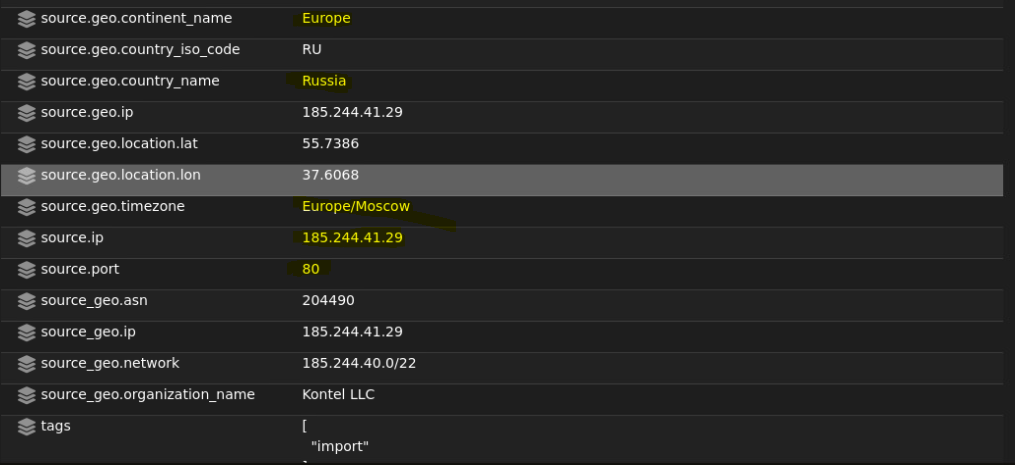
**Mamadou Bah**

**Pcap Analysis**

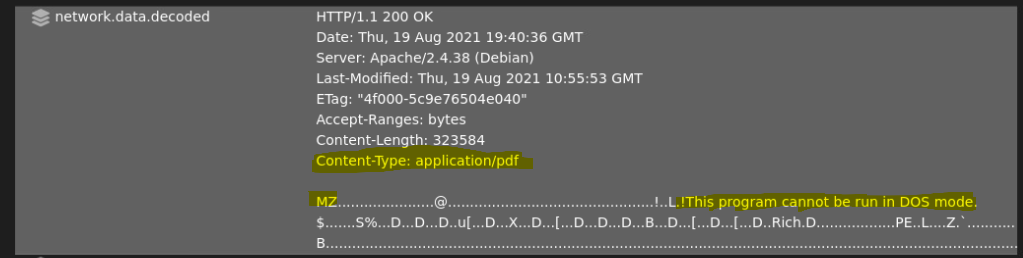
**11/08/2024**



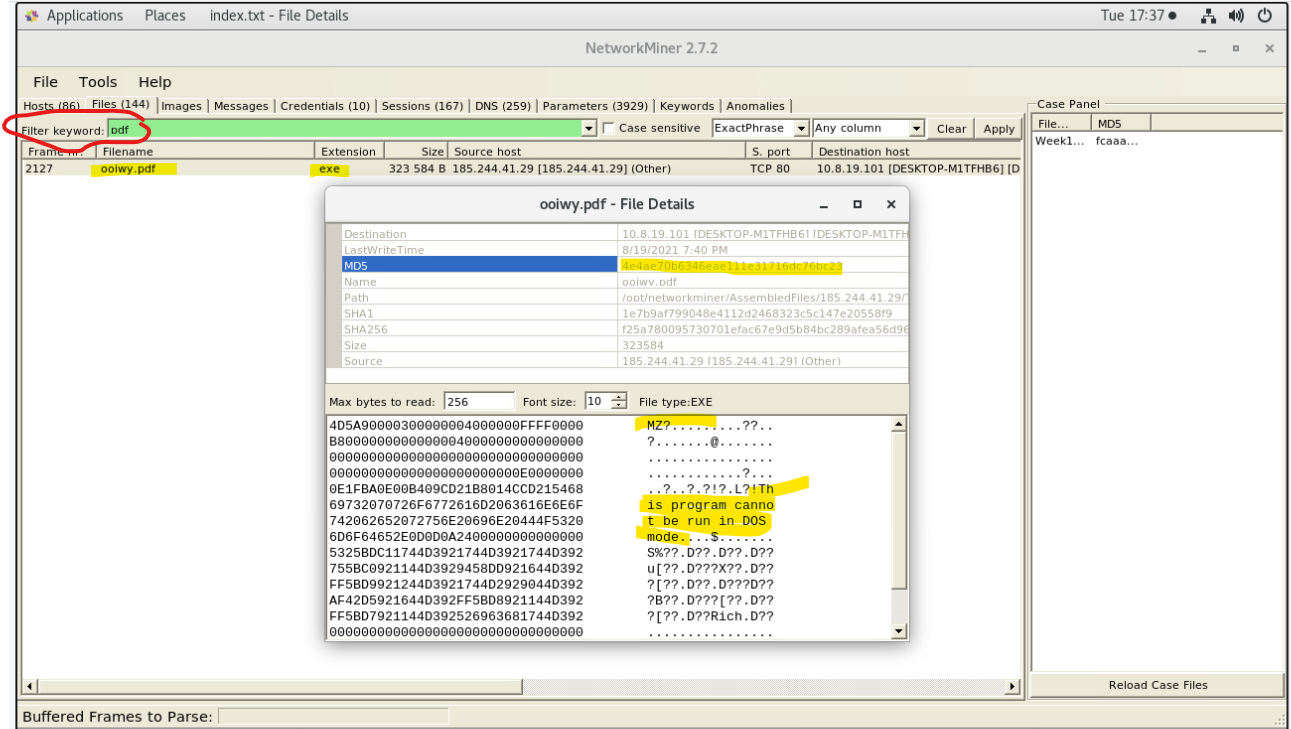




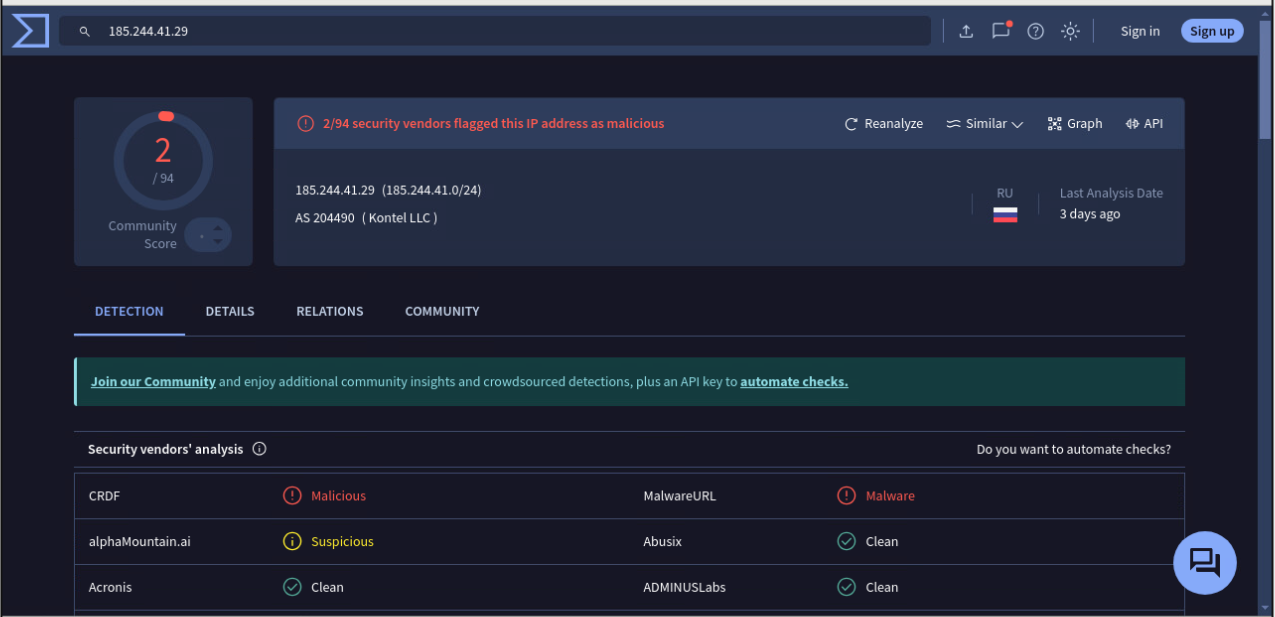
The file was downloaded at 19:40:36.717 on 2021-08-19 and it was downloaded to 10.8.19.101(internal machine) from 185.244.41.29 port 80.

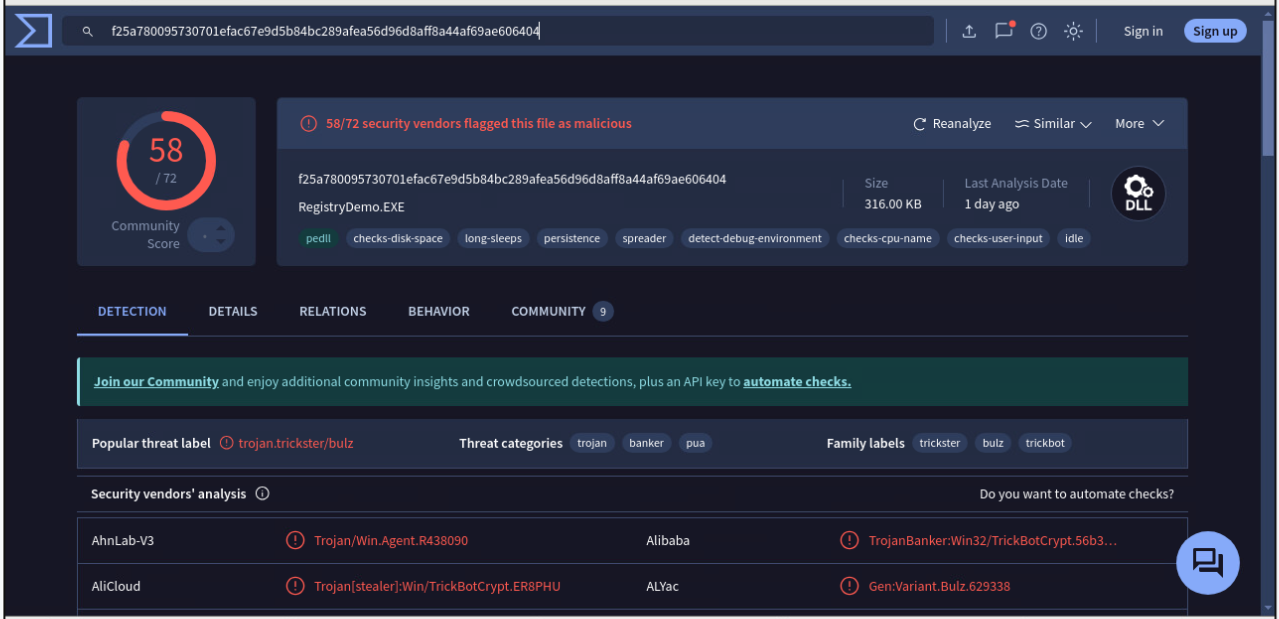


The network.data.decoded shows that a windows executable was downloaded and the Content-Type is an application/pdf.



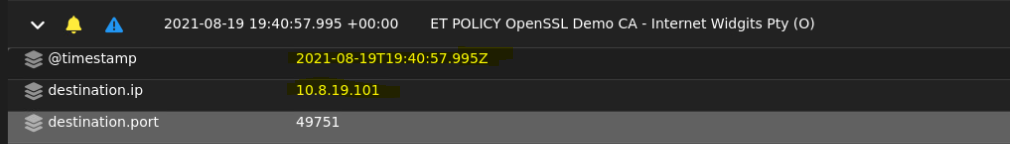
After finding out the type of file that was downloaded, filtering for “pdf” in the files tab on networkminer shows the filename “oolwy.pdf”

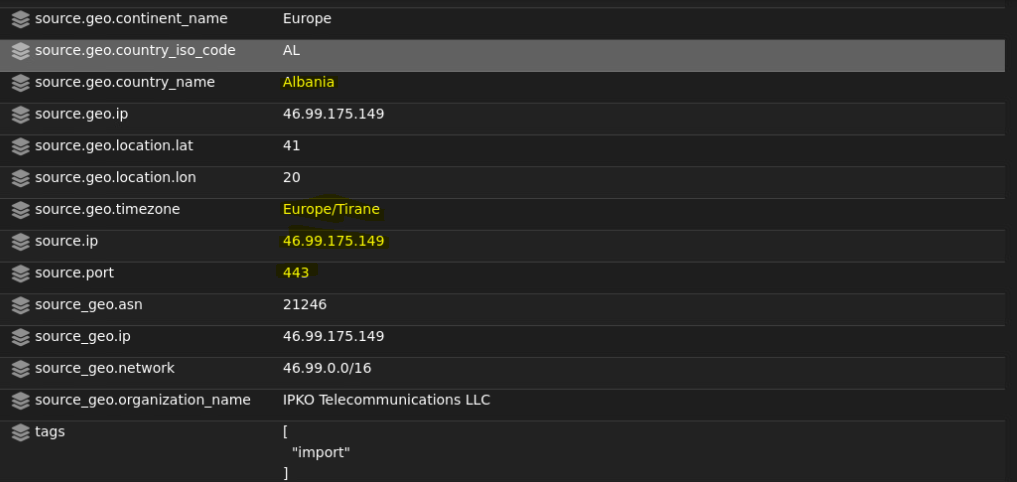




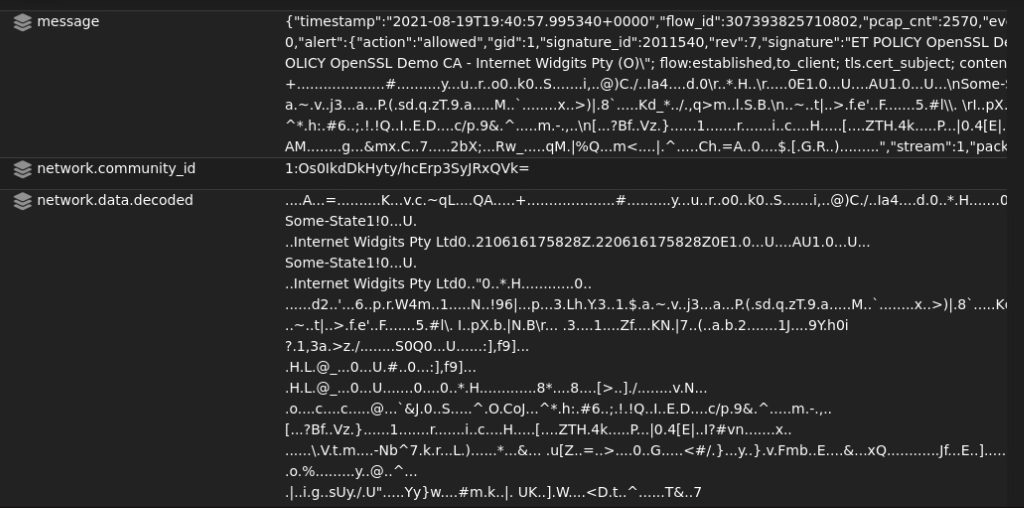
After looking up the MD5 hash of the oolwy.pdf file in virustotal it shows that the file is associated with TrickBot, a notorious banking trojan. TrickBot is designed to steal sensitive financial information, like online banking credentials, by using methods such as keylogging, form grabbing, and injecting malicious code into web browsers. It also often serves as a downloader for other malware, enabling attackers to install ransomware or gain remote control over infected systems.

**Summary:** The alert indicates a suspicious file download over HTTP, which was confirmed to be a Windows executable disguised as a PDF. At 19:40:36 on 08/19/2021, an internal machine at 10.8.19.101 downloaded a file from an external IP, 185.244.41.29 on port 80. Although the file was labeled as a PDF (application/pdf), network analysis revealed it to be a Windows executable with the filename oolwy.pdf. Further investigation into the file’s MD5 hash on VirusTotal identified it as linked to TrickBot, a well-known banking trojan that typically targets financial information. TrickBot can spread through networks, steal credentials, and facilitate other malware. This alert and subsequent findings indicate a potentially severe threat, as TrickBot often serves as a precursor for more extensive attacks, such as ransomware infections.

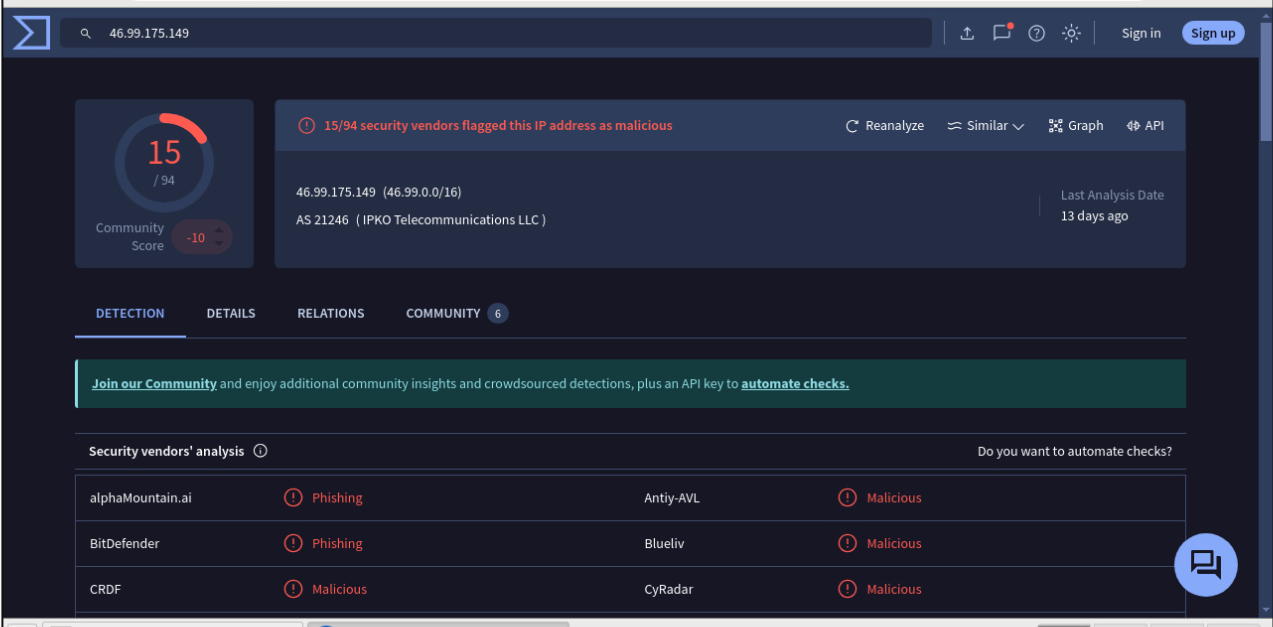
****



The source IP is 46.99.175.149 port 443 and destination IP is 10.8.19.101 (Internal Machine).

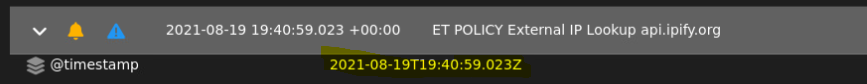
****

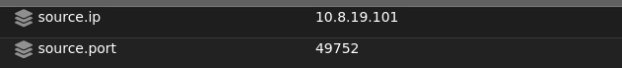
This alert indicates that a network connection is using an SSL/TLS certificate issued by the OpenSSL Demo Certificate Authority (CA), specifically from the organization "Internet Widgits Pty Ltd." This type of certificate is typically used for testing or demonstration purposes, not for secure communications in a production environment.

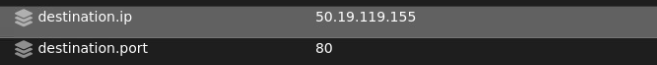


virustotal shows the source IP 46.99.175.149 as malicious.

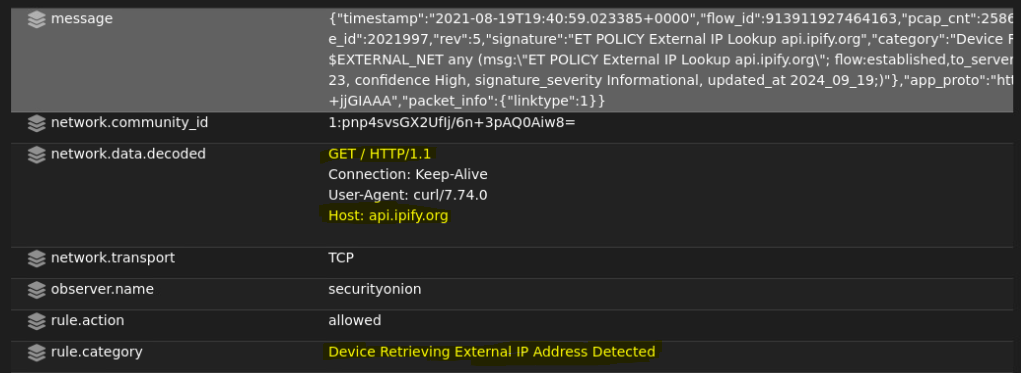
**Summary:** This alert indicates a network connection from a potentially malicious external source, IP 46.99.175.149 (using port 443), attempting to establish communication with an internal machine at 10.8.19.101. The SSL/TLS certificate involved in this connection is issued by the OpenSSL Demo Certificate Authority (CA) from the organization "Internet Widgits Pty Ltd." This specific demo certificate is intended only for testing purposes and lacks the security assurances needed for production use, making it vulnerable to interception and misuse. Additionally, VirusTotal flags the source IP as malicious, which raises further concern. A malicious IP using a demo CA certificate for SSL/TLS traffic suggests that this connection could be part of an attempt to disguise malicious activities under encrypted traffic. Attackers often exploit these insecure certificates to bypass security controls, avoid detection, or establish a foothold for further attacks, such as data exfiltration or command-and-control communications.

****

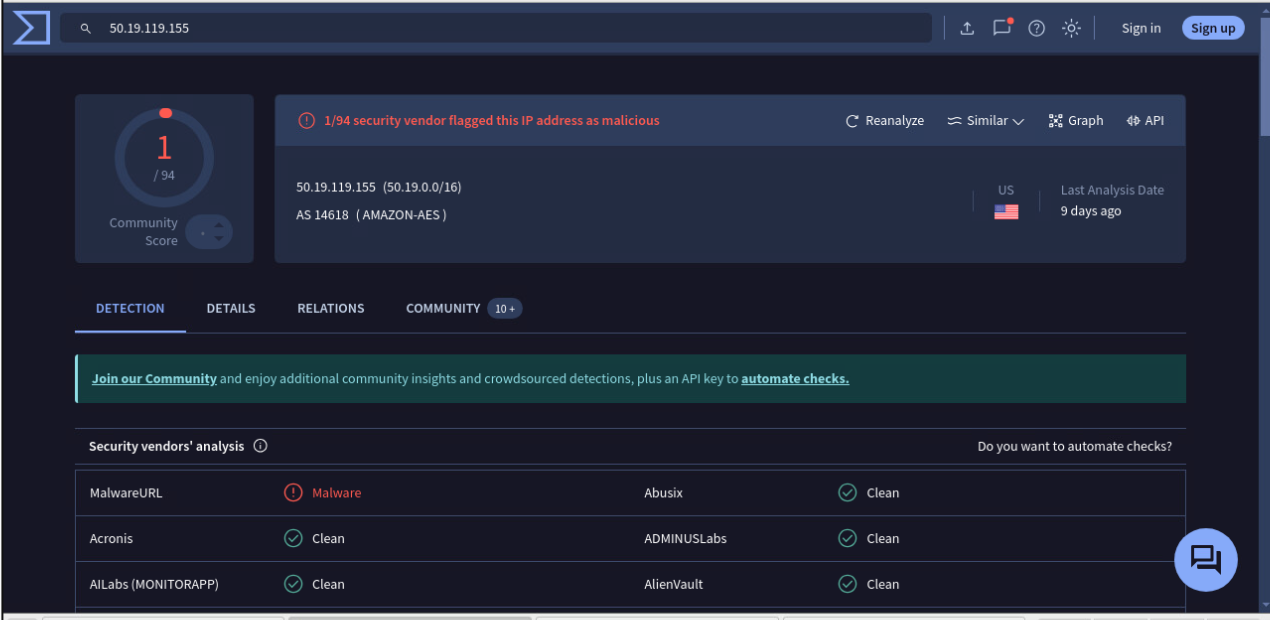
****

****

The source IP is 10.8.19.101 (internal machine) and destination IP is 50.19.119.155 port 80.

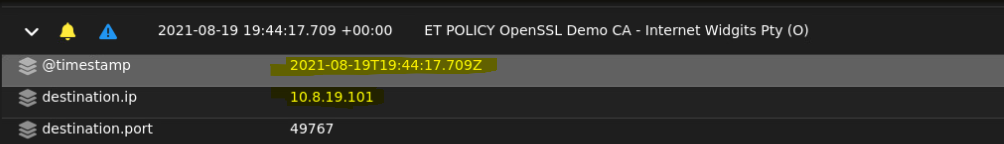
****

network.data.decoded shows the http.method used is GET and the Host is api.ipify.org

****

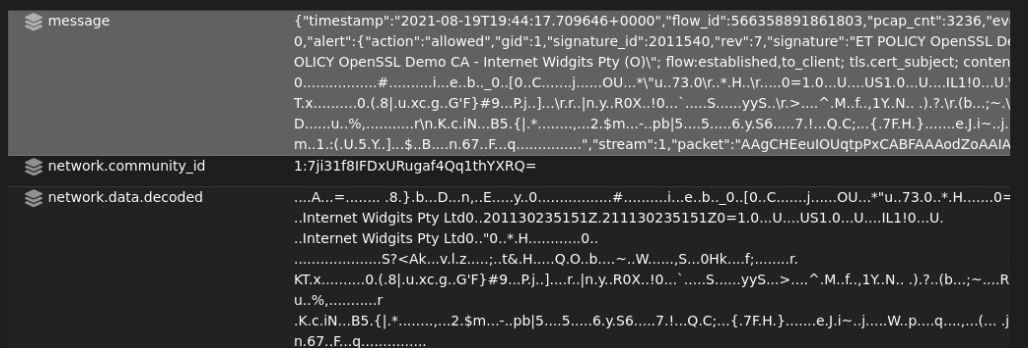
virustotal shows the destination IP 50.19.119.155 as potentially malicious.

**Summary:** Upon investigating the alert, it appears that an internal machine with IP address 10.8.19.101 made an outbound HTTP GET request to api.ipify.org hosted at 50.19.119.155 on port 80. The Host field in the request confirms the connection to api.ipify.org, which is commonly used to identify the external (public facing) IP of the requesting machine. The external IP address 50.19.119.155 has been flagged on VirusTotal as potentially malicious, which raises concerns. This activity may indicate an attempt by malware or an unauthorized user to confirm the public IP address of the network, potentially for establishing or maintaining external communication channels.

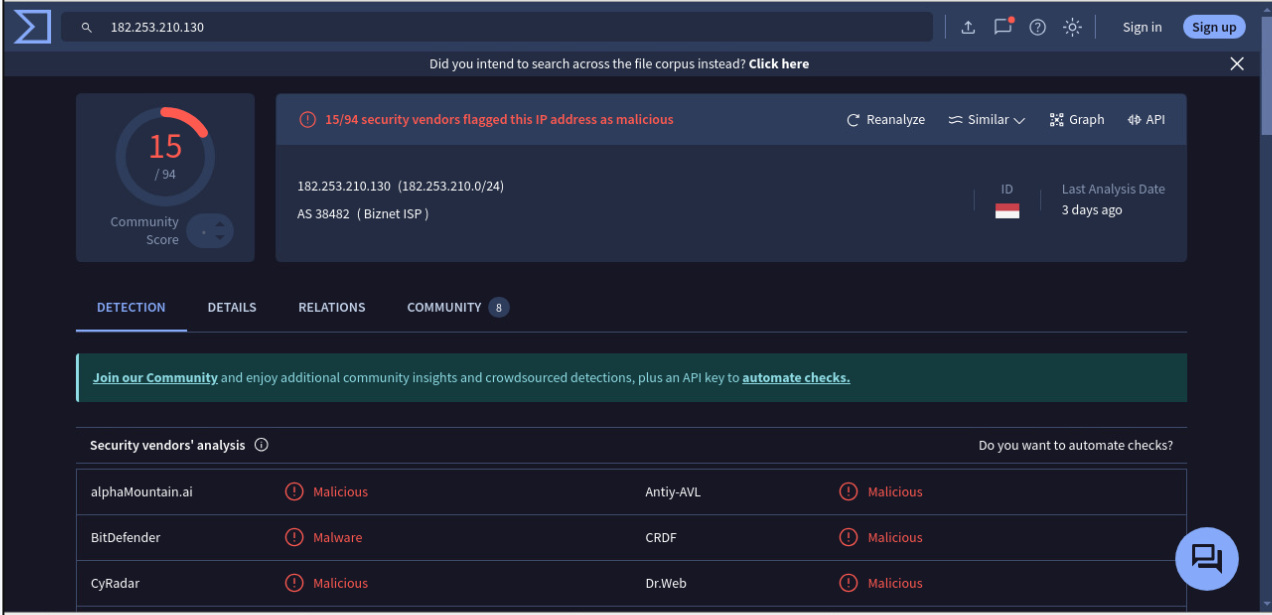
****

****

The source IP is 182.253.210.130 port 443 and destination IP is 10.8.19.101 (Internal Machine).

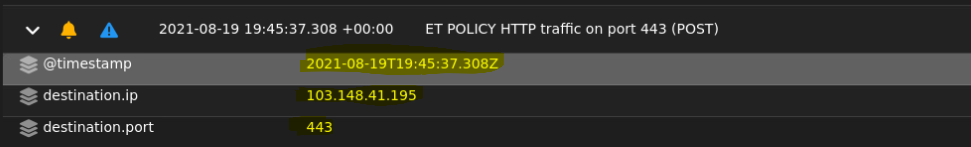
****

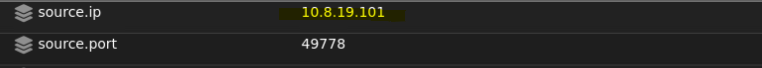
This alert indicates that a network connection is using an SSL/TLS certificate issued by the OpenSSL Demo Certificate Authority (CA), specifically from the organization "Internet Widgits Pty Ltd." This type of certificate is typically used for testing or demonstration purposes, not for secure communications in a production environment.

****

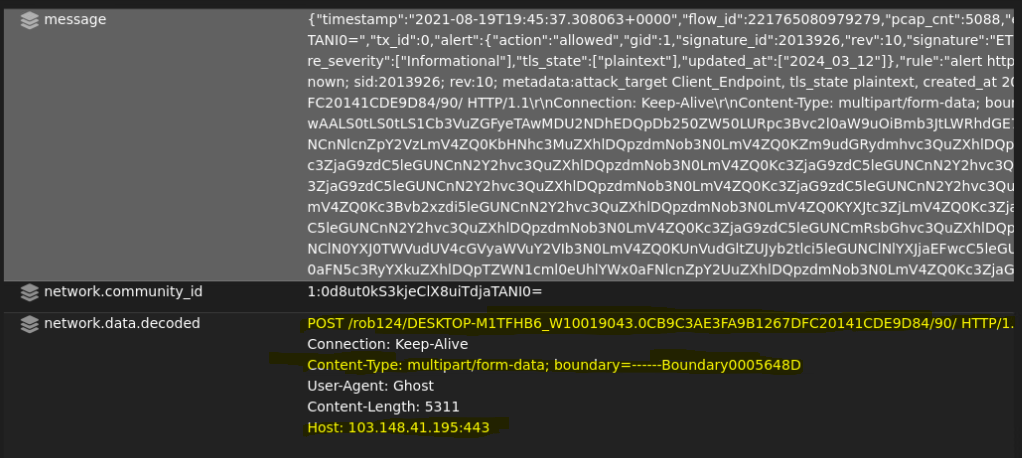
virustotal shows the source IP 182.253.210.130 as malicious.

**Summary:** This alert indicates a network connection from a potentially malicious external source, IP 182.253.210.130 (using port 443), attempting to establish communication with an internal machine at 10.8.19.101. The SSL/TLS certificate involved in this connection is issued by the OpenSSL Demo Certificate Authority (CA) from the organization "Internet Widgits Pty Ltd." This specific demo certificate is intended only for testing purposes and lacks the security assurances needed for production use, making it vulnerable to interception and misuse. Additionally, VirusTotal flags the source IP as malicious, which raises further concern. A malicious IP using a demo CA certificate for SSL/TLS traffic suggests that this connection could be part of an attempt to disguise malicious activities under encrypted traffic. Attackers often exploit these insecure certificates to bypass security controls, avoid detection, or establish a foothold for further attacks, such as data exfiltration or command-and-control communications.

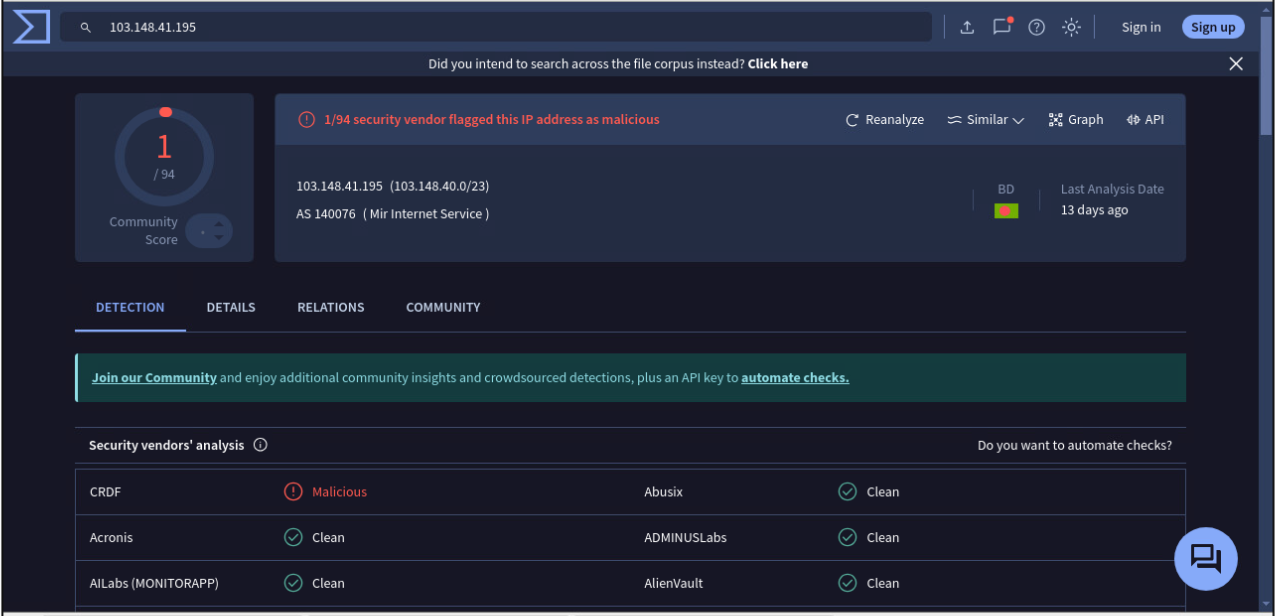
****

****

The source IP is 10.8.19.101 (internal machine) and destination IP is 103.148.41.195 port 443.

****

Network.data.decoded shows the post request and the Content-Type (multipart/form-data) which is commonly used for file uploads or transmitting structured data in HTTP POST requests. The User-Agent string typically identifies the software making the request (such as a web browser or legitimate app). Ghost isn’t a common User-Agent and may indicate a custom or potentially malicious script or tool designed to interact with the target server covertly. The host is the destination IP address.

****

virustotal shows the destination IP 103.148.41.195 as potentially malicious.

**Summary:** An internal machine with IP address 10.8.19.101 initiated a connection to a potentially malicious external server at 103.148.41.195 on port 443. Despite using port 443, which is typically reserved for encrypted HTTPS traffic, the connection contained HTTP POST requests with a Content-Type of multipart/form-data—a format commonly used for file uploads or structured data transmission. This choice of content type suggests that the request might be used to upload files or exfiltrate data to the remote server. Additionally, the User-Agent "Ghost" is unusual and may indicate the use of a non-standard or custom tool rather than a common web browser. This could point to a covert tool or script, possibly designed for malicious activity or data transfer, aiming to avoid detection by appearing as legitimate HTTPS traffic on port 443. VirusTotal flags the destination IP 103.148.41.195 as potentially malicious, reinforcing the likelihood that this connection is part of unauthorized activity, potentially for data exfiltration or command-and-control purposes.