

Author : Muoki Caleb  
Date : 02/08/2019

# Introduction.

The aim of this project is to analyse the pcap provided and come up with a report containing:

- Date and approximate time of the infection.
- The infected computer's IP address.
- The infected computer's MAC address.
- The infected computer's host name.
- What caused the infection

The tools used will be:

- wireshark

An extensive description of the lab is in the provided pdf file.

## The infected computer's IP address.

For a computer to communicate on a network it needs an ip address. There are two types; a static ips and dynamic ips. Most networks use a dynamic ips using a wireshark filter bootp we can get the ips that are being used on the network.

bootp			
Time	Source	Source Port	Destination
2015-11-24 16:13:42	10.1.25.1	67	10.1.25.119
2015-11-24 16:13:45	10.1.25.1	67	10.1.25.119
2015-11-24 16:13:48	10.1.25.1	67	10.1.25.119
2015-11-24 16:18:42	10.1.25.1	67	10.1.25.119
2015-11-24 16:18:44	10.1.25.1	67	10.1.25.119
2015-11-24 16:18:49	10.1.25.1	67	10.1.25.119
2015-11-24 16:20:18	10.1.25.1	67	10.1.25.119
2015-11-24 16:13:42	0.0.0.0	68	255.255.255.255
2015-11-24 16:13:45	0.0.0.0	68	255.255.255.255
2015-11-24 16:13:48	10.1.25.119	68	255.255.255.255
2015-11-24 16:18:42	0.0.0.0	68	255.255.255.255
2015-11-24 16:18:44	0.0.0.0	68	255.255.255.255
2015-11-24 16:18:49	10.1.25.119	68	255.255.255.255
2015-11-24 16:20:18	10.1.25.119	68	255.255.255.255

There are 2 ips 10.1.25.1 and 10.1.25.119. 10.1.25.1 is the server ip while 10.1.25.119 is a client ip. This network has one host machine. This method makes the assumption that the network is using dhcp. A better way would be to get all the ips this takes care of the fact that the network may be using static ips. In wireshark there is a option to view the statistics of the pcap . We can view all the ipv4 ips in the pcap.

private/local ip address ranges are usually:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255

- 192.168.0.0 – 192.168.255.255

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	B
▼ Source IPv4 Addresses	24240				0.0465	100%	3.3100	2
0.0.0.0	4				0.0000	0.02%	0.0100	0
10.1.25.1	7				0.0000	0.03%	0.0100	0
10.1.25.119	12666				0.0243	52.25%	1.7500	1
107.21.201.133	8				0.0000	0.03%	0.0200	1
107.21.249.50	6				0.0000	0.02%	0.0200	1
108.168.240.194	8				0.0000	0.03%	0.0200	4
128.177.96.9	38				0.0001	0.16%	0.2600	1
130.211.114.37	9				0.0000	0.04%	0.0400	8

From this we can tell that there are 2 local ips on the network, 10.1.25.1 and 10.1.25.119. The host device is 10.1.25.119. To find more details about the device we can use filter `bootp && ip.addr==10.1.25.119`.

```

▼ Bootstrap Protocol (Inform)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0xc51e3d5a
  Seconds elapsed: 0
  ▼ Bootp flags: 0x0000 (Unicast)
    0... .. = Broadcast flag: Unicast
    .000 0000 0000 0000 = Reserved flags: 0x0000
  Client IP address: 10.1.25.119
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: Dell_a6:9c:1b (a4:1f:72:a6:9c:1b)
  Client hardware address padding: 000000000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  ▶ Option: (53) DHCP Message Type (Inform)
  ▶ Option: (61) Client identifier
  ▼ Option: (12) Host Name
    Length: 10
    Host Name: Turkey-Tom
  ▶ Option: (60) Vendor class identifier
  ▶ Option: (55) Parameter Request List

```







from this can tell that the:

- Ip address is 10.1.25.119
- Mac address is a4:1f:72:a6:9c:1b
- Host name is Turkey-Tom

## Identifying the cause of infection.

One can replay the pcap using `tcpdump` then listen to using an ids like `snort` to identify infections. In my case I opted to using an online platform to analyze the traffic due to lack of

system resources. I uploaded the pcap to [packettotal](#).

<input type="text" value="Search in results"/>				
Timestamp	Alert Description	Alert Signature	Severity	Sender IP
 2015-11-24 16:15:06 Z	Potential Corporate Privacy Violation	ET POLICY Outdated Flash Version M1	1	10.1.25.119
 2015-11-24 16:16:15 Z	Potential Corporate Privacy Violation	ET POLICY Outdated Flash Version M1	1	10.1.25.119
 2015-11-24 16:16:38 Z	A Network Trojan was detected	ET TROJAN Possible Bedep Connectivity Check	1	10.1.25.119
 2015-11-24 16:16:38 Z	A Network Trojan was detected	ET TROJAN Bedep Connectivity Check M2	1	10.1.25.119
 2015-11-24 16:16:42 Z	A Network Trojan was detected	ET TROJAN Bedep HTTP POST CnC Beacon	1	10.1.25.119
 2015-11-24 16:16:43 Z	A Network Trojan was detected	ET TROJAN Known Sinkhole Response	1	166.78.145.90

Among the alert signatures I found the name Bedep . I did a google search on Bedep and found that:

Bedep is a trojan that opens a backdoor on a compromised system and can provide a malicious actor with full control over the system, as well as download additional malware. Once executed, Bedep can facilitate the theft of information or be used to perform click fraud to visit specific websites for financial gain. According to TrendMicro, the Bedep trojan is also used to turn infected systems into botnets for other malicious activities. Users are typically infected with Bedep through exposure to malicious advertising (malvertising) or exploit kits on compromised websites. When a user visits a webpage hosting a malvertisement, an exploit kit (EK) such as Angler or Hanjuan identifies a vulnerability on the user's machine to exploit and deliver Bedep. According to F-Secure, Bedep creates a hidden virtual desktop on the victim's computer, with an instance of Internet Explorer which is used to view unsolicited websites. Bedep has primarily targeted victims in the United States, followed by Japan.

We can also tell that the infection happened around 2015-11-24 16:16:38. using the

sha256sum provided a search on virus total showed that the malware is also known as :

### Names ⓘ

---

d16ad130daed5d4f3a7368ce73b87a8f84404873cbfc90cc77e967a83c947cd2.bin.exe

BackUp1086666136.exe

backup2350556040.exe

We can say this is what infected the device.

### Summary.

- Date and approximate time of the infection. - 2015-11-24 16:16:38
- The infected computer's IP address. -10.1.25.119
- The infected computer's MAC address. -a4:1f:72:a6:9c:1b
- The infected computer's host name. - Turkey-Tom
- What caused the infection - Bedep trojan from an insecure website.