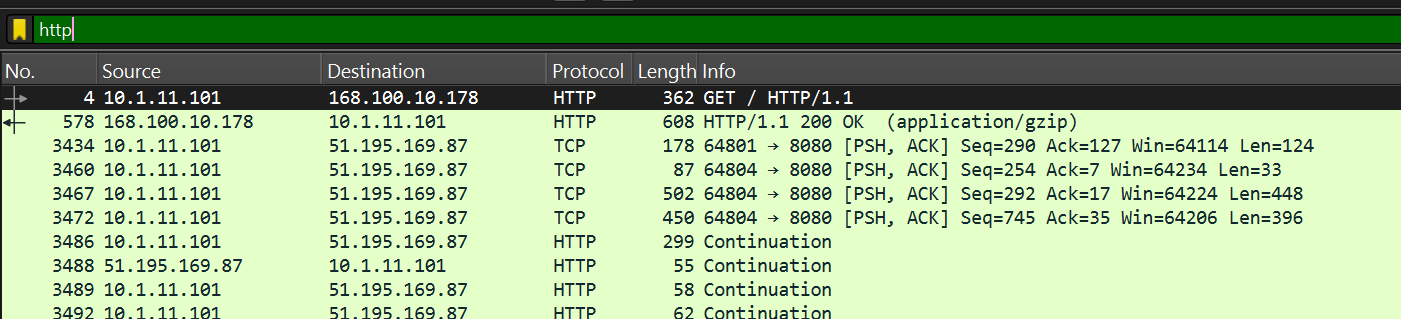
CT6034 Moc PCAP

**Part 1 - Basic Information:**

1. **What is the timestamp of the first packet in the capture?**
   * **Answer:** 2023-01-16 19:31:40.668975
2. **What is the IP address of the infected machine?**
   * **Answer:** Private IP 10.1.11.101
3. **What are some other IP addresses linked to?**
   * **Answer:**
   * 168.100.10.178 – initial download
   * 10.1.11.2 – DNS server
   * 89.44.9.157 – ICEDID C2 (ijoyzymama.com)
   * 5.230.74.203 – ICEDID C2 (felzater.lol)
   * 45.12.109.195 – ICEDID C2 (siantdarik.lol)
   * 51.195.169.87 – Backconnect traffic and keyhole vnc
   * 23.227.202.188 – Colbalt strike traffic (carkitservices.com)
4. **What ports were used for communication?**
   * **Answer: 80 http, 443 https, 8080 http proxy, tcp but unsuccessful**

**Part 2 - Traffic & Protocol Analysis:**

1. **What protocol is used for the initial malware download?**
   * **Answer:** http get request at line 4
2. **What is the URL used to download the malware?**
   * **Answer:** drgormiuatox.com – found following the http stream of packet 4

A screenshot of a computer

AI-generated content may be incorrect.

1. **What file type was downloaded as part of the infection?**
   * **Answer:** a gzip also found in the stream above
2. **What are the domain names contacted by the infected machine?**
   * **Answer:** all found simple dns query and seen on multiple packets
   * ijoyzymama.com
   * felzater.lol
   * A screenshot of a computer

     AI-generated content may be incorrect.siantdarik.lol
3. **What is the User-Agent string used during the malicious HTTP request?**
   * A screenshot of a computer

     AI-generated content may be incorrect.**Answer:** apply a user agent filter and look for any post request. Then, in the bottom left, expand the http section and see your answer in the user agent tab or hex
4. **How long does the infected machine communicate with the C2 server?**

* **Answer:** can filter or look at the conversations then go to TCP or UDP
* **Remember there are 3 C2 servers:**
  + 89.44.9.157 – ICEDID C2 (ijoyzymama.com) – roughly 3 mins all together
  + 5.230.74.203 – ICEDID C2 (felzater.lol) – 21 seconds
  + 45.12.109.195 – ICEDID C2 (siantdarik.lol) – 30 mins+ all together

**Part 3 - Suspicious Behaviour & Indicators:**

1. **Is there evidence of encrypted traffic? If so, what protocol is used?**

* **Answer:** apply a tls or ssl filter to see all data. Look for key exchange packets and find out the encryption used in tls
* A screenshot of a computer

  AI-generated content may be incorrect.you can also look at protocol hierarchy in statistics. A high amount of tls end packets indicates encrypted c2 traffic

1. **Does the infected machine attempt to resolve suspicious domains?**

* **Answer:** apply a ds request filter then I the info column, look for responses with odd looking names
  + ijoyzymama.com
  + felzater.lol
  + siantdarik.lol
  + carkitservices.com

A screen shot of a computer

AI-generated content may be incorrect.

**Part 4 - Anomaly Detection:**

1. **Does the infected machine scan for open ports on other devices?**

* **Answer:** tcp.flags.syn == 1 && tcp.flags.ack == 0

A screenshot of a computer

AI-generated content may be incorrect.Using this will get rick of ACK responses usually scanning doesn’t have this.

1. **Is there any evidence of lateral movement? What IPs are contacted internally?**

* A screenshot of a computer

  AI-generated content may be incorrect.**Answer:** Take your source IP as the infected then map it with a private IP address as the destination.

1. **What is the longest TCP session observed in the pcap?**

* **Answer:** go into conversation then statistic. Look at tcp and find the longest duration

A screenshot of a computer screen

AI-generated content may be incorrect.

1. **Is there evidence of data exfiltration? If so, how much data was sent externally?**

* A screenshot of a computer

  AI-generated content may be incorrect.**Answer:** Filter for large amounts of packets to only external IP addresses

1. Are there any certificates that you can find and if so, what are the issues with them

* A screenshot of a certificate

  AI-generated content may be incorrect.You will see that the certificates being sent are being singed and issued by localhost

1. How is persistence achieved with backconnect and vnc

* A screenshot of a computer

  AI-generated content may be incorrect.Look over the localhost from the certificate and see if any malware was sent with the http

1. Attempt to create a timeline of events from start to finish.
2. Draw/map out all network-based devices