**Cybersecurity 401**

**Module 7 - Threat Hunting**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

## **Lab 32 - Malware Traffic Analysis with Wireshark**

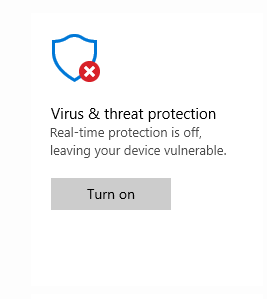
## 

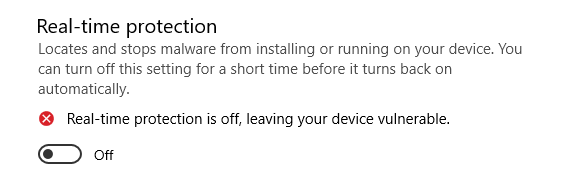
**| Rodrigo Brasil 12/2023 |**

### **Part 1: Staging**

Time to figure out what really took place based on the evidence we have available.

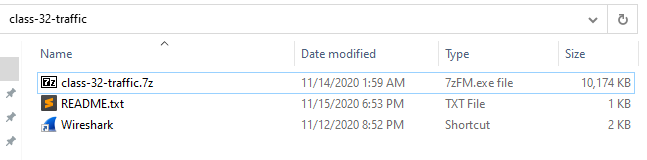
* Disable Windows Defender Antivirus in FLARE VM

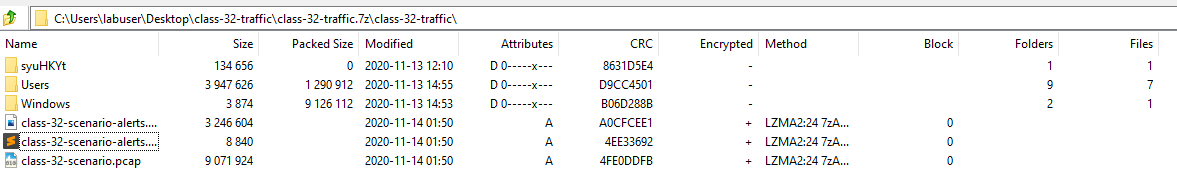


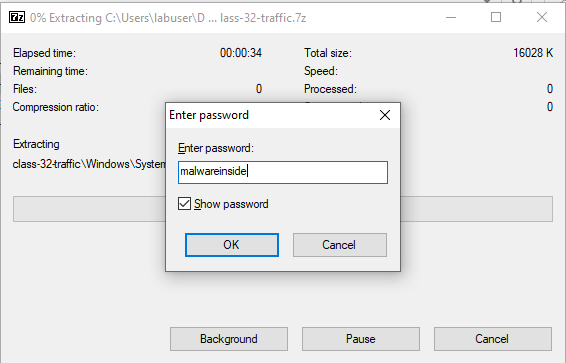


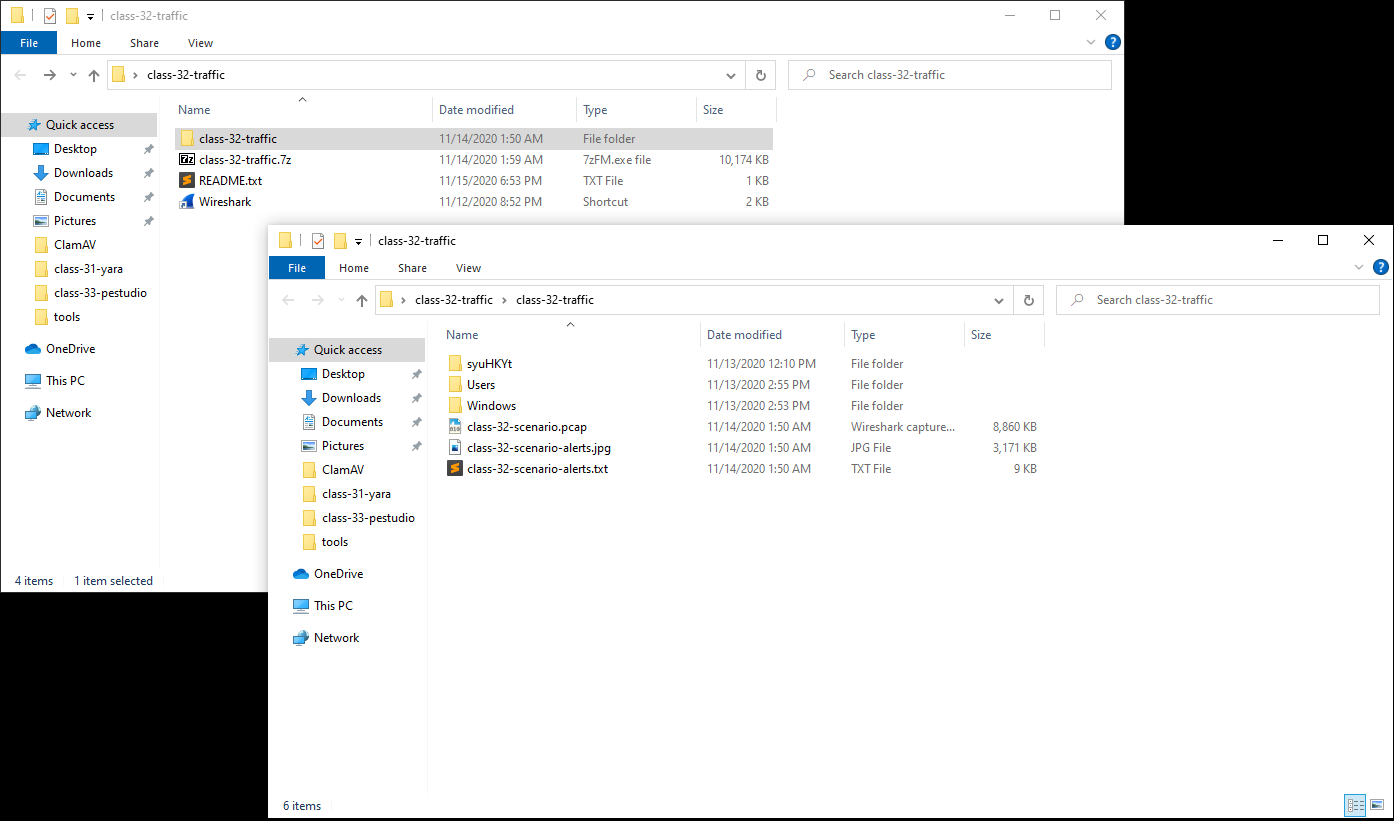
* Open the evidence package named “class-32-traffic.7z” on your FLARE VM desktop using password “malwareinside” to open.











### 

### **Part 2: Malware Traffic Analysis**

Refer to this information about the environment:

* LAN segment range: 192.168.200.0/24 (192.168.200.0 through 192.168.200.255)
* Domain: quiethub.net
* Domain controller: 192.168.200.8 - Quiethub-DC
* LAN segment gateway: 192.168.200.1
* LAN segment broadcast address: 192.168.200.255



This shows that the inside IP (192.168.200.8) is connecting to 2 outside IP’s (205.185.113.20 & 52.114.159.22), indicating that there seems to be a reverse shell.



The source port is not the same as the destination port which is 443, default for HTTPS. if it was a normal connection it should be using the port 443 as well.





A RST packet is known as a TCP reset. normally happens when it is trying to connect to a server port where no process is listening.

When an unexpected TCP packet arrives at a host, that host usually responds by sending a reset packet back on the same connection. A reset packet is simply one with no payload and with the RST bit set in the TCP header flags.



Looking at this packet which is using CLDAP protocol which is mostly encountered in networks using microsoft active directory where clients use it to retrieve server information we can assume that after gaining reverse shell the threat actor started retrieving server information about the root which was successful.



In Wireshark, DCERPC is a protocol used for communication between different processes on a network. When you see DCERPC in Wireshark, it means that the captured network traffic includes communication using the DCERPC protocol. This protocol is commonly used in Windows networking for tasks such as remote administration and file sharing.

This can indicate that the threat actor is

Evaluate the evidence; use the tools you’ve learned thus far to piece together the details of what took place. In order to complete this lab, you’ll need to use critical thinking and careful analysis to reconstruct the events that took place.

*Forensic analysis of data files can be tedious, dry, tiresome, and even frustrating! If you ever get stuck, start with the most obvious signals and let those clues guide your next steps. Ask yourself: “Did the evidence lead me here?” If the answer is no, go back to the beginning and rethink your approach.*

### 

### **Part 3: Reporting**

Write an incident report based on your findings. Include the following components:

* Executive Summary
  + Include when, who, and what happened.
* Details
  + Include details of the victim such as hostname, IP address, MAC address, Windows user account name.
* Indicators of Compromise (IOCs)
  + Include SHA256 hashes and details of the malware and/or artifacts, IP addresses, domains and URLs associated with the infection.

*Take care not to accidentally transmit malware. All artifacts should remain on your FLARE VM.*