

## **Lab 6 – Static Malware Analysis**

Sai Sasaank Srivatsa Pallerla

University of Maryland, Baltimore County

Presented to: Gina Scaldaferri

Date: 10/29/2019

## About the Lab

BinText is a file text scanner / extractor that helps find character strings buried in binary files. The program can extract text from any kind of file and display plain ASCII text, Unicode (double byte ANSI) text, as well as Resource strings. Additional useful information for each item is included in the "Advanced" mode. Uniquely, the program will show both the file offset and the memory offset of each string found.

IDA Pro is primarily a multi-platform, multi-processor dis-assembler that translates machine executable code into assembly language source code for purpose of debugging and reverse engineering. It can be used as a local or as a remote debugger on various platforms. Plug-ins can be developed and supports a variety of executable formats for different processors and operating systems.

VirusTotal aggregates many antivirus products and online scan engines to check for viruses that the user's own antivirus may have missed, or to verify against any false positives. Anti-virus software vendors can receive copies of files that were flagged by other scans but passed by their own engine, to help improve their software. Users can also scan suspect URLs and search through the VirusTotal dataset

### 1. Analysis of Suspicious Executable

1. What release version of Putty does this executable contain?

Putty Version: 0.63.0.0

**LairNetPutty.exe Properties**

General Compatibility Security Details Previous Version

Property Value

Description

File description SSH, Telnet and Rlogin client

Type Application

File version **0.63.0.0**

Product name PuTTY suite

Product version Release 0.63

Copyright Copyright © 1997-2013 Simon Tatham.

Size 504 KB

Date modified 4/26/2017 9:14 PM

Language English (United Kingdom)

Original filename PuTTY

[Remove Properties and Personal Information](#)

OK Cancel Ready AN: 4112 UN: 126 RS: 0 versio

Type here to search

**Advanced view**

File pos	Mem pos	ID	Text
00000007D5C0	0000004831C0	0	TORT OR OTHERWISE
00000007D634	000000483234	0	CONNECTION WITH 1
00000007D6A4	0000004832A4	0	OTHER DEALINGS IN
00000007D7A0	0000004833A0	0	VS_VERSION_INFO
00000007D7FC	0000004833FC	0	StringFileInfo
00000007D820	000000483420	0	08090480
00000007D838	000000483438	0	CompanyName
00000007D852	000000483452	0	Simon Tatham
00000007D874	000000483474	0	ProductName
00000007D88E	00000048348E	0	PuTTY suite
00000007D8AC	0000004834AC	0	FileDescription
00000007D8CE	0000004834CE	0	SSH, Telnet and Rlogin
00000007D910	000000483510	0	InternalName
00000007D92A	00000048352A	0	PuTTY
00000007D93C	00000048353C	0	OriginalFilename
00000007D95E	00000048355E	0	PuTTY
00000007D970	000000483570	0	FileVersion
00000007D98A	00000048358A	0	Release 0.63
00000007D9AC	0000004835AC	0	ProductVersion
00000007D9CA	0000004835CA	0	Release 0.63
00000007D9EC	0000004835EC	0	LegalCopyright
00000007DA20	000000483620	0	1997-2013 Simon Tatham
00000007DA58	000000483658	0	VarFileInfo
00000007DA78	000000483678	0	Translation
00000000004D	00000040004D	0	This program cannot be run in DOS mode
0000000000E0	0000004000E0	0	Rich...
0000000001F0	0000004001F0	0	.text
000000000218	000000400218	0	.idata
00000000023F	00000040023F	0	@.data
000000000268	000000400268	0	.rsrc
00000000028F	00000040028F	0	@.text
0000000002B8	0000004002B8	0	.idata
0000000002E0	0000004002E0	0	.rsrc
000000000513	000000401113	0	YYu.9]
000000000552	000000401152	0	VhLwE
000000000560	000000401160	0	YYu.9]

2. What email addresses are contained in relation to an encryption cipher?

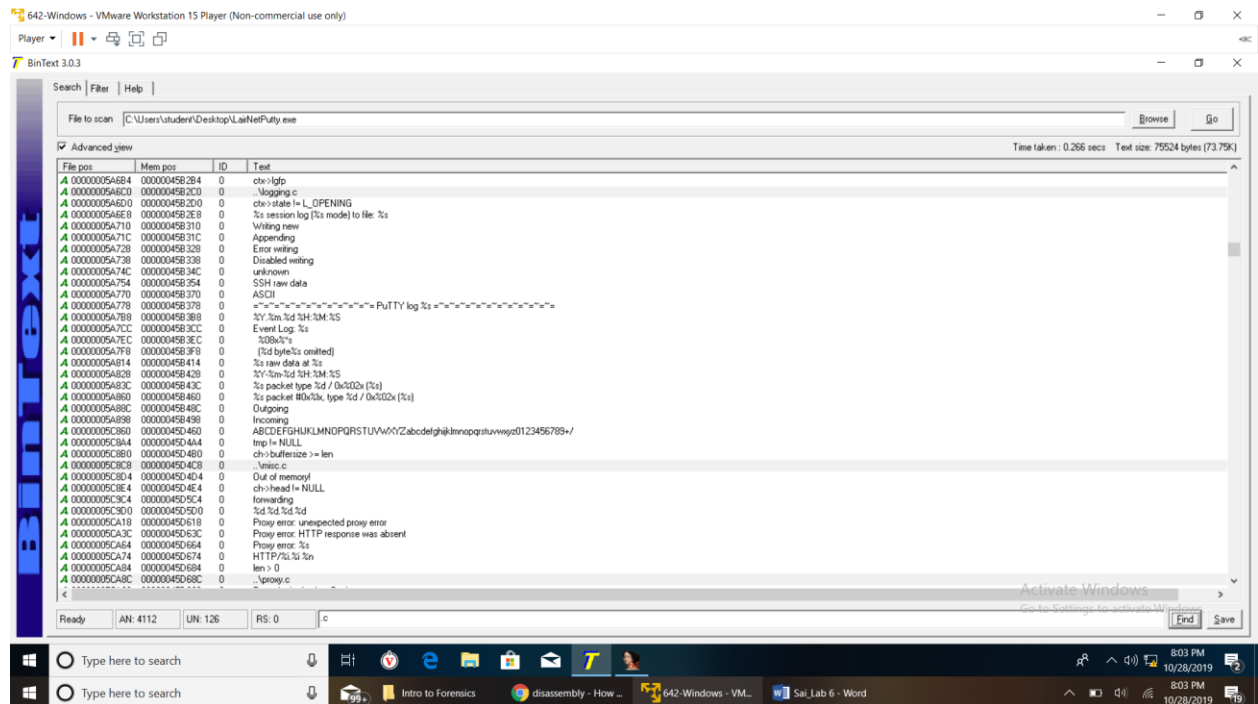
[zlib@openssh.com](mailto:zlib@openssh.com)

[des-cbc@ssh.com](mailto:des-cbc@ssh.com)

[auth-agen@openssh.com](mailto:auth-agen@openssh.com)

3. What programming language does this executable appear to be based on?

Upon examining the stings in putty.exe we can see many file with '.c' extension which implies that the language putty was written in is C.



4. What are some function names used within the executable? Do any appear to be malicious?

Functions used with the executable:

- GetDC
- DestroyWindow
- GetSysColor
- CreateWindowExA
- Shadow Window
- PlaySoundAC
- losePrinter
- GetOpenFileNameA and so on

Few functions that look suspicious are: GetProcAddress, GetKeyboardState

## 5. What are some Windows DLLs that are referenced?

Window DLLs that are referred are:

- User32
- Kernel32
- WinMM
- WinSpool
- Comdlg32
- Ole32
- Advapi32
- Gdi32

## 1.2. Analysis of Suspicious Executable

### 1. Does the executable appear to be malicious?

46 out of 69 antivirus software found the executable to be malicious. They identifies it as a Trojan.

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
Ad-Aware	Win32/Rozena.B	AegisLab	Trojan.Win32.Generic.ILEe
AhniLab-V3	Win-Trojan/Swrotr	ALYac	Win32/Rozena.B
Arcabit	Win32/Rozena.B	Avast	Win32/Swrotr-I [Trj]
AVG	Win32/Swrotr-I [Trj]	Avira (no cloud)	TR/Patched.Gen
BitDefender	Win32/Rozena.B	CAT-QuickHeal	Trojan.DorvPMF.5608193
ClamAV	Win.Trojan.MSShellcode-6360726-0	Comodo	TrojWare.Win32.Swrotr.DA@5rgp0d
CrowdStrike Falcon	Win/malicious_confidence_100% (D)	Cyberrason	Malicious/236eb0
Cylance	Unsafe	Cyren	W32/S-d32c59baEldorado
DrWeb	Trojan.Swrotr.10	Emsisoft	Win32/Rozena.B (B)
Endgame	Malicious (high Confidence)	eScan	Win32/Rozena.B

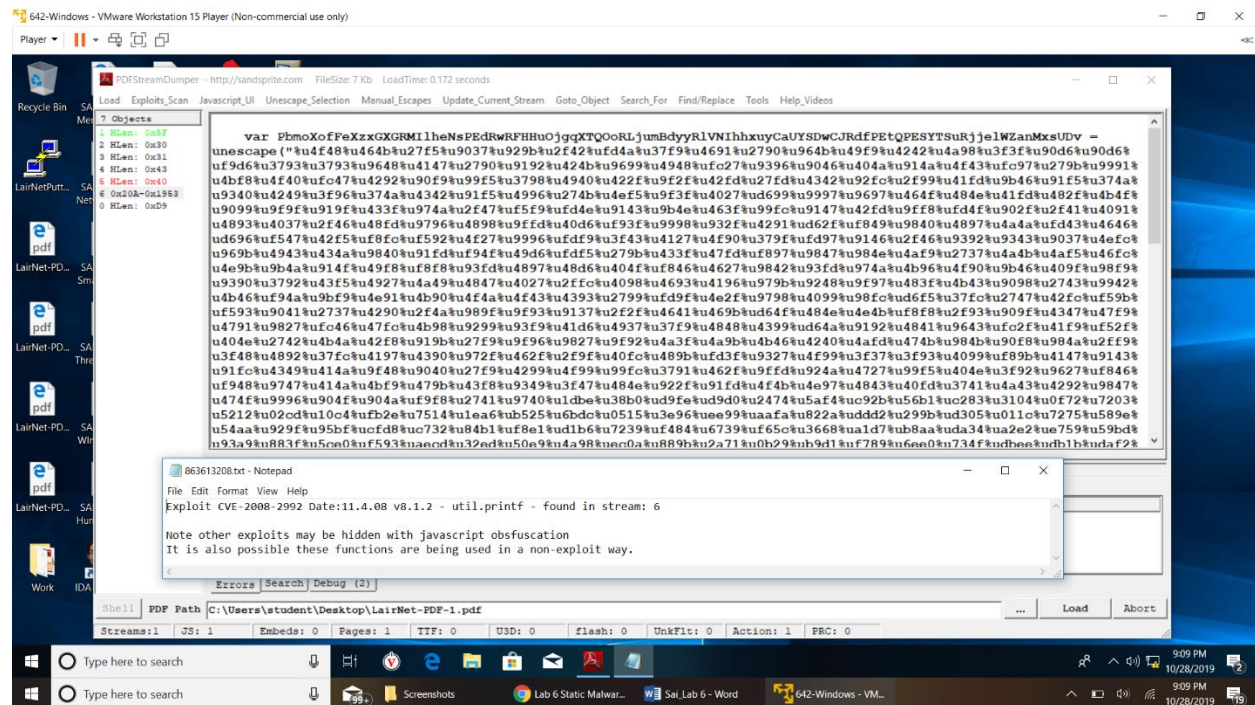
### 2. Based on the analysis, what does it appear this executable appears to be?

Based on the analysis done by virustotal the executable appears to be a Trojan.

## 2. Analysis of Suspicious PDFs

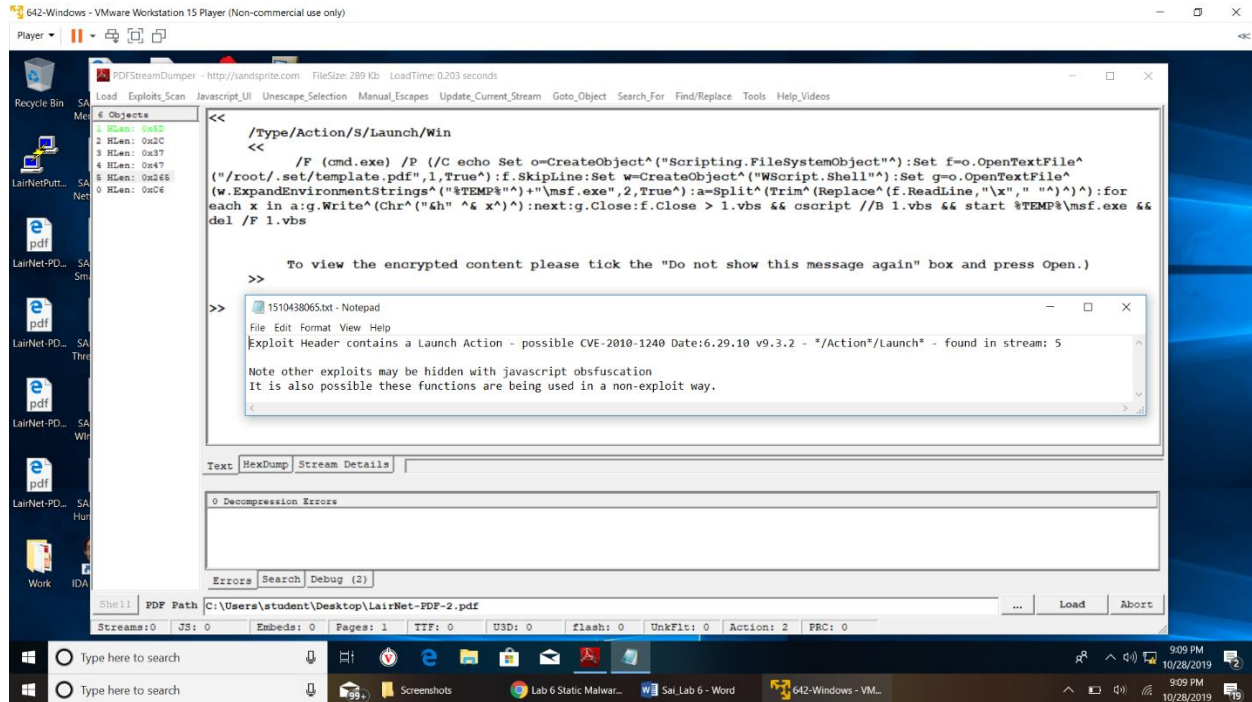
PDF Stream Dumper is a specialized tool for dealing with obfuscated javascript, low level pdf headers and objects, and shellcode. In terms of shellcode analysis, it has an integrated interface for libemu sctest. It is a self-contained program that runs on Microsoft Windows and contains a convenient graphical user interface.

### Exploits found in PDF-1

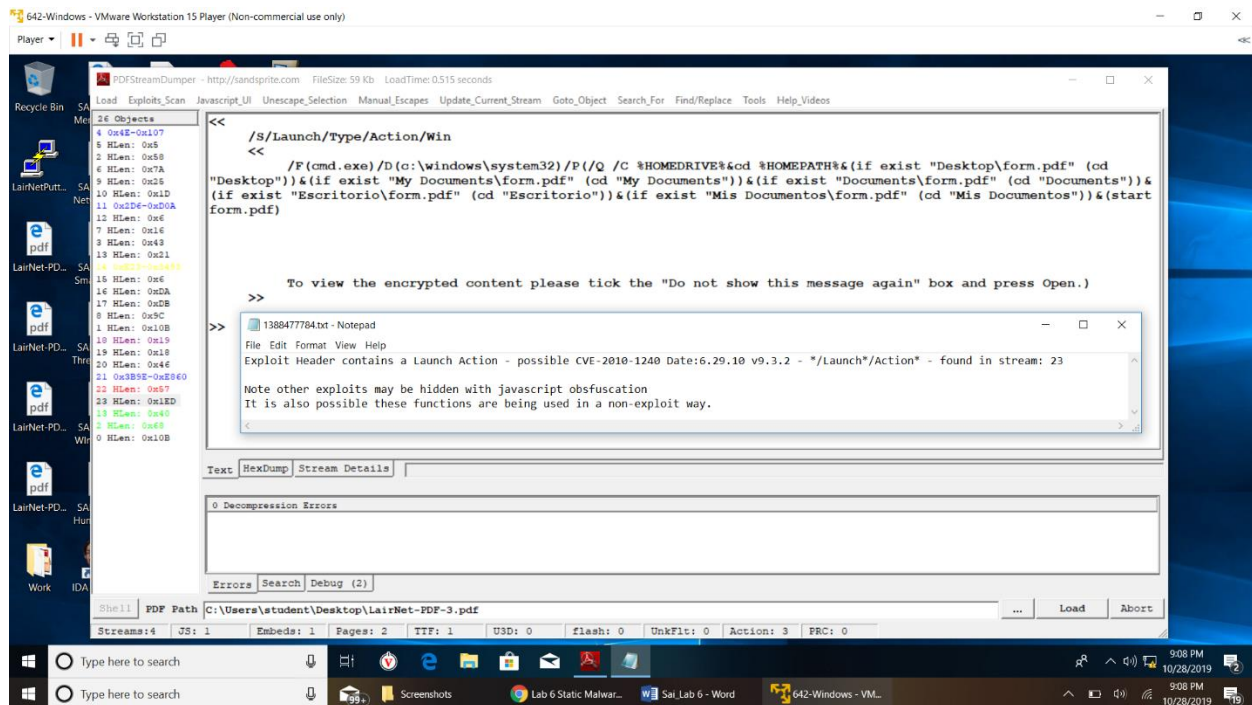




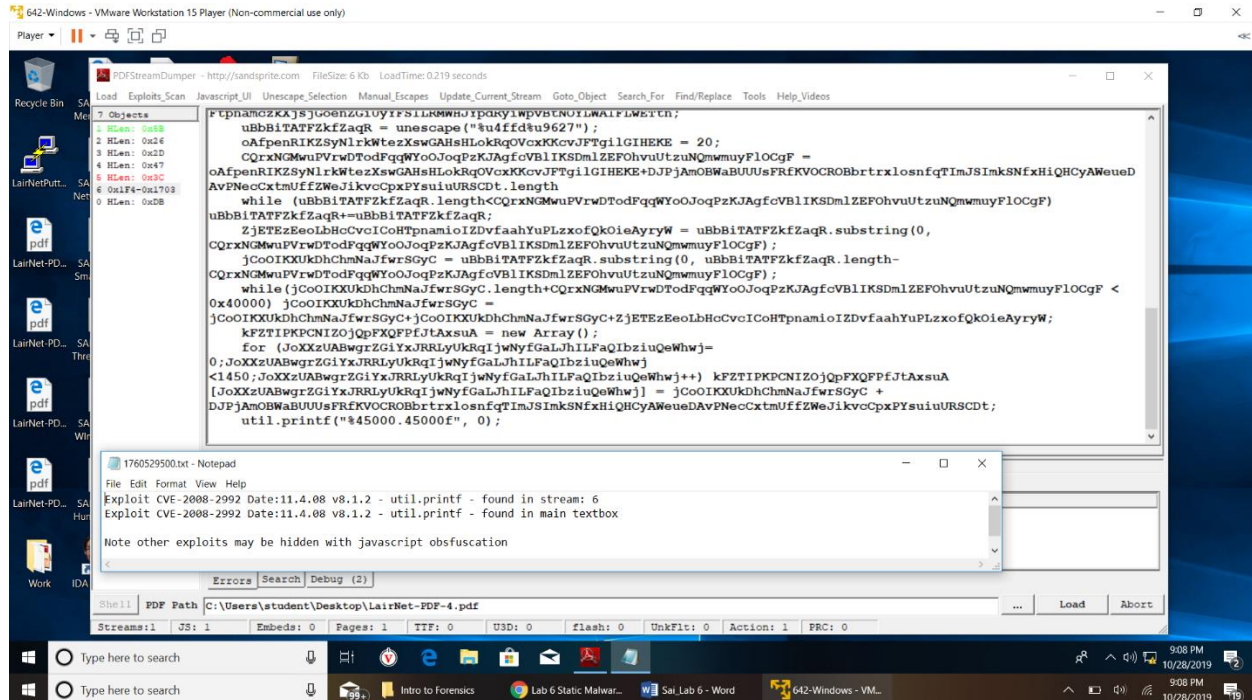
## Exploits found in PDF-2



## Exploits found in PDF-3



## Exploits found in PDF-4



## Conclusion

In this lab we learn how to explore strings section in an executable file to find more information about the file like, what dlls are used in the file, what function in from dlls are used, extracting mail IDs and other human readable strings. We learn how to use Virus Total to scan file and check if they are malicious. We also learn how to use PDF Stream Dumper to scan pdfs and check if they are malicious and find what exploit they are using to perform the malicious action.