna	lysis-Labs-master\Practical	Malware Analysis Labs\BinaryCollection\Chapte
File View Go Help				
😑 Lab01-03.exe	pFile	Data	Description	Value
IMAGE_DOS_HEADER	00000180	00 00 00 00	Name	
MS-DOS Stub Program	00000184	74 61 00 00		
	00000188	00001000	Virtual Size	
IMAGE_SECTION_HEADER	0000018C	00004000	RVA	
MAGE_SECTION_HEADER	00000190	0000028C	Size of Raw Data	
IMAGE_SECTION_HEADER	00000194	00001000	Pointer to Raw Data	
SECTION	00000198	00000000	Pointer to Relocations	
SECTION	0000019C	00000000	Pointer to Line Numbers	
	000001A0	0000	Number of Relocations	
	000001A2	0000	Number of Line Numbers	
	000001A4	C00000E0	Characteristics	
			00000020	IMAGE_SCN_CNT_CODE
			00000040	IMAGE_SCN_CNT_INITIALIZED_DATA
			00000080	IMAGE_SCN_CNT_UNINITIALIZED_DATA
			4000000	IMAGE_SCN_MEM_READ
			8000000	IMAGE_SCN_MEM_WRITE

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

ः, PEview - C:\Documents and Settings\Administrator\	Desktop\Pract	ticalMalwareAna	lysis-Labs-master\Practical I	Malware Analysis Labs\BinaryCollection\Chapte
File View Go Help				
🖃 Lab01-03.exe	pFile	Data	Description	Value
IMAGE_DOS_HEADER	000001A8	00 00 00 00	Name	
- MS-DOS Stub Program	000001AC	61 00 00 00		
	000001B0	00001000	Virtual Size	
IMAGE_SECTION_HEADER	000001B4	00005000	RVA	
IMAGE_SECTION_HEADER	000001B8	00000200	Size of Raw Data	
MAGE_SECTION_HEADER	000001BC	00000E00	Pointer to Raw Data	
SECTION	000001C0	00000000	Pointer to Relocations	
SECTION	000001C4	00000000	Pointer to Line Numbers	
	000001C8	0000	Number of Relocations	
	000001CA	0000	Number of Line Numbers	
	000001CC	C00000E0	Characteristics	
			0000020	IMAGE_SCN_CNT_CODE
			0000040	IMAGE_SCN_CNT_INITIALIZED_DATA
			0000080	IMAGE_SCN_CNT_UNINITIALIZED_DATA
			4000000	IMAGE_SCN_MEM_READ
			8000000	IMAGE_SCN_MEM_WRITE

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

艦 PEiD v0.	95								
File: C:\Documents and Settings\Administrator\Desktop\PracticalMalwareA									
Entrypoint:	00005000	EP Section:							
File Offset:	00000E00	First Bytes: BB,D0,01,40 >							
Linker Info:	0.0	Subsystem: Win32 console >							
FSG 1.0 -> Multi Scan	dulek/xt Task Viewer Option	15 About Exit							
Stay on	top	>> ->							

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
 - o stop
 - o Clear data
 - o Set filter
 - o 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.

Apa	teDNS			<u> </u>
Capture	Window DNS Hex View			
Time	Domain Requested		DNS Returned	
<u> </u>			1	
1				
DN	S Reply IP (Default: Current Gatway/DNS):	192.168.1.1	Start S	erver
# o	f NXDOMAIN's:	0		
Sel	ected Interface:	VMware Accelerated AMD PCNet Adapter - Packet Sc	Stop S	Server

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.

🔍 PEview - C:\Documents and Settings\Administrator\I	Desktop\Pract	icalMalwareAna	lysis-Labs-master\Practical	Malware Analysis Labs\BinaryCollection
File View Go Help				
Lab03-01.exe	pFile	Data	Description	Value
IMAGE_DOS_HEADER	000001A8	2E 74 65 78	Name	.text
MS-DOS Stub Program	000001AC	74 00 00 00		
	000001B0	00000068	Virtual Size	
MAGE_SECTION_HEADER .text	000001B4	00000200	RVA	
IMAGE_SECTION_HEADER .data	000001B8	00000200	Size of Raw Data	
	000001BC	00000200	Pointer to Raw Data	
SECTION .data	000001C0	00000000	Pointer to Relocations	
	000001C4	00000000	Pointer to Line Numbers	
	000001C8	0000	Number of Relocations	
	000001CA	0000	Number of Line Numbers	
	000001CC	60000020	Characteristics	
			00000020	IMAGE_SCN_CNT_CODE
			2000000	IMAGE_SCN_MEM_EXECUTE
			4000000	IMAGE_SCN_MEM_READ

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

C PEview - C:\Documents and Settings\Administrator\	Desktop\Pract	ticalMalwareAna	lysis-Labs-master\Practical M	alware Analysis Labs\BinaryCollection\Cha
File View Go Help				
😑 Lab03-01.exe	pFile	Data	Description	Value
IMAGE_DOS_HEADER	000001D0	2E 64 61 74	Name	.data
MS-DOS Stub Program	000001D4	61 00 00 00		
IMAGE_NT_HEADERS	000001D8	0000168F	Virtual Size	
IMAGE_SECTION_HEADER .text	000001DC	00000400	RVA	
MAGE_SECTION_HEADER .data	000001E0	00001800	Size of Raw Data	
. SECTION .text	000001E4	00000400	Pointer to Raw Data	
SECTION .data	000001E8	00000000	Pointer to Relocations	
	000001EC	00000000	Pointer to Line Numbers	
	000001F0	0000	Number of Relocations	
	000001F2	0000	Number of Line Numbers	
	000001F4	C0000040	Characteristics	
			0000040	IMAGE_SCN_CNT_INITIALIZED_DATA
			4000000	IMAGE_SCN_MEM_READ
			8000000	IMAGE_SCN_MEM_WRITE



艦 PEiD v0.	95			_	
File: C:\Do	ocuments and Setting	gs\Administrator\	Desktop\Pr	acticalMalwareA	
Entrypoint:	00000208	E	P Section:	,text	>
File Offset:	00000208	F	irst Bytes:	B8,00,04,40	>
Linker Info:	5.12	S	ubsystem:	Win32 GUI	>
		_			
PEncrypt 3.	1 Final -> junkcode				
Multi Scan	Task Viewer	Options	Abo	ut Exi	t
Stay on	top			***	->

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.

🔤 Sele	ct Comman	d Prompt					
!This	program	cannot	be	run	in	DOS	mode.
Rich							
.text							
.data	1						
ExitPr	ocess						
kerne	132.d11						
ws2_32	2						
A)							
-~							
"p7							
cks=u							
ttp=							
cks=			_				
CONNEC	T %s:%i	HTTP/1	.0				
QSRW							

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).

Enable Advanced Output		laners.				
		Process Monitor	Filter			×
Filter	Ctrl+L	Display entries match	ing these conditions			
Reset Filter	Ctrl+R	biopidy circles indeel				
Load Filter	•	Architecture	💌 is 💌	l <u>j </u>	Then Inclu	ide 🔳
Save Filter						
Organize Filters		Reset			Add Re	move
Drop Eiltered Events						
- Brop Hitered Events		Column	Relation	Value	Action	
Highlight	Ctrl+H	Process	is	Procmon.exe	Exclude	
		Process	is	Procexp.exe	Exclude	
		Process	is	Autoruns.exe	Exclude	
		Process	is	System	Exclude	
		🗹 🐼 Operation	begins with	IRP_MJ_	Exclude	
		🗹 😵 Operation	begins with	FASTIO_	Exclude	-
		1				
				OK	Cancel A(pply

Figure 24 Filtering pop up

Process Hollitor Filter Display entries matching these conditions: Process Name Is Isolary and the entries matching these conditions: Reset Add Reset Column Relation Value Add Reset Column Relation Value Add Remove Column Relation Value Action Process is Process is Process is System Exclude Process is OK Cancel Apply	Due and Mariha	Tik			
Display entries matching these conditions: Process Name Reset Column Relation Value Add Remove Column Relation Value Add Remove Column Relation Value Action Add Remove Column Relation Value Action Action Add Remove Column Relation Value Action Action Add Remove Add Remove Add Remo	Process Monitor	ritter			
Process Name Is Lab03-01.exe then Indude Reset Add Remove Column Relation Value Action Image: Second Seco	Display entries match	ning these conditions	:		
Reset Add Remove Column Relation Value Action Image: Column Relation Value Action Image: Column Process is Procent Action Image: Column Process is Procesp.exe Exclude Image: Column Remove Process is Procesp.exe Exclude Image: Column Remove Remove Exclude Image: Column Image: Column Image: Column Remove Remove Exclude Image: Column Image: Column Image: Column Remove Remove Remove Image: Column Image: Column Image: Column Remove Remove Remove Remove Image: Column Image: Column Remove Remove Remove Remove Image: Column Remo	Process Name	🔹 jis 💌	Lab03-01.exe	▼ ther	Indude 💌
Column Relation Value Action Image: Column Stress Process is Procexp exe Exclude Image: Column Stress Process is Procexp exe Exclude Image: Column Stress Process is Autoruns.exe Exclude Image: Column Stress Process is System Exclude Image: Column Stress Process is Column Stress Process is System Image: Column Stress Process is System Process is Exclude Image: Column Stress Process is Column Stress Process is Exclude Image: Column Stress Process is Column Stress is Exclude <th>Reset</th> <th></th> <th></th> <th>Add</th> <th>Remove</th>	Reset			Add	Remove
Column Relation Value Action ☑ ※ Process is Procexp exe Exclude ☑ ※ Process is Procexp exe Exclude ☑ ※ Process is Autoruns.exe Exclude ☑ ※ Process is System Exclude ☑ ※ Process is System Exclude ☑ ※ Process is System Exclude ☑ ※ Operation begins with IRP_MJ_ Exclude ☑ ※ Operation begins with FASTIO_ Exclude					
Image: Second system Second system Exclude Image: Second system Second system Exclude Image: Second system System Exclude Image: Second system Second system Second system Image: Second system Second syste	Column	Relation	Value	Action	
Image: Second system is Procexp.exe Exclude Image: Second system Second system Exclude Image: Second system FASTIO_ Exclude Image: Second system FASTIO_ Exclude Image: Second system Image: Second system Mage: Second system Image: Second system Second system Image: Second system Image: Second system Second system Second system Image: Second system Image: Second system Second system Second system Image: Second system Image: Second system Second system Second system Second system Image: Second system Second system Second system Se	🗹 🔇 Process	is	Procmon.exe	Exclude	
Image: Constraint of the second se	Process	is	Procexp.exe	Exclude	
Image: System Exclude	Process	is	Autoruns.exe	Exclude	
Image: Constraint of the second se	Process	is	System	Exclude	
Operation begins with FASTIO_ Exclude OK Cancel Apply	🗹 🔕 Operation	begins with	IRP_MJ_	Exclude	
OK Cancel Apply	🗹 🔕 Operation	begins with	FASTIO_	Exclude	-
OK Cancel Apply	-				
			OK	Cancel	Apply

Figure 25 Entering the Process name to be filtered and shown

Process Monitor	Filter	ions		2
Process Name	▼ is	Lab03-01.exe	•	then Include 💌
Reset			Add	Remove
Column	Relation	Value	Action	
Process	is	Lab03-01.exe	Include	
Process	is	Procmon.exe	Exclude	
🗹 🔇 Process	is	Procexp.exe	Exclude	
🗹 🔇 Process	is	Autoruns.exe	Exclude	
🗹 🔇 Process	is	System	Exclude	
🗹 🔇 Operation	begins with	IRP_MJ_	Exclude	-
_		ОК	Cancel	Apply

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

nals: ww	w.sys	intern	als.c	om		
Options	Help					
ኞ 🔺	@	(E)		М	5	🌋 🔒 🔔 🌌 🙇

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.

Process Monitor	Filter			X
Filters were in effect	the last time you exi	ted Process Monitor:		
Display entries match	ing these conditions:			
Operation	💌 is 💌	RegSetValue	💌 t	hen Include 💌
Reset			Add	Remove
Column	Relation	Value	Action	
Process	is	Lab03-01.exe	Include	
🛛 🕑 Operation	is	WriteFile	Include	
🛛 🖸 😳 Operation	is	RegSetValue	Include	
Process	is	Procmon.exe	Exclude	
Process	is	Procexp.exe	Exclude	
Process	is	Autoruns.exe	Exclude	•
		ОК	Cancel	Apply

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

🂐 Process Explo	rer - Sysint	ternals	www.s	ysinter	nals.com [XPSP3VU	ILNERABLE\Admin	istrator] 💶 🗖	×
File Options Vie	w Process	Find	Handle	Users	Help			
Process			PID	CTU	Private Bytes	Working Set	Description	
vm	vmtoolsd.exe	е	516		11,416 K	14,980 K	VMware Tools Core	5
	alg.exe		1824		1,096 K	3,484 K	Application Layer G	1
	inetinfo.exe		2268		1,776 K	5,160 K	Internet Information	
- Isa	ss.exe		696		3,784 K	5,956 K	LSA Shell (Export V	1
🖃 😡 explorer.exe			1440		20,240 K	2,828 K	Windows Explorer	
jusched.e	xe		1516		1,244 K	4,764 K	Java(TM) Platform	5
vm vmtoolsd.	exe		1532		16,016 K	19,944 K	VMware Tools Core	
📝 ctfmon.ex	e		1540		900 K	3,500 K	CTF Loader	
📩 Procmon.	exe		740		7,664 K	992 K	Process Monitor	
👿 apateDN	S.exe		3212		23,820 K	24,916 K	Mandiant	
Lab03-01	.exe		1404		688 K	2,084 K		-
💓 procexp.e	xe		•			1	•	
-	[11							—
lype ≜	Name	TELLO		0.41.0				_
Key	HKLM\SYS	TEM\Co	ontrolSet(J01\Sen	vices \WinSock2\Parai	meters \Protocol_Cat	alog9	
Key	HKLM\SYS	TEMAC	ontrol Set(001\Sen	vices \WinSock2\Parai	meters \NameSpace_	Catalogo	
Key	HKLM\STS	TEMICO	ontrol Set(JUT\Sen	vices \Tcpip \Linkage	-		
Key		TEMICO	ritrol Set(101\Sen	vices (Topip (Farameter	s m\leterfaces		
Key		TEM\C	introl Set(101\Sen	vices (Net DT \ Paramete	as vintenaces		
KevedEvent	\KemelOhie	ote\Crit 9	SecOutO	Memory	Event	75		
Mutant	\RaseName	dObject	s\WinVN	IX32	Event			
Semaphore	\BaseName	dObject	s\shell {/	48F1A3	32-A340-11D1-BC6B-00	DA0C90312E1}		
Thread	Lab03-01.ex	(e(1404)	: 3952					
Thread	Lab03-01.ex	(1404)	: 3952					
WindowStation	\Windows\\	Window	Stations\	WinSta()			
WindowStation	\Windows\\	Window	Stations\	WinSta()			•
CPU Usage: 0.99%	Commit (Charge:	67.56%					1.

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.

/var/log/inetsim/report/report.1943.txt [Read Only] - Mousepad
File Edit Search View Document Help
Warning, you are using the root account, you may harm your system.
⊨ Report for session '1943' ≕
Real start date : 2021-05-17 12:14:58
Simulated start date : 2021-05-17 12:14:58
Time difference on startup : none
2021-05-17 12:15:38 First simulated date in log file
2021-05-17 12:15:38 DNS connection, type: A, class: IN, requested name: google.com
2021-05-17 12:15:38 HTTP connection, method: GET, URL: http://google.com/, file name: /var/lib/inetsim/http/fakefiles/sample.html
2021-05-17 12:15:38 HTTP connection, method: GET, URL: http://google.com/favicon.ico, file name: /var/lib/inetsim/http/fakefiles/favicon.ico
2021-05-17 12:16:09 DNS connection, type: A, class: IN, requested name: www.wireshark.org
2021-05-17 12:16:59 DNS connection, type: A, class: IN, requested name: www.practicalmalwareanalysis.com
2021-05-17 12-17-42 DNS connection, type: A, class: IN, requested name: time.windows.com
2021-05-17 12:17:42 NTP connection, time received: 1621268263, time sent: 1621268267, difference: 4
2021-05-17 12:17:42 Last simulated date in log file

Figure 31 INetSim report

No.		Time	Source	Destination	Protocol Len	Linfo
	1	0.000000	0 192.168.1.200	192.168.1.1	DNS	92 Standard query Oxdb99 A www.practicalmalwareanalysis.com
	2	0.0207190	0192.168.1.1	192.168.1.200	DNS	108 Standard query response Oxdb99 A 192.108.1.1
	3	0.0210500	0 192.168.1.200	192.168.1.1	TCP	62 dab-sti-c > https [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1
	4	0.0262180	0192.168.1.1	192.168.1.200	TCP	62 https > dab-sti-c [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 MSS=1460 SACK_PERM=1
	5	0.0262350	0 192.168.1.200	192.168.1.1	TCP	54 dab-sti-c > https [ACK] Seq=1 Ack=1 Win=64240 Len=0
	6	0.0263100	0 192.168.1.200	192.168.1.1	SSL	310 Continuation Data
	7	0.0269290	0192.168.1.1	192.168.1.200	TCP	60 https > dab-sti-c [ACK] Seq=1 Ack=257 Win=63984 Len=0
	8	0.0392360	0192.168.1.1	192.168.1.200	тср	60 https > dab-sti-c [RST, ACK] Seq=1 Ack=257 Win=63984 Len=0
	9	5.0704370	0 Vmware_74:d1:a3	Vmware_82:97:8d	ARP	60 who has 192.168.1.200? Tell 192.168.1.1
	10	5.0704510	0 Vmware_82:97:8d	Vmware_74:d1:a3	ARP	42 192.168.1.200 is at 00:0c:29:82:97:8d
	11	15.569674	0 fe80::20c:29ff:fe7	4ff02::2	ICMPv6	70 Router Solicitation from 00:0c:29:74:d1:a3
	12	30.042052	0 192.168.1.200	192.168.1.1	TCP	62 imgames > https [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
	13	30.047866	0192.168.1.1	192.168.1.200	TCP	62 https > imgames [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1
	14	30.047889	0 192.168.1.200	192.168.1.1	TCP	54 imgames > https [ACK] Seq=1 Ack=1 Win=64240 Len=0
	15	30.047952	0 192.168.1.200	192.168.1.1	SSL	310 Continuation Data
	16	30.048102	0192.168.1.1	192.168.1.200	TCP	60 https > imgames [ACK] Seq=1 Ack=257 Win=63984 Len=0
	17	30.060438	0192.168.1.1	192.168.1.200	тср	60 https > imgames [RST, ACK] Seq=1 Ack=257 Win=63984 Len=0
	18	42.680548	0 192.168.1.200	192.168.1.1	DNS	76 Standard query 0x64f7 A time.windows.com
	19	42.696029	0192.168.1.1	192.168.1.200	DNS	92 Standard query response 0x64f7 A 192.168.1.1
	20	10 202800	0 102 168 1 200	107 169 1 1	NTD	OO NITE Vorcion 2 symmetric active
÷F	rame	2 1: 92 by	tes on wire (736 bi	ts), 92 bytes captur	ed (736 bi	its) on interface 0
÷.	ther	net II, S	rc: Vmware_82:97:8d	(00:0c:29:82:97:8d)	, Dst: Vmw	vare_74:d1:a3 (00:0c:29:74:d1:a3)
E I	Inter	net Proto	col Version 4, Src:	192.168.1.200 (192.	168.1.200)	, Dst: 192.168.1.1 (192.168.1.1)
000	0 0	0 Oc 29 74	4 d1 a3 00 0c 29 83	2 97 8d 08 00 45 00)t)E.
001	0 0	0 4e a8 8	d 00 00 80 11 0d f	8 c0 a8 01 c8 c0 a8	. N	······
1002	0 0	1 01 04 1	f 00 35 00 3a 34 07	7 db 99 01 00 00 01		4
1001		0 00 00 00	c 6d 61 6c 77 61 73	7 18 70 72 61 63 74 2 65 61 6e 61 6c 79	icalmalw	/ ww.pract
1004	ň 7	2 60 72 0	2 62 6F 64 00 00 0	00 01	cie_com	a cana iy

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).

C Dependent	cy Wa	lker - [La	1 b03-0	2.dll]
📲 🛱 File Edit	View	Options	Profile	Wi
) 🚅 🖬 🔎	h.	c:/ <u>c</u> +	<u> -</u> 🛃	P
E···· 🔲 LAB	03-02.	DLL		
÷ 🔲	KERI	NEL32.DLL		
÷ 🔟	ADV	API32.DLL		
÷ 🖾	WS2	_32.DLL		
÷ 🔟	WIN	INET.DLL		
<u> </u>	MSV	CRT.DLL		

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

腸 PEiD v0.	95	_	
File: C:\Do	ocuments and Settings\Administra	tor\Desktop\PracticalMalwareA	
Entrypoint:	00004E4D	EP Section: ,text	>
File Offset:	0000424D	First Bytes: 55,8B,EC,53	>
Linker Info:	6.0	Subsystem: Win32 GUI	>
Microsoft Vi	sual C++ 6.0 DLL [Overlay]		
Multi Scan	Task Viewer Options	About Exit	
Stay on	top	**	->

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).

Select Command Prompt
HttpSendRequestA
HttpOpenRequestA
InternetConnectA
InternetOpenA
InternetCloseHandle
WININET.dll
memset
wcstombs
strncpy
strcat
strcpy
atoi
fclose
fflush
??3@YAXPAX@Z
furito

Figure 36 Strings search - HTTP Request

Select Command Prompt
MSVCRT.dl
??1type_info@@UAE@XZ
tree
malloc adjust fdiv
_aujust_ruiv
chdir
stricmp
Lab03-02.dll
Install
ServiceMain
UninstallService
InstallA
practicalmalwareanalysis com
convo html
dW5zdXBwb3J0
c2x1ZXA=
Y21k
cXVpdA==
/
Windows XP 6.11
Createprocessa konnol22 dll
GFT
HTTP/1.1
%s %s
1234567890123456

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.

🔓 Regshot 1.9.0 x86 Unicode	
Compare logs save as:	1st shot
Plain TXT O HTML document	2nd shot
Scan dir 1[;dir 2;dir 3;;dir nn]:	Compare
C:\WINDOWS	Clear
Output path:	Quit
C:\DOCUME~1\ADMINI~1'	About
Add comment into the log:	
	English 💌
Keys:96365 Values:177941	Time:2s694ms

Figure 39 Regshot

C:\WINDOWS\system32>rundll32.exe I	Lab03-02.dll, installA								
Figure 40 Running the malicious Lab03-02.dll									
Regshot 1.9.0 x86 Unicode									
Compare logs save as: Plain TXT O HTML document	1st shot								
Scan dir 1[;dir2;dir3;;dir nn]: C:\WINDOWS	Clear E								
Output path:	Quit								
C:\DOCUME~1\ADMINI~1'	About								
Add comment into the log:	English V								
Keys:96384 Values:178051	Time:3s244ms								

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.



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.

🂐 Process Explorer - Sysinternals	www.sysinter	nals.com [XPSP3VUL	NERABLE\Admin	istrator] (Ad	dministrator)	
File Options View Process Find	DLL Users Hel	p				
Process	PID CPU	Private Bytes	Working Set	Description		Company Name
services.exe	684	3,532 K	5,620 K	Services and	Controller app	Microsoft Corporation
vmacthlp.exe	856	588 K	2,544 K	VMware Activ	ration Helper	VMware, Inc.
= svchost.exe	868	2,676 K	5,104 K	Generic Host	Process for Wi	Microsoft Corporation
wmiprvse.exe	1316	3,692 K	8,528 K	WMI		Microsoft Corporation
- evehest.exe	932	1,760 K	4,188 K	Generic Host	Process for Wi	Microsoft Corporation
svchost.exe	1064 0.98	13,844 K	23,772 K	Generic Host	Process for Wi	Microsoft Corporation
sychosticke	1112	1,248 K	3,464 K	Generic Host	Process for Wi	Microsoft Corporation
svchost.exe	Command Line				Process for Wi	Microsoft Corporation
spoolsv.exe	C:\WINDOV	VS\system32\svchost.e	exe -k netsvcs		ystem App	Microsoft Corporation
iqs.exe	Path:				ck Starter Servi	Sun Microsystems, Inc.
MDM.EXE	C:\WINDOV	VS\system32\svchost.e	exe (netsvcs)		ug Manager	Microsoft Corporation
pg_ctl.exe	Computer Br	owser [Browser]			stops/restarts	PostgreSQL Global Develo
postgres.exe	Cryptographi	c Services [CryptSvc]			erver	PostgreSQL Global Develo
Toostares.exe	COM+ Even	t System [EventSystem]]		erver	PostgreSQL Global Develo
m postares.exe	DHCP Client	[Dhcp]			erver	PostgreSQL Global Develo
	Error Report	ink Tracking Client [Trk ing Service [ERSvc]	CVVKSJ			-
Name A Description	Help and Su	poort helpsvc]				
hnetcfg.dll Home Networking	Co Intranet Netv	work Awareness (INA+)	[IPRIP]			
iertutil.dll Run time utility for	Int Logical Disk	Manager [dmserver]				
imagehlp.dll Windows NT Imag	ge Network Loc	ation Awareness (NLA)) [NIa]			
imm32.dll Windows XP IMM	32 Network Cor	nections [ivetman] ess Connection Manag	er (BasMan)			
index.dat	Shell Hardwa	are Detection [ShellHW	Detection1			
index.dat	System Ever	nt Notification [SENS]				
index.dat	Secondary L	.ogon [seclogon]				
Ipcont.tsp Microsoft Multicas	t G Server [lanm	anserver]				
iphipapi.dli IP Helper API	Task Sched	rapionyj uler [Schedule]				
Ipnatnip.dli Microsoft NAT He	Workstation	[anmanworkstation]				
Kerberos.ali Kerberos.Security	Windows Fin	ewall/Internet Connecti	ion Sharing (ICS) [S	haredAccess]		
Kernersz.dli vvindows NT BAS	Windows Tir	ne [W32Time]				
Lab02-02 dll	Windows Ma	anagement Instrumenta	tion [winmgmt]			
	windows Au	iaio (AudioSrv)			1	
morani dli Windows NT MP	Router Administr	Microsoft Compration	5 1 2600	5512		

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

/root/Desktop/report.2366.txt [Read Only] - Mousepad
File Edit Search View Document Help
Warning, you are using the root account, you may harm your system.
⊨ Report for session '2366' ━
Real start date : 2021-05-17 14:39:50
Simulated start date : 2021-05-17 14:39:50
Time difference on startup : none
2021-05-17 14:39:51 First simulated date in log file
2021-05-17 14:39:51 DNS connection, type: A, class: IN, requested name: www.practicalmalwareanalysis.com
2021-05-17 14:39:52 DNS connection, type: A, class: IN, requested name: practicalmalwareanalysis.com
2021-05-17 14:39:52 HTTP connection, method: GET, URL: http://practicalmalwareanalysis.com/serve.html, file name: /var/lib/inetsim/http/fakefiles/sample.html
2021-05-17 14:39:52 Last simulated date in log file

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).

Getting Things Ready	>
Lab01-01.exe (16.0KiB)	
Your E-Mail (analysis completed notification, optional)	
Your Comment (optional)	
This is an example comment with a #tag	
Do not submit my sample to unaffiliated third parties A	
□ Allow community members to access sample €	
I consent to the Terms & Conditions and Data Protection Policy *	
100%	
Continue »	

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

		🗑 Sandbox 🗸	🖞 Quick Scans 👻	📕 File Collections	Resources -	🛿 Request Info 🗸	Q IP, E
Malicious Inc	dicators						٩
External Syste	ems s identified a	s malicious by a la	rge number of Antivi	rus engines			~
details source relevance	30/37 Antiviru 60/72 Antiviru External Syste 10/10	is vendors marked sa is vendors marked sa m	mple as malicious (81% c mple as malicious (83% (detection rate) detection rate)			

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.

	Sandbox 🗸	🖥 Quick Scans 👻	File Collections	Resources 👻	😮 Request Info 👻	Q, IP, E
Suspicious Indicators						18
Anti-Detection/Stealthy	rness					
Queries kernel debugg details "Lab01-03.o source API Call relevance 6/10	er information exe" at 00039837-00	001860-00000105-77	87420308			^
Anti-Reverse Engineerin	ıg					
PE file has unusual ent details ta with unus source Static Parsen relevance 10/10	tropy sections ual entropies 7.361855	514453				^
Environment Awareness	;					
Reads the active comp details "Lab01-03.e source Registry Acc	outer name exe" (Path: "HKLM\SYS ess	TEM\CONTROLSET001\	CONTROL\COMPUTERNA	MEVACTIVECOMPUTEI	RNAME"; Key: "COMPUTERNAME")	^

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

	<table-cell> Sandbox 🗸</table-cell>	🖞 Quick Scans 👻	File Collections	Resources 🗸	🕜 Request Info 👻	Q IP, C
Timestamp in PE head	er is very old or in t	the future				~
Hiding 3 Suspicious Indi	cators					
All indicators are availa	life only in the priv	ate webservice or sta	relatione version			
Informative						(9
Anti-Reverse Engineerin	g					
PE file contains zero-si details Raw size of " source Static Parser relevance 10/10	ize sections t" is zero					^
General						
Contacts server						~
Creates a writable file i	n a temporary dire	ctory				*

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).

Getting Thing	zs Ready	
	LabO3-01.exe (7.0KiB)	
Your E-Mail (ana	LabO3-O1.exe (7.0KiB)	
Your E-Mail (ana	LabO3-O1.exe (7.0KB)	
Your E-Mail (ana Your Comment I This is an exan	LabO3-O1.exe (7.0KB)	
Your E-Mail (ana Your Comment I This is an exan	LabO3-O1.exe (7.0KB) Ilysis completed notification, optional) (optional) pple comment with a #tag	

Figure 52 Uploading Lab03-01.exe

Analysis Envir Name LabO3 Size 7.0KiB Type perze MIME applica SHA256 eb843	ronments I-OLexe reconstate 0 ation/x-dosexec 160cs4e33b_fd507d2ffcedd B	×
Available:		
O 📕 Windows	7 32 bit	
O 📕 Windows	7 32 bit (HWP Support) 😫	
🔍 🗮 Windows 7	7 64 bit	
🔿 🔬 Linux (Ubu	untu 16.04, 64 bit)	
🔿 洒 Android S	Static Analysis 😫	
🔿 🎝 Quick Sca	an 🔁	
Currently, th	There are no files in the processing queue. he average processing time per sample is 9 minutes and 8 seconds seconds.	
	Runtime Options 🔹 Generate Public Report	A

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

											Minima
iitial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		Hooking 1	Hooking 1		Hooking 1		Remote Deskt op Protocol 1				

Figure 55 Technique Detection for Lab03-01.exe

	<table-cell> Sandbox 🗸</table-cell>	🕈 Quick Scans 👻	🕒 File Collections	Resources 👻	🕜 Request Info 👻	Q, IP, I
Malicious Indicators						Θ
External Systems						
Sample was identified a	as malicious by a la	arge number of Antiv	irus engines			^
details 61/70 Antivin cource External Syst relevance 10/10	us vendors marked sa æm	Imple as malicious (87%	detection rate)			
Sample was identified a	as malicious by at	least one Antivirus er	gine			^
details 61/70 Antivin	us vendors marked sa em	Imple as malicious (87%	detection rate)			
relevance 8/10						
Hiding 1 Malicious Indica	tors					
Al indicators are available	the only in the priv	ate softworker or sta	ndalane version.			
Suspicious Indicators						•

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

	Sandbox 🗸	🕈 Quick Scans 🗸	File Collections	Resources 🗸	🕜 Request Info 👻	Q
Suspicious Indicato	rs					3
External Systems					_	
Found an IP/URL ar details 2/88 rep source External relevance 10/10	tifact that was identi utation engines marked System	fied as malicious by a "http://www.practicalmal	t least one reputation e wareanalysis.com" as malici	ngine ious (2% detection rat	e)	^
Remote Access Relate	ed					
Reads terminal serv details " <input s<br=""/> source Registry, relevance 10/10 ATT&CK ID T1076 (S	vice related keys (ofte sample>" (Path: "HKLM\S Access show technique in the M	en RDP related) YSTEM\CONTROLSETO(ITRE ATT&CK TH matrix)	D1\CONTROL\TERMINAL SI	ERVER"; Key: "TSUSER	'ENABLED")	^
Unusual Characteristi	ics					
Input file contains A details Found st	API references not pa ring "ExitProcess" (Sourc	rt of its Import Addre	ss Table (IAT) is part of module: KERNELE	BASE.DLL)		^

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

	<table-cell> Sandbox 🗸</table-cell>	🕈 Quick Scans 🗸	File Collections	Resources 🗸	🕜 Request Info 👻	Q IP,
source String relevance 10/10						
Installs hooks/patches	the running proces	S				~
Informative						0
Network Related						
Found potential URL in details Pattern mat source String relevance 10/10	n binary/memory ch: "www.practicalmalı	wareanalysis.com"				^

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.

Getting Things Ready	×
LabO3-O2.dll (23.5KiB)	
Your E-Mail (analysis completed notification, optional)	
Your Comment (optional)	
This is an example comment with a #tag	
100%	
Continue >>	

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).

Network Analysis Overview				×
Contacted Hosts Login to Download Contacted Hosts (CSV)				
IP Address	Port/Protocol	Associated Process	Details	
80.65.238.8	80 TCP	-	France	
23.57.4.240	80 TCP		🔜 United States	
				Close

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.

	🗑 Sandbox 🗸	🖞 Quick Scans 🗸	File Collections	Resources -	🕜 Request Info 🗸	Q, 1P, 1
Malicious Indicators						0
External Systems						
Sample was identified details 57/69 Antivi source External Sys relevance 10/10	as malicious by a l rus vendors marked sa tem	arge number of Antiv ample as malicious (82%	irus engines detection rate)			^
Sample was identified details 57/69 Antivi source External Sys relevance 8/10	as malicious by at rus vendors marked sa tem	least one Antivirus er ample as malicious (82%	gine detection rate)			^
Hiding 1 Malicious Indica	ators					
All indicators are availa	life only in the priv	ate webservice or sta	ndalarse version			
Suspicious Indicators						0

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

	BRID	🗑 Sandbox 🗸	🕈 Quick Scans 👻	File Collections	Resources 👻	🕜 Request Info 🗸	Q, IP,
Suspicious	Indicators						0
Installation/	Persistence						
Creates ne	w processes						^
details	"rundll32.exe" i APLCall	s creating a new pro	ocess (Name: "%WINDIR	%\System32\WerFault.exe	", Handle: 236)		
relevance	8/10						
Unusual Cha	aracteristics						
Installs ho	oks/patches th	e running proces	s				^
details	"rundll32.exe" v "rundll32.exe" v "rundll32.exe" v 2286477ee296 of module "NS	wrote bytes "b8101! wrote bytes "a011ec wrote bytes "c04e6 47700000000d I.DLL")	5ed6effe0" to virtual add 16e" to virtual address "0) 27720546377e0656377 2695375000000007dl	ress "0x753811F8" (part of 7606E324" (part of modu 553864770000000000 bb497600000000009be	module "SSPICLI.DLL") le "WININET.DLL") 0d04976000000000 5375000000000ba18	5ea4976000000088ea4976 49760000000" to virtual add	^ 500000000e96853758 dress "0x75831000" (part
	"rundll32.exe" v "rundll32.exe" v "rundll32.exe" v	wrote bytes "48120 wrote bytes "48120 wrote bytes "48123 wrote bytes "48123	000" to virtual address " 000" to virtual address " 875" to virtual address "0 10d66ffa0" to virtual add	Dx7538139C" (part of mod Dx753812DC" (part of mod x753983DC" (part of mod x753983DC" (part of mod	ule "SSPICLI.DLL") Jule "SSPICLI.DLL") ule "SSPICLI.DLL") modulo "WS2_32 DLL	a)	
	"rundll32.exe" v "rundll32.exe" v "rundll32.exe" v	wrote bytes "68130 wrote bytes "f81100 wrote bytes "f8100	000" to virtual address " 000" to virtual address " 2006effe0" to virtual address address "	2x762F1680" (part of mod x75381408" (part of mod ress "0x75381248" (part of	Induite "WS2_32.DLL") Jule "WS2_32.DLL") f module "SSPICLI.DLL")	·)	

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

HYB	Sand	- xodb	Quick Scans 🗸	File Collections	Resources 🗸	🕜 Request Info 👻	Q IP,
Informative							6
General							
Creates muta details "" source C relevance 3	ants Geodons/1\BaseNamed DBWinMutex" ireated Mutant /10	Objects\DBW	/inMutex*				^
Spawns new	processes						~
details S S S S S	pawned process "rundli pawned process "rundli pawned process "rundli pawned process "rundli pawned process "rundli pawned process "rundli	32.exe" with a 32.exe" with a 32.exe" with a 32.exe" with a 32.exe" with a	commandline ""C:\Lak commandline ""C:\Lak commandline ""C:\Lak commandline ""C:\Lak commandline ""C:\Lak	003-02.dll",#1" (Show Pro 003-02.dll",#2" (Show Pro 003-02.dll",#3" (Show Pro 003-02.dll",#4" (Show Pro 003-02.dll",#5" (Show Pro	tess) cess) cess) cess) cess) cess)		
source N relevance 3	/10 /10						
Spawns new	processes that are r	not known c	hild processes				*
Installation/Pe	rsistence						

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

		🗑 Sandbox 🗸	🔓 Quick Scans 👻	📙 File Collections	R
Installation/F	Persistence				
Touches file	es in the Wir	dows directory			
details	"rundll32.exe "rundll32.exe "rundll32.exe "rundll32.exe "rundll32.exe	touched file "%WIN touched file "%WIN touched file "%WIN touched file "%WIN touched file "%WIN	IDIR%\Globalization\Sort IDIR%\AppPatch\sysmain IDIR%\System32\rundll3 IDIR%\AppPatch\AcLaye IDIR%\System32\en-US	ting\SortDefault.nls" n.sdb" 12.exe" rs.dll" \rundll32.exe.mui"	
source	API Call				
Network Rela	ated				
Found pote	ential URL in	binary/memory			
details	Heuristic mat	ch: "practicalmalware	eanalysis.com"		
source relevance	String 10/10				

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/Proces sMonitor.zip [Accessed 20 April 2021].

Docs.microsoft.com.2018. CreateProcessAfunction(processthreadsapi.h)-Win32apps.[online]Availablefrom:https://docs.microsoft.com/en-us/windows/win32/api/processthreadsapi/nf-processthreadsapi-createprocessa[Accessed 5May 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%20durin g%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_Anal ysis [Accessed 4 May 2021].

Oxpat.github.io. 2020. *Malware development part 5*. [online] Available from: https://Oxpat.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/enus/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%20B ehavioral%20Analysis&text=Examination%20of%20a%20contaminated%20file,general%20beh avior%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.ht m [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-codeanalysis.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

← -	→ C	l.com/gui/file/58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b3	27bd6fe47/detection				☆	* =	:
Σ	58898bd42c5bd3b	f9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47		Q	<u> </u>	\Box	Sign in	Sign up	
	50	① 50 security vendors flagged this file as malicious					C	88 200 88	
-	× Community √	58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ee838a0b327bd6fe47 LabOI-01.exe armadlio peexe via-tor	16.00 KB Size	2021-05-18 23 11 hours ago	:09:45 UTC		EXE		
	DETECTION	DETAILS RELATIONS BEHAVIOR COMMUNITY 💇							
	AegisLab	Trojan.Win32.Ulise.4Ic	AhnLab-V3	() Trojan/Wir	132.Agent.C957	504			
	Alibaba	① Trojan:Win32/Aenjaris.94b5660f	ALYac	() Trojan.Age	ent.16384SS				
	SecureAge APEX		Arcabit	() Trojan.Ulis	e.D1BC1E				
	Avast	() Win32:Malware-gen	AVG	() Win32:Mal	lware-gen				
	Avira (no cloud)	① HEUR/AGEN.1120198	BitDefender	() Gen:Varia	nt.Ulise.113694				
	CAT-QuickHeal	() Trojan.Aenjaris	ClamAV	() Win.Malwa	are.Agent-6342	616-0			
	Comodo	() Malware@#3eb40r99afetz	CrowdStrike Falcon	() Win/malici	ious_confidence	e_100% (W	0		

58898bd42c5bd3bf9b13	89f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47		Q <u>↑</u> 888 □ Sign in
Comodo	① Malware@#3eb40r99afetz	CrowdStrike Falcon	() Win/malicious_confidence_100% (W)
Cybereason	() Malicious.82141a	Cylance	() Unsafe
Cynet	() Malicious (score: 99)	Cyren	U 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

58898bd42c5bd3bf9b138	9f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47		Q <u>↑</u> 🚟 💭 Sign in
Sangfor Engine Zero	1 Trojan.Win32.Aenjaris.CT	Sophos	() Mal/Generic-R
Symantec	① Trojan.Gen.2	TACHYON	① Trojan/W32.Agent.16384.BFW
Tencent	() Malware.Win32.Gencirc.10baf903	TrendMicro	TROJ_GEN.R002C0DID20
TrendMicro-HouseCall	TROJ_GEN.R002C0DID20	VBA32	① Trojan.Tiggre
VIPRE	() Trojan.Win32.Generic!BT	Webroot	() W32.Malware.Gen
Yandex	() Trojan.GenAsalcGc9XwKYsAs	Zillya	Downloader.Amonetize.Win32.3112
Acronis	O Undetected	Ad-Aware	⊘ Undetected
Baidu	O Undetected	BitDefenderTheta	⊘ Undetected
Bkav Pro	⊘ Undetected	CMC	⊘ Undetected
DrWeb	⊘ Undetected	eGambit	⊘ Undetected
Jiangmin	O Undetected	Kaspersky	⊘ Undetected
Kingsoft	O Undetected	MaxSecure	⊘ Undetected
Panda	⊘ Undetected	Qihoo-360	⊘ Undetected
SentinelOne (Static ML)	Undetected	SUPERAntiSpyware	 Undetected

\leftrightarrow \rightarrow C $relation virustotal.com/gui$	i/file/58898bd42c5bd3bf9b1389f0eee5b39cd59180e83	70eb9ea838a0b32	7bd6fe47/detection					☆	* =
58898bd42c5bd3bf9b1389f	0eee5b39cd59180e8370eb9ea838a0b327bd6fe47				Q	<u> </u>		Sign in	Sign up
Bkav Pro	O Undetected		CMC	🕑 Und	detecte	d			
DrWeb	✓ Undetected		eGambit	🕢 Und	detecte	d			
Jiangmin	⊘ Undetected		Kaspersky	🕢 Und	detecte	d			
Kingsoft	⊘ Undetected		MaxSecure	🕢 Und	detecte	d			
Panda	⊘ Undetected		Qihoo-360	🕢 Und	detecte	d			
SentinelOne (Static ML)	⊘ Undetected		SUPERAntiSpyware	🕗 Und	detecte	d			
ViRobot	⊘ Undetected		ZoneAlarm by Check Point	🕢 Und	detecte	d			
Zoner	O Undetected		Avast-Mobile	📎 Una	able to p	process file t	type		
BitDefenderFalx	W Unable to process file type		Symantec Mobile Insight	📎 Una	able to p	process file t	type		
Trapmine	📎 Unable to process file type		Trustlook	📎 Una	able to p	process file t	type		
VirusTotal	Community	Tools	Premium S	ervices		D	ocumentation	n	
Contact Us	Join Community	API Scripts	Intelligence			G	et Started		

b. Lab01-01.DLL

\leftrightarrow \rightarrow C \cong virustot	al.com/gui/file/f50e42c8dfaab649bde0398867e930b86c2a599e8db83b826039308	32268f2dba/detection				☆	* 🛎 E
f50e42c8dfaab64	9bde0398867e930b86c2a599e8db83b8260393082268f2dba		Q	<u> </u>	\Box	Sign in	Sign up
38	38 security vendors flagged this file as maliclous					C	
X Community V	f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba Lab01-01.dll armadillo pedit via-tor	160.00 KB Size	2021-05-19 09 1 hour ago	:42:03 UTC		DLL	
DETECTION	DETAILS RELATIONS COMMUNITY						
AegisLab	Trojan.Win32.Ulise.4!c	Alibaba	() Trojan:Win	32/SuspectCRC	C.6956aaeb		
SecureAge APEX	Malicious	Avast	() Win32:Mal	ware-gen			
AVG	() Win32:Malware-gen	Avira (no cloud)	() TR/Dldr.Wa	aski.163840.1			
BitDefender	() Gen:Variant.Ulise.105796	BitDefenderTheta	() Gen:NN.Ze	edlaF.34690.kq	4@aGkQVt	р	
CAT-QuickHeal	() Trojan.Skeeyah	ClamAV	() Win.Malwa	are.Agent-6369	668-0		
Comodo	 Malware@#2dsw4albnce61 	CrowdStrike Falcon	() Win/malici	ous_confidence	e_100% (W)		
Cylance	① Unsafe	Cynet	() Malicious ((score: 100)			

\leftarrow	→ C 🌲 virustotal.com/gui/f	ile/f50e42c8dfaab649bde0398867e930b86c2a599e8db83b82603930822	268f2dba/detection	x) 🛊 😩 E
Σ	f50e42c8dfaab649bde03988	67e930b86c2a599e8db83b8260393082268f2dba		Q 🛧 🎆 💭 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-RTI290934C61DE9	McAfee-GW-Edition	() GenericRXFO-RTI290934C61DE9
	Microsoft	① 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.GenAsalHoPrb0Qvul0	Zillya	() Adware.InstallCore.Win32.1036
	Acronis	Undetected	Ad-Aware	⊘ Undetected .

\leftrightarrow \rightarrow C $$ virustotal.com,	/gui/file/f50e42c8dfaab649bde0398867e930b8	36c2a599e8db83b8260393082268f2dba/detection		* 🛊 😩 :
f50e42c8dfaab649bde0	398867e930b86c2a599e8db83b8260393082	268f2dba	Q <u>↑</u>	Sign in Sign up
Acronis	O Undetected	Ad-Aware	⊘ Undetected	
AhnLab-V3	Undetected	Arcabit	⊘ Undetected	
Baidu	Undetected	Bkav Pro	⊘ Undetected	
CMC	O Undetected	Cyren	⊘ Undetected	
DrWeb	O Undetected	F-Secure	⊘ Undetected	
Jiangmin	O Undetected	K7AntiVirus	⊘ Undetected	
K7GW	O Undetected	Kaspersky	⊘ Undetected	
Kingsoft	O Undetected	Malwarebytes	⊘ Undetected	
MaxSecure	O 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	Ţ

\leftrightarrow \rightarrow C $($ virustotal.com/	/gui/file/f50e42c8dfaab649bde0398867e930b86c2a	599e8db83b82603930822	268f2dba/detection				☆	* • •
f50e42c8dfaab649bde0	398867e930b86c2a599e8db83b8260393082268f2	dba		Q	<u>^</u>	; 🖓	Sign in	Sign up
Panda	⊘ Undetected		Qihoo-360	🕢 Undete	cted			
SentinelOne (Static ML)	⊘ Undetected		SUPERAntiSpyware	🕑 Undete	cted			
TACHYON	⊘ Undetected		Tencent	🕑 Undete	cted			
VBA32	⊘ Undetected		ViRobot	🚫 Undete	cted			
ZoneAlarm by Check Point	⊘ Undetected		Zoner	🕑 Undete	cted			
eGambit	🛞 Confirmed timeout		Avast-Mobile	📎 Unable	to process file typ	ре		
BitDefenderFalx			Cybereason	📎 Unable	to process file typ	pe		
Symantec Mobile Insight			Trapmine	📎 Unable	to process file typ	pe		
Trustlook	⊗ Unable to process file type		ALYac					
								_
VirueTotal	Community	Tools	Pr	mium Son <i>ico</i> c	Dec	ourmontation		
Contact Us	Join Community	API Scripts	Int	elligence	Gel	t Started		
How It Works	Vote and Comment	YARA	Hu	nting	Sea	arching		- -

2) Lab01-03.exe

_									
> 7983a582939924d	c70e3da2da80fd3352ebc90de7b8c4c427d484ff4f050f0aec			Q	<u></u>	000	\square	Sign in	Sk
51	() 51 security vendors flagged this file as malicious							C	20
X Community V	7983a582939924c70e3da2da80fd3352ebc90de7b8c4c427d484ff4f050f0ae Lab01-03.exe (direct-cpu-clock-access) (fsg) overlay) peexe runtime-modules via-tor	ac	4.64 KB 20 Size 14	21-05-04 17 days ago	7:48:29 UT	гс		EXE	
DETECTION	DETAILS RELATIONS BEHAVIOR COMMUNITY	Abol ab-V2	0	Trojan/Wij	132 Acent	t C 28943	155		
DETECTION AegisLab	DETAILS RELATIONS BEHAVIOR COMMUNITY	AhnLab-V3	0	Trojan/Win	n32.Agent	t.C28943	355		
DETECTION AegisLab Alibaba	DETAILS RELATIONS BEHAVIOR COMMUNITY ① Trojan.Multi.Generic.IVbD ① TrojanClicker:Win32/Agentb.3bb840a6	AhnLab-V3 SecureAge APEX	() ()	Trojan/Win Malicious	n32.Agent	t.C28943	355		
DETECTION AegisLab Alibaba Avast	DETAILS RELATIONS BEHAVIOR COMMUNITY ① Trojan.Multi.Generic.IVbD ① Trojan.Clicker:Win32/Agentb.3bb840a6 ① Win32:Matware-gen	AhnLab-V3 SecureAge APEX AVG		Trojan/Win Malicious Win32:Ma	n32.Agent Iware-ger	t.C28943 n	355		
DETECTION AegisLab Alibaba Avast Baidu	DETAILS RELATIONS BEHAVIOR COMMUNITY ① Trojan.Multi.Generic.IVbD ① Trojan.Clicker:Win32/Agentb.3bb840a6 ① Win32:Matware-gen ① Win32:Trojan.Clicker.Agent.z	AhnLab-V3 SecureAge APEX AVG BitDefenderTheta		Trojan/Win Malicious Win32:Ma Gen:NN.Z	n32.Agent Iware-gei exaF.3468	t.C28943 n 88.ambd	855 aODfLcf		
DETECTION AegisLab Alibaba Avast Baidu CAT-QuickHeal	DETAILS RELATIONS BEHAVIOR COMMUNITY ① Trojan:Mutil:Generic:IVbD ① Trojan:Clicker:Vin32/Agentb:3bb840a6 ① Win32:Matware-gen ① Win32:Trojan:-Clicker:Agent.z ② Trojan:Agentb	AhnLab-V3 SecureAge APEX AVG BitDefenderTheta Comodo		Trojan/Win Malicious Win32:Ma Gen:NN.Z TrojWare.N	h32.Agent Iware-gen exaF.3468 Win32.Tro	t.C28943 n 88.ambd ijan.Inor.E	855 aODfLcf 3_10@1qri	a8i	
DETECTION AegisLab Alibaba Avast Baidu CAT-QuickHeal CrowdStrike Falcon	DETAILS RELATIONS BEHAVIOR COMMUNITY ① Trojan.Multi.Generic.IVbD ① Trojan.Clicker:Win32/Agentb.3bb840a6 ① Win32:Malware-gen ① Win32:Trojan.Clicker.Agent.z ① Trojan.Agentb ① Trojan.Agentb	AhnLab-V3 SecureAge APEX AVG BitDefenderTheta Comodo Cylance		Trojan/Wii Malicious Win32:Ma Gen:NN.Z TrojWare.1 Unsafe	h32.Agent Iware-get exaF.3468 Min32.Tro	t.C28943 n 88.ambd ijan.Inor.E	155 IaODfLcf 3_10@1qri	881	

\leftarrow	→ C 🗎 virustotal.com/gui/f	ile/7983a582939924c70e3da2da80fd3352ebc90de7b8c4c427d484ff4f05	50f0aec/detection	☆ 🛊 😩 ፤
Σ	7983a582939924c70e3da2da	80fd3352ebc90de7b8c4c427d484ff4f050f0aec		Q <u>↑</u> 👯 🖵 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.E76Altr
	GData	() Win32.Trojan.Agent.B25F01	Gridinsoft	() Trojan.Win32.Agent.ns
	Ikarus	() Trojan.Win32.Genome	Jiangmin	() Trojan/Genome.bmbp
	K7AntiVirus	() Spyware (0055e3f61)	K7GW	(j) 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/TnegalMSR	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

7983a582939924c70e3da2	da80fd3352ebc90de7b8c4c427d484ff4f050f0aec		Q 🛧 👯 🖓 Sign in
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.GenomelqjszR3auxbA	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	Ø Undetected
Bkav Pro	⊘ Undetected	ClamAV	Ø Undetected
CMC	⊘ Undetected	Emsisoft	⊘ Undetected
eScan	⊘ Undetected	F-Secure	⊘ Undetected
MaxSecure	✓ Undetected	Panda	 Undetected

\leftrightarrow \rightarrow C $rightarrow$ virustotal.com/gu	i/file/7983a582939924c70e3da2da80fd3352ebc90d	e7b8c4c427d484ff4f050f0ae	c/detection				☆	* 6	1 I
7983a582939924c70e3da2c	7983a582939924c70e3da2da80fd3352ebc90de7b8c4c427d484ff4f050f0aec								
Avira (no cloud)	O Undetected	Bit	Defender	O Undetected	i				
Bkav Pro	⊘ Undetected	Cla	amAV	O Undetected	i				
CMC	⊘ Undetected	Em	sisoft	O Undetected	i				
eScan	O Undetected	F-5	Secure	O Undetected	i				
MaxSecure	✓ Undetected	Pai	nda	O Undetected	i				
Qihoo-360	✓ Undetected	SU	PERAntiSpyware	O Undetected	ł				
Zoner	⊘ Undetected	Су	bereason	👸 Timeout					
Avast-Mobile	W Unable to process file type	Bit	DefenderFalx	📎 Unable to p	rocess file type				
Symantec Mobile Insight	🛞 Unable to process file type	Tra	pmine	🗞 Unable to p	rocess file type				
Trustlook	🛞 Unable to process file type								
VirusTotal	Community	Tools	Premium Ser	vices	Docu	mentation		Q	
Contact Us	Join Community	API Scripts	Intelligence		Get S	tarted			

Basic Static Analysis:

1) Lab01-01.exe





Dependency Walker - [Lab01-01.exe] Control Contro Control Control Control Con								_ 8 ×
PI	Ordinal	Hint	Function ^		[Entry Point		
E KERNEL 32.DLL	N/A	157 (0x009D)	_adjust_fdiv			Not Bound		
NTDLL.DLL	N/A	183 (0x00B7)	_controlfp			Not Bound		
msvcrt.dll	N/A	202 (0x00CA)	_except_handler3			Not Bound		
E M KERNEL32.DLL	N/A	211 (0x00D3)	_exit			Not Bound		
TOLL.DLL	N/A	585 (0x0249)	exit			Not Bound		
M NTDLL.DLL	N/A	271 (0x0 10E)	geuildilidigs			Not Bound		
	N/A	657 (0x0 29 1)	malloc			Not Bound		
	N/A	100 (0x0064)	p initeny			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		
	1							
Module File Time Stamp Link Time Stamp File Size Attr. Link Checksu	um Real Check	sum CPU	Subsystem Symbols	Preferred Base Actual	Base Virtual Size L	oad Order H	File Ver Product Ver	Image V 🔺
KERNEL32.DLL 14/04/2008 05:41 14/04/2008 05:41 989,696 A 0x000F444	42 0x000F44	A2 X86	Console CV	UX/C800000 Unknor	Nn 0x000F6000 N	lot Loaded	5.1.2600.5512 5.1.2600.55	12 5.1
(•)								▶
For Help, press F1								
🏄 Start 🞯 🔤 🐺 🛩 👘 🏀 🥹 🚷 👘 🗠 C: \Documents and Settin 🔁 C: \D	ocuments and Sett	in 📑 🕻 Depe	ndency Walker					00:11
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.							🗔 🛈 🖪	3 da 🛛 🖓

Project Exploitable XP SP3 ×										
Dependency Walker - [Lab01-01.exe]										-
File Edit View Options Profile Window Help										-
🎽 🖬 🔎 🖹 🕬 🖭 💭 📽 🗒 🖳 🔍 📑 🚿 🖷 🗖 🗍	N ?									
∃ 🔲 LAB01-01.EXE	PI	Ordinal	Hint	Function ^	Entry	Point				
🚊 🔲 KERNEL 32. DLL	C	N/A	28 (0x001C)	Веер	0x7C8	37A8F				_
🔲 NTDLL.DLL	C	N/A	49 (0x0031)	CloseHandle	0x7C8	098D7				
😑 🔲 MSVCRT.DLL		N/A	55 (0x0037)	CompareStringA	0x7C8	0D107				
KERNEL32.DLL		N/A	56 (0x0038)	CompareStringW	0x7C8	0A3EE				
TTDLL.DLL		N/A	/1 (0x0047)	CreateDirectoryA	0x7C8	21/94				
NTDLL.DLL		N/A	74 (0x004A) 70 (0x004E)	CreateDirectoryW	0x7C8	01429				
		N/A	82 (0x0052)	CreateFileW	0x7C8	107E0				
		N/A	97 (0x0061)	CreatePipe	0x7C8	1D827				
		N/A	98 (0x0062)	CreateProcessA	0x7C8	0236B				
	C	N/A	102 (0x0066)	CreateProcessW	0x7C8	02336				
	C	N/A	108 (0x006C)	CreateThread	0x7C8	106C7				
		N/A	127 (0x007F)	DeleteCriticalSection	0x7C9	1135A				
		N/A	129 (0x0081)	DeleteFileA	0x7C8	31EC5				
		N/A	130 (0x0082)	DeleteFileW	0x7C8	31F48				
		N/A N/A	145 (0x0091) 150 (0x0096)	Dupicatemandie EnterCriticalSection	0x7C8	000088				
		N/A	172 (0x0096)	EnumSystemLocalesA	0x7C8	37CE9				
		N/A	182 (0x00B6)	ExitProcess	0x7C8	1CAFA				
		N/A	183 (0x00B7)	ExitThread	0x7C8	OCOE8				
		N/A	194 (0x00C2)	FileTimeToLocalFileTime	0x7C8	0E8F6				
		N/A	195 (0x00C3)	FileTimeToSystemTime	0x7C8	0E87C				
		N/A	204 (0x00CC)	FindClose	0x7C8	10EE67				
		N/A	208 (0x00D0)	FindFirstFileA	0x7C8	13869				
		N/A	211 (0x00D3)	FindHirstHieW	0x7C8	UEF / 1				
		N/A	217 (0x00D9) 218 (0x00D4)	FindNextFileW	0x7C8	IDEECA				
			1212 (000000)		0.700			<u> </u>		_
A Madula Ella Tima Channa Link Tima Channa Ella Cina A	te Link Charles	m Deal Ches	kaum CDLL	Cubeusten Cumbele	Drafarrad Page	Actual Page	Victual Size		Dreduct Ver	
KEDNEL32 DLL 14/04/2008 05:41 14/04/2008 05:41 089 606 A	0x000E44/	2 0x000E4	4A2 V86	Console CV	0x7C800000	Linknown	0x000E6000 Not	Loaded 5.1.26	500 5512 5 1 2600 5512	1
- 1001/000000000000000000000000000000000			100 L						00.0012 0.1.2000.0012	1.

Project Exploitable XP SP3 - VMware Workstation								- o ×
File Edit View VM Tabs Help 📙 🕶 🖶 🚇 🚇		>- 2 -	-					
C Project Evoluitable VP SP3								
Dependency Walker - [1 ab01-01 eye]								
File Edit View Options Profile Window Help								_ 2 ×
E LAB01-01.EXE	PI Ordinal	Hint	Function ^		Entry	Point		
Emel32.0LL	N/A	N/A	RtlAllocateHeap		Not B	ound		
Intoll.oll	C N/A	N/A	RtIDeleteCriticalSection		Not B	ound		
MSVCRT.DLL	N/A N/A	N/A	RtEnterCriticalSection		Not B	ound		
E D KERNEL32.DLL	N/A N/A	N/A	RtiGetLastWin32Error		Not B	ound		
	C N/A	N/A	RtlLeaveCriticalSection		Not B	ound		
M WIDERDEE	N/A	N/A	RtReAllocateHeap		Not B	ound		
	N/A	N/A	RtlSetLastWin32Error		Not B	ound		
	C N/A	N/A	RtiSizeHeap		Not B	ound		
	N/A	N/A	Raunwind		NOT B	ouna		
	1	1	1			1		
Module File Time Stamp Link Time Stamp File Size Attr. Link Ch	ecksum Real Ched	ksum CPU	Subsystem Symbols	Preferred Base	Actual Base	Virtual Size Load Order	File Ver F	Product Ver Image V
KERNEL32.DLL 14/04/2008 05:41 14/04/2008 05:41 989,696 A 0x000F	F44A2 0x000F4	4A2 x86	Console CV	0x7C800000	Unknown	0x000F6000 Not Loaded	5.1.2600.5512 5	5.1.2600.5512 5.1
			Le i lu	10.00400000	1	• • • • • • • • •	1	
Ear Mala arras 51								
	CulDen ments and Sat	5a	and an an and all and					00.11
🐱 start 🔮 📟 🧏 🥗 📢 🧑 🤎 🐨 🛄 C: pocurients and Settin	c. pocuments and set	- C Debe	engency walker					00:11

Project Exploitable XP SP3 - VMware Workstation						- o ×
File Edit View VM Tabs Help 📙 🛪 🛱 🚇 🚇		>- 2 *				
Project Exploitable XP SP3 ×						
Comparison Comparison (Lab01-01.exe)						_ 8 ×
File Edit View Options Profile Window Help						X
😂 🖬 🔎 🙀 📣 📼 💭 🗳 🗒 🍓 💷 🚿 🖷 📰 🕺						
E LAB01-01.EXE	PI Ordinal	Hint	Function ^	Entry Po	int	
	N/A	608 (0x0260)	RüGetVtVersionNumbers	0x7C92	130F	
A Madula Eila Tina Stana Link Tina Stana Eila Siaa Attr. Link	Checkrum Real Check		ubovotam Symbola Drav	ferred Race Actual Race Virt	tual Size Load Order Eile	Ver Product Ver Image V
KERNEL32.DLL 14/04/2008 05:41 14/04/2008 05:41 989,696 A 0x0	00F44A2 0x000F4+	4A2 x86 C	Console CV 0x7	C800000 Unknown 0x0	000F6000 NotLoaded 5.1	.2600.5512 5.1.2600.5512 5.1
			- Iu Iaa	araaaa luu lar	·····	
For Help, press F1						
			lana Mallan			
🛫 Start 🔮 🔤 🧟 🕊 🕅 🧶 🤎 🚯 👘 🛄 C: pocuments and Settin	copocuments and Set	un] =c Depend	iency 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











b. Lab01-01.dll





2) Dynamic analysis

a. Lab03-01.exe







b. Lab03-02.dll











APPENDIX D – REGSHOT

Project Exploitable XP SP3 - VMware Workstation						- o ×
File Edit View VM Tabs Help 📙 🛪 🖧 💭 🕰 💭 🗔 🗍	>- 2 -					
Kali-Linux-2019.4-vmware-am ×						
C:\Documents and Settings\Administrator\Local Settings\Temp\~res-x86.txt - Notepad++						_ 8 ×
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?						Х
1. 🖶 🗄 🖻 🔓 🕼 🗶 🕼 🏦 🗩 🖒 🕋 🍇 🔍 🤜 🖼 🚍 💷 🛚 羅 🖉] 🛃 🚍 💿 🔳 🔳 💌					
🔚 MSVCRTD.DLL 🖾 🔚 Copy (2) of Proof of Concept.pl 🖾 🔚 readme.txt 🖾 🚍 ~resx86.txt 🗵						
1 Regshot 1.9.0 x86 Unicode						<u> </u>
2 Comments:						
3 Datetime: 2021/5/17 18:12:17 , 2021/5/17 18:20:36						
4 Computer: XPSP3VULNERABLE , XPSP3VULNERABLE						
6 Seriale. Administrator, Administrator						
7						
8 Kevs added: 19						
9						
10 HKLM\SYSTEM\ControlSet001\Services\IPRIP						
11 HKLM\SYSTEM\ControlSet001\Services\IPRIP\Parameters						
12 HKLM\SYSTEM\ControlSet001\Services\IPRIP\Security						
13 HKLM\SYSTEM\CurrentControlSet\Services\IPRIP						
14 HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Parameters						
15 HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Security						
16 HKU\S-1-5-21-1960408961-/06699826-839522115-500\Software\Microso	It (Windows ShellNokoam)	BagMRU\U\1\2\(J\4			
17 RK0(5-1-5-21-1960406961-7066099626-839522115-500(S0ftware\Microso)	ft/Windows/ShellNoRoam/	BagMPII\0\1\2\0	3\4\0\0			
10 HKU\S-1-5-21-1960408961-706609826-839522115-500\Software\Microso	ft/Windows/ShellNoRoam/	BagMRU(0(1(2))	14000			
20 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Migroso	ft/Windows/ShellNoRoam)	BagMRU\0\1\2\0	0\4\0\0\0\0			
21 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microso	ft\Windows\ShellNoRoam\	Bags\156				
22 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microso	ft\Windows\ShellNoRoam\	Bags\156\Shell	L			
23 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microso	ft\Windows\ShellNoRoam\	Bags\157				
24 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microso	ft\Windows\ShellNoRoam\	Bags\157\Shell				
25 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microso	ft\Windows\ShellNoRoam\	Bags\158				
26 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microso	ft\Windows\ShellNoRoam\	Bags\158\Shell	1			
27 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microso	ft\Windows\ShellNoRoam\	Bags\159				
28 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microso:	ft\Windows\ShellNoRoam\	Bags\159\Shell	1			
29						-
Normal text file	length : 30,144 lines :	209 Ln ; 1	Col: 1 Sel: 0 0	Windows (CR LF)	UCS-2 Little Endian	INS
🥂 Start 🔯 📷 🍘 🛥 🍘 🖉 🕲 📣 🔷 🍅 Criwindowskyste 🛛 📼 Command Brownt	P Dependency Walker	arshot 1 9 0 x86 U	C:\Documents and S	Or Process Explorer - Sv	Documents and	23.52
	- Coperioency Walker	.ganoe 1.5.0 X00 0	- copocuments and sto	So nocessexpioler - Sym	(bocuments allo	23.32



Project Exploitable XP SP3 - VMware Workstation	
File Edit View VM Tabs Help + 🕂 🖧 💭 🕰 💭 🔲 🗍 🖓 🖓 🖉	
[] Kall-Unuc-2019.4-vmware-am× [] Project Exploitable XP SP3 ×	
🖹 G\Documents and Settings\Administrator\Local Settings\Temp\~res-x86.bxt - Notepad++	8 ×
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?	х
🖀 MSVCRTD.D.LL 🗵 🗮 Copy (2) of Proof of Concept pl 🗵 🗮 readme bit 🗵 🚍 "resx86bit 🗵	
56 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRcam\BagMRU\0\1\2\0\4\0\NodeSlot: 0x0000009C	-
57 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\1\2\0\4\0\MRUListEx: 00 00 00 0F FF FF FF	_
58 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 46 40 23 8C 10 00 50 52 4	1 🕐
59 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\1\2\0\4\0\0\NodeSlot: 0x000009D	
60 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 0F FF FF FF	
61 HKU\S-1-5-22-1960409961-70669926-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMKU\0\1/2\0\4\0\0\0: 50 00 31 00 00 00 00 04 40 C6 8B 10 00 42 49	41
62 HKU\S-1-5-21-1960403961-706699326-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMKU\0\1/2\0\4\0\0\0\NodeSlot: 0x000009E	
63 HKU/S-1-5-21-1960409961-706699926-83952215-500/Software/Microsoft/Windows/ShellNoRoam/BagMRU/0/1/2/0/4/0/0/(RUListex: 00 00 00 00 FFFFFFF	40 -
64 HKU(S-1-5-22-196040951-706599226-83952215-500/SOTUMFE/NICTOSOTUMINGONS/SHELINGKOAM/BAGHKU(D/1/2/0/4/0/0/0): 44 00 31 00 00 00 00 46 00 B8 10 00 43	48
<pre>0 RKU(5-1-5-21-1904905961-70669926-859522115-500/S016Water Material Windows/ShellKokodM/BdgRkd(V/1/2(0/+)/0/U/0/ModeSide: 0x0000097 64 Wind(S-1-5-21-1904905961-70669926-859522115-500/S016Water) Material Windows/ShellKokodWater(V/1/2(0/+)/0/U/0/ModeSide: 0x0000097 64 Wind(S-1-5-21-1904905961-70669926-859522115-500/S016Water) Material Windows/ShellKokodWater(V/1/2(0/+)/0/U/0/ModeSide: 0x0000097 64 Wind(S-1-5-21-1904905961-70669926-859522115-500/S016Water) Material Waterial Waterial</pre>	
<pre>67 HUUS-1-5-21-196040951-70605922-035922115-500(Software)Wigners/fwlindows/ShellModam/BagNav(01126104)Undows/BagNav6504125040(Windows/ShellModaw)</pre>	
68 HKUS-1-5-21-10604096061-706609826-830522115-500/Software/Microsoft/Windows/Shell/Negary/Software/Microsoft/Windows/Shell/W	
69 HKU/S-1-5-21-1960408961-706699826-839522115-500/Software/Microsoft/Windows/ShellNoRoam/Bags/156/Shell/MinPos1364x616(1),v: 0xFFFF8300	
70 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bacs\156\Shell\MaxPos1364x616(1).x: 0xFFFFFFF	
71 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\MaxPos1364x616(1).y: 0xFFFFFFFF	
72 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\WinFos1364x616(1).left: 0x0000005A	
73 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\WinPos1364x616(1).top: 0x00000058	
74 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\WinFos1364x616(1).right: 0x000002FF	
75 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\WinPos1364x616(1).bottom: 0x0000021E	
76 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\Rev: 0x00000002	
77 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\WFlags: 0x0000000	
78 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNcRoam\Bags\156\Shell\ShowCmd: 0x0000001	
79 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\FFlags: 0x0000001	
80 HKU\S-1-5-21-1960409961-70669926-83952215-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\Horkey: 0x00000000	
81 HKU(5-1-5-21-190408391-706639226-839522115-500/Software/Wiccosoft/Windows/SoftiNokoam/Bags/156/SoftiNottons/ OwerFirth	
<pre>32 HKU\5-1-5-21-1960405961-06693626-83552115-500\SOITWAFE\NICTOSOIT\WINDOWS\SHELINGKOAM\BAg\$\156\Shell\Links; UXUUUUUUU 33 HVU\5-1-5-111660405961-76650696826552115-500\SOITWAFE\NICTOSOIT\WINDOWS\SHELINGKOAM\BAg\$\156\Shell\Links; UXUUUUUUU 34 HVU\5-1-5-21-1960405961-7665096826552115-500\SOITWAFE\NICTOSOIT\WINDOWS\SHELINGKOAM\BAg\$\156\Shell\Links; UXUUUUUUU 35 HVU\5-1-5-21-1960405961-7665096826552115-500\SOITWAFE\NICTOSOIT\WINDOWS\SHELINGKOAM\BAg\$\156\Shell\Links; UXUUUUUUU 34 HVU\5-1-5-21-1960405961-7665096826552115-500\SoitwaFe\Nictosoit\Windows\Shell\Nictosoft\Windows\Shell\Links; UXUUUUUUU 35 HVU\5-1-5-21-1960405961-76650968265552115-500\SoitwaFe\Nictosoit\Windows\Shell\Nictosoft\Windows\Shell\Links; UXUUUUUU 34 HVU\5-1-5-21-196040596 35 HVU\5-1-5-21-196040596 35 HVU\5-1-5-21-19604055 35 HVU\5-1-5-21-19604055 35 HVU\5-1-5-21-19604055 35 HVU\5-1-5-21-19604055 35 HVU\5-1-5-21-19604055 35 HVU\5-1-5-21-19604055 35 HVU\5-100405 35 HVU\5-1005 35 HVU\5-1</pre>	
<pre>34 WW15-1-E-1156640851-000552203522115-000/0504Wate (Windows)0HE1N0Codm(BdgS(150)HE1N0Codm(BdgS(150)HE1N0Codm)0504) 44 WW15-1-E-11566408641-70660954293011E-E001064Frase(Windows)0HE1N0Codm(BdgS(150)HE1N0Codm)040440455 45 WW15-1-E-11566408641-70660954293011E-E001064Frase(Windows)0HE1N0Codm(BdgS(150)HE1N0Codm)0404 45 WW15-1-E-11566408641-7066954293011E-E001064 45 WW15-1-E-11566408641-7066954293011E-E001064 45 WW15-1-E-11566408641-7066954293011E-E001064 45 WW15-11E-115664 45 WW15-11E-115664 45 WW15-11E-115664 45 WW15-11E-1156 45 WW15-11E-1156 45 WW15-11E-1156 45 WW15-11E-115 45 WW15</pre>	-
	•
Normal text file ength : 30,144 lines : 209 Ln : 56 Col : 127 Sel : 0 0 Windows (CR LF) UCS-2 Little Endian 1	IS
🐮 Start 🕜 🖾 😨 🛩 🏟 🏈 🎱 🕹 🔷 🐡 🚞 C:\VINDOWS/syste 🔯 Command Prompt 🛛 🗬 Dependency Waker 🔹 Registri 1.9.0 x86 U 🔁 C:Documents and S 🖓 Process Explorer - Sy 🔐 C:Documents and	23:53

Project Exploitable XP SP3 - VMware Workstation	- o ×
File Edit View VM Tabs Help - 🛱 🔉 🕰 🔛 🗔 🗗	
🕞 Kal-Unux-2019.4-vimware-am X 🕞 Project Exploitable XP SP3 X	
C\Documents and Settings\Administrator\Local Settings\Temp\~res-x86.txt - Notepad++	_ 8 ×
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?	х
🖷 MSVCRTD.DLL 🔟 🔤 Copy (2) of Proof of Concept pl 🗵 📑 readme tot 🗵 🚍 "Pres-ABEtat 🖾	
83 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\Address: 0xFFFFFFF	
84 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\Vid: "{655125E5-7BE1-4810-BA9D-D271C8432CE3}"	
85 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\Mode: 0x0000006	
86 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\ScrollPos1364x616(1).x: 0x00000000	
87 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\ScrollPos1364x616(1).y: 0x00000000	
88 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\Sort: 0x0000000	
89 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\SortDir: 0x00000001	
90 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\156\Shell\Col: 0xFFFFFFF	
91 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 FI
92 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\FolderType: "Documents"	
93 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\MinPos1364x616(1).x: 0xFFFF8300	
94 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\MinPos1364x616(1).y: 0xFFFF8300	
95 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\MaxPos1364x616(1).x: 0xFFFFFFF	
96 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\MaxPos1364x616(1).y: 0xFFFFFFF	
97 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\WinPos1364x616(1).left: 0x0000005A	
98 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\WinPos1364x616(1).top: 0x00000058	
99 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\WinPos1364x616(1).right: 0x000002FF	
100 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\WinPos1364x616(1).bottom: 0x0000021E	
101 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\Rev: 0x0000002	
102 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\WFlags: 0x0000000	
103 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\ShowCmd: 0x00000001	
104 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\FFlags: 0x00000001	
105 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\HotKey: 0x0000000	
106 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\Buttons: 0xFFFFFFF	
107 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\Links: 0x0000000	
108 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\Address: 0xFFFFFFF	
109 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\Vid: "{65F125E5-7BE1-4810-BA9D-D271C8432CE3}"	
110 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\Mode: 0x00000006	-1
EXTIN S-1-5-21-106/04/806/1-706608826-830522115-50N\Software\Viorosoft\Viodows\ShallWoDosm\Bane\157\Shall\Sortlase\157\Shall\Shall\Sortlase\157\Shall\Shall\Sortlase\157\Shall\Shall\Sortlase\157\Shal	<u> </u>
Normal text file ength : 30,144 ines : 209 Ln : 83 Col : 122 Sel : 0 0 Windows (CR LF) UC5-2 Little Enc	ian INS
🍠 Start 🕜 🕿 👿 🛩 🏟 🏈 🕘 🔴 — * 🗋 C: (VDDOWS/syste) 🔤 Command Prompt 📃 🔩 Dependency Walker) 🚘 Registro 1.9.0 x86 U 🔁 C: Documents and S) 💜 Process Explorer - Sy 🔐 C: (Documents and System)	d 23:53

Project Exploitable XP SP3 - VMware Workstation	- 🛛 ×
File Edit View VM Tabs Help 📙 - 母 🔉 💭 🕰 🖓	
[c] Kali-Linux-2019.4-immare-am× [c] Project Exploitable XP SP3 ×	
🚰 C\Documents and Settings\Administrator\Local Settings\Temp\~res-x86.bxt - Notepad++	_ 8 ×
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?	х
,	
🖀 MSVCRTD.DLL 🗓 🗮 Copy (2) of Froof of Concept pl 🖾 📄 readme bit 🕮 🔚 Yee x86 bit 🕮	
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\ShellNoRcam\Bags\157\Shell\Sort: 0x00000000	
114 HRU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\SortDir: 0x00000001	
115 HKU\S-1-5-21-1960408961-706699926-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\157\Shell\Col: 0xFFFFFFFF	
116 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRcam\Bags\157\Shell\ColInfo: 00 00 00 00 00 00 00 00 00 00 00 00 00	0 00 00 FI
117 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\FolderType: "Documents"	
118 HKU\S-1-5-21-1960408961-706699226-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\MinPosl364x616(1).x: 0xFFFF8300	
119 HKU\S-1-5-21-1960408961-706699226-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\MinPosl364x616(1).y: 0xFFFF8300	
120 HKU(S-1-5-21-1960408961-706699226-839522115-500\Software\Microsoft\Windows\ShellNokoam\Bags\158\Shell\MaxPosl364x616(1).x: 0xFFFFFFF	
121 HKU\S-1-5-21-1960408961-706699226-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\MaxPosl364x616(1).y: 0xFFFFFFF	
122 HKU\S-1-5-21-1960408961-706699926-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\WinPosl364x616(1).left: 0x0000005A	
123 HKU\S-1-5-21-1960408961-706699226-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\WinPos1364x616(1).top: 0x0000058	
124 HKU\S-1-5-21-1960408961-706699226-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\WinPosl364x616(1).right: 0x000002FF	_
125 HK0\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\WinPosl364x616(1).bottom: 0x0000021E	
126 HKU\S-1-5-21-1960408961-706699226-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\Rev: 0x0000002	
127 HKU\S-1-5-21-1960408961-706699926-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\WFlags: 0x0000000	
128 HKU/S-1-5-21-1960408961-706699926-839522115-500/Software/Microsoft/Windows/ShellNoRoam/Bags/158/Shell/ShowCmd: 0x00000001	
129 HKU\S-1-5-21-1960408961-706699226-839522115-500\Software\Microsoft\Windows\ShellNcRoam\Bags\158\Shell\FFlags: 0x0000001	
130 HKU\S-1-5-21-1960408961-706699926-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\158\Shell\HotKey: 0x0000000	
131 HKU(S-1-5-21-1960408961-706699226-839522115-500/Software/Microsoft/Windows/Shell/NcKoam/Bags/158/Shell/Buttons: 0xFFFFFFF	
132 HKU(5-1-5-21-196404894)-/06699226-839522115-500/SOTEWare/Microsoft/Windows/ShellNckam/Bág3/158/Shell/Link3: 0X00000000	
133 HKU(5-1-5-21-190408961-706699226-839522115-500/S0TEWHICOSOTU/WHIGOWS/SAELINGKOM/SAG2/ISS/SAELINGADESS/ UKTFFFFF	
134 MRU/3-1-3-X1-1804408461-00634326-534322113-500/3012WHIGHAICOGOIC/WHIGOW3/SAEINOKOGM/Bags/258/SAEI/V/d; "(6512555-/BEI-4810-BA9H-D2/1084320E3)"	
135 hol/3-1-5-X1-1960408961-706039226-53922X115-500/3012WarteWarteWarteWarteWarteWarteWarteWarte	
136 HKU(5-1-5-21-1904048961-706699226-83952211-500/S0TEWHICOSOTU/WHICOMS/SAFILINGKOM/SAG9(155/SAFIL/SCTOLPOSI364X516(1).X: 0X0000000	
137 RAU(5-1-5-21-19040493)-/0699226-53922115-500/5074484/Mindows/ShellNokoam/58g3(155/Shell/Soroll/Sor	-
	Þ
Normal text file ength : 30,144 ines : 209 Ln : 111 Col : 123 Sel : 0 0 Windows (CR LF) UCS-2 Little Er	dian INS
🐮 Start 😥 📾 😨 🛥 🛱 🏈 🍪 🕹 🕘 🔹 CuWhDOWS byste 🛛 🗰 Command Prompt 🔄 💐 Dependency Walker 🧯 Regarbot 1.9.0 x86 U 🔂 Ci Documents and S 🛇 Process Explorer - Sy 🕅 Ci Documents and	nd 23:53



Project Exploitable XP SP3 - VMware Workstation	- 🛛 ×
File Edit View VM Tabs Help 📙 - 母 🔉 🕰 😩 🔲 🗆 🖓 🖓 🖕	
[]↓ Kali-Linux-2019.4-immare-am× []↓ Project Exploitable XP SP3 ×	
C\Documents and Settings\Administrator\Local Settings\Temp\~res-x86.bxt - Notepad++	_ 8 ×
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?	х
🔚 MSVCRTD.DLL 🗓 🗮 Copy (2) of Proof of Concept pl 以 🔚 readme bit. 🗓 📄 "Peeed66.bit 💟	
167 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNcRoam\BagMRU\10\MRUListEx: 09 00 00 00 08 00 00 02 00 00 00 07 00 00	00 06 0
168 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\10\MRUListEx: 04 00 00 00 00 00 00 00 00 00 00 00 00	00 07 0
169 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\146\Shell\MinPos1364x616(1).x: 0xFFFFFFF	
170 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\146\Shell\MinPos1364x616(1).x: 0xFFFF8300	
171 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\146\Shell\MinPos1364x616(1).y: 0xFFFFFFF	
172 HKU\5-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\146\Shell\MinPos1364x616(1).y: 0xFFFF8300	
173 HKU\5-1-5-21-1960408961-706699226-839522115-500\Software\Microsoft\Windows\ShellNORoam\Bags\146\Shell\WinPos1364x616(1).left: 0x0000002	
174 HKU\S-1-5-21-1960408961-7066999226-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\146\Shell\WinPos1364x616(1).left: 0x0000002E	
1/5 HKU(S-1-5-21-1960408961-706699922-839522115-500\Software\Microsoft\Windows\ShellNokkoam\Bags\146\Shell\Windos3364x616(1).top: (xU0000000	
1/6 HKU(3-1-5-21-1960408961-706699226-839522115-500/SOTEWare(Microsoft/Windows/ShellNokoam/Bagg/166/Shell(WinhostS64x616(1),top://www.upudous/	
1// HKU(5-1-5-21-1960408961-706699226-83952211-500/S0TEWER/MICCOSOTE/WINDOWS/ShellNokoam/Bags/146/Shell/WinHosl364X616(1).right: 0000000A/	
1/3 RU(S-1-S-21-19040891-10699226-3392211-S0U)SOTEWATE(MICONG)SALANDAS AREINKORMAN, Daga (166)SALI)WILOUISSEX016(), INIGAT: WULOUUDUDS	
1/3 RAU(3-1-3-21-1960408961-706608926-839322113-500/Software/Nicosoft/Windows/Software/Negs/140/Softwire/Softwire/Softwire/Nicosoftwi	
101 HKU-1-5-21-1500-0051-706055220-053522115-500 (Software) Microsoft (Windows (Shell McCam(Sag) (16(Shell (Windows (Software) Windows (Shell McCam(Sag) (16(Shell (Windows (Shell McCam)))))	
192 WW1\51\5211106040861_7060926522115500\Seftware\Wignard* Wignard* Wig	
HVIN S_1_S_21_J06000051 / 0000025620 00002511500 (Software/Microsoft/Windows/Software/Microsoft/United United Software/Microsoft/Windows/Software/Microsoft/Windows/Software/Microsoft/Windows/Software/Microsoft/Windows/Software/Microsoft/Windows/Software/Microsoft/Windows/Software/Microsoft/Windows/Software/Microsoft/Windows/Software/Microsoft/Windows/Software/Microsoft/Windows/Software/Microsoft/Windows/Software/Microsoft/Windows/Software/Microsoft/Windows/Software/Microsoft/Windows/Software/Microsoft/Windows/Software/Microsoft/Windows/Software/Microsoft/Windows/Software/Microsoftwar	
194 HWIS-1-5-21-196040691-7060926-93522115-500(Software(Wickows(Soft)Windows(Soft)Modam(Bage(196)Soft)(Hindows(Soft)), Withows(Soft)	
185 HKUNS-1-5-21-1960408961-706699826-839522115-500 Software/Wicrosoft/Windows/ShellNoRoaw/Barg/146/ShellNoRoa/Sde/G(d).jeft: 0x00000002E	
186 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoBoam\Bacs\148\Shell\WinDos1364x616(1).left: 0x0000005a	
187 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\WinPos1364x616(1).top: 0x0000002C	
188 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bacs\148\Shell\WinPos1364x616(1).top: 0x0000058	
189 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\WinPos1364x616(1).right: 0x000002D3	
190 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\WinPos1364x616(1).right: 0x000002FF	
191 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\WinPos1364x616(1).bottom: 0x000001F2	
192 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\WinPos1364x616(1).bottom: 0x0000021E	
193 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\155\Shell\MinPos1364x616(1).x: 0xFFFFFFF	
194 HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\155\Shell\MinPos1364x616(1).x: 0xFFFF8300	_
10 HWIN S_1_S_1_LOSAAAROSI_TASSOORDS_RROS22115_SANN SAFWERE Microsoft Windows Shell MaDaen Bare 1551 Shell WinDos1264v515(1) AVEFFFFFF	
Normal text file ength : 30,144 lnes : 209 Ln : 168 Col : 146 Sel : 0 0 Vindows (CR LF) UCS-2 Little Env	lian INS
🤹 Start 😥 🔤 🕎 🛩 🛱 🏈 🍓 🐥 🦇 🙄 C:\UDHDOWS byste 🔤 Command Prompt 🔤 Dependency Waker 🚔 Regshot 1.9.0 x86 U 💆 C:\Documents and S 👰 Process Explorer - Sy 🔐 C:\Documents and	d 23:53
To direct input to this VM, move the mouse pointer inside or pross Ctoly G	5 4

ø	Project Exploitable XP SP3 - VMware Workstation	- o ×
File	Edit View VM Tabs Help 📙 - 믑 💭 🕰 🕰 💭 🛄 🖸 🖓 - 🖓	
	dal-Inux-2019.4+vmware-am×	
💓 C:	\Documents and Settings\Administrator\Local Settings\Temp\~res-x86.txt - Notepad++	_ 8 ×
File	Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?	Х
M	SVCRTD DLL 🖸 🗮 Capy (2) of Proof of Concept pl 🗵 🗮 readine bd 🗵 📄 "resv86 bd 🖸	
182	HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bacs\148\Shell\MinPos1364x616(1).x: 0xFFFF8300	
183	HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\MinFos1364x616(1).y: 0xFFFFFFF	_
184	HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\MinPos1364x616(1).y: 0xFFFF8300	
185	HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\WinPos1364x616(1).left: 0x0000002E	
186	HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\WinPos1364x616(1).left: 0x0000005A	
187	HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\WinPos1364x616(1).top: 0x0000002C	
188	HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\WinPos1364x616(1).top: 0x00000058	
189	HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\WinPos1364x616(1).right: 0x000002D3	
190	HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\WinPos1364x616(1).right: 0x000002FF	
191	HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\WinFos1364x616(1).bottom: 0x000001F2	
192	HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\148\Shell\WinPos1364x616(1).bottom: 0x0000021E	
193	HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\155\Shell\MinPos1364x616(1).x: 0xFFFFFFF	
194	HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\155\Shell\MinFos1364x616(1).x: 0xFFFF8300	
195	HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\155\Shell\MinPos1364x616(1).y: 0xFFFFFFF	
196	HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\155\Shell\MinPos1364x616(1).y: 0xFFFF8300	
197	HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\92\Shell\WinPos1364x616(1).left: 0x00000044	
198	HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\92\Shell\WinPos1364x616(1).left: 0x0000005A	
199	HKU\S-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\92\Shell\WinPos1364x616(1).top: 0x0000042	
200	HXU\S-1-5-22-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNGRoam\Bags\92\Shell\WinPosl364x616(1).top: 0x0000058	
201	HKU\5-1-5-21-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\92\Shell\WinPosl364x616(1).right: 0x00000259	
202	HUU\S-1-5-22-1960408961-706699826-839522115-500\Software\Microsoft\Windows\ShellNoRoam\Bags\92\Shell\WinPosl364x616(1).right: 0x000002FF	
203	HUU/S-1-5-22-1960408961-706699826-83952215-500/SoftWare/Microsoft/Windows/SneliNokoam/Bags/92/Sneli/WinPosi364x616(1).Dottom: 0X00000208	
209	HK0/2-1-2-21-1260408361-706633876-833255112-200/201fMare/Microsoft/Windows/2061100Kogm/Bags/32/20611/WinPos1364%616(1).DOffom: 0X0000021F	
205		_
200		
207	Iblai Changes: 156	
200		
205		•
		Þ
Norma	I text file ength : 30,144 lines : 209 lin : 194 Col : 134 Sel : 0 0 Windows (CR LF)	UCS-2 Little Endian INS
📇 SI	tart 📴 🗃 🖉 🛥 🛱 🎉 🥹 📣 — " 🗀 C:\/UDNDWS/syste 🔤 Command Prompt 🔄 🔩 Dependency Walker 👞 Registrot 1.9.0 x86 U 🟠 C:\Documents and S 🐊 Process Explorer - Sy 😭 C:\D	ocuments and 23:54
-		