2024-08-15 - TRAFFIC ANALYSIS EXERCISE ANSWERS

Link to the exercise:

- https://www.malware-traffic-analysis.net/2024/09/04/index.html

Links to some tutorials I've written that should help with this exercise:

- Wireshark Tutorial: Changing Your Column Display
- Wireshark Tutorial: Identifying Hosts and Users
- Wireshark Tutorial: Display Filter Expressions

ENVIRONMENT:

- LAN segment range: `172.17.0.0/24` (`172.17.0.0` through `172.17.0.255`)
- Domain: `bepositive.com`
- AD environment name: `BEPOSITIVE`
- Domain Controller: `172.17.0.17 - WIN-CTL9XBQ9Y19`
- LAN segment gateway: `172.17.0.1`
- LAN segment broadcast address: `172.17.0.255`

BACKGROUND:

- Reviewing the alerts in your network environment, you find indicators that a host within your environment has been infected with malware.

TASK:

- Write an incident report based on traffic from the packet capture (pcap) and the alerts.

RealTime Events | Escalated Events

ST	CNT	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	2024-09-04 ...	172.17.0.99	59123	172.17.0.17	53	17	ET POLICY Reserved Internal IP Traffic
RT	1	2024-09-04 ...	172.17.0.17	53	172.17.0.99	59123	17	ET POLICY Reserved Internal IP Traffic
RT	25	2024-09-04 ...	172.17.0.17	53	172.17.0.99	62363	17	ET DNS Standard query response, Name Error
RT	3	2024-09-04 ...	172.17.0.99	49766	23.220.251.149	80	6	ET INFO Terse Request for .txt - Likely Hostile
RT	2	2024-09-04 ...	172.17.0.99	49766	23.220.251.149	80	6	ET INFO Microsoft Connection Test
RT	1	2024-09-04 ...	172.17.0.99	49769	172.17.0.17	139	6	ET INFO Potentially unsafe SMBv1 protocol in use
RT	10	2024-09-04 ...	172.17.0.99	49769	172.17.0.17	139	6	GPL NETBIOS SMB Session Setup NTMLSSP unicode asn1 overflow attempt
RT	5	2024-09-04 ...	172.17.0.99	49769	172.17.0.17	139	6	GPL NETBIOS SMB IPC$ unicode share access
RT	10	2024-09-04 ...	172.17.0.99	49769	172.17.0.17	139	6	GPL NETBIOS SMB SMB_COM_TRANSACTION Max Data Count of 0 DOS Attempt
RT	1	2024-09-04 ...	172.17.0.99	49774	172.17.0.17	88	6	GPL RPC kerberos principal name overflow TCP
RT	50	2024-09-04 ...	172.17.0.99	49813	79.124.78.197	80	6	ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1
RT	48	2024-09-04 ...	172.17.0.99	49813	79.124.78.197	80	6	ETPRO TROJAN Win32/Koi Stealer CnC Checkin (POST) M2

Shown above: Screenshot of alerts for this exercise.

2024-08-15 - TRAFFIC ANALYSIS EXERCISE ANSWERS

ANSWER (EXAMPLE OF AN INCIDENT REPORT):

Executive Summary:

- As early as Wednesday 2024-09-04 at 17:35 UTC, a Windows host used by Andrew Fletcher showed signs of being infected with Koi Stealer malware.

Victim Details:

- Host name: `DESKTOP-RNVO9AT`
- IP address: `172.17.0.99`
- MAC address: `18:3d:a2:b6:8d:c4`
- Windows user account name: `afletcher`
- Name of victim: Andrew Fletcher

Indicators of Compromise (IOCs):

Alert information:

Src IP:port	Dest IP:port	Alert name
172.17.0.99:49813	79.124.78.197:80	ETPRO TROJAN Win32/Koi Stealer CnC Checkin (POST) M2

URLs generating the alert traffic:

79.124.78.197:80 – **79.124.78.197** – POST /foots.php
79.124.78.197:80 – **79.124.78.197** – POST /index.php?id&subid=qIOuKk7U
79.124.78.197:80 – **79.124.78.197** – POST /index.php

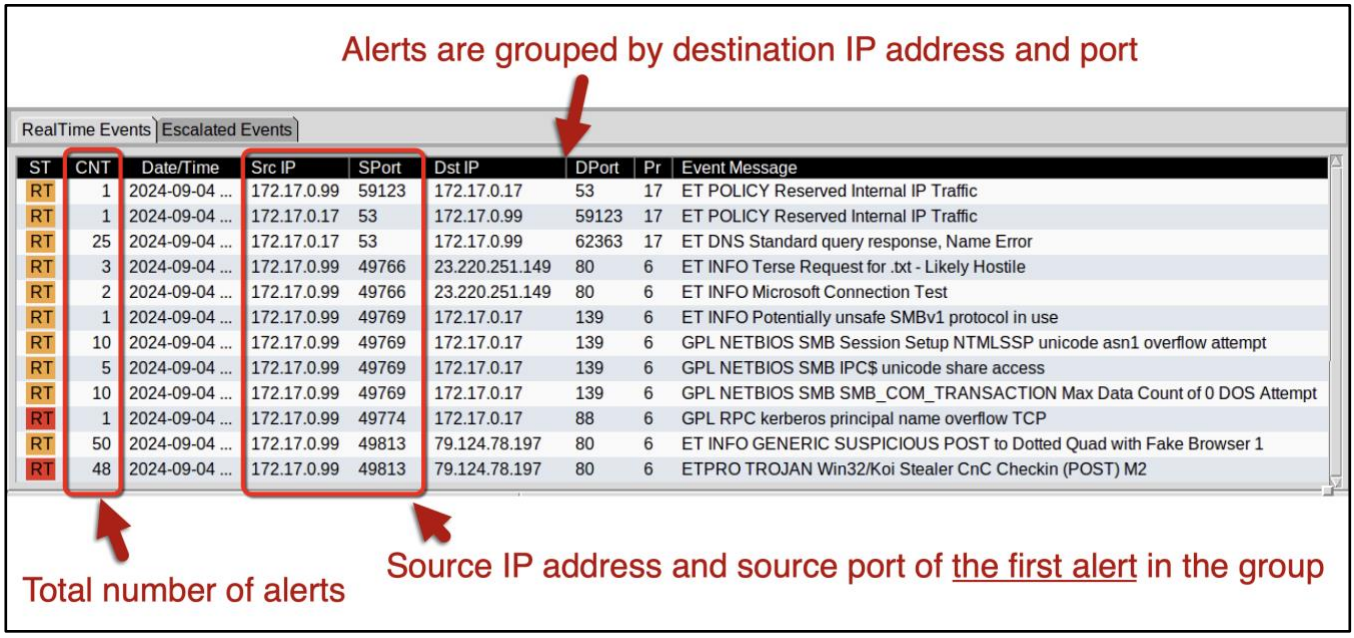
HINTS:

Note: The alerts are grouped according to the destination IP address. In the alert image and text files, we only see the source IP and source port from the first in a group of alerts.

The **ETPRO TROJAN Win32/Koi Stealer CnC Checkin (POST) M2** entry shows 48 alerts. The Source IP `172.17.0.99` and port `49813` is only for the first alert.

2024-08-15 - TRAFFIC ANALYSIS EXERCISE ANSWERS

If we had access to the alert system, we could confirm that all the alerts for this entry were from `172.17.0.99` with several different source ports.



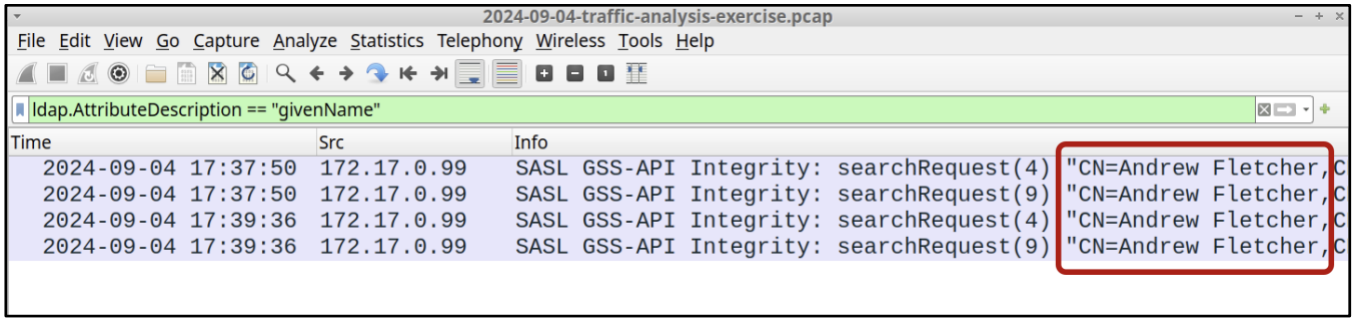
ST	CNT	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	2024-09-04 ...	172.17.0.99	59123	172.17.0.17	53	17	ET POLICY Reserved Internal IP Traffic
RT	1	2024-09-04 ...	172.17.0.17	53	172.17.0.99	59123	17	ET POLICY Reserved Internal IP Traffic
RT	25	2024-09-04 ...	172.17.0.17	53	172.17.0.99	62363	17	ET DNS Standard query response, Name Error
RT	3	2024-09-04 ...	172.17.0.99	49766	23.220.251.149	80	6	ET INFO Terse Request for .txt - Likely Hostile
RT	2	2024-09-04 ...	172.17.0.99	49766	23.220.251.149	80	6	ET INFO Microsoft Connection Test
RT	1	2024-09-04 ...	172.17.0.99	49769	172.17.0.17	139	6	ET INFO Potentially unsafe SMBv1 protocol in use
RT	10	2024-09-04 ...	172.17.0.99	49769	172.17.0.17	139	6	GPL NETBIOS SMB Session Setup NTMLSSP unicode asn1 overflow attempt
RT	5	2024-09-04 ...	172.17.0.99	49769	172.17.0.17	139	6	GPL NETBIOS SMB IPC$ unicode share access
RT	10	2024-09-04 ...	172.17.0.99	49769	172.17.0.17	139	6	GPL NETBIOS SMB SMB_COM_TRANSACTION Max Data Count of 0 DOS Attempt
RT	1	2024-09-04 ...	172.17.0.99	49774	172.17.0.17	88	6	GPL RPC kerberos principal name overflow TCP
RT	50	2024-09-04 ...	172.17.0.99	49813	79.124.78.197	80	6	ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1
RT	48	2024-09-04 ...	172.17.0.99	49813	79.124.78.197	80	6	ETPRO TROJAN Win32/Koi Stealer CnC Checkin (POST) M2

Shown above: Explanation of alert groupings.

The common internal, non-routable IPv4 address for all of the alerts is `172.17.0.99`. To find further victim information, use the [Identifying Hosts and Users](#) Wireshark tutorial I wrote.

This is slightly different than what I have in my Wireshark tutorial, but you can use the following Wireshark filter to help find the victim's first and last name in the pcap:

```
ldap.AttributeDescription == "givenName"
```

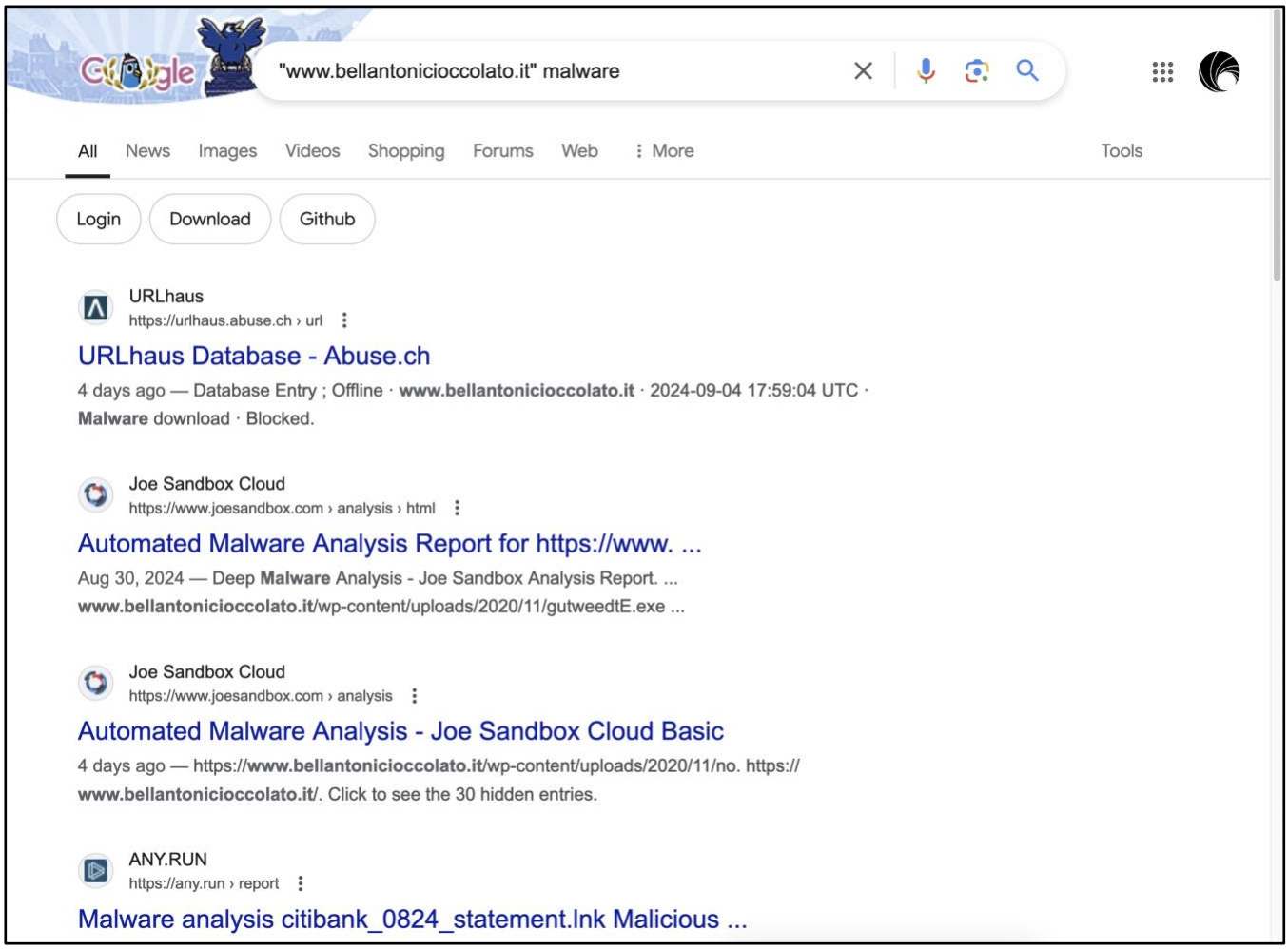


Shown above: Finding the victim's first & last name in the pcap using above Wireshark filter for LDAP.

2024-08-15 - TRAFFIC ANALYSIS EXERCISE ANSWERS

Unlike last month's exercise, we don't have any indication of how this host was infected with Koi Stealer. If the infected host is a laptop, it may have been infected while the user was at home and not connected to the monitored corporate network.

HTTPS traffic to `www.bellantonicioccolato.it` is also in this pcap, and it is likely associated with this infection. If you search Google for the domain plus the term "malware" you should find sandbox analysis and other entries that indicate the site is associated with Koi Loader/Koi Stealer activity.



Shown above: Google search results linking `www.bellantonicioccolato.it` to malware or malicious activity.

The site appears to be legitimate, even if was compromised and used by the criminals behind this malware. Based on our pcap alone, we cannot 100% confirm the traffic here is related to the Koi Stealer infection, but we could add it to the indicators of compromise section as likely or probably related.