dns.pcap

1.

DNS: associates information with domain names, allows you to type letters to reach web sites instead of numbers

HTTP: made for transmitting hypermedia documents such as HTTP, used for communication between servers and browsers.

ARP: Address resolution protocol. Determines the link layer of address of an IP address.

DHCP: Dynamic Host Configuration Protocol. Assigns IP's dynamically so that devices scan communicate via other IP networks.

DHCPv6: Dynamic Host Configuration Protocol version 6. DHCP but for IPv6.

TCP: Transmission Control Protocol. Is a standard which determines how to maintain a conversation over a network. Works with IP.

TLSv1: Transport Layer Security version 1. Is used to add a security layer across a network.

2. There where 170 packets sent.

3. User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C)\r\n

The user agent helps identify what browser is being used and on what oerating system.

They are using Firefox and windows.

4. There is a response from oavpyybehhjtn.biz and from nnbqohfijmxfv.net based on this, I believe that the malware was able to establish a connection

http.pcap

1. Domain: http://trondyfeveryfeellnas.com/TZ/goboti.pyc

IP: 192.168.110.129

2. It is requesting a .pyc file. It is what the python interpreter creates when you import a library. The response is is an executable file.

unk.pcap

1. TCP and some UDP

2. 5002

3. Username: Josh

Password: password

4. The user logs in and then changes the working directory. He then enters admin mode, and lists everything in the current working directory. The user then sends some binary data.