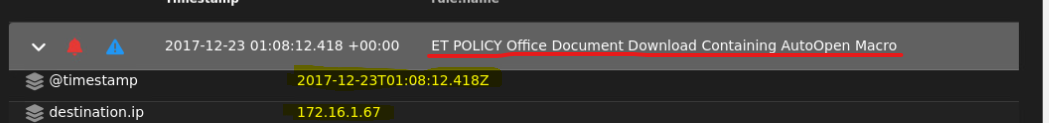
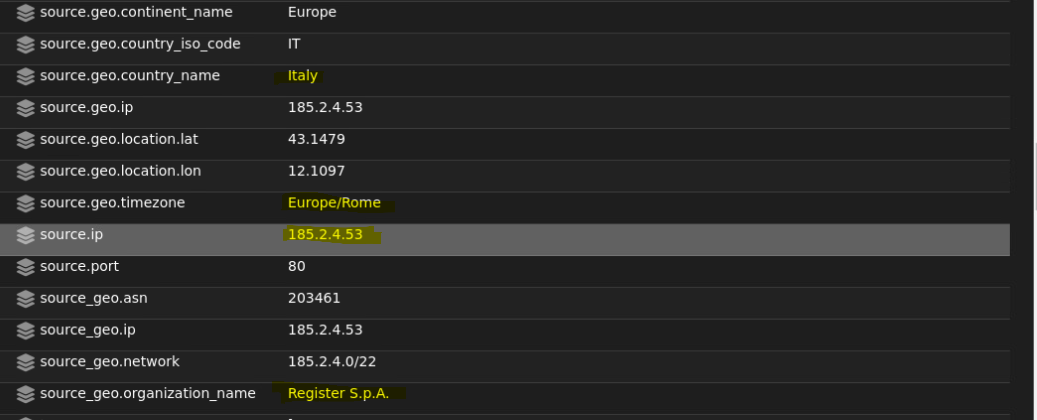
**Mamadou Bah**

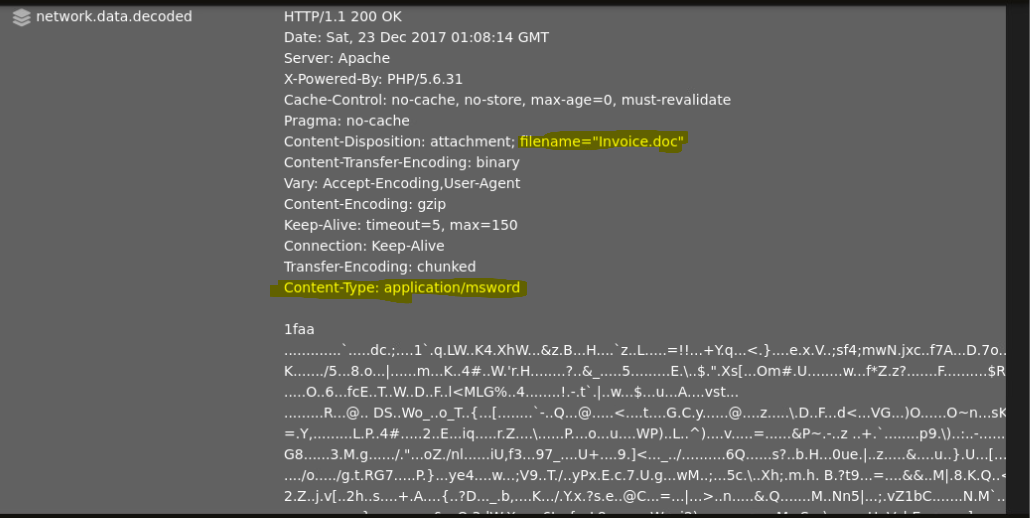
**Pcap analysis**

**11/07/2024**

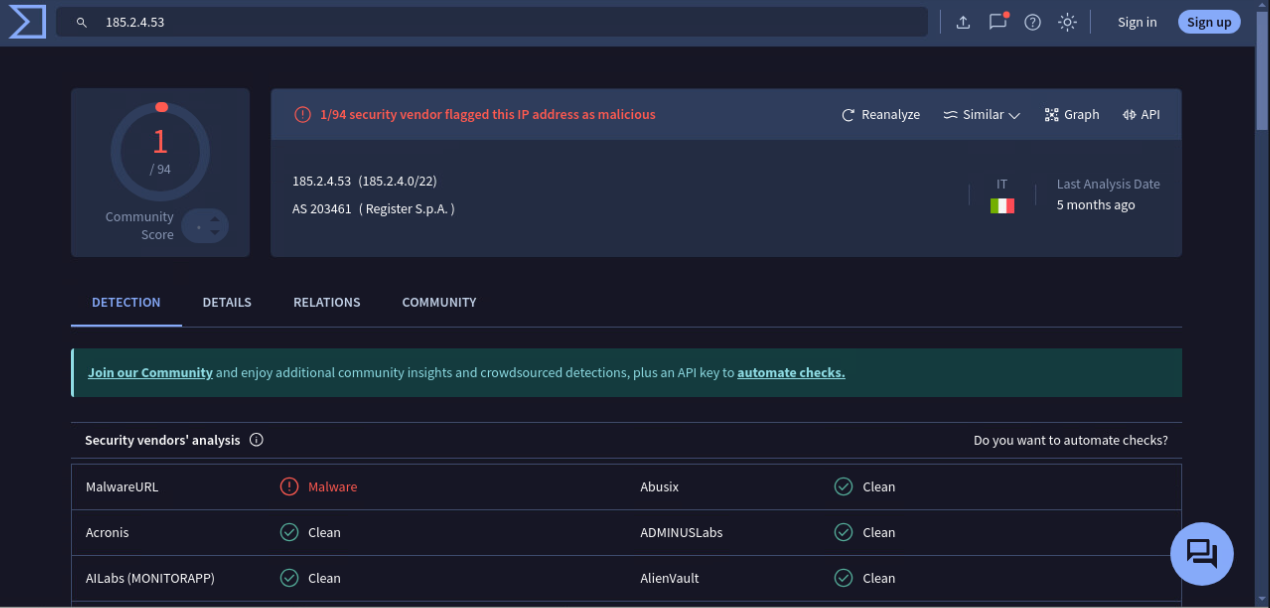


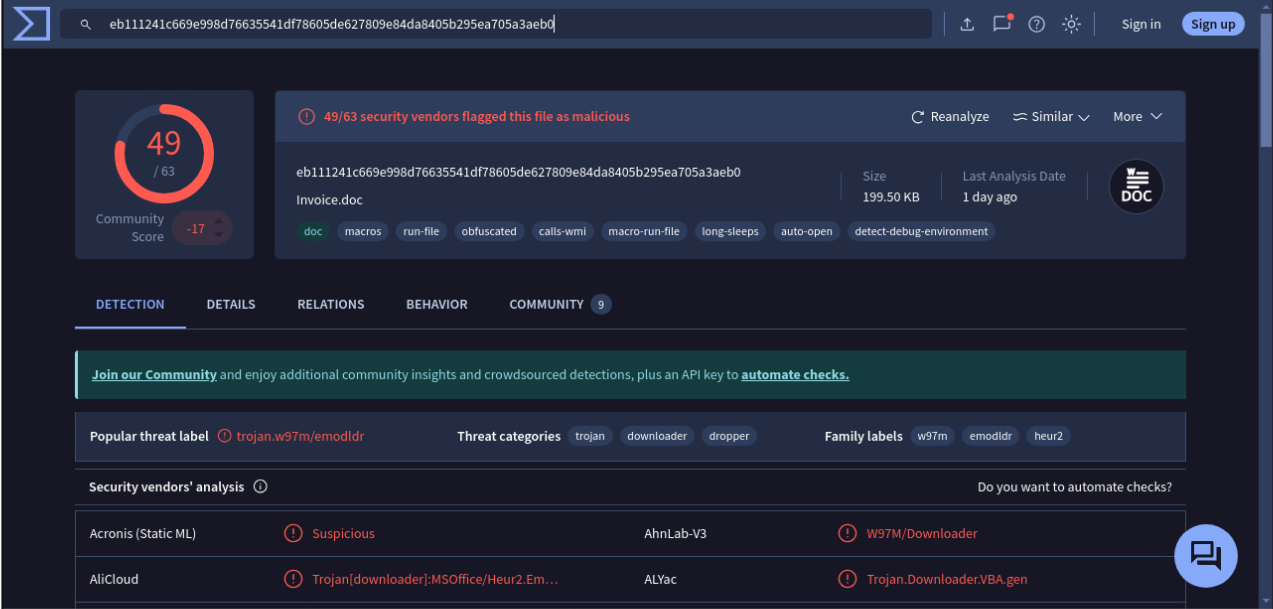


The file was downloaded at 01:08:12.418 on 2017-12-23 and it was downloaded to 172.16.1.67(internal machine) from 185.2.4.53 port 80.



The network.data.decoded shows that the type of file downloaded(application/msword) and the filename “invoice.doc”

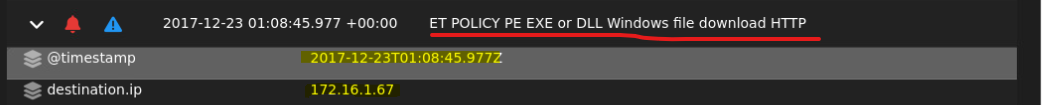


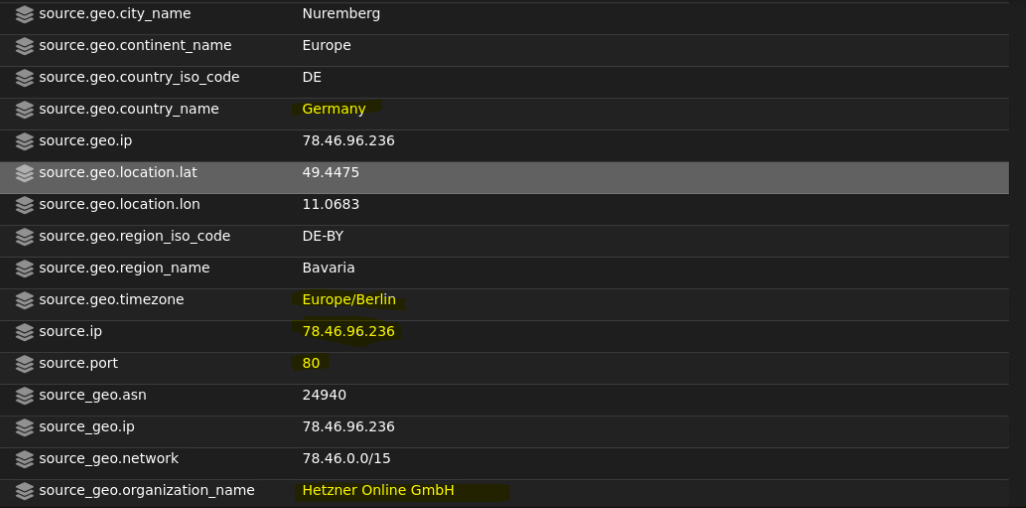


After looking up the MD5 hash of the invoice.doc file in virustotal it shows that the file contains a trojan downloader. This type of malware typically uses malicious macros embedded in Office files to download additional malware onto the system once the document is opened.

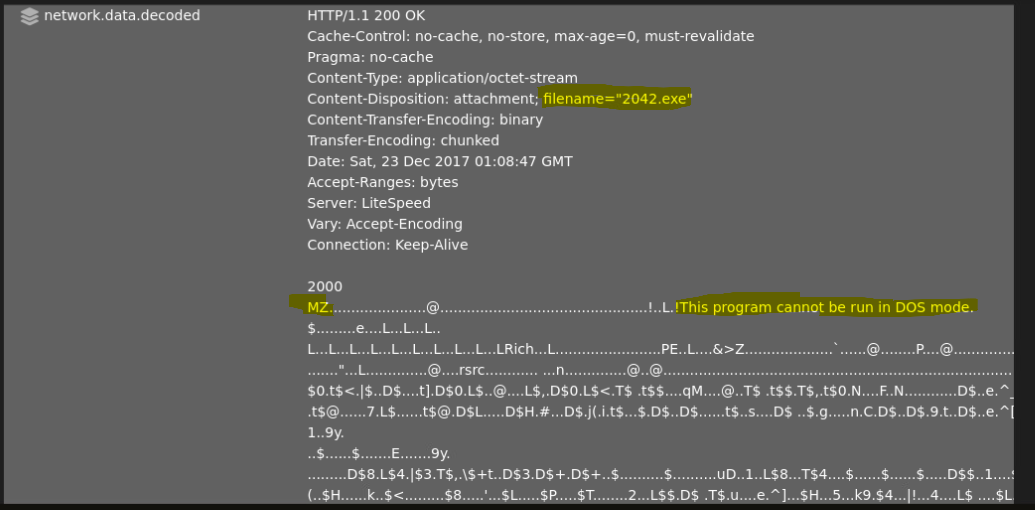
**Summary:** This alert indicates that an internal machine at IP address **172.16.1.67** downloaded a potentially harmful Office document, invoice.doc, from an external server at **185.2.4.53** over port 80 on **2017-12-23 at 01:08:12.418**. The file type, identified as **application/msword**, suggests it’s a Word document. After investigating the MD5 hash on VirusTotal, it was flagged as a **trojan downloader**. This type of malware often exploits embedded macros (like AutoOpen) to execute code that downloads more malware once the document is opened.

**Reference:** <https://learn.microsoft.com/en-us/office/troubleshoot/word/autoexec-autoopen-macros-word>

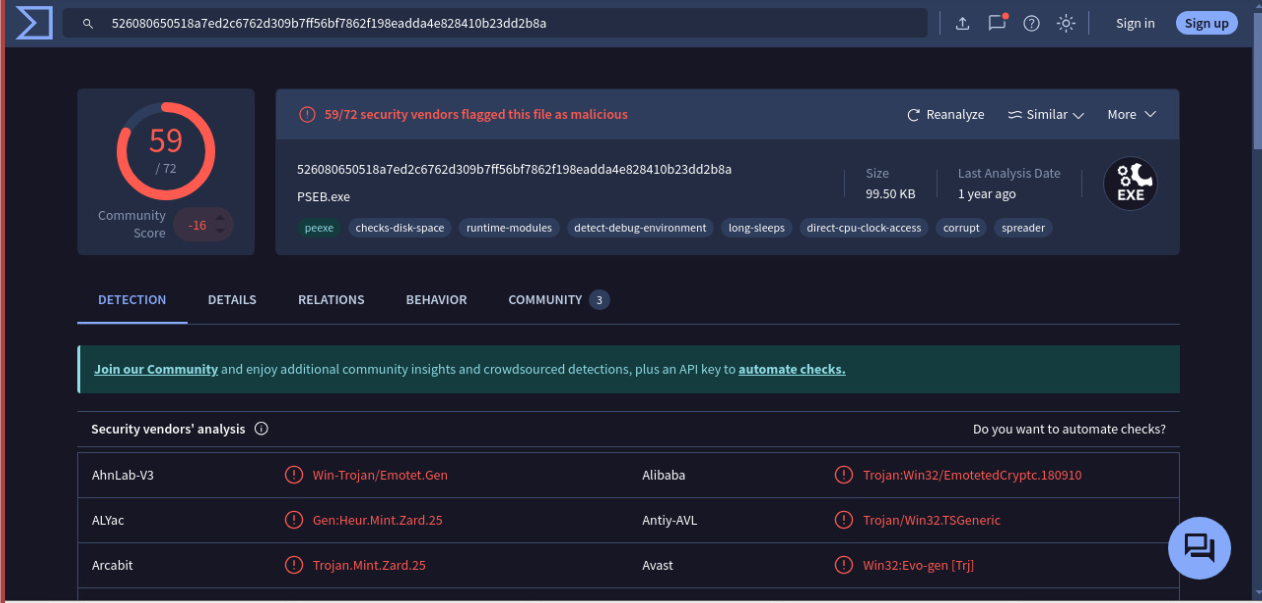




The file was downloaded at 01:08:45.977 on 2017-12-23 and it was downloaded to 172.16.1.67(internal machine) from 78.46.96.236 port 80.

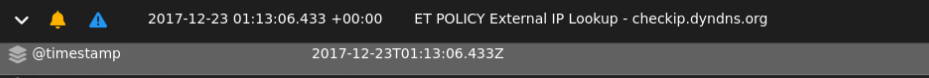


The network.data.decoded shows that a windows executable was downloaded and the filename “2042.exe”.

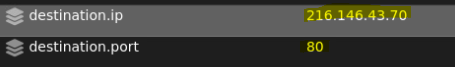


After looking up the MD5 hash of the 2042.exe file in virustotal it shows that the file contains a trojan downloader. This type of malware is designed to download and install additional malicious software onto an infected system, often using deceptive files (such as an Office document) to evade detection and lure users into opening them. Once active, it can connect to remote servers to retrieve other payloads, potentially leading to more severe infections.

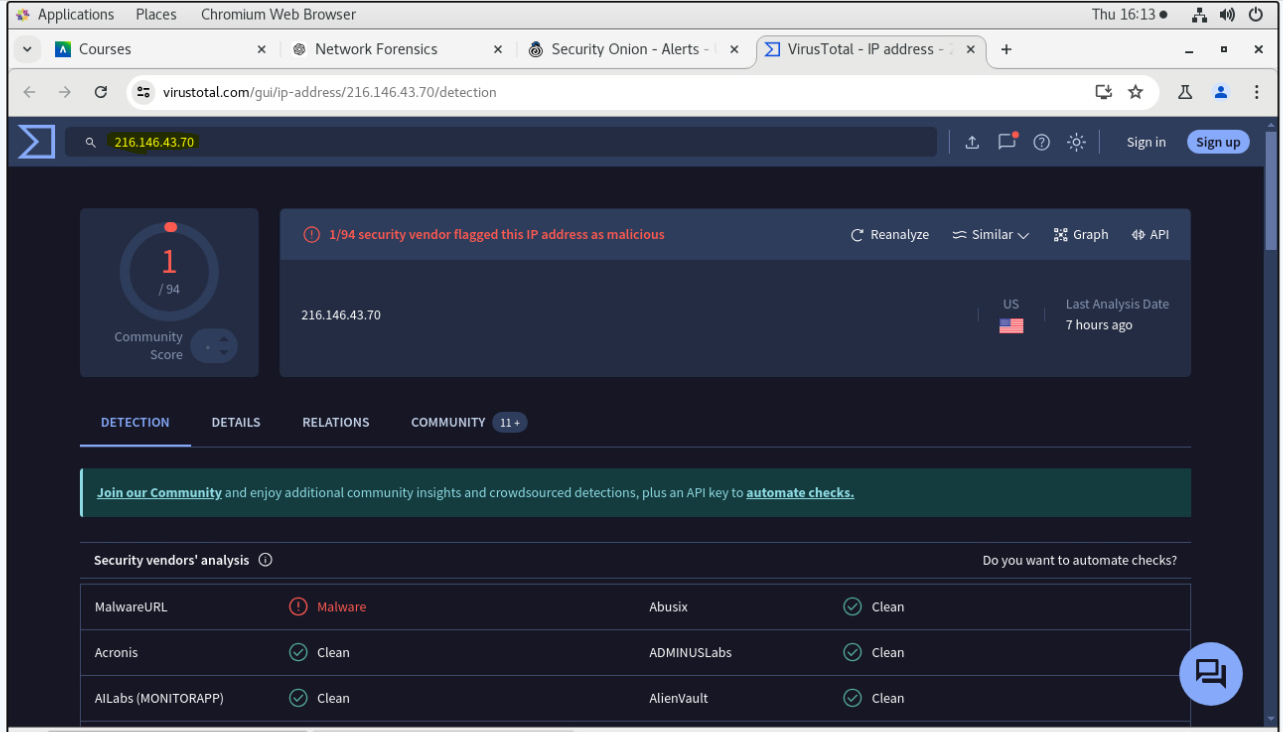
**Summary:** The alert flagged a download of a Windows executable file, 2042.exe, from IP address 78.46.96.236 on port 80 to an internal machine, 172.16.1.67, at 01:08:45.977 on December 23, 2017. Further investigation shows that invoice.doc, a document identified as a Trojan downloader, likely triggered this sequence. Trojan downloaders often hide in innocuous-looking Office documents that, once opened, prompt users to enable macros. If macros are enabled, the Trojan activates, executing code that connects to a remote server to download additional payloads in this case, 2042.exe. Meaning invoice.doc acted as the initial infection vector, making contact with the remote server and downloading 2042.exe onto the internal machine. The 2042.exe file then likely continued the infection process, either by executing further malicious actions or by downloading additional malware

****

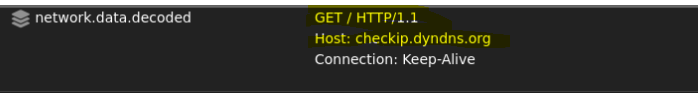
****

****

The source IP is 172.16.1.89 (internal machine) and destination IP is 216.146.43.70 port 80.

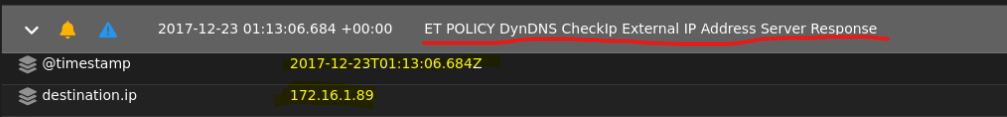
****

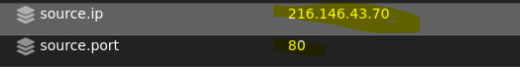
virustotal shows the destination IP as potentially malicious.

****

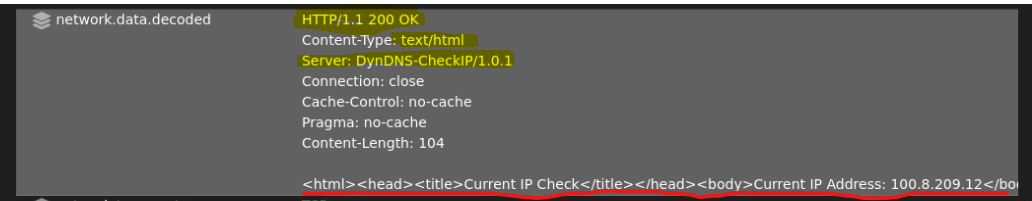
network.data.decoded shows the http.method used is GET and the Host is checkip.dyndns.org

**Summary:** This alert shows that a device with IP address 172.16.1.89 made an HTTP GET request to checkip.dyndns.org (destination IP 216.146.43.70 on port 80). This HTTP request is often used to retrieve the public IP address of the requester. The Host header confirms the connection is intended for checkip.dyndns.org, a known IP lookup service.



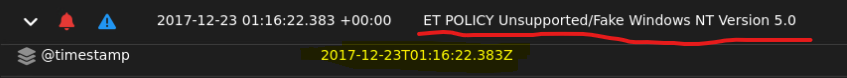


The source IP is 216.146.43.70 port 80 and destination IP is 172.16.1.89 (internal machine).

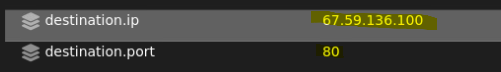


The network.data.decoded field shows that the server response has been decoded, containing the network’s external IP(100.8.209.12), which the internal machine might be using for tasks like remote access.

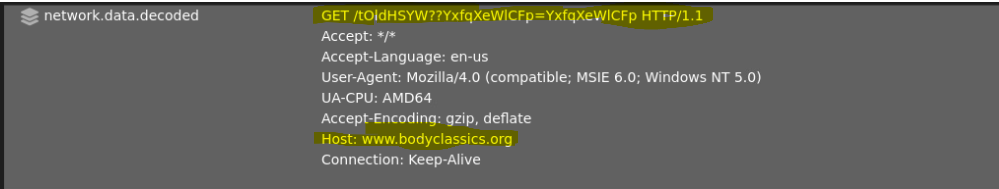
**Summary:** The **ET POLICY DynDNS CheckIp External IP Address Server Response** alert indicates that an internal machine at IP address 172.16.1.89 has communicated with an external DynDNS service hosted at 216.146.43.70 on port 80. This service response was decoded and contained the network's public IP address (100.8.209.12). Suggesting that the internal machine is using the DynDNS service to retrieve its external IP address, likely for functions such as remote access or monitoring.

****

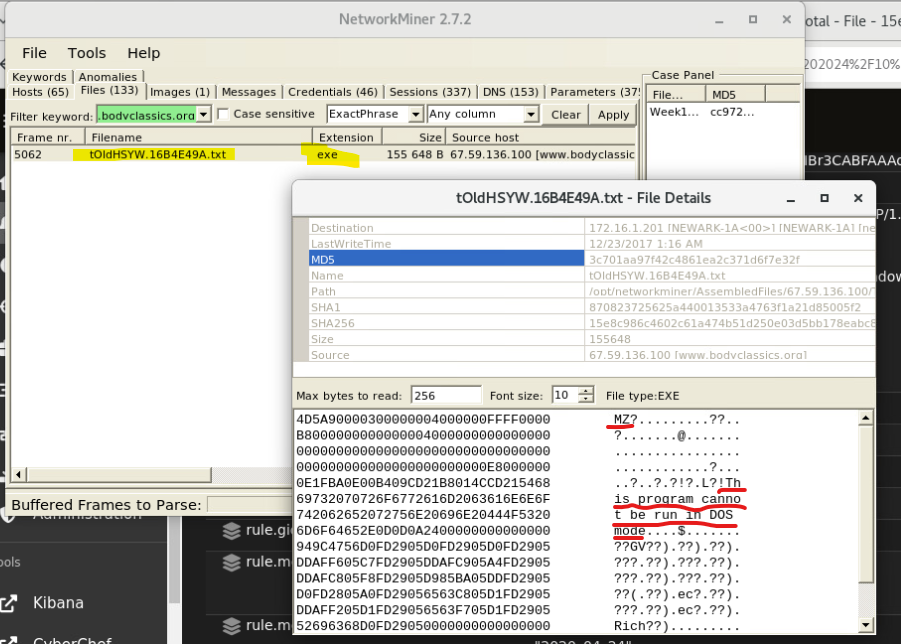
****

****

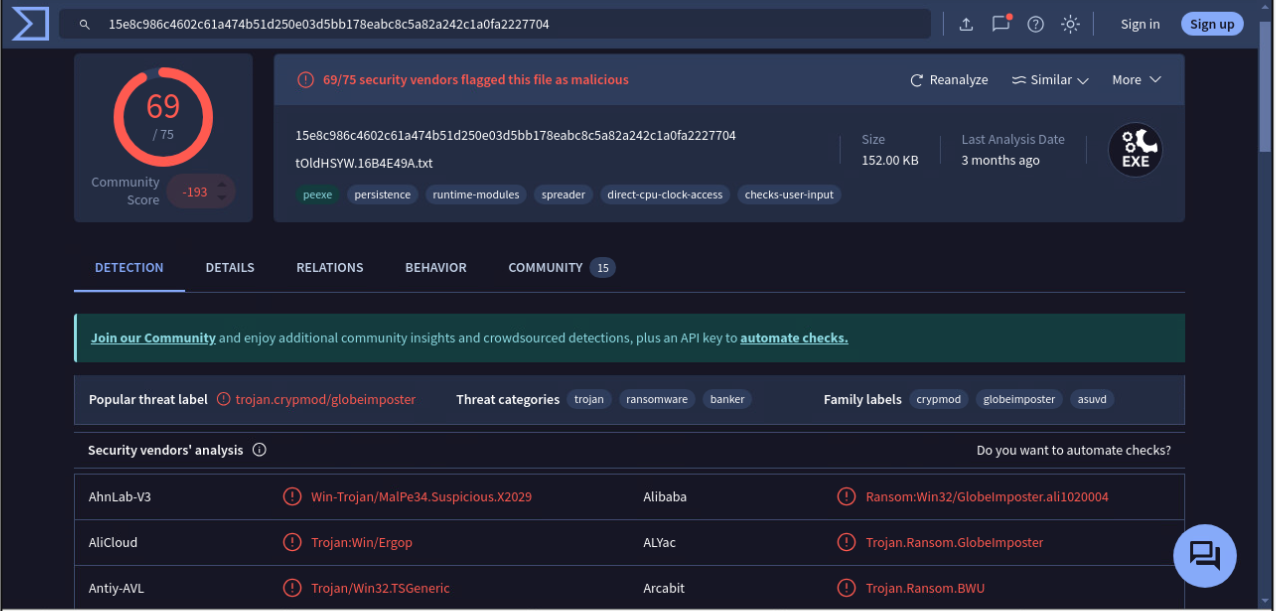
The source IP is 67.59.136.100 port 80 and destination IP is 172.16.1.201 (internal machine).

****

network.data.decoded shows the http.method used is GET and the Host is www.bodyclassics.org

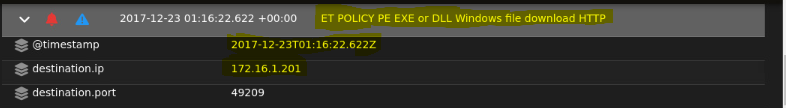
****

Network miner shows there was an executable file downloaded.

****

Virustotal shows the MD5 hash of the downloaded file to be malicious.

**Summary:** After investigating the alert, it appears that an external IP address, 67.59.136.100 on port 80, attempted to communicate with an internal machine at 172.16.1.201. The HTTP method used in this interaction was a GET request, targeting the host www.bodyclassics.org. Further analysis using Network Miner revealed that an executable file was downloaded during this session. When checking the MD5 hash of the downloaded file on VirusTotal, the file was flagged as malicious. Given that the alert references an unsupported or fake Windows NT Version 5.0, it’s possible the external source attempted to disguise itself using this outdated version, potentially to evade security filters or appear less suspicious.





The file was downloaded at 01:16:22.622 on 2017-12-23 and it was downloaded to 172.16.1.67(internal machine) from 78.46.96.236 port 80.

