Wireshark Analysis

LAB ONE

Robert Christopherson | 9/18/2022 | Difficulty: Easy

Objective

A generated alert requires investigation to determine authenticity.

Assess a pcap log and determine if this alert is a true positive or a false positive. This will require basic Wireshark capabilities.

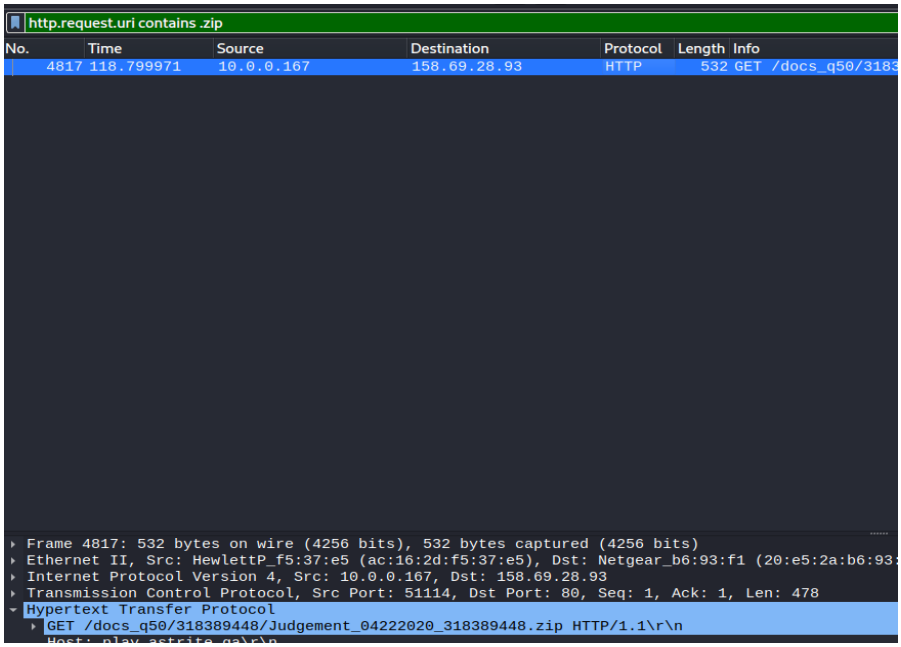
Method

Basic enumeration.

- Used search query “kerberos.CNameString” to determine hostnames and show endpoints caught in this pcap capture.
- From this we can extract two machine IP addresses, hostnames, and current user.
    - 10.0.0.149 | DESKTOP-C10SKPY | alyssa.fitzgerald
    - 10.0.0.167 | DESKTOP-GRIONXA | elmer.obrien

Get Requests

- Wireshark search query: http.request.method == GET && ip.addr == 10.0.0.149
    - Device is running Windows 10 (Discovered from the User-Agent tag)
- Wireshark search query: http.request.method == GET && ip.addr == 10.0.0.167
    - Device is running Windows 10 (Discovered from the User-Agent tag)
    - Found a suspicious .ZIP file downloaded from 158.69.28.93
    - Ran the raw binary through VirusTotal.



Result

- VirusTotal returned 23 hits indicating this .ZIP file is the QakBot Trojan (AKA: Qbot or Pinkslipbot).
- https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/qakbot
- With the confirmed positive result, appropriate steps can be taken to remove the malware and secure the systems affected.