|  |  |  |  |
| --- | --- | --- | --- |
|  |  | Wireshark Analysis (Core)  Otis Smith / Cybersecurity Professional / 8.29.23 |  |
|  |  |  |  |
| Pipette dropping liquid in a petri dish | | | |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | |
|  |  | TABLE OF CONTENTS |  |
|  |  | Summary …………………………..  Discovery……………………………  Vulnerability……………………….  Exploitation………………………..  References.………………………..  Mitigation………………………….. |  |



|  |  |  |
| --- | --- | --- |
| Summary |  | |
| This Wireshark analysis focused on investigating a potential security breach through the examination of a pcap file. The primary objectives were to identify Windows hosts, associate user account names, pinpoint the infected client, and determine the type of malware involved. The process involved downloading associated resources, utilizing Wireshark for packet analysis, and employing external tools such as VirusTotal to validate findings.  A hand holding a glowing city  Description automatically generated | |  |
| Discovery   1. Resource Acquisition:    * Successfully downloaded the required image and pcap file for analysis. 2. Wireshark Exploration:    * Utilized Wireshark to analyze network traffic and identify Windows hosts.    * Employed network filters and techniques from Unit 42 to narrow down Windows hosts (SBNS, http.request && ip.addr, Kerberos search).      1. Host Identification:    * Verified two Windows hosts (IP: 10.0.0.167 and 10.0.0.149) through TCPFlow stream inspection.        * + Associated user account names with Host1 (elmer.obrien) and Host2 (alyssa.fitzgerald). | |  |
|  | |  |

|  |  |  |
| --- | --- | --- |
| Vulnerability |  | |
| 1. Infection Determination:    * Conducted packet count analysis, revealing IP 10.0.0.167 as the infected station with 61% of the total packets.   A screenshot of a computer  Description automatically generated   * + Investigated HTTP traffic associated with 10.0.0.167, identifying a suspicious .ga domain and signs of malware.   A close-up of a document  Description automatically generated   1. Malware Analysis:    * Searched for "GET" commands with executable signs in HTTP traffic.    * Discovered a "Judgement\_04222020" zip file from Host: play.astrite.ga, indicating a potential malware transfer.    * A screenshot of a computer       Description automatically generated    * Converted data into Raw format and uploaded to VirusTotal, identifying the malware as "trojan.maltzur/qakbot."   A screenshot of a computer  Description automatically generated  VirusTotal  A screenshot of a computer  Description automatically generated | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Exploitation |  | |  | |  |
| 1. Qakbot Malware:    * Conducted a Google search for Qakbot, revealing its classification as a modular second-stage malware with backdoor capabilities.    * Qakbot functions as a banking trojan, worm, and remote access trojan (RAT), noted for credential stealing and network propagation. | |  | |  | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | | References |  |  |  |  1. [Unit 42 - Wireshark Identifying Hosts and Users](https://unit42.paloaltonetworks.com/using-wireshark-identifying-hosts-and-users/) 2. [VirusTotal](https://www.virustotal.com/) |  | |
|  | |  |

|  |  |  |
| --- | --- | --- |
|  |  | |
|  | |  |

Mitigation:

* + Patch and Update:
    - Regularly update and patch systems to address known vulnerabilities.
  + Network Segmentation:
    - Implement network segmentation to isolate critical servers.
  + Security Training:
    - Provide security awareness training for users and administrators.
  + Vulnerability Scanning:
    - Conduct regular vulnerability scans to identify and remediate weaknesses.
  + Access Control:
    - Implement strong access controls to restrict unauthorized access.

In conclusion, this analysis successfully uncovered a potential security breach, identified the infected Windows client (10.0.0.167), and determined the malware type as Qakbot. The process involved a meticulous examination of packet data using Wireshark, leveraging external resources, and validating findings through VirusTotal. The provided mitigation steps emphasize the importance of regular updates, network segmentation, user training, vulnerability scanning, and access control to enhance overall cybersecurity.