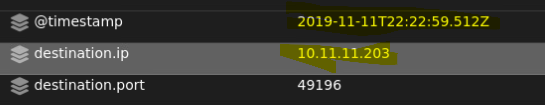
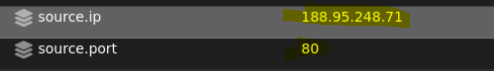
**Mamadou Bah**

**Pcap Analysis**

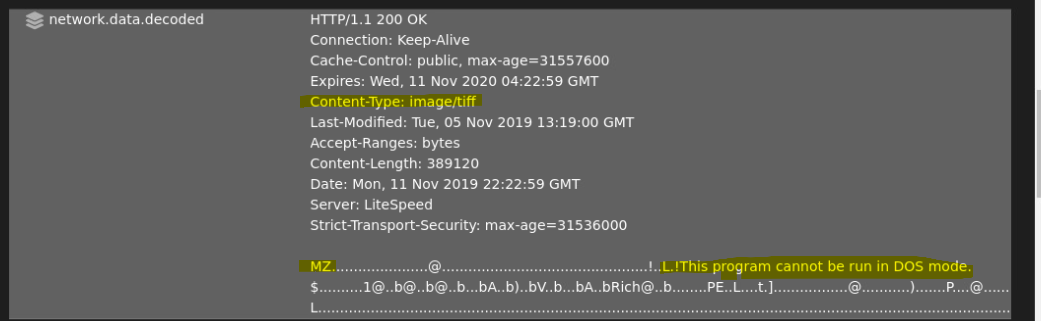
**11/12/2024**



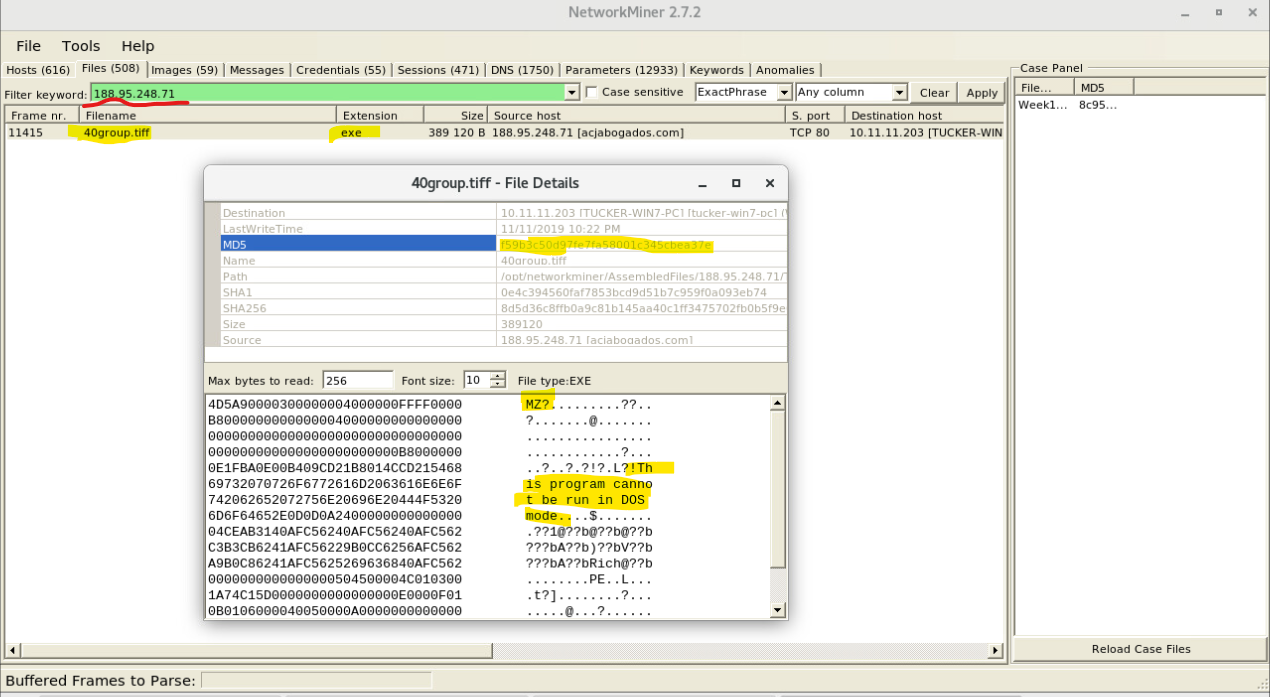




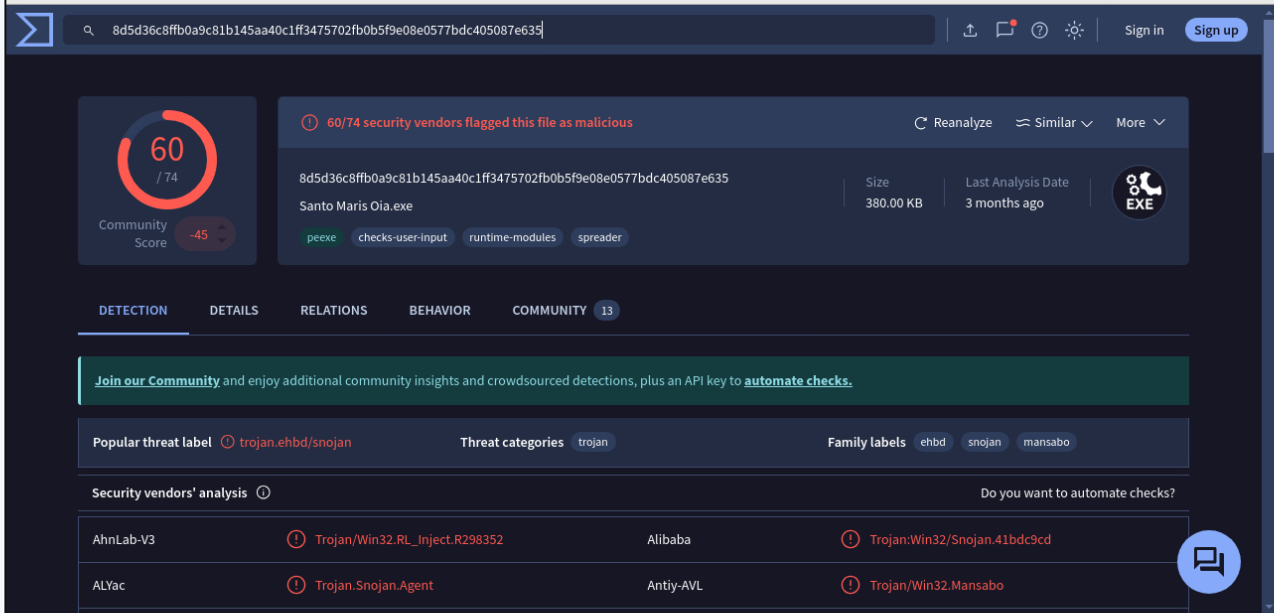
The source IP is 188.95.248.71 on port 80 and destination IP is 10.11.11.203 (internal machine)



Network.data.decoded shows the content type of the downloaded executable to be an image/tiff

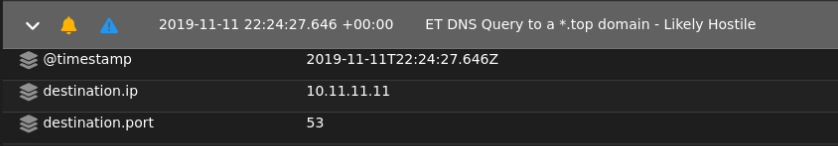


Network miner shows the name of the file that was downloaded and the file type to be an executable



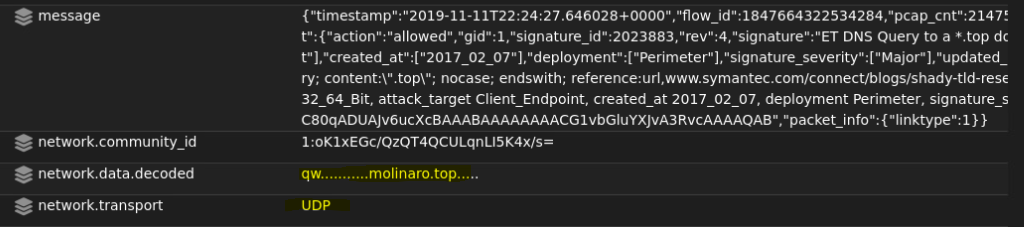
Looking up the md5 hash of the file in virustotal shows it to be malicious

**Summary:** This alert indicates that an internal machine with IP 10.11.11.203 downloaded a file from an external source at 188.95.248.71 over port 80. The content type was labeled as image/tiff, suggesting it might be a harmless image file, further analysis using Network Miner revealed that the file was actually a Windows executable. This mislabeling technique can be used by attackers to evade detection by security tools that filter based on content type. Additionally, a VirusTotal scan of the file's MD5 hash confirmed it to be malicious, indicating that this download likely posed a security risk, potentially introducing malware onto the internal machine.

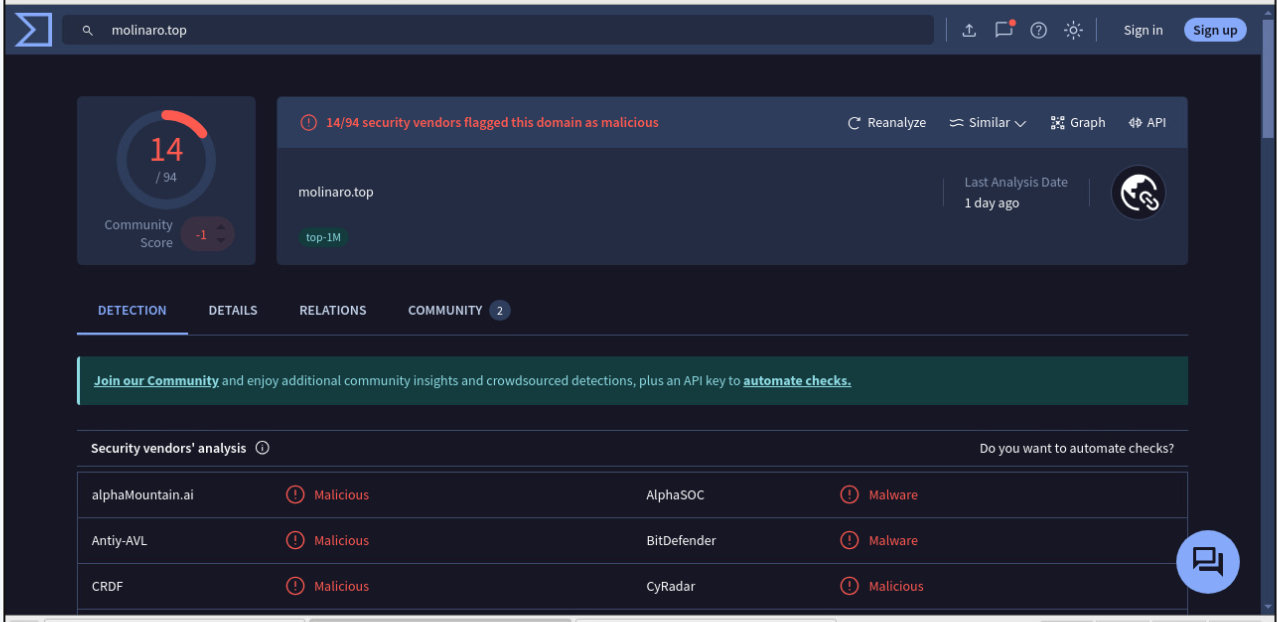




The source IP 10.11.11.203 (internal machine) and destination IP 10.11.11.11 (DNS server)

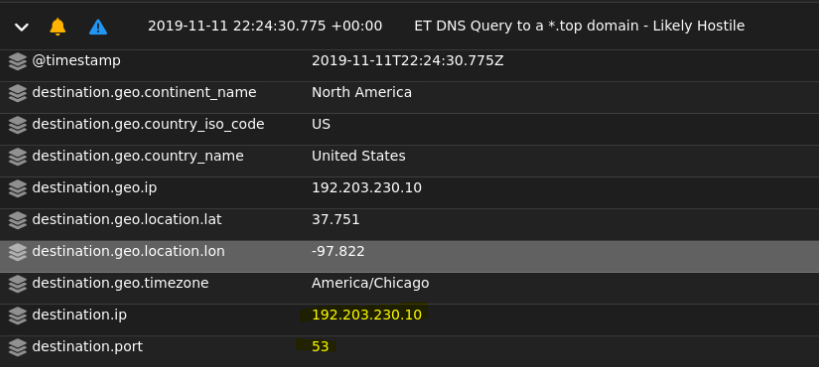


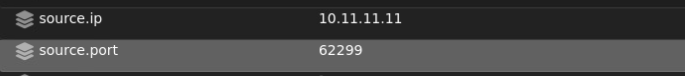
Network.data.decoded shows the DNS query to a .top domain and the network.transport is UDP



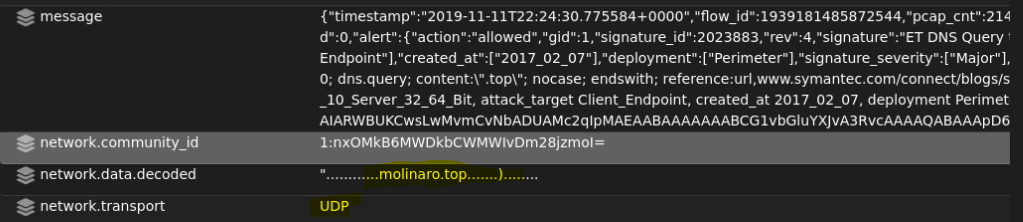
Virustotal shows the .top domain to be malicious

**Summary:** The alert indicates that an internal machine with IP 10.11.11.203 sent a DNS query to its DNS server at 10.11.11.11 over UDP to resolve a .top domain. Domains with the .top TLD are often associated with suspicious or malicious activities, and VirusTotal has flagged this specific domain as malicious. This DNS query likely indicates that the internal machine is attempting to communicate with a potentially hostile domain, which could be related to malware activity or an attempt to reach a command-and-control server.

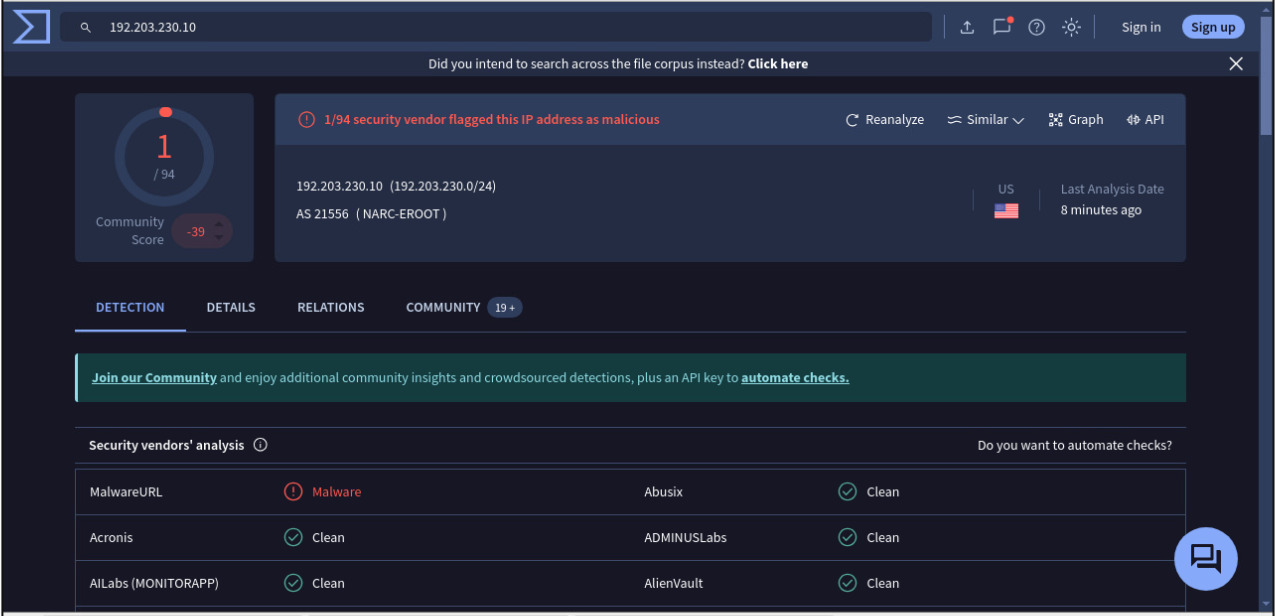




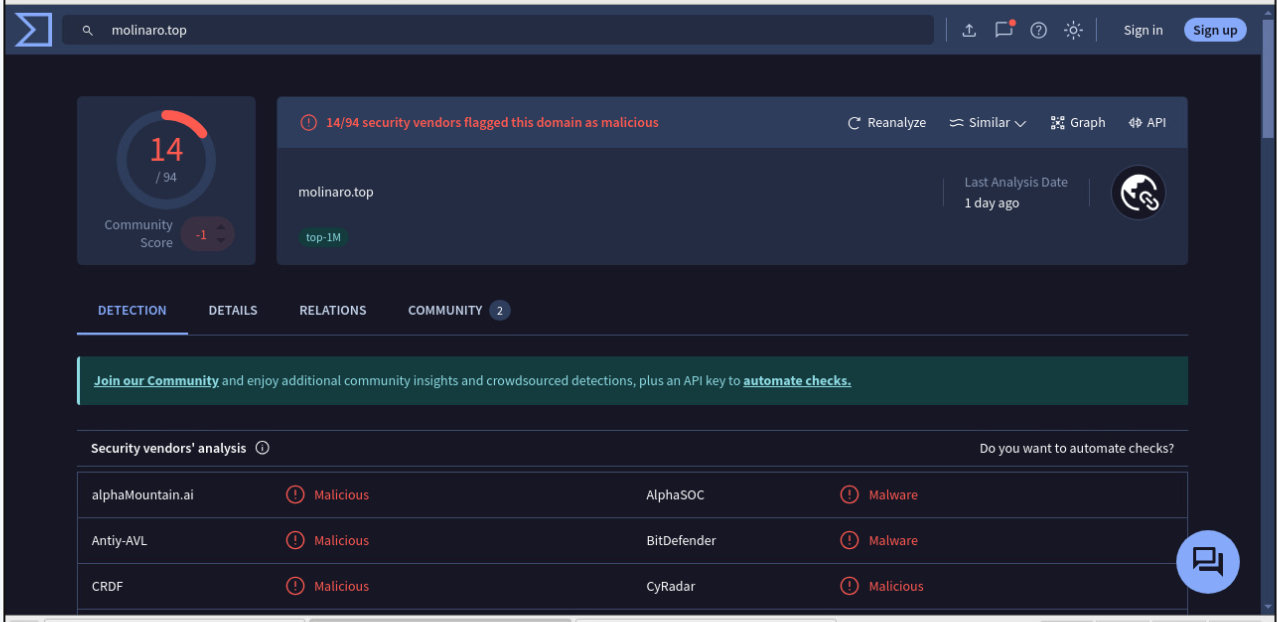
The source IP 10.11.11.11 (DNS server) and destination IP 192.203.230.10 on port 53



Network.data.decoded shows the DNS query to a .top domain and the network.transport is UDP



Virustotal shows the destination IP 192.203.230.10 to be potentially malicious



Virustotal shows the .top domain to be malicious

**Summary:** This alert shows that a DNS server within the network, with IP 10.11.11.11, made a DNS query to an external .top domain—a TLD often associated with malicious activities. The query was directed to 192.203.230.10 on port 53 using UDP as the transport protocol. Both the .top domain and the destination IP have been flagged as potentially malicious on VirusTotal, suggesting they may be used for harmful purposes, such as malware distribution or command-and-control operations. This DNS request likely represents an attempt by a device on the network to resolve a known malicious domain, potentially as part of a malware infection or unauthorized activity.