

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**

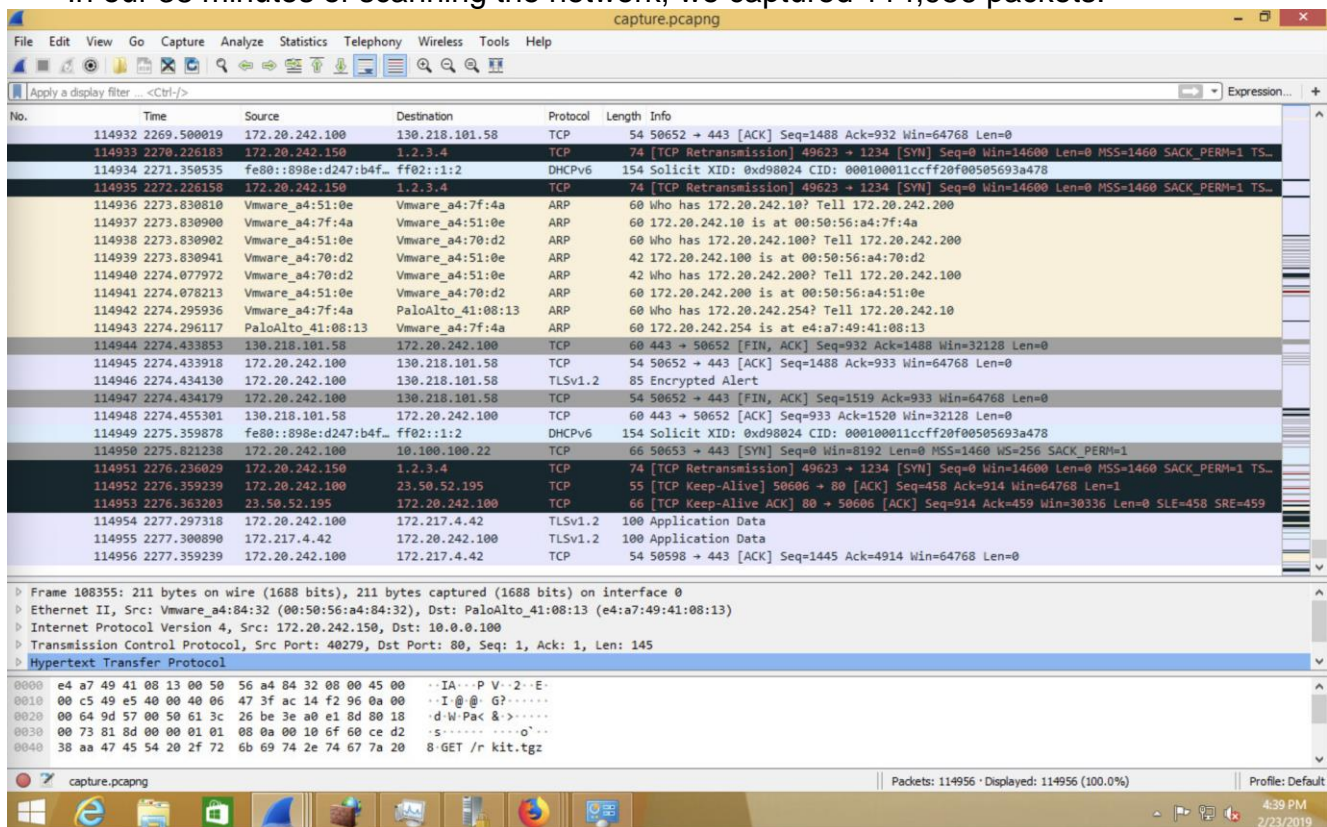


www.halcorp.biz

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.

capture.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 3640

No.	Time	Source	Destination	Protocol	Length	Info
1083	1774.449657	172.20.242.150	10.0.0.100	TCP	74	40279 → 80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=1077086 TSecr=0 WS=128
1083	1774.472441	10.0.0.100	172.20.242.150	TCP	74	80 → 40279 [SYN, ACK] Seq=0 Ack=1 Win=27200 Len=0 MSS=1372 SACK_PERM=1 TSval=3469883562 TSecr=1077086
1083	1774.472480	172.20.242.150	10.0.0.100	TCP	66	40279 → 80 [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=1077088 TSecr=3469883562
1083	1774.472552	172.20.242.150	10.0.0.100	HTTP	211	GET /rkit.tgz HTTP/1.1
1083	1774.498670	10.0.0.100	172.20.242.150	TCP	66	80 → 40279 [ACK] Seq=1 Ack=146 Win=28288 Len=0 TSval=3469883588 TSecr=1077088
1083	1774.500512	10.0.0.100	172.20.242.150	TCP	1426	80 → 40279 [ACK] Seq=1 Ack=146 Win=28288 Len=1360 TSval=3469883588 TSecr=1077088 [TCP segment of a re..
1083	1774.500551	172.20.242.150	10.0.0.100	TCP	66	40279 → 80 [ACK] Seq=146 Ack=1361 Win=17536 Len=0 TSval=1077091 TSecr=3469883588
1083	1774.500696	10.0.0.100	172.20.242.150	TCP	1426	80 → 40279 [ACK] Seq=1361 Ack=146 Win=28288 Len=1360 TSval=3469883588 TSecr=1077088 [TCP segment of a..
1083	1774.500724	172.20.242.150	10.0.0.100	TCP	66	40279 → 80 [ACK] Seq=146 Ack=2721 Win=20480 Len=0 TSval=1077091 TSecr=3469883588
1083	1774.502457	10.0.0.100	172.20.242.150	TCP	1426	80 → 40279 [ACK] Seq=2721 Ack=146 Win=28288 Len=1360 TSval=3469883588 TSecr=1077088 [TCP segment of a..
1083	1774.502486	172.20.242.150	10.0.0.100	TCP	66	40279 → 80 [ACK] Seq=146 Ack=4081 Win=23296 Len=0 TSval=1077091 TSecr=3469883588
1083	1774.503095	10.0.0.100	172.20.242.150	TCP	1426	80 → 40279 [ACK] Seq=4081 Ack=146 Win=28288 Len=1360 TSval=3469883588 TSecr=1077088 [TCP segment of a..
1083	1774.503097	10.0.0.100	172.20.242.150	HTTP	335	HTTP/1.1 200 OK (application/x-gzip)
1083	1774.503119	172.20.242.150	10.0.0.100	TCP	66	40279 → 80 [ACK] Seq=146 Ack=5441 Win=26240 Len=0 TSval=1077091 TSecr=3469883588
1083	1774.504552	172.20.242.150	10.0.0.100	TCP	66	40279 → 80 [ACK] Seq=146 Ack=5710 Win=28928 Len=0 TSval=1077091 TSecr=3469883588
1083	1774.504553	172.20.242.150	10.0.0.100	TCP	66	40279 → 80 [FIN, ACK] Seq=146 Ack=5710 Win=28928 Len=0 TSval=1077091 TSecr=3469883588
1083	1774.529998	10.0.0.100	172.20.242.150	TCP	66	80 → 40279 [FIN, ACK] Seq=5710 Ack=147 Win=28288 Len=0 TSval=3469883619 TSecr=1077091
1083	1774.530042	172.20.242.150	10.0.0.100	TCP	66	40279 → 80 [ACK] Seq=147 Ack=5711 Win=28928 Len=0 TSval=1077094 TSecr=3469883619

Frame 108364: 335 bytes on wire (2680 bits), 335 bytes captured (2680 bits) on interface 0
 Ethernet II, Src: PaloAlto_41:08:13 (e4:a7:49:41:08:13), Dst: Vmware_b4:84:32 (00:50:56:a4:84:32)
 Internet Protocol Version 4, Src: 10.0.0.100, Dst: 172.20.242.150
 Transmission Control Protocol, Src Port: 80, Dst Port: 40279, Seq: 5441, Ack: 146, Len: 269
 [5 Reassembled TCP Segments (5709 bytes): #108357(1360), #108359(1360), #108361(1360), #108363(1360), #108364(269)]

0000 00 50 56 a4 84 32 e4 a7 49 41 08 13 08 00 45 00 PV. 2. IA...E..
 0010 01 84 22 99 40 00 3e 06 70 0f 0a 00 00 64 ac 14 @ > p...d..
 0020 f2 96 00 50 9d 57 3e a0 f6 cd 61 3c 27 4f 80 18 ..P.W...ac'O..
 0030 00 dd 9f 00 00 01 01 00 0a ce d2 38 c4 00 10B...

Frame (335 bytes) Reassembled TCP (5709 bytes)

capture.pcapng

Packets: 114956 · Displayed: 18 (0.0%)

Profile: Default

4:29 PM 2/23/2019

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.