

2019-03-19 TRAFFIC ANALYSIS EXERCISE - ANSWERS

Link to exercise: <https://www.malware-traffic-analysis.net/2019/03/19/index.html>

My tutorials, so far, for Wireshark:

- Wireshark setup: <https://researchcenter.paloaltonetworks.com/2018/08/unit42-customizing-wireshark-changing-column-display/>
- Wireshark display filters: <https://unit42.paloaltonetworks.com/using-wireshark-display-filter-expressions/>

LAN SEGMENT DATA

- LAN segment range: 10.0.90.0/24 (10.0.90.0 through 10.0.90.255)
- Domain: littletigers.info
- Domain controller: 10.0.90.9 - LittleTigers-DC
- LAN segment gateway: 10.0.90.1
- LAN segment broadcast address: 10.0.90.255

YOUR TASK

Review the pcap and alerts, then write an incident report for this infected Windows host. The zip archive of malware and artifacts is a bonus, provided to help you better understand this infection, if needed. See below for a suggested template for an incident report.

Executive Summary:

On 2019-03-19 at ??:?? UTC, a Windows host used by ?????????? was infected with ????????

Details of the infected Windows host:

- IP address:
- MAC address:
- Host name:
- Windows user account name:

Indicators of Compromise:

[List of URLs, domains, IP addresses, and SHA256 hashes related to the infection should appear in this section]

2019-03-19 TRAFFIC ANALYSIS EXERCISE - ANSWERS

ANSWERS

Executive Summary:

On 2019-03-19 at 01:49 UTC, a Windows host used by Bobby Tiger was infected with Remcos RAT and Dridex.

Details of the infected Windows host:

- IP address: 10.0.90.215
- MAC address: 64:32:a8:57:2b:42 (IntelCor_57:2b:42)
- Host name: BOBBY-TIGER-PC
- Windows user account name: bobby.tiger

Indicators of Compromise:

IP addresses, ports, domains, and HTTP requests:

- 209.141.34.8 port 80 - 209.141.34.8 - GET /test1.exe
- 103.1.184.108 port 2404 - toptoptop1.online - Remcos RAT traffic
- 217.23.14.81 port 80 - 217.23.14.81 - GET /f4.exe
- 31.22.4.176 port 3389 - HTTPS/SSL/TLS traffic caused by Dridex
- 203.45.1.75 port 443 - HTTPS/SSL/TLS traffic caused by Dridex
- 115.112.43.81 port 443 - HTTPS/SSL/TLS traffic caused by Dridex
- 46.105.131.77 port 443 - HTTPS/SSL/TLS traffic caused by Dridex
- 109.230.231.176 port 443 - attempted TCP connections, no response from the server
- 189.189.64.242 port 443 - attempted TCP connections, no response from the server

Files extracted from the infection traffic:

SHA256 hash: 2a9b0ed40f1f0bc0c13ff35d304689e9cadd633781cbcad1c2d2b92ced3f1c85

File size: 811,520 bytes

File location: <http://209.141.34.8/test1.exe>

File identification: PE32 executable (GUI) Intel 80386, for MS Windows

File description: First EXE file retrieved by the infected Windows host for Remcos RAT

SHA256 hash: 5865e801e6324166d6d05b39a14f2a8a798c6eb652831f78c2634f2b7a400eaf

File size: 176,128 bytes

File location: <http://217.23.14.81/f4.exe>

File identification: PE32 executable (console) Intel 80386, for MS Windows

File description: Second EXE file retrieved by the infected Windows host for Dridex

2019-03-19 TRAFFIC ANALYSIS EXERCISE - ANSWERS

NOTES

All of the alerts were based on the internal Class A IP address of 10.0.90.215, so we have the IP address of our infected Windows client. We can easily correlate the IP address with the MAC address in the frame details section in Wireshark. To get the associated host name and Windows user account name, we can review Kerberos traffic.

Step 1: Filter on Kerberos.CNameString

Step 2: In the results, select the first frame

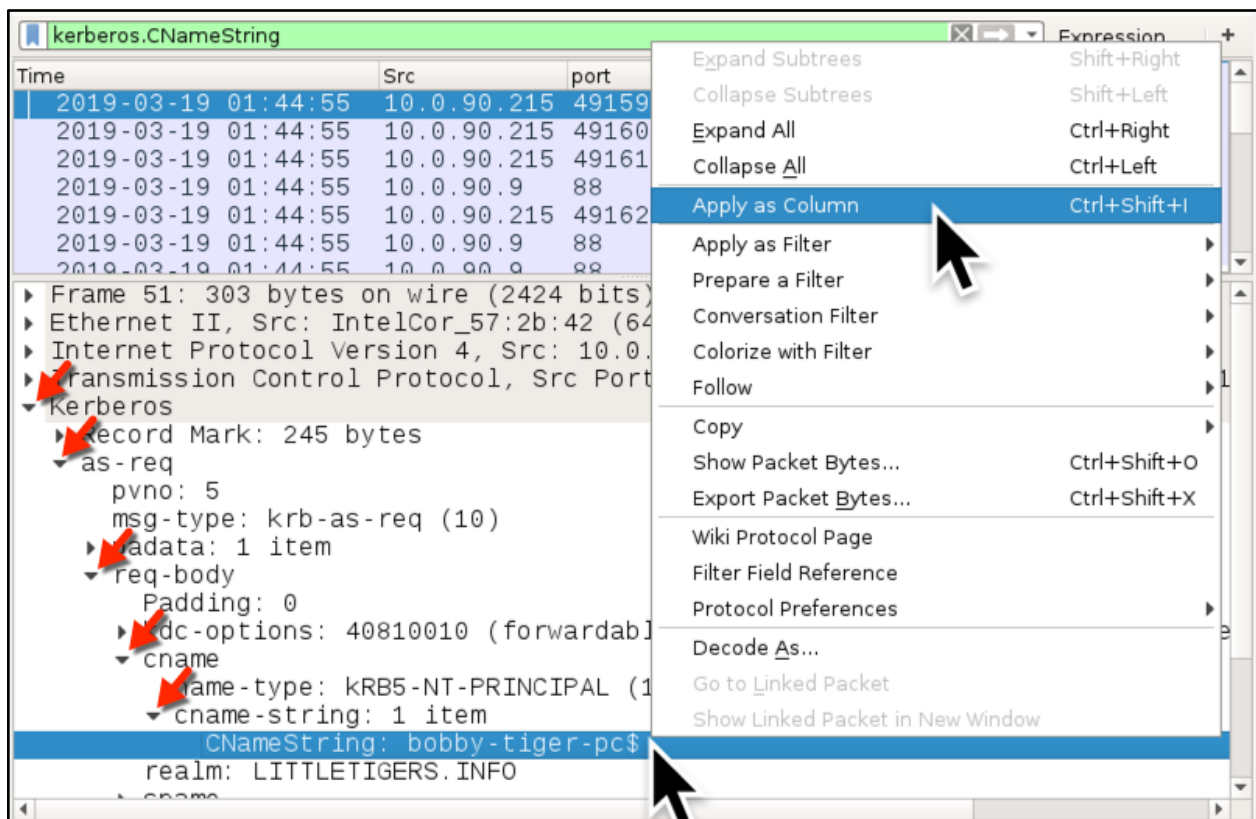
Step 3: In the frame details section, expand the **Kerberos** line, the **as-req** line, the **req-body** line, the **cname** line, and finally the **cname-string** line.

Step 4: Left-click on the line for **CNameString: bobby-tiger-pc\$** to select the value

Step 5: Right-click on the above line to bring up a menu and select **Apply as Column**

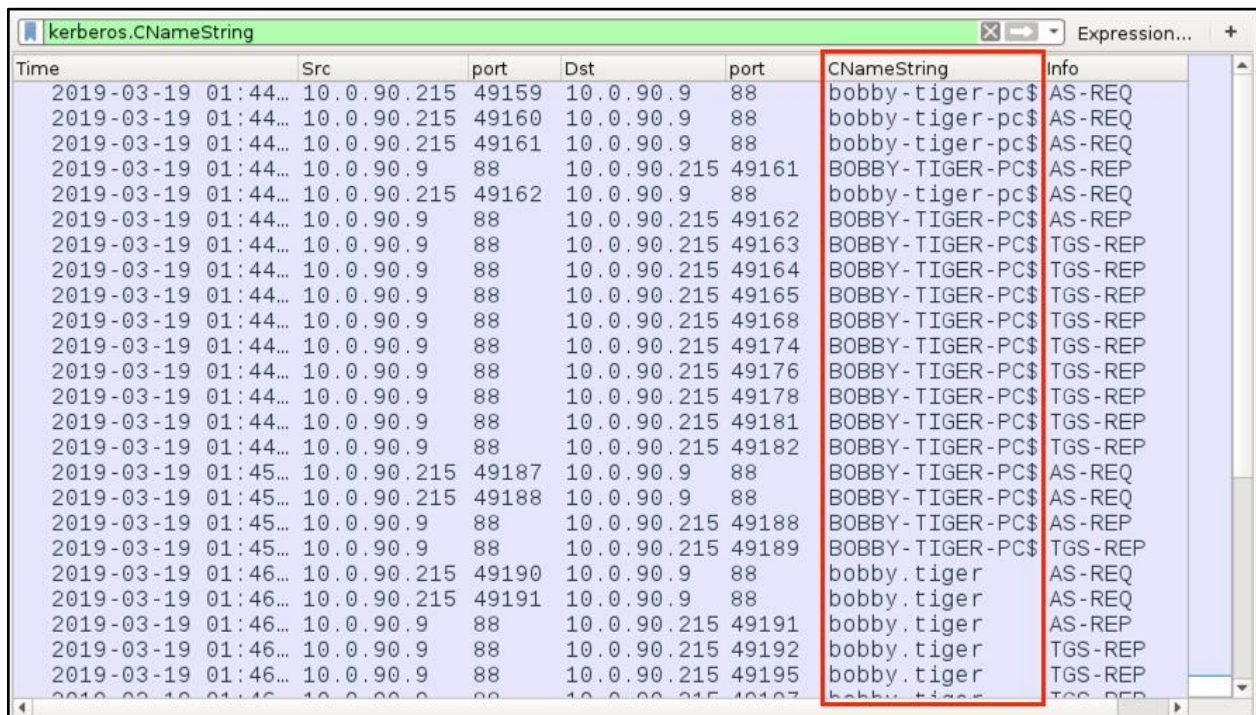
This will create a CNameString column that has the host name and Windows user account name values. The host name value always ends with a dollar sign (\$). The user account name does not end with a dollar sign. The two values are:

- **BOBBY-TIGER-PC\$** (also seen in lower-case letters)
- **Bobby.tiger**



Shown above: Using a **Kerberos.CNameString** value to create a custom column.

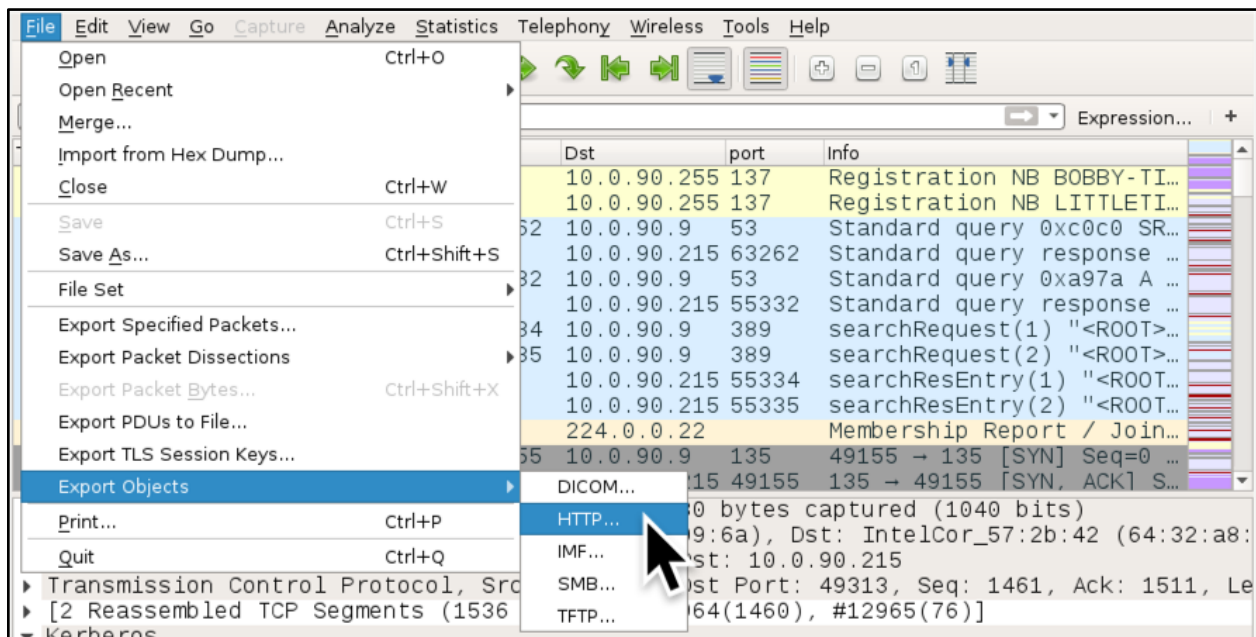
2019-03-19 TRAFFIC ANALYSIS EXERCISE - ANSWERS



Time	Src	port	Dst	port	CNameString	Info
2019-03-19 01:44...	10.0.90.215	49159	10.0.90.9	88	bobby.tiger-pc\$	AS-REQ
2019-03-19 01:44...	10.0.90.215	49160	10.0.90.9	88	bobby.tiger-pc\$	AS-REQ
2019-03-19 01:44...	10.0.90.215	49161	10.0.90.9	88	bobby.tiger-pc\$	AS-REQ
2019-03-19 01:44...	10.0.90.9	88	10.0.90.215	49161	BOBBY-TIGER-PC\$	AS-REP
2019-03-19 01:44...	10.0.90.215	49162	10.0.90.9	88	bobby.tiger-pc\$	AS-REQ
2019-03-19 01:44...	10.0.90.9	88	10.0.90.215	49162	BOBBY-TIGER-PC\$	AS-REP
2019-03-19 01:44...	10.0.90.9	88	10.0.90.215	49163	BOBBY-TIGER-PC\$	TGS-REP
2019-03-19 01:44...	10.0.90.9	88	10.0.90.215	49164	BOBBY-TIGER-PC\$	TGS-REP
2019-03-19 01:44...	10.0.90.9	88	10.0.90.215	49165	BOBBY-TIGER-PC\$	TGS-REP
2019-03-19 01:44...	10.0.90.9	88	10.0.90.215	49168	BOBBY-TIGER-PC\$	TGS-REP
2019-03-19 01:44...	10.0.90.9	88	10.0.90.215	49174	BOBBY-TIGER-PC\$	TGS-REP
2019-03-19 01:44...	10.0.90.9	88	10.0.90.215	49176	BOBBY-TIGER-PC\$	TGS-REP
2019-03-19 01:44...	10.0.90.9	88	10.0.90.215	49178	BOBBY-TIGER-PC\$	TGS-REP
2019-03-19 01:44...	10.0.90.9	88	10.0.90.215	49181	BOBBY-TIGER-PC\$	TGS-REP
2019-03-19 01:44...	10.0.90.9	88	10.0.90.215	49182	BOBBY-TIGER-PC\$	TGS-REP
2019-03-19 01:45...	10.0.90.215	49187	10.0.90.9	88	BOBBY-TIGER-PC\$	AS-REQ
2019-03-19 01:45...	10.0.90.215	49188	10.0.90.9	88	BOBBY-TIGER-PC\$	AS-REQ
2019-03-19 01:45...	10.0.90.9	88	10.0.90.215	49188	BOBBY-TIGER-PC\$	AS-REP
2019-03-19 01:45...	10.0.90.9	88	10.0.90.215	49189	BOBBY-TIGER-PC\$	TGS-REP
2019-03-19 01:46...	10.0.90.215	49190	10.0.90.9	88	bobby.tiger	AS-REQ
2019-03-19 01:46...	10.0.90.215	49191	10.0.90.9	88	bobby.tiger	AS-REQ
2019-03-19 01:46...	10.0.90.9	88	10.0.90.215	49191	bobby.tiger	AS-REP
2019-03-19 01:46...	10.0.90.9	88	10.0.90.215	49192	bobby.tiger	TGS-REP
2019-03-19 01:46...	10.0.90.9	88	10.0.90.215	49195	bobby.tiger	TGS-REP

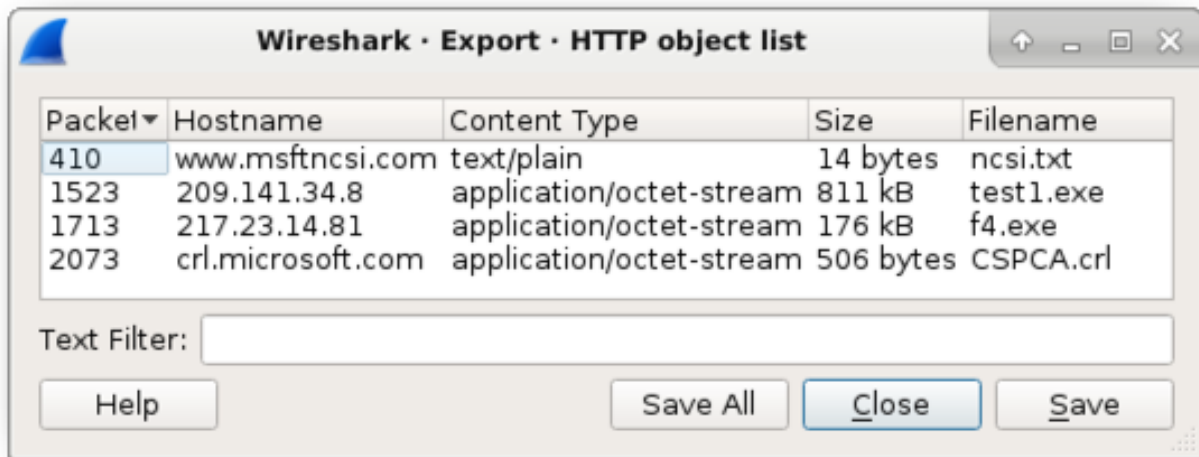
Shown above: Newly-created **CNameString** column shows the host and user account names.

The alerts file shows a Windows executable file being sent from two different IP addresses. You can export these from the pcap by using **File → Export Objects → HTTP...**



Shown above: Exporting objects from HTTP traffic in Wireshark.

2019-03-19 TRAFFIC ANALYSIS EXERCISE - ANSWERS



Shown above: Export HTTP Object list where you can save the Windows executable files in traffic sent from 209.141.34.8 and 217.23.14.81.