This guide walks through the analysis of a "Trojan" machine, a digital forensics and incident response (DFIR) challenge. The analysis utilizes disk artifacts, memory captures, and packet captures to uncover details about the compromise.

**1. Initial Setup and Data Overview**

Upon downloading the challenge files, three directories are identified: disk artifacts, memory capture, and packet capture.

A screenshot of a computer

AI-generated content may be incorrect.

**2. Identifying the Operating System Build Version**

To determine the operating system from the memory capture, Volatility is used. The analysis reveals that the OS build version is 19041. This corresponds to Windows 10, version 2004 (20H1).

A screenshot of a computer

AI-generated content may be incorrect.

**3. Discovering the Computer Hostname**

The computer hostname is identified by examining the packet capture files. Opening the .pcap file with Wireshark and filtering by the infected machine's IP address, 192.168.116.133 , reveals an NBNS (NetBIOS Name Service) packet containing the hostname. NBNS is responsible for mapping NetBIOS names to IP addresses. The hostname is found to be DESKTOP-S08VPDR.

A screen shot of a computer

AI-generated content may be incorrect.

**4. Identifying the Downloaded ZIP File**

To find the name of the downloaded ZIP file, a Wireshark filter for http.content\_type contains "zip" is applied. This filter successfully identifies the packet containing the ZIP file download. The downloaded file is named 2023/05/Data\_Recovery.zip.

A screenshot of a computer

AI-generated content may be incorrect.

**5. Determining the Download Domain**

The domain from which the ZIP file was downloaded is found within the same packet identified in the previous step. The domain is updates.glarysoft.com.

A black background with white text

AI-generated content may be incorrect.

**6. Analyzing the Malicious Application Execution**

After the suspicious ZIP file was downloaded, an application within it was executed.

* **Process PID**: Volatility is used on the memory logs to extract the Process ID (PID) of the suspicious application. By running python3 /opt/volatility3-develop/vol.py -f memory.vmem windows.pstree | grep -i data, the search is narrowed down to processes containing "data". The PID of the suspicious process is 484.
* **Full Path**: The full path of the suspicious process is found in the same Volatility output: C:\Users\John\AppData\Local\Microsoft\OneDrive\Recovery\_Setup.exe.
* **SHA-256 Hash**: To obtain the SHA-256 hash, the executable is first dumped from memory using python3 /home/kali/volatility3/vol.py -f memory.vmem windows.dumpfiles --pid 484. After reconstructing the executable file, its SHA-256 hash is determined to be C34601c5da3501f6ee0efce18de7e6145153ecfac2ce2019ec52e1535a4b3193.

A screenshot of a computer screen

AI-generated content may be incorrect.

* **First Execution Time**: The malicious program was first executed on 2023-05-30 02:06:29.
* **Total Executions**: The malicious application was executed a total of 2 times.

**7. Identifying Referenced .TMP Files**

The malicious application references two .TMP files. One is IS-NJBAT.TMP. The other is found by running sudo strings memory.vmem | grep tmp, which reveals IS-R7RFP.TMP.

A screen shot of a computer code

AI-generated content may be incorrect.

**8. Malicious URLs Contacted by the Application**

To determine how many URLs contacted by the malicious application were flagged as malicious by VirusTotal, the SHA-256 hash is searched on VirusTotal and cross-referenced with the packet capture file. Using Zeek with **cat http.log | zeek-cut id.orig\_h id.resp\_h uri | grep php** and Wireshark with an HTTP filter, it is found that puk.php was a malicious file. Further analysis indicates that 4 URLs contacted were detected as malicious by VirusTotal.

A screenshot of a computer

AI-generated content may be incorrect.

**9. Identifying the Program the Malware is Impersonating**

Searching online for the SHA-256 hash of the malicious executable reveals that the malware is pretending to be FinalRecovery v3.0.7.0325

A screenshot of a computer

AI-generated content may be incorrect.