**Incident Report:** CH-15061-Defensive-Malware-Traffic

**Date:** 10-19-2022

**Executive Summary:**

After using multiple websites to download free movies, my friend contacted me for help because his computer has been encrypted. Using Wireshark as my primary resource, my goal was to identify the hostnames responsible for the infection, as well as the name of the malware file.

**Methodology:**

To complete this task successfully, I took the following actions, in order:

1. I reviewed the Reserved Story: Intro to Wireshark video and associated exercises on malware-traffic-analysis.net.
2. To become more familiar with recognizing and identifying what malware looks like in network traffic packets, I performed a Google search and reviewed the following resources:
   1. <https://unit42.paloaltonetworks.com/unit42-customizing-wireshark-changing-column-display/>
      1. Used this tutorial to set up my columns in Wireshark
   2. <https://www.malware-traffic-analysis.net/tutorials/index.html>
      1. Used the tutorials linked to this page to access additional features and learn more about the functionality of Wireshark
         1. Saved several of the recommended filter expressions for use with future queries
   3. Completed the Pluralsight course: Identify Common Cyber Network Attacks with Wireshark
      1. Course link: <https://app.pluralsight.com/course-player?courseId=ecd1360b-a2a1-4b75-a293-dc0382b15317>
      2. Learned about some of the common characteristics that malware can show up in packets
3. Armed with a better understanding of how to use Wireshark filters and the ways in which malware can be identified by reviewing network packet details, I downloaded the associated Story PCAP file, opened it in Wireshark, and performed the following actions:
   1. File → Export Objects → HTTP
      1. Observed activity from a limited number of hosts:
         1. Grouprograms.in
         2. 62.75.195.236
         3. Ip-addr.es
         4. Runlove.us
         5. Comarksecurity.com
         6. Gigapay.sun
      2. A quick scan of the associated file Content Types revealed a Shockwave application
         1. File name = **%2f**
         2. Noted the source host for this file - **Groupprograms.in**
         3. Saved this file to my local device and uploaded it into VirusTotal database (<https://www.virustotal.com/gui/home/upload>)
         4. File had been flagged MALICIOUS by multiple security vendors
         5. To identify further information about the host who sent this malicious file:
            1. Performed an http filter to locate all non-encrypted communications
            2. Search yielded several rows of results, including an entry with the identified malicious file (was listed as an HTTP request in the “info” column)
            3. Viewed additional details about this communication and located the IP address of the source of this file - **62.75.195.236**

Conducted a search of this IP address using the online database What’s My IP Address (<https://whatismyipaddress.com/>)

Hostname was identified as **static-ip-62-75-195-236.inaddr.ip-pool.com**

Checked against the VirusTotal database to confirm that this was a known source of malware

* + 1. To identify the remaining infection hosts:
       1. Returned to http filter and continued to check the IP addresses and available hostnames against the databases previously mentioned
          1. Noted several http requests from a source located at IP address **95.163.121.204**

Searched using the What’s My IP Address database and associated hostname was revealed to be **insconsulting.ru**

Searched for additional information about this source using the VirusTotal database

Flagged as malicious

* + - 1. The details of the remaining http filter results did not yield any new information.
      2. Reviewed notes to identify another strategy to use to sniff out malicious network activity:
         1. One suggestion mentioned in the Pluralsight course was to check the available name resolutions within Wireshark because malware will often attempt to connect to its C2 server

Statistics → Resolved Addresses → Hosts tab → Hosts filter

A quick scan of the results showed an address that looked suspect: **ip-addr.es**

When searched against the VirusTotal database, this had been flagged by multiple security vendors as a malicious source

Confirmed IP address of this source matched what was in Wireshark using the Details tab of VirtualTotal database

**Findings/Solutions:**

Based on my findings in Wireshark, I suspect the following hosts are responsible for the infection of my friend’s computer:

* 62.75.195.236 - static-ip-62-75-195-236.inaddr.ip-pool.com
* 95.163.121.204 - insconsulting.ru
* 188.165.164.184 - ip-addr.es

Based on my findings in Wireshark, I suspect the name of the file that was used to execute the malware on my friend’s computer is %2f, which was downloaded as a shockwave application from source 62.75.195.236.

**\*\*Amended Findings/Solutions:**

Upon further review of the HTTP object files listed in Files → Export Objects → HTTP, I suspect the malicious file is **packet number 426 - file name: %3fb514ee6f0fe486009a6d83b035a4c0bd (221KB, type: text/html), sent from source 6275.195.236.**