Internal Memorandum

To: Paula Alexander <hal.cio@seccdc.org>

CC: judge_29@seccdc.org

From: hal29@seccdc.org

Date: February 23, 2019

Memo #: 011

Re: Wireshark Network Data Capture and Analysis

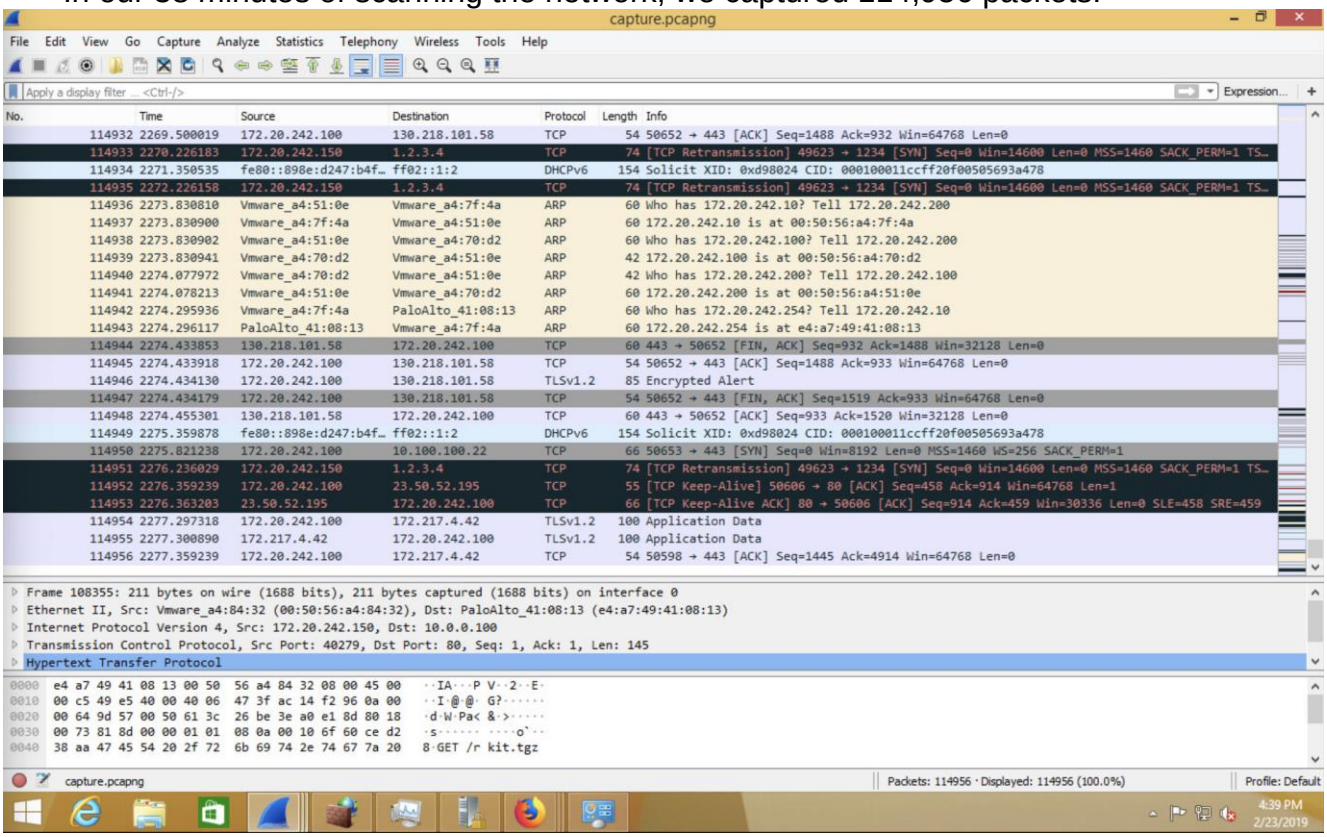
Hierarchical Access Limited Corporation

www.halcorp.biz

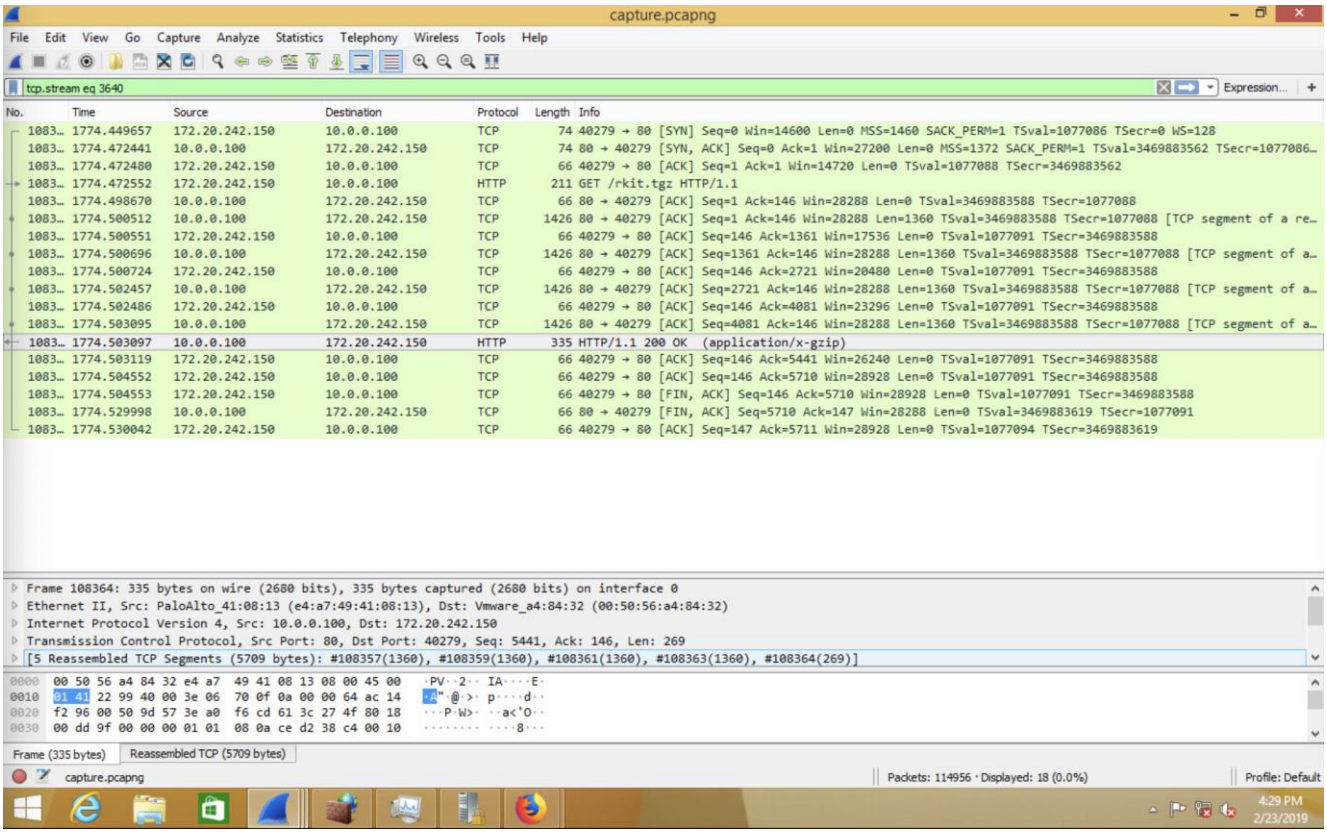
Greetings CIO,

Regarding your request to monitor our network traffic for potential data exfiltration or any other anomalous behavior. To facilitate this task, we have downloaded and installed Wireshark on our Windows 8.1 workstation to collect and analyze network traffic. Wireshark has been configured to save only the last hour of data collected.

In our 38 minutes of scanning the network, we captured 114,956 packets.



In our time monitoring the network, we came across an example of a malicious file being downloaded to a HAL server.



In this example, a file called “rkit.tgz” is downloaded from “10.0.0.100”. We can then extract the file from the packet capture and analyze what was contained within the file. This file was then unzipped and analyzed. We have determined that it was a rootkit sent to our Phantom server. This wireshark capture made us aware of this incident.

While this has been a quick solution we recommend that Wireshark be used as a temporary solution. If we desired a more permanent network monitoring solution our recommendation would be to deploy a Network Intrusion Detection System (IDS). In comparison to a wire shark scan, a network IDS is built to run for long spans of time and parse network traffic information into a human-readable format.

Regards,
Team 9

In accordance with HAL Memorandum policy, the entire header must be completed or the recipient may not acknowledge this as an official memorandum. Professional communications methods and decorum must be observed at all times.