tasks

- What is the IP address of the infected Windows client?

=> 10[.]1[.]17[.]215

- What is the mac address of the infected Windows client?

=> 00:d0:b7:26:4a:74

- What is the host name of the infected Windows client?

=> DESKTOP-L8C5GSJ

- What is the user account name from the infected Windows client?

=> shutchenson

- What is the likely domain name for the fake Google Authenticator page?

=> burleson-appliance.net

- What are the IP addresses used for C2 servers for this infection?

=> 5[.]252[.]153[.]241
45[.]125[.]66[.]32
45[.]125[.]66[.]252
239[.]255[.]255[.]250
204[.]79[.]197[.]203