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.

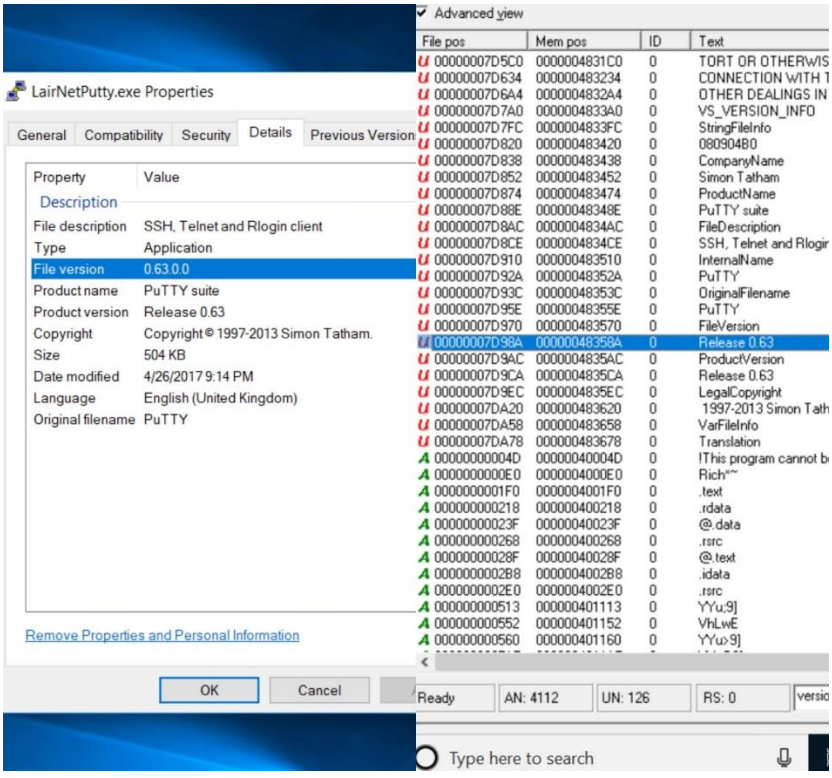
IDA Pro is primarily a multi-platform, multi-processor dis-assembler that translates machine executable code into assembly language source code for purpose of debugging and reverse engineering. It can be used as a local or as a remote debugger on various platforms. Plug-ins can be developed and supports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



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

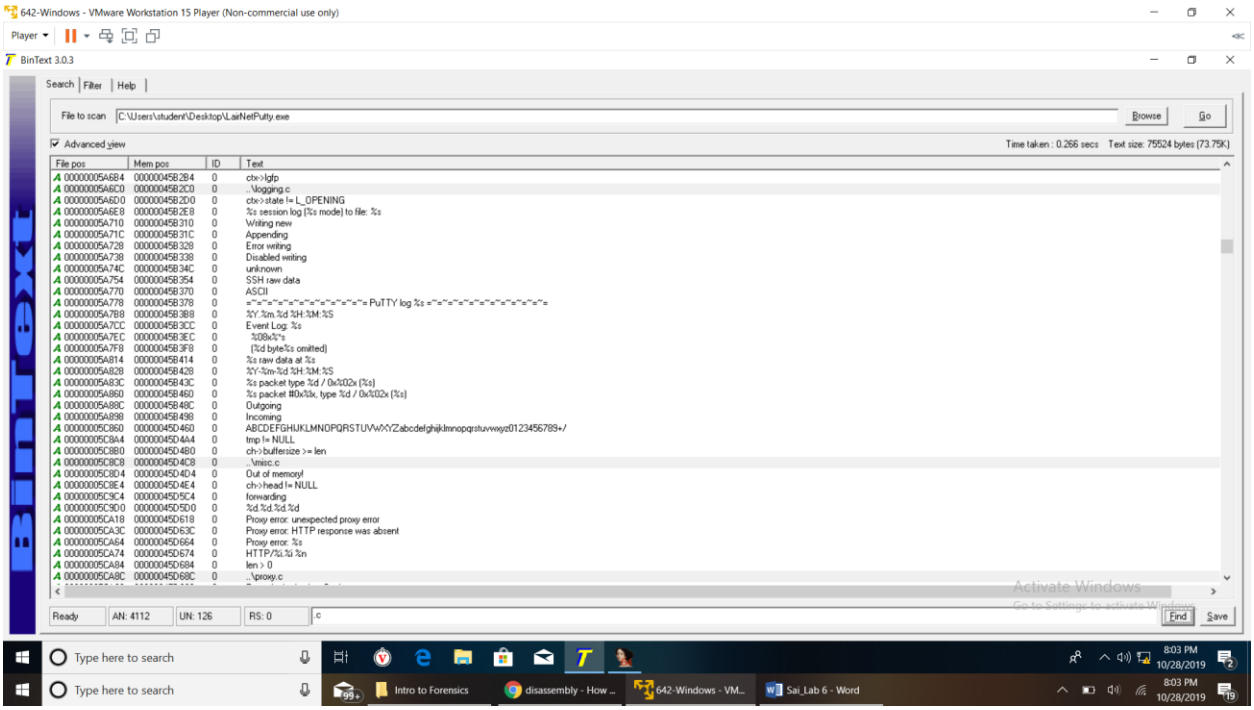
   zlib@openssh.com

   des-cbc@ssh.com

   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?

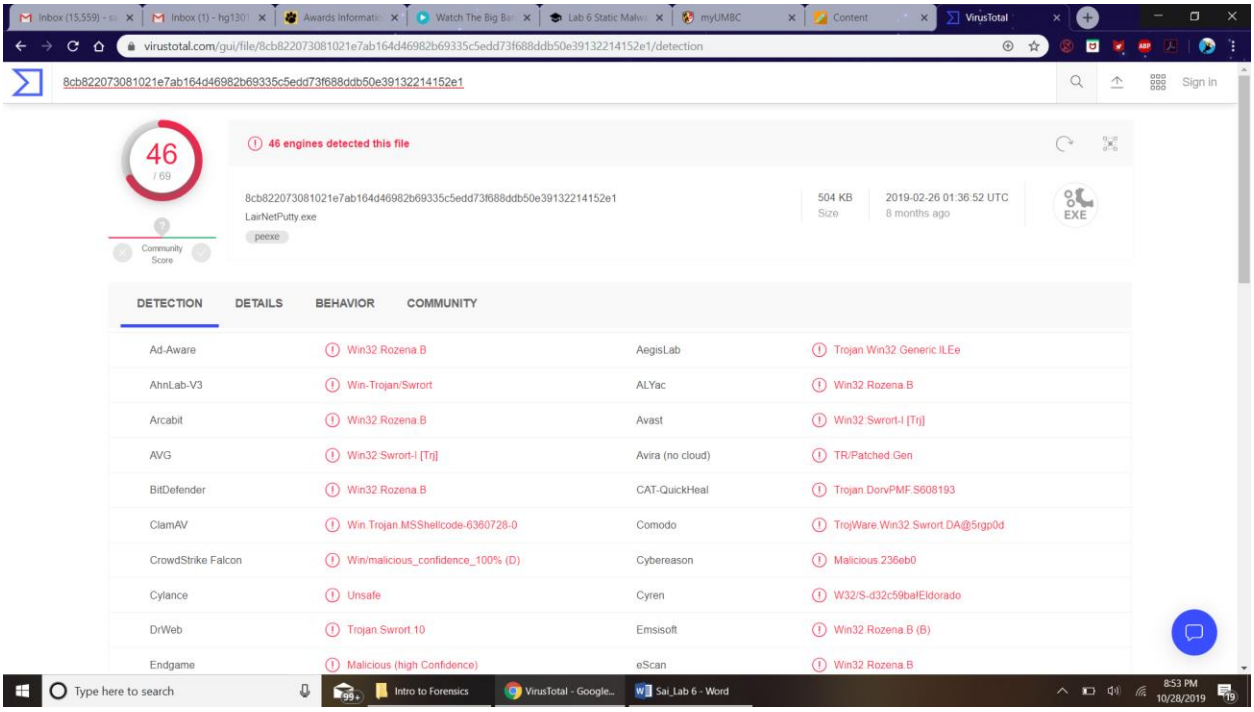
   Window DLLs that are referred are:

   - 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.



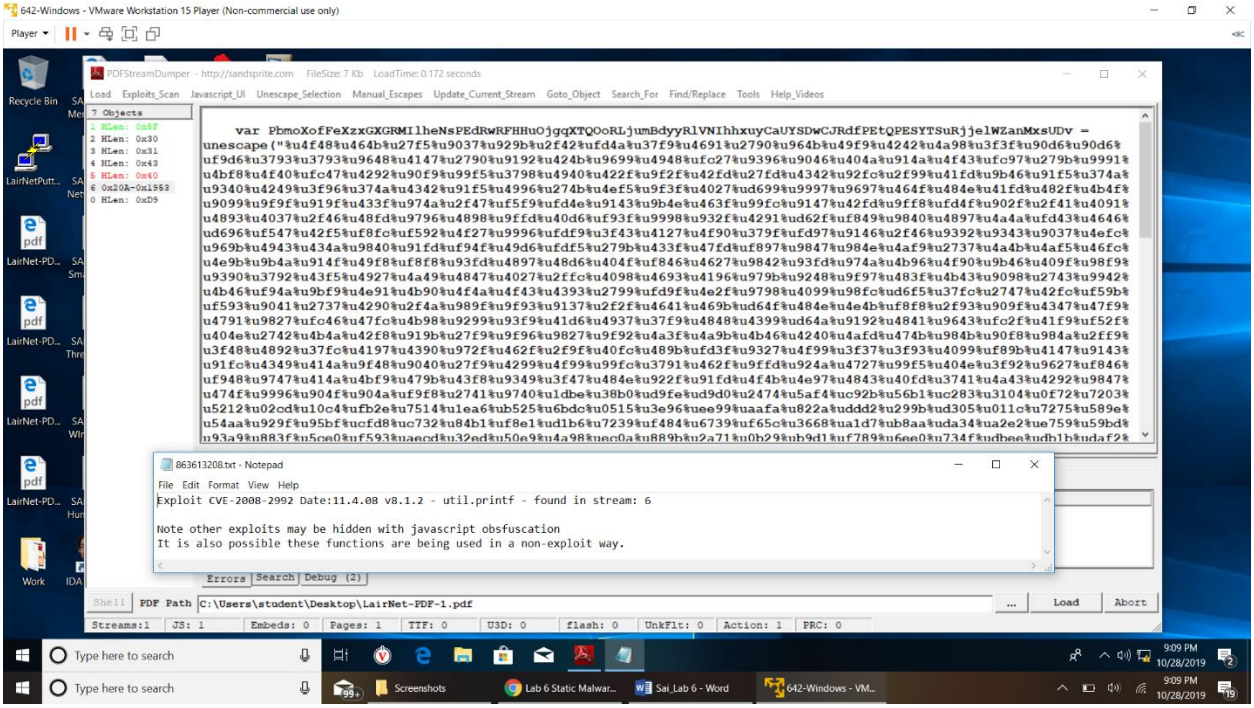
2. Based on the analysis, what does it appear this executable appears to be?

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

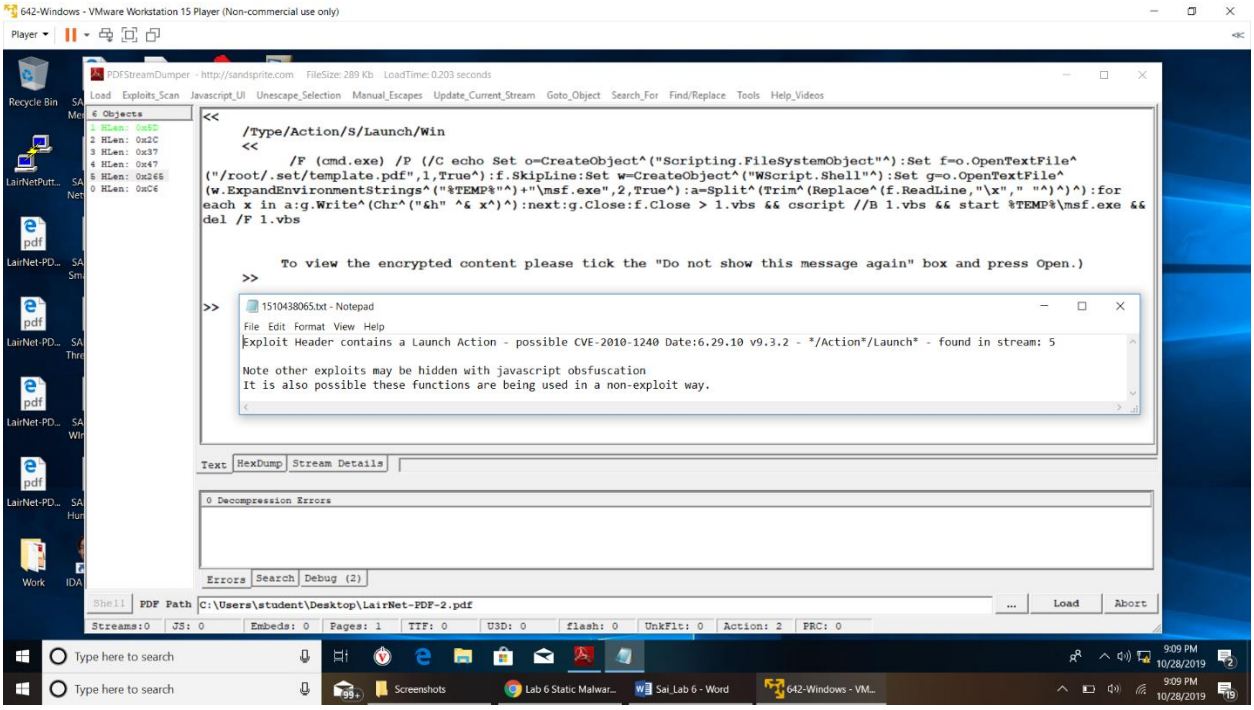
2. Analysis of Suspicious PDFs

PDF Stream Dumper is a specialized tool for dealing with obsfuscated 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.

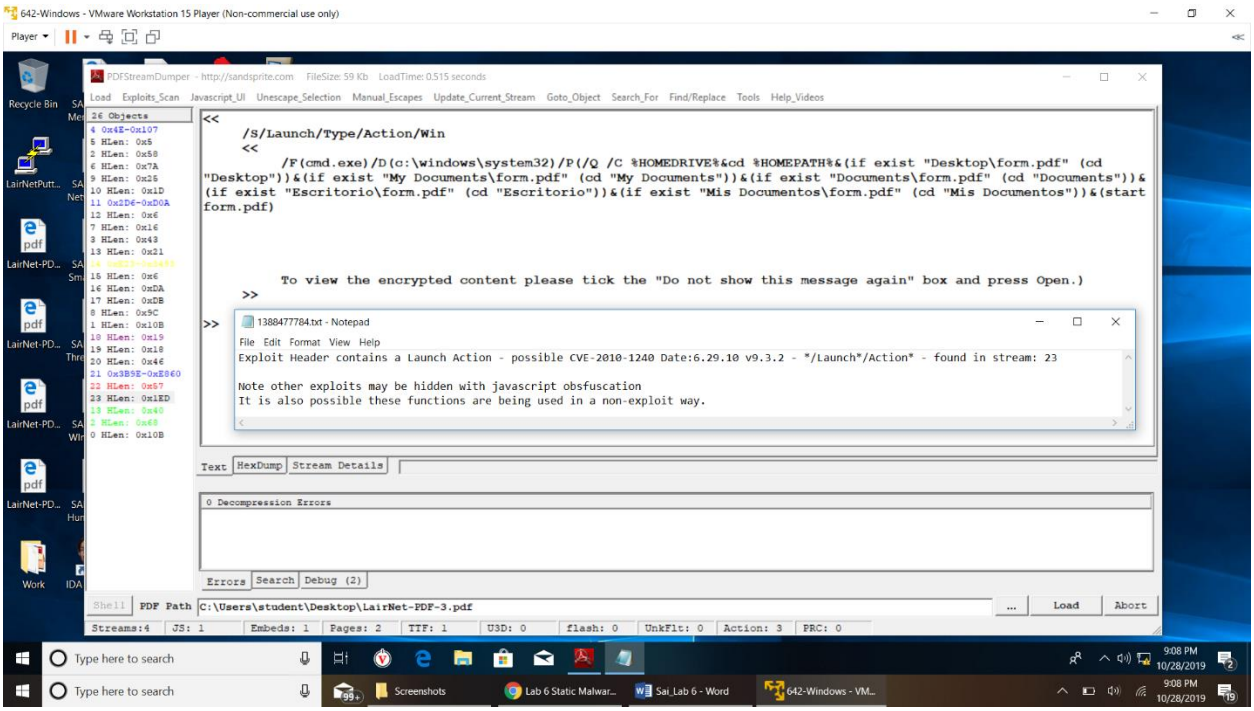
Exploits found in PDF-1



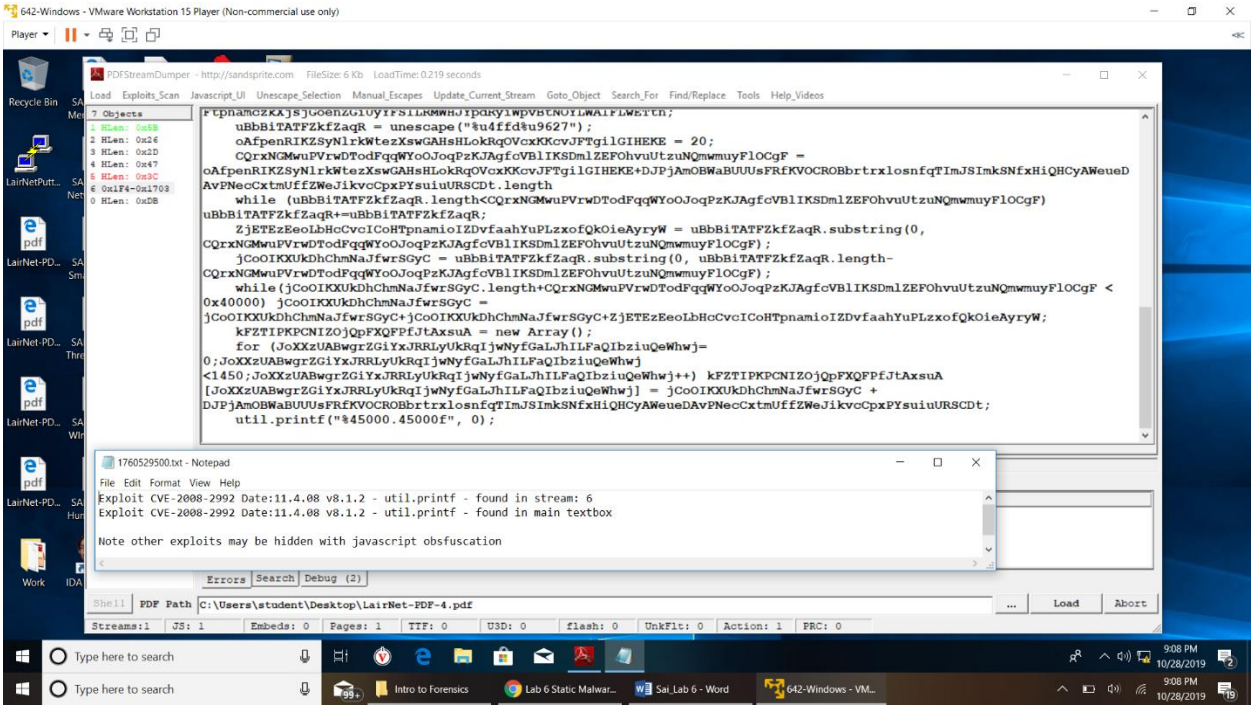
Exploits found in PDF-2



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.