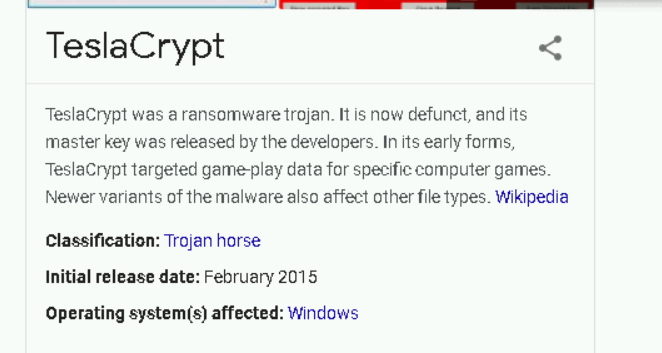
Afeefah Manzoor

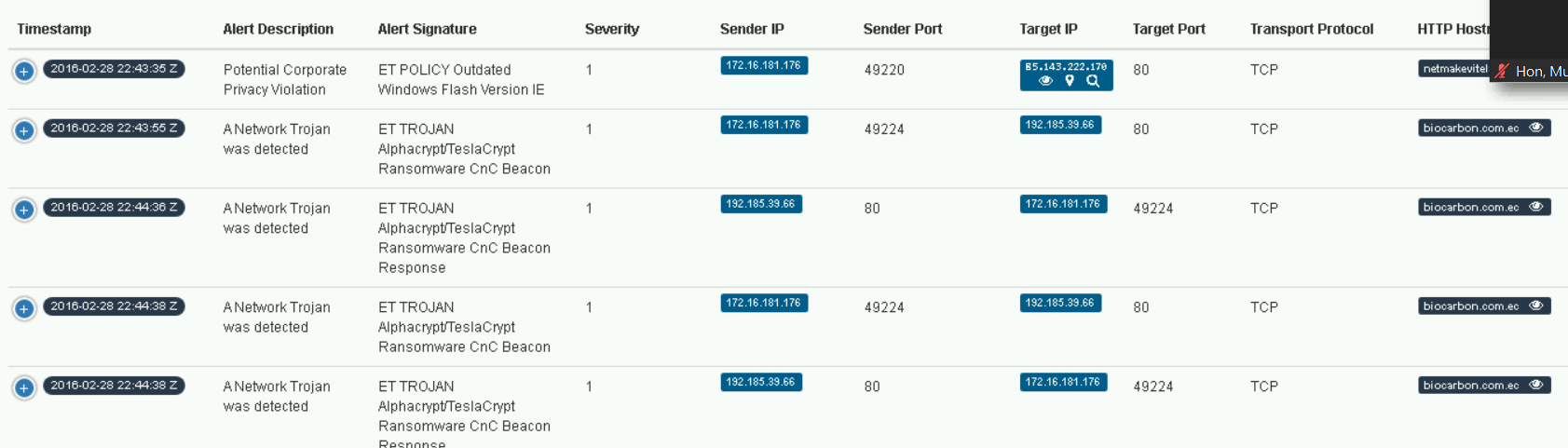
ITN 261

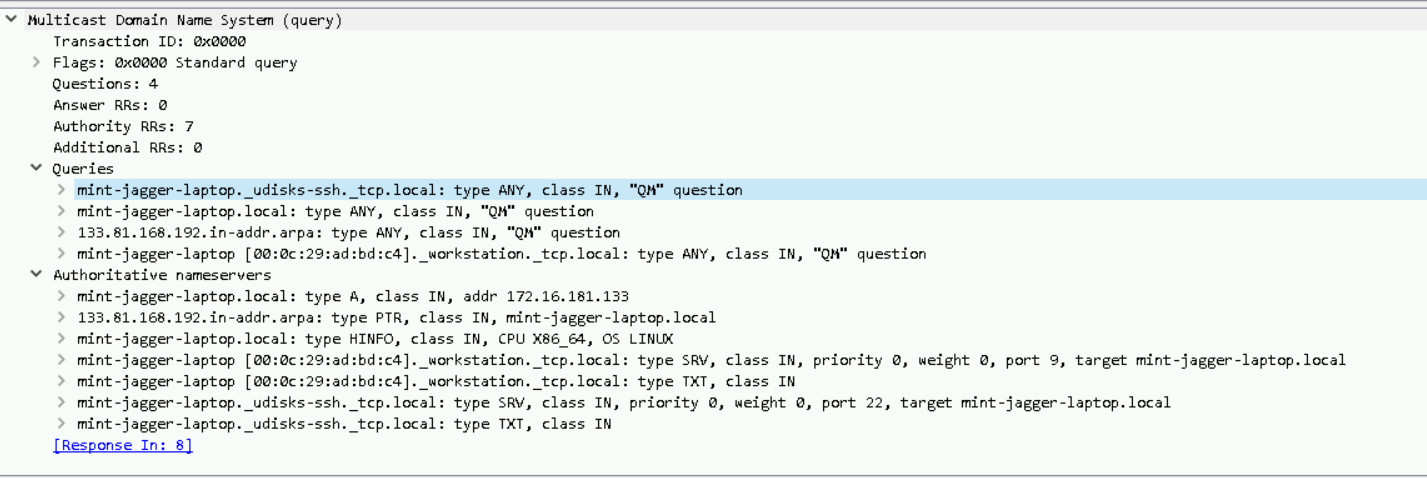
Quiz 2 Part 2

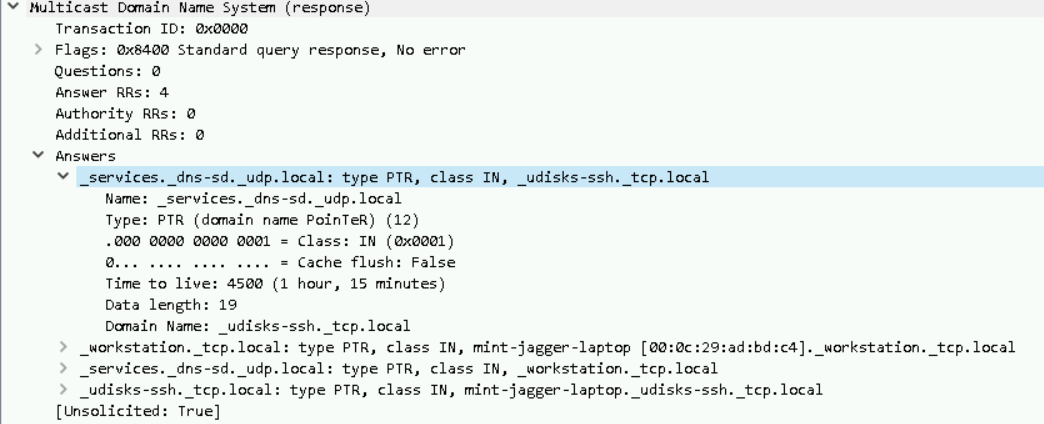
1. What Happened?

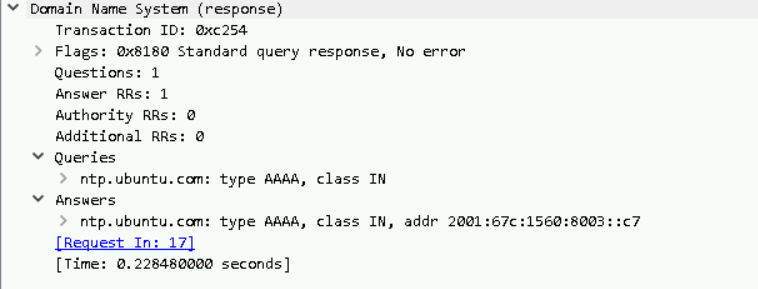






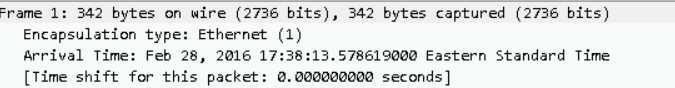


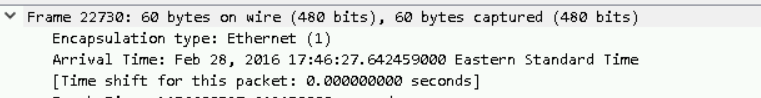




It seems like the hacker downloaded the TeslaCrypt Trojan on the infected device and was injected from another user creating access to log into the device and allowed itself access for an hour and 15 minutes and allowing access from an ubuntu OS.

1. Date/Time of activity?

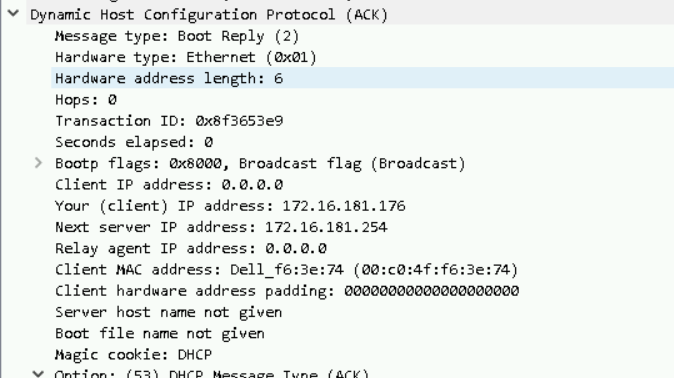




Started on Feb 28, 2016 at 5:38:13PM EST

Ended on Feb 28, 2016 at 5:46:27PM EST

1. IP address, MAC address, host name of infected device?



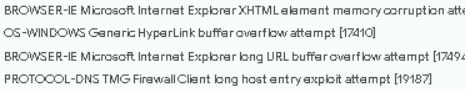
IP: 172.16.181.176 AND 172.16.181.254

MAC: 00:c0:4f:f6:3e:74

Host Name: not given

1. Conclusion with recommendations

The infected windows machine was infected with a Trojan name TelsaCrypt, injected through a shockwave application. The machine was taken over by an Ubuntu machine creating a privilege for them to connect themselves though the MDNS into the workgroup. The company should take a stricter authentication process and closing all unneeded ports.

1. Determine OS and applications of infected device.
2. 

OS: Windows

Applications: Microsoft Internet Explorer