Afeefah Manzoor

ITN261

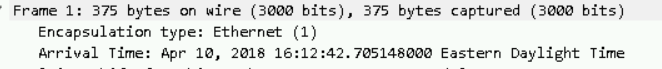
Quiz2 part 2

* Date/Time of the infection?

The machine was infected on April 10, 2018 at 8:14:26 PM UTC.

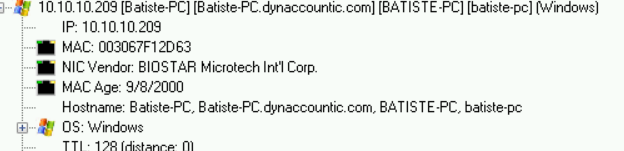
The pcap packet started on April 10,2018 at 4:12:42pm to 17:45:15pm EST





* Who was infected (IP address, host name, MAC address, and user account name)?

Batiste-PC was infected. They have an IP address of 10.10.10.209, MAC address of 00:30:67:f1:2d:63.



* What malware is involved?

A trickbot was installed on the machine

* The likely source of this infection?

The likely source of this infection came from <http://caveaudelteatro.it/ser0410.bin> thinking it was a legitimate website.

* Indicators associated with this infection (IP addresses, domains, URLs, and file hashes, if any)?

The IP of caveaudelteatro.it is 95.110.193.132

The MAC is 00:09:7b:fe:c2:8e

The hash is c2c1e2c22f67dda6553cbcc173694b68677b77319243684925e8dc3f78b3dbf8

And the File Type is PE32 executable (GUI) Intel 80386, for MS Windows