**Incident Report: KG-19110-Defensive:-Malware-Analysis  
Date:** 09-18-2024

### **Executive Summary**

In this task, I analyzed network traffic related to a malware infection on a victim machine using Wireshark. I identified the hostnames, IP addresses, MAC addresses, and SHA256 hash of the malware responsible for the infection. The malicious executable was downloaded via HTTP from a suspicious domain.

### **Methodology**

To complete this analysis, I followed these steps:

1. **Captured and Analyzed Network Traffic:**I used Wireshark to monitor the network traffic on the victim's machine, focusing on HTTP GET requests that could be linked to malicious downloads. The traffic revealed a request to download a potentially malicious file from a suspicious domain.
2. **Identified the Hostnames, IP Addresses, and MAC Addresses Responsible:**By analyzing the traffic, I identified the following information related to the infection:
   * **Victim Source IP:** 10.2.8.101
   * **Victim Source MAC Address:** 00:12:79 (Hewlett Packard)
   * **Destination IP (Malicious Source):** 8.208.10.147
   * **Destination MAC Address:** F0:29:29 (Cisco Systems, Inc.)
   * **Victim’s Windows User Account:** Bill Cook
   * **Malicious Domain:** **roanokemortgages.com**
3. **Found the Executable File:**The analysis revealed that the victim machine requested and downloaded the file **6lhjgfdghj.exe** via an HTTP GET request to **roanokemortgages.com**. This file contained the **"trojan.zudochka/doina"** malware and was responsible for encrypting the victim’s computer.
   * **SHA256 Hash of Malware Binary:** 94e60de577c84625da69f785ffe7e24c889bfa6923dc7b017c21e8a313e4e8e1
   * **VirusTotal Detection Score:** 63/74

### **Findings/Solutions**

The malware infection originated from the download of the executable file **6lhjgfdghj.exe** from the domain **roanokemortgages.com**. The victim’s machine, with IP 10.2.8.101 and MAC address 00:12:79 (Hewlett Packard), was compromised. To prevent similar infections, users should avoid downloading from untrusted sources and implement security measures like antivirus software and real-time monitoring of network traffic to detect and block malware.

**Project Description**

For this story, you will be using Wireshark.

Jack has brought in a laptop that is an expensive brick right now. We’ve managed to pull some logs from the hard drive. Analyze these logs and write a report on what you found. There are three different Mal-wares affecting this laptop. They are all well know and popular Malware.

* Write an incident report based on the PCAP and the alerts.
* The incident report should contains 3 sections:
* State in simple, direct terms what happened (when, who, what).
* Details of the victim (hostname, IP address, MAC address, Windows user account name).
* IP addresses, domains and URLs associated with the infection.  SHA256 hashes if any malware binaries can be extracted from the PCAP.

Resources for Malware info:

* [www.cisecurity.org/resources/?type=white-papers%2f](https://www.cisecurity.org/resources/?type=white-papers/)
* [www.microsoft.com/en-us/wdsi/threats](https://www.microsoft.com/en-us/wdsi/threats)

As per your first defensive story, find the folder with the matching name of this story, this will contain your PCAP for this story.