Lab 11 – Creating and Using IOCs

Shrutika Joshi

University of Maryland Baltimore County

Presented To – Gina Marie

Date – 13th Aug 2023

Introduction

Create a list of indicators of compromise using the Mandiant's IOC editor specific to a malicious application 'LairNetPutty' in order to share as well as use this as an artifact across the organization for additional victims. After creating the IOC list, use this list to search for attributes of LairNetPutty malicious application.

Pre-Lab

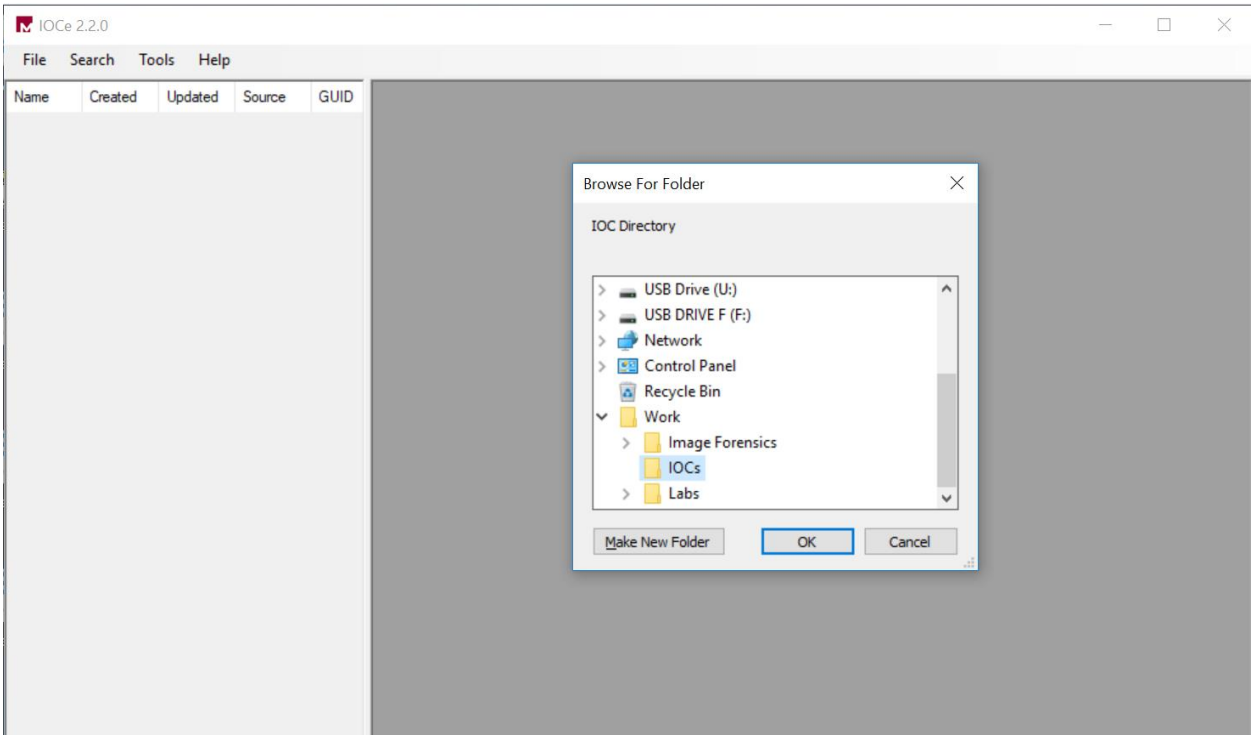
For this lab, we will be using Windows VM, Mendiant's IOC Editor to create an IOC list of LairNetPutty malicious applications, and the Redline tool to further search attributes of malicious application LairNetPutty.

Analysis

1. Creating an Indicator of Compromise

Using Mandiant's IOC Editor, create a new working directory somewhere on your desktop. I have created IOCs directory under path C:\Users\student\Desktop\Work\IOCs.

What is Mandiant's IOC Editor - The Mandiant IOC Finder is a free tool that collects data from a host and checks it against an Indicator of Compromise (IOC). The tool can also be used to search other endpoints. [2] (Mandiant, 2015)



Within the application, choose File → New → Indicator

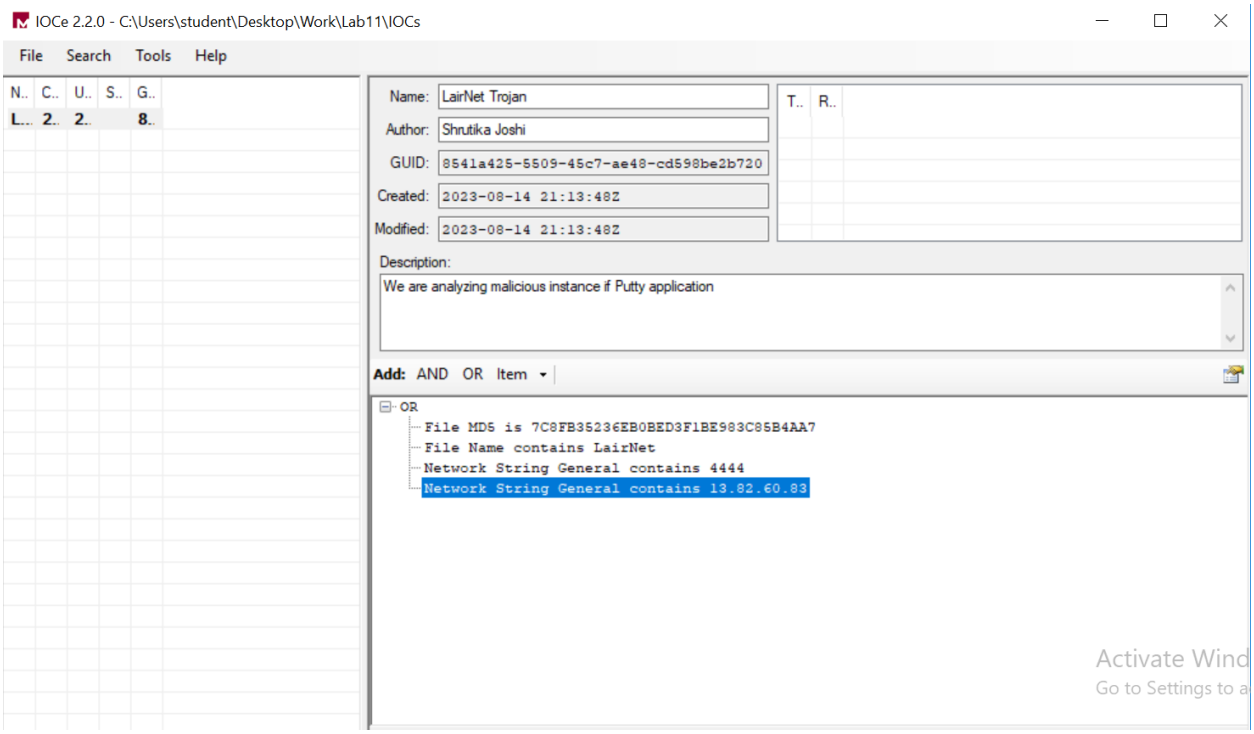
Fill out the Name and Author portion of the IOC header, then below, start adding indicator values related to the LairNetPutty.exe file we started to investigate in Week 1.

What is Putty application - PuTTY is an SSH and telnet client, developed originally by Simon Tatham for the Windows platform. It provides a text user interface to remote computers running any of its supported protocols, including SSH and Telnet. [1] (Erfan, 2021)

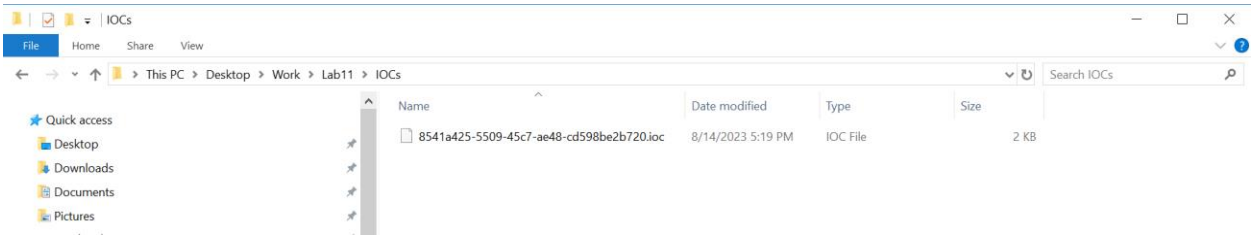
I have filled out the details below:

Name – LairNetPutty IOCs, I have added all the IOCs details which detected during Lab week 1.

After that I have saved the file.



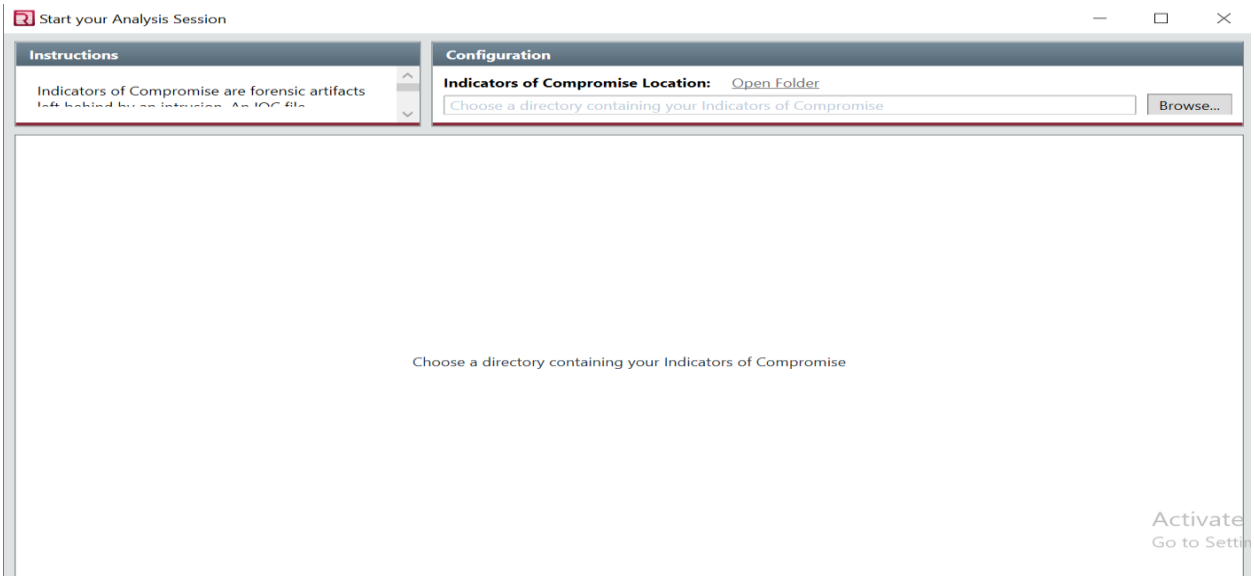
Save this file into your IOC directory.



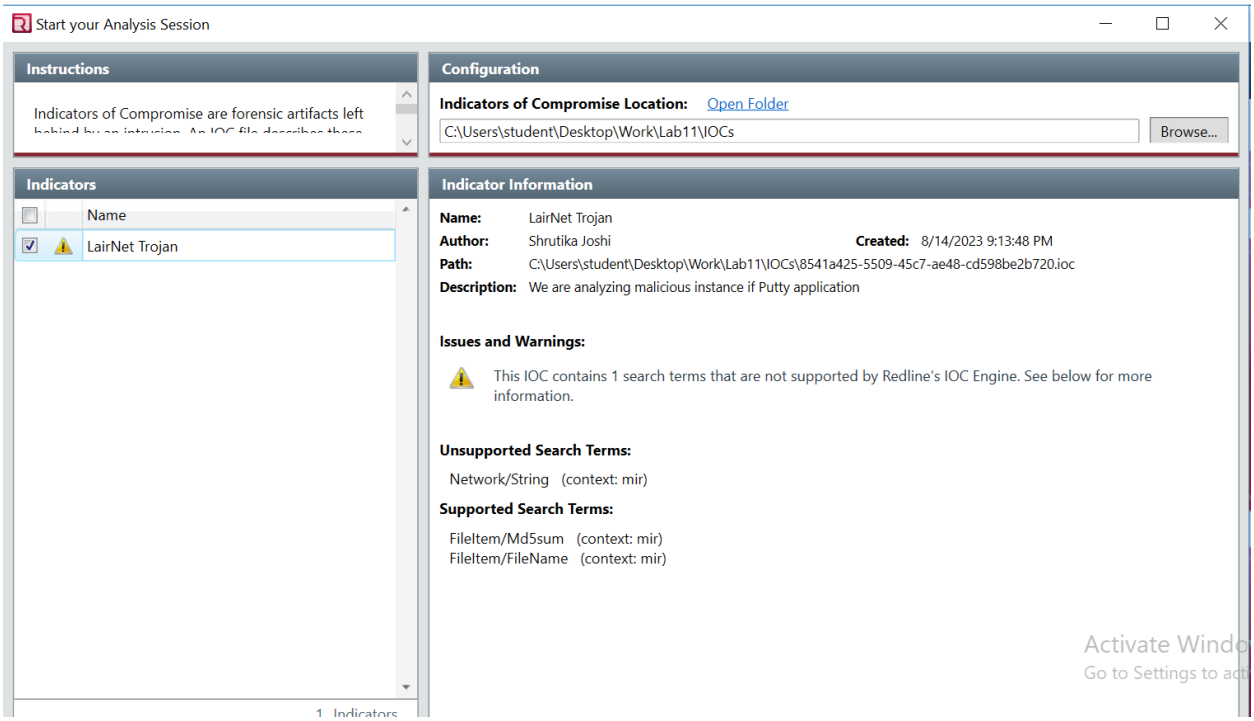
2. Using an Indicator of Compromise

Using Mandiant's Redline application, create a new IOC Search Collector, and point it to the directory you've saved your IOC from above

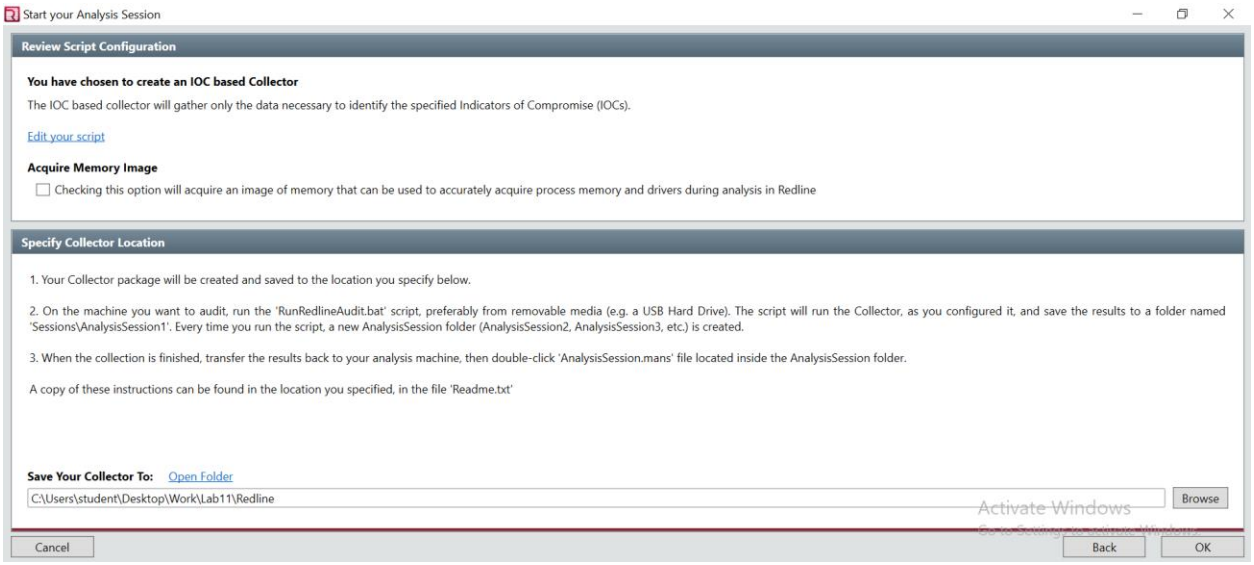
What is Redline tool - Using Redline, you can analyze a potentially compromised endpoint through the memory dump, including various file structures. With a nice-looking GUI (Graphical User Interface) – you can easily find the signs of malicious activities. [3] (Motasem, n.d.)



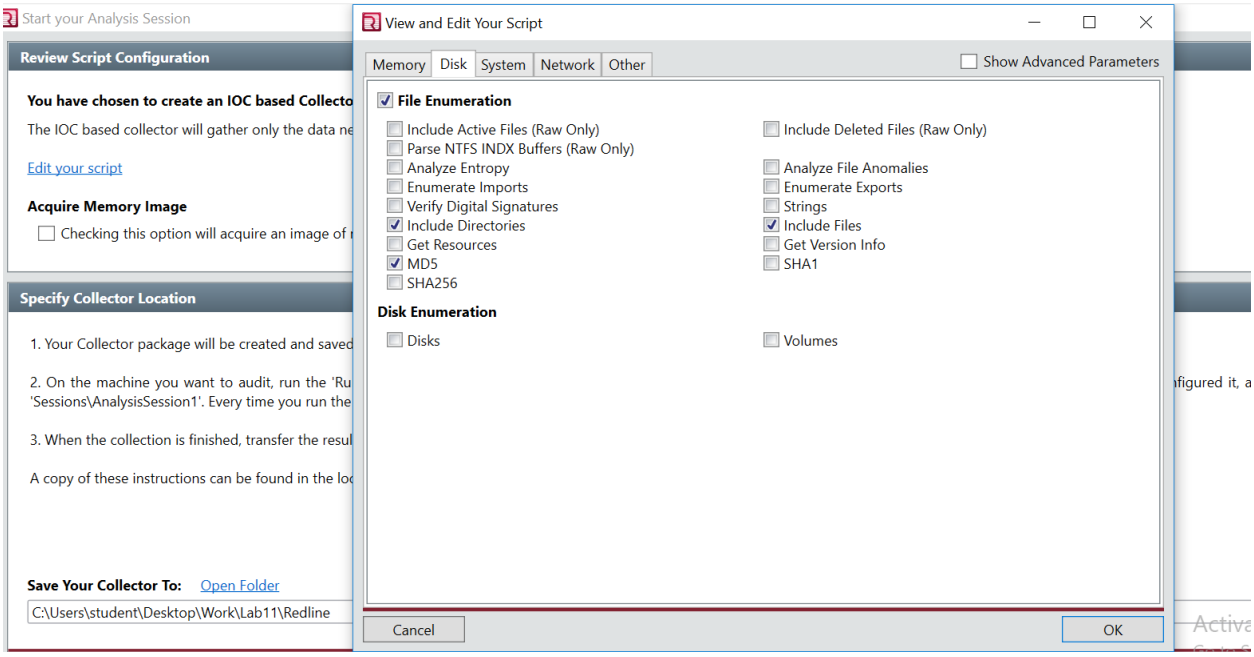
I have chosen the IOC directory as a location for Indicators of Compromise. Now after selecting indicators from the left tab, I could see all the details including Unsupported and supported terms, creation date and filename.



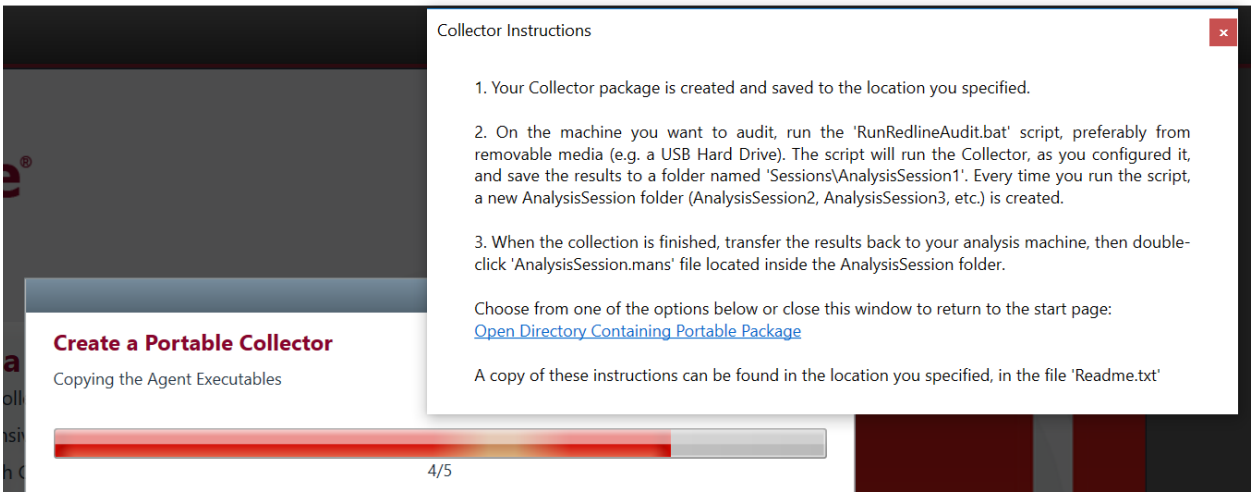
Click on "Edit Script" to make a note of what the application has decided to capture based on the IOCs you created in your file. Make sure they align.



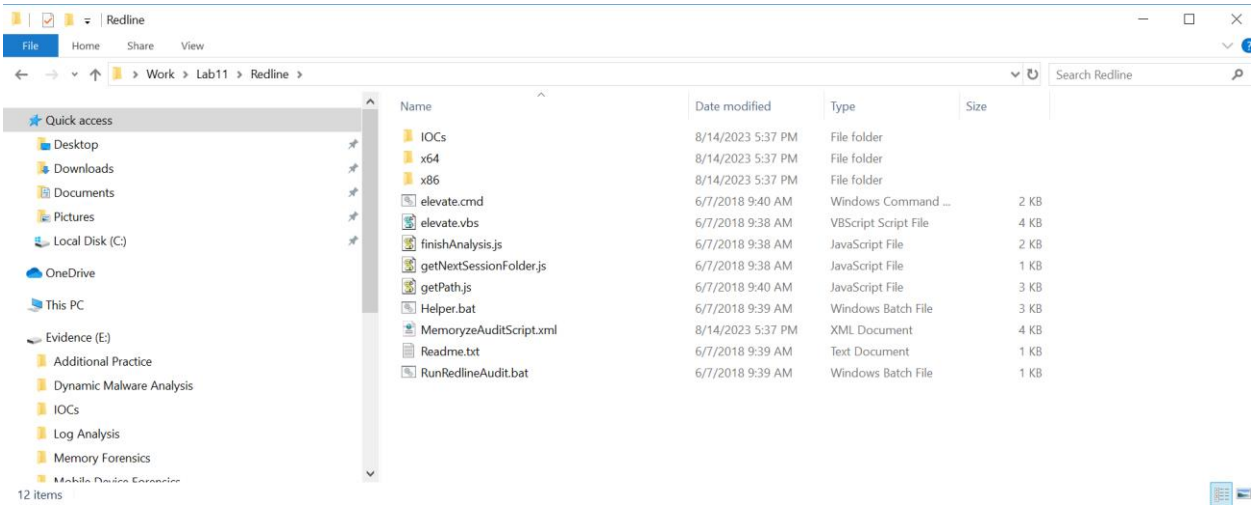
Below are the details of IOC which Redline tool have captured.



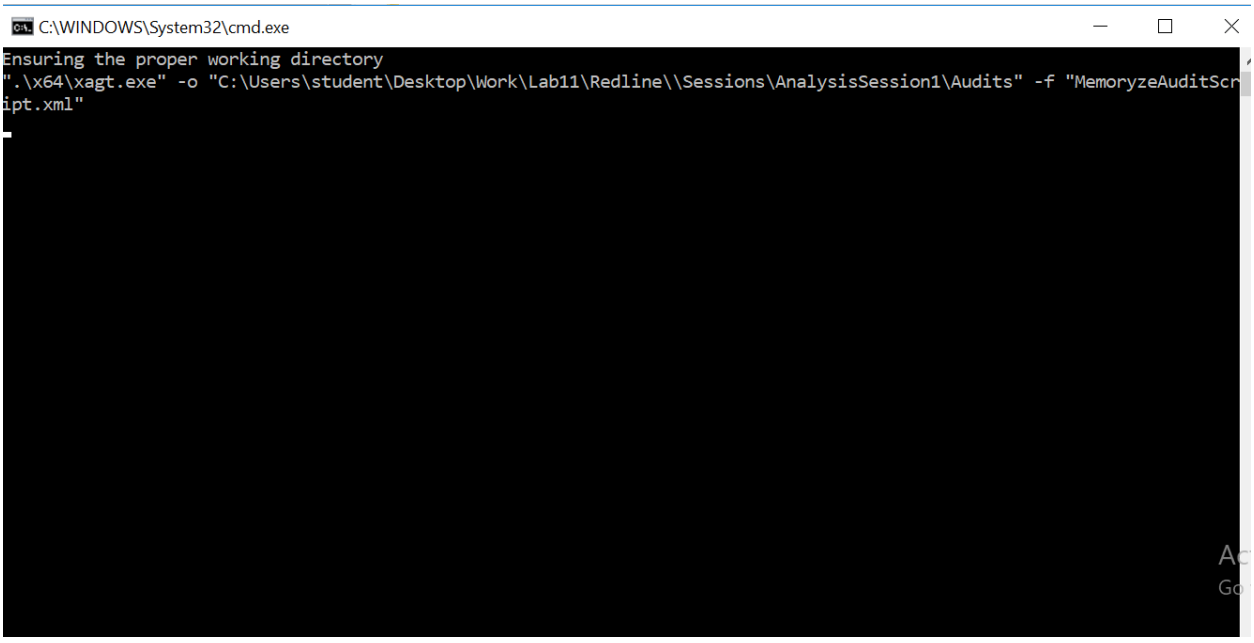
Save your collector script to a new directory, such as "Redline" under your work folder on your desktop. After saving the script one window popup which contains all the instructions.



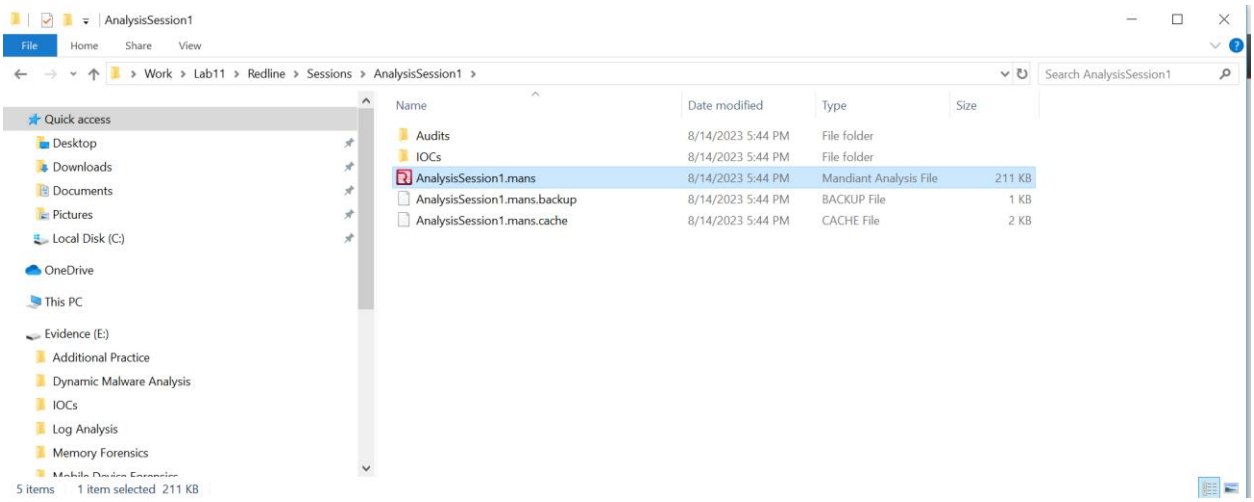
After the Collector Script is created, navigate to the Redline directory and doubleclick the "RunRedlineAudit.bat" file.

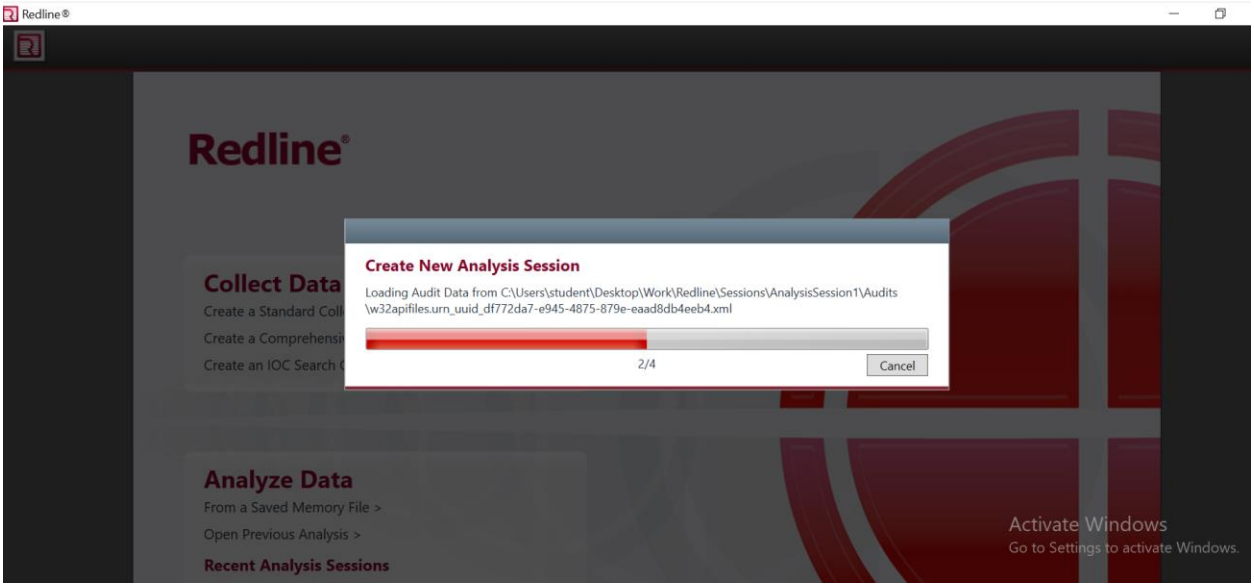


After double-clicking the "RunRedlineAudit.bat" file, I could see a script file running in the background.

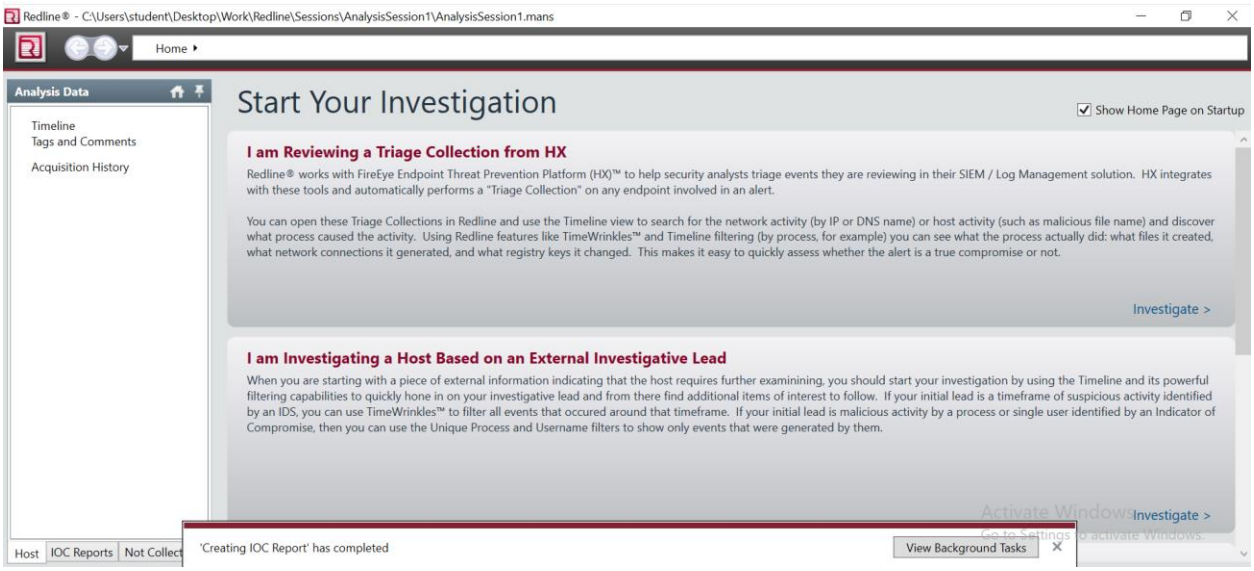


After it's run (should only take a few seconds-minutes depending on how many indicators you create), open the Sessions folder and double click on AnalyzeSession#.mans file to open it in Redline.



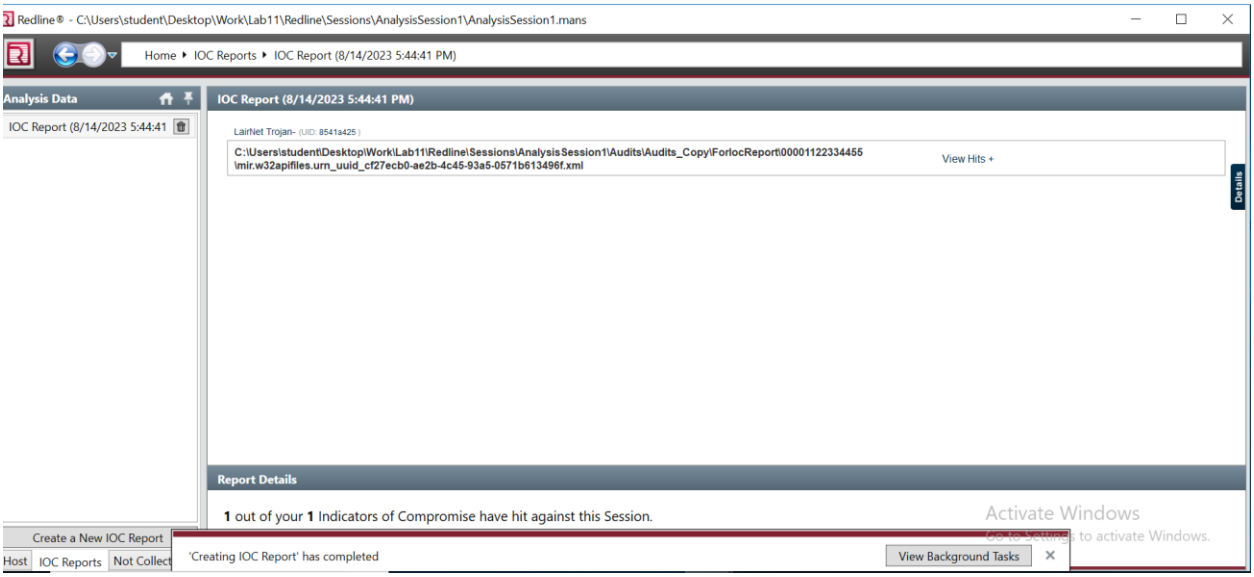


On the left side of the Redline application, click on the IOC Report tab to review the results of the search against your IOC file.

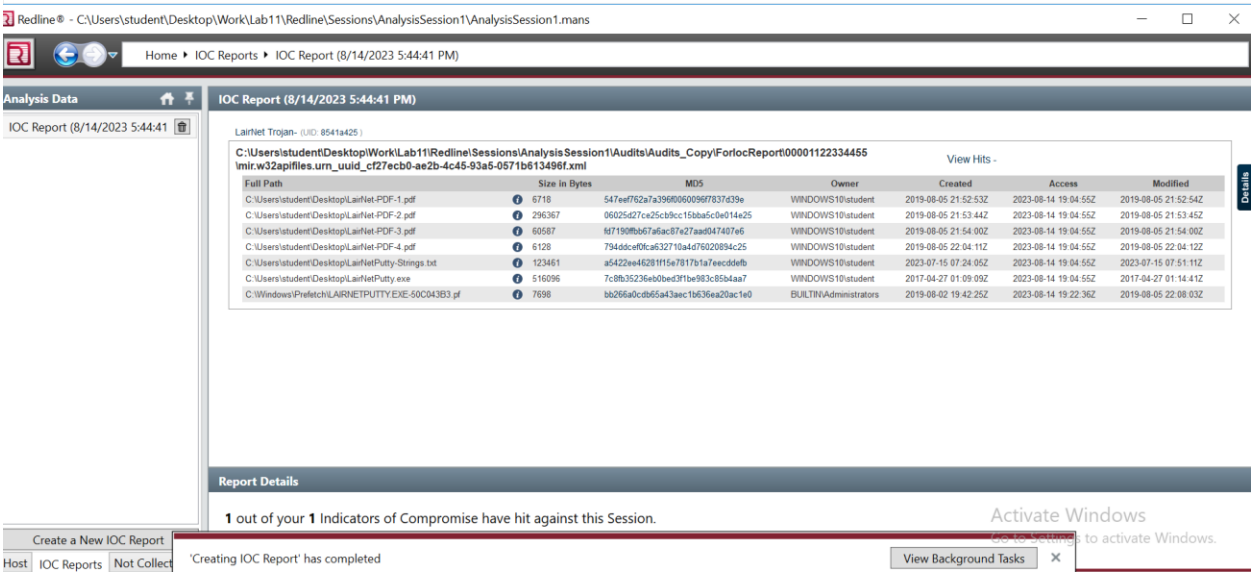


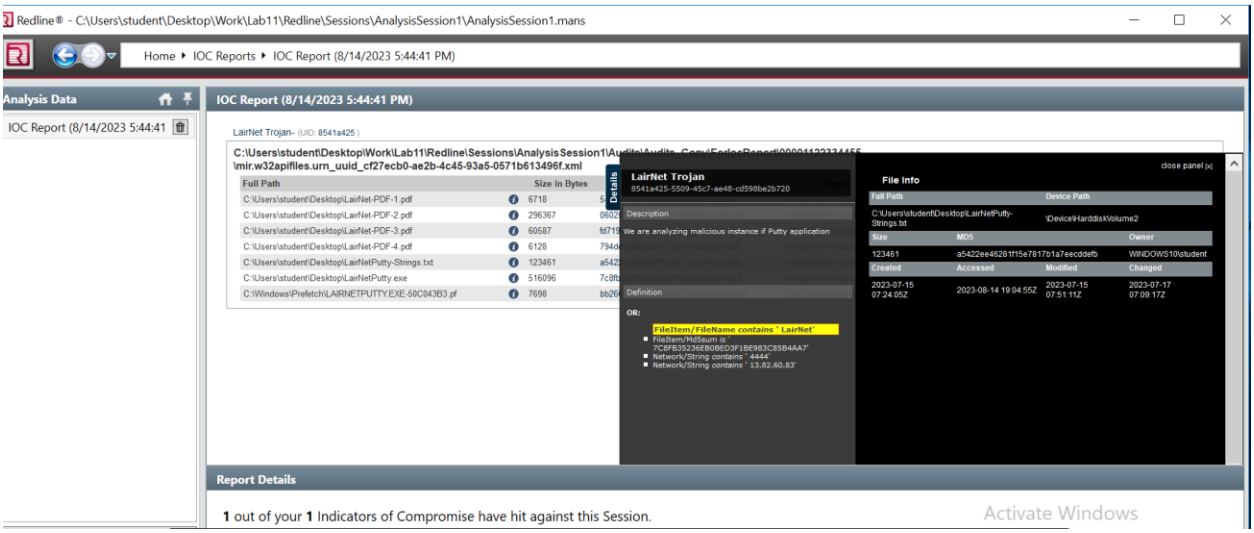
Were you able to detect the suspicious LairNetPutty application?

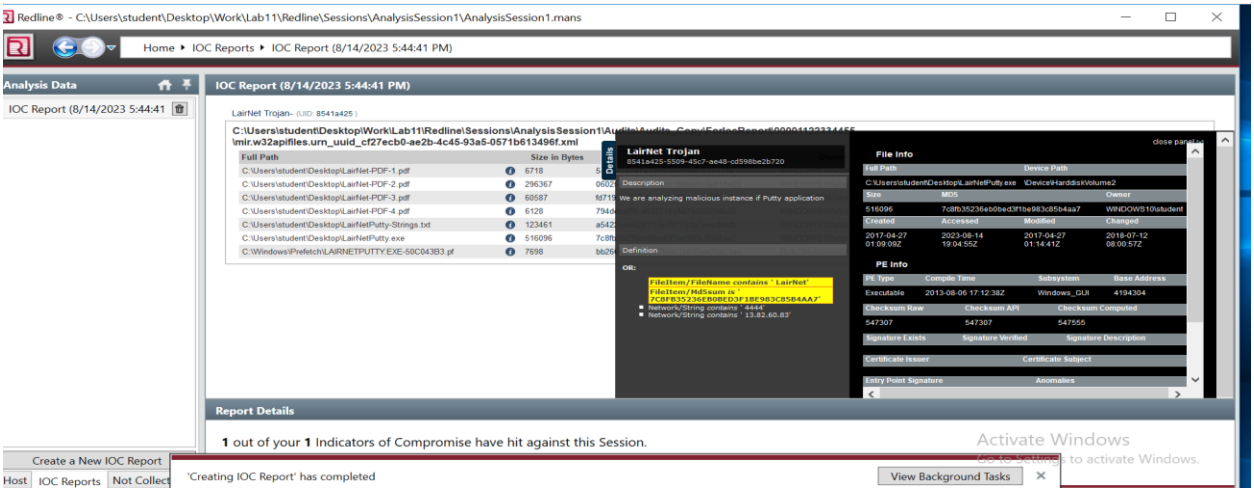
After selecting the IOC Reports tab I could see IOC report with the date mention.

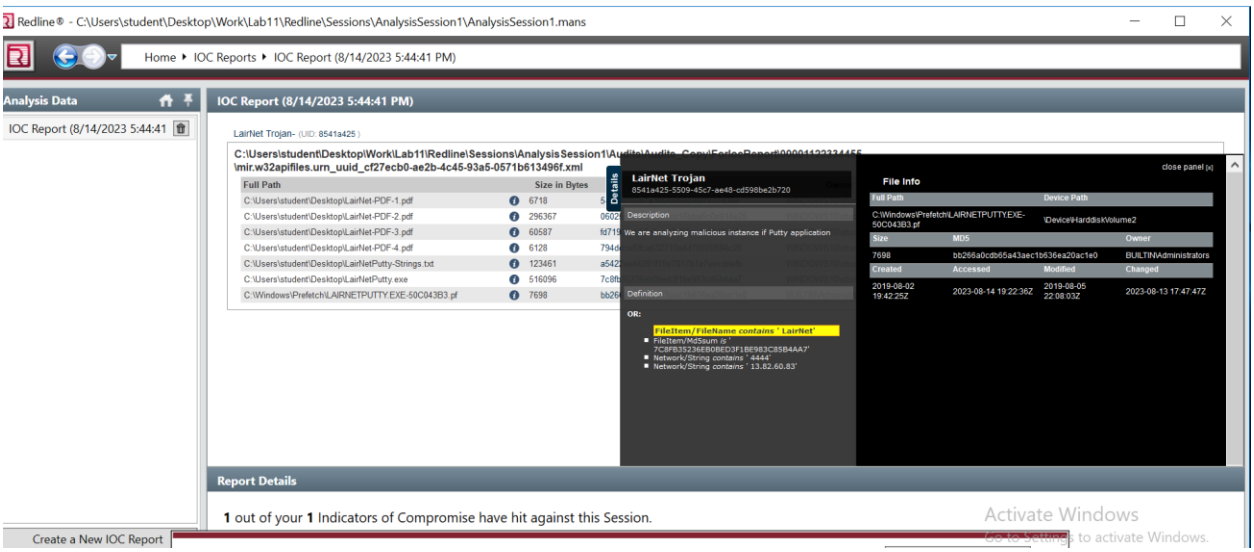


Now further expanding the LairNetPutty IOCs, I can see two files detected s malware by the Redline tool namely ‘LairNetPutty.exe’ and ‘LAIRNETPUTTY.EXE-50C043B3.pf’ based on the IOC details we have provided.


Redline® - C:\Users\student\Desktop\Work\Lab11\Redline\Sessions\AnalysisSession1\AnalysisSession1.mans
Home ▸ IOC Reports ▸ IOC Report (8/14/2023 5:44:41 PM)
Analysis Data
IOC Report (8/14/2023 5:44:41
IOC Report (8/14/2023 5:44:41 PM)
LairNet Trojan- (UID: 8541a425)
C:\Users\student\Desktop\Work\Lab11\Redline\Sessions\AnalysisSession1\Audits\Audits_Copy\ForlocReport\00001122334455\mir.w32apifiles.urn_uuid_cf27ecb0-ae2b-4c45-93a5-0571b613496f.xml
View Hits -
Full Path
Size in Bytes
MD5
Owner
Created
Access
Modified
C:\Users\student\Desktop\LairNet-PDF-1.pdf 6718 547eef762a7a396f0060096f7837d39e WINDOWS10\student 2019-08-05 21:52:53Z 2023-08-14 19:04:55Z 2019-08-05 21:52:54Z
C:\Users\student\Desktop\LairNet-PDF-2.pdf 296367 06025d27ce25cb9cc15bba5c0e014e25 WINDOWS10\student 2019-08-05 21:53:44Z 2023-08-14 19:04:55Z 2019-08-05 21:53:45Z
C:\Users\student\Desktop\LairNet-PDF-3.pdf 60587 fd7190ffbb67a6ac87e27aad047407e6 WINDOWS10\student 2019-08-05 21:54:00Z 2023-08-14 19:04:55Z 2019-08-05 21:54:00Z
C:\Users\student\Desktop\LairNet-PDF-4.pdf 6128 794ddcef0fca632710a4d76020894c25 WINDOWS10\student 2019-08-05 22:04:11Z 2023-08-14 19:04:55Z 2019-08-05 22:04:12Z
C:\Users\student\Desktop\LairNetPutty-Strings.txt 123461 a5422ee46281f15e7817b1a7eecddefb WINDOWS10\student 2023-07-15 07:24:05Z 2023-08-14 19:04:55Z 2023-07-15 07:51:11Z
C:\Users\student\Desktop\LairNetPutty.exe 516096 7c8fb35236eb0bed3f1be983c85b4aa7 WINDOWS10\student 2017-04-27 01:09:09Z 2023-08-14 19:04:55Z 2017-04-27 01:14:41Z
C:\Windows\Prefetch\LAIRNETPUTTY.EXE-50C043B3.pf 7698 bb266a0cdb65a43aec1b636ea20ac1e0 BUILTIN\Administrators 2019-08-02 19:42:25Z 2023-08-14 19:22:36Z 2019-08-05 22:08:03Z
Details
Report Details
1 out of your 1 Indicators of Compromise have hit against this Session.
Activate Windows
Create a New IOC Report
Host
IOC Reports
Not Collect
'Creating IOC Report' has completed
View Background Tasks


Redline® - C:\Users\student\Desktop\Work\Lab11\Redline\Sessions\AnalysisSession1\AnalysisSession1.mans
Home ▸ IOC Reports ▸ IOC Report (8/14/2023 5:44:41 PM)
Analysis Data
IOC Report (8/14/2023 5:44:41
IOC Report (8/14/2023 5:44:41 PM)
LairNet Trojan- (UID: 8541a425)
\mir.w32apifiles.urn_uuid_cf27ecb0-ae2b-4c45-93a5-0571b613496f.xml
Details
LairNet Trojan
8541a425-5509-45c7-ae48-cd598be2b720
Description
We are analyzing malicious instance if Putty application
Definition
OR:
FileItem/FileName contains ' LairNet'
FileItem/Md5sum is '7C8FB35236EB0BED3F1BE983C85B4AA7'
Network/String contains ' 4444'
Network/String contains ' 13.82.60.83'
close panel
File Info
Full Path
Device Path
C:\Users\student\Desktop\LairNetPutty-Strings.txt
\Device\HarddiskVolume2
Size
MD5
Owner
123461
a5422ee46281f15e7817b1a7eecddefb
WINDOWS10\student
Created
Accessed
Modified
Changed
2023-07-15 07:24:05Z
2023-08-14 19:04:55Z
2023-07-15 07:51:11Z
2023-07-17 07:09:17Z
Report Details
1 out of your 1 Indicators of Compromise have hit against this Session.
Activate Windows


Redline® - C:\Users\student\Desktop\Work\Lab11\Redline\Sessions\AnalysisSession1\AnalysisSession1.mans
Home ▸ IOC Reports ▸ IOC Report (8/14/2023 5:44:41 PM)
Analysis Data
IOC Report (8/14/2023 5:44:41
IOC Report (8/14/2023 5:44:41 PM)
LairNet Trojan- (UID: 8541a425)
\mir.w32apifiles.urn_uuid_cf27ecb0-ae2b-4c45-93a5-0571b613496f.xml
Details
LairNet Trojan
8541a425-5509-45c7-ae48-cd598be2b720
Description
We are analyzing malicious instance if Putty application
Definition
OR:
FileItem/FileName contains ' LairNet'
FileItem/Md5sum is '7C8FB35236EB0BED3F1BE983C85B4AA7'
Network/String contains ' 4444'
Network/String contains ' 13.82.60.83'
close panel
File Info
Full Path
Device Path
C:\Users\student\Desktop\LairNetPutty.exe
\Device\HarddiskVolume2
Size
MD5
Owner
516096
7c8fb35236eb0bed3f1be983c85b4aa7
WINDOWS10\student
Created
Accessed
Modified
Changed
2017-04-27 01:09:09Z
2023-08-14 19:04:55Z
2017-04-27 01:14:41Z
2019-07-12 08:00:57Z
PE Info
PE Type
Compile Time
Subsystem
Base Address
Executable
2013-08-06 17:12:38Z
Windows_GUI
4194304
Checksum Raw
Checksum API
Checksum Computed
547307
547307
547555
Signature Exists
Signature Verified
Signature Description
Certificate Issuer
Certificate Subject
Entry Point Signature
Anomalies
Report Details
1 out of your 1 Indicators of Compromise have hit against this Session.
Activate Windows
Create a New IOC Report
Host
IOC Reports
Not Collect
'Creating IOC Report' has completed
View Background Tasks



Citations –

1. Erfan. (2021, July 18). What is PuTTY? Advantages and Disadvantages and its Installation Tutorial. Ded9. https://ded9.com/what-is-putty-advantages-and-disadvantages-and-its-installation-tutorial/
2. **Mandiant's IOC Editor** – It is a free editor for Indicators of Compromise (IOCs). IOCs are XML documents that help incident responders capture diverse information about threats including attributes of malicious files, characteristics of registry changes, artifacts in memory, and so on. Mandiant. (2015). IOC Editor User Guide. FireEye. https://fireeye.market/assets/apps/S7cWpi9W//9cb9857f/ug-ioc-editor.pdf
3. **Redline Tool -** Redline is a free endpoint security tool that provides users with host investigative capabilities. It analyzes memory and files to find signs of malicious activity and develop a threat assessment profile. Redline can be used on Windows, Linux, or macOS endpoints. Motasem. (n.d.). How to use FireEye Redline for Incident Response - TryHackMe Redline. Motasem's Notes. https://motasem-notes.net/how-to-use-fireeye-redline-for-incident-response-tryhackme-redline/

4. Toulas, B. (2022, September 15). Hackers Trojanize PuTTY SSH Client to Backdoor Media Company. BleepingComputer. https://www.bleepingcomputer.com/news/security/hackers-trojanize-putty-ssh-client-to-backdoor-media-company/