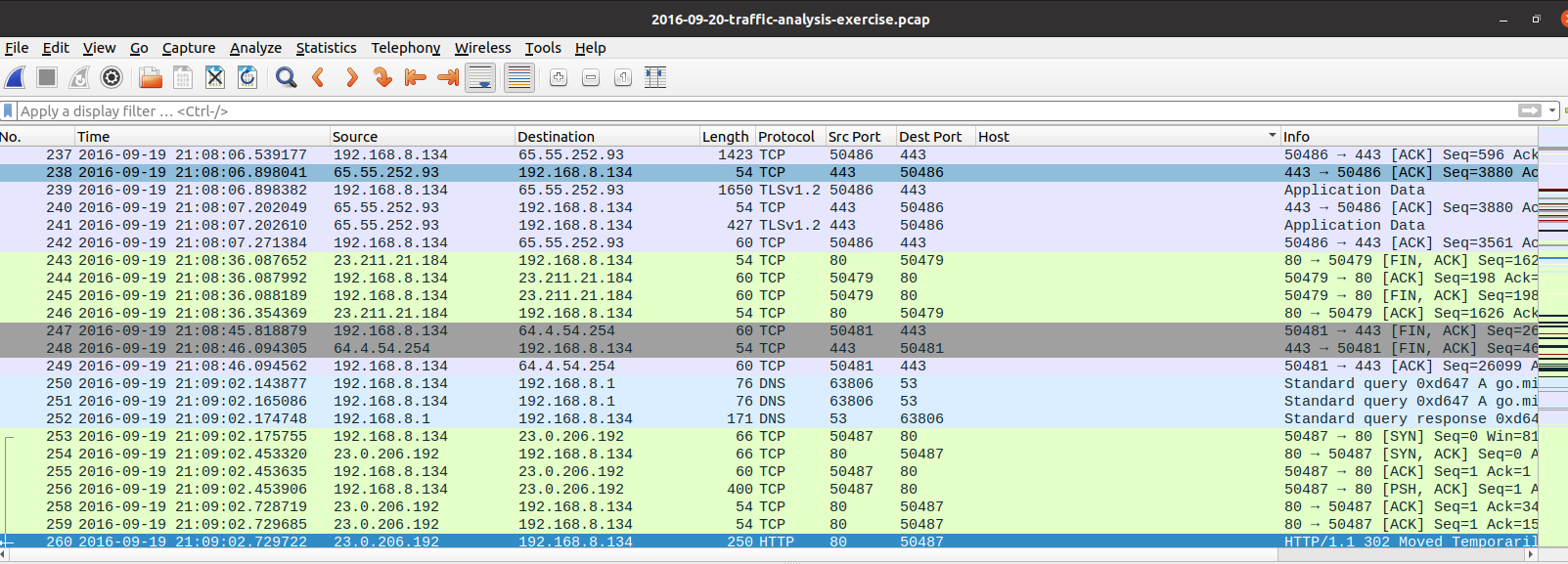
The Systems administrator of Superfake Inc, has been notified of possible malware attack on a computer within Superfake Inc. Response to this, the systems administrator has performed a network capture of all devices on the sales subnetwork. The networks are facing a variety of threats then just viruses, such as malware, denial of service, port scanning convert channels and information theft. It is required to perform an analysis by capturing network packets to identify any potential malware. The tools used for this will be Wireshark. Wireshark is a network protocol analyser that is able to capture packets from a network connection. Packets can be defined as small pieces of data sent over a network, which includes information such as the source, destination as well as the content or data being passed, hence analysis of these It can be used for troubleshooting and detecting any suspicious content within.

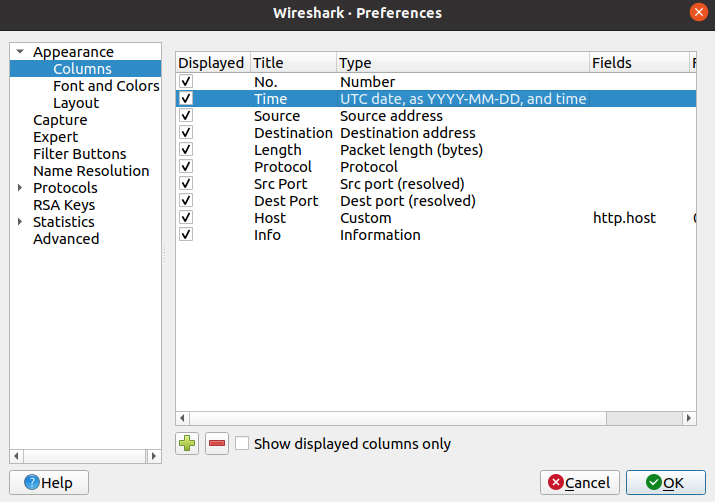
The example pcap file provided for this case came from https://www.malware-traffic-analysis.net/2020/02/21/index.html

In order to use Wireshark, a pcap file is needed. This can be added by clicking the file tab on the top left, and clicking open, upon which select the pcap file and Wireshark should display all of the packets and network traffic contained.

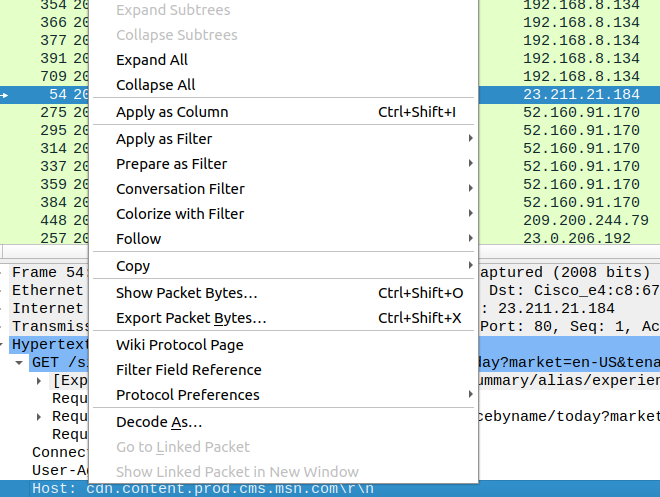


Initially, a number of data is shown, the packet number, the time the packet was sent, the source the packet came from, the destination the packet is going to, the size, the protocol and finally some information.

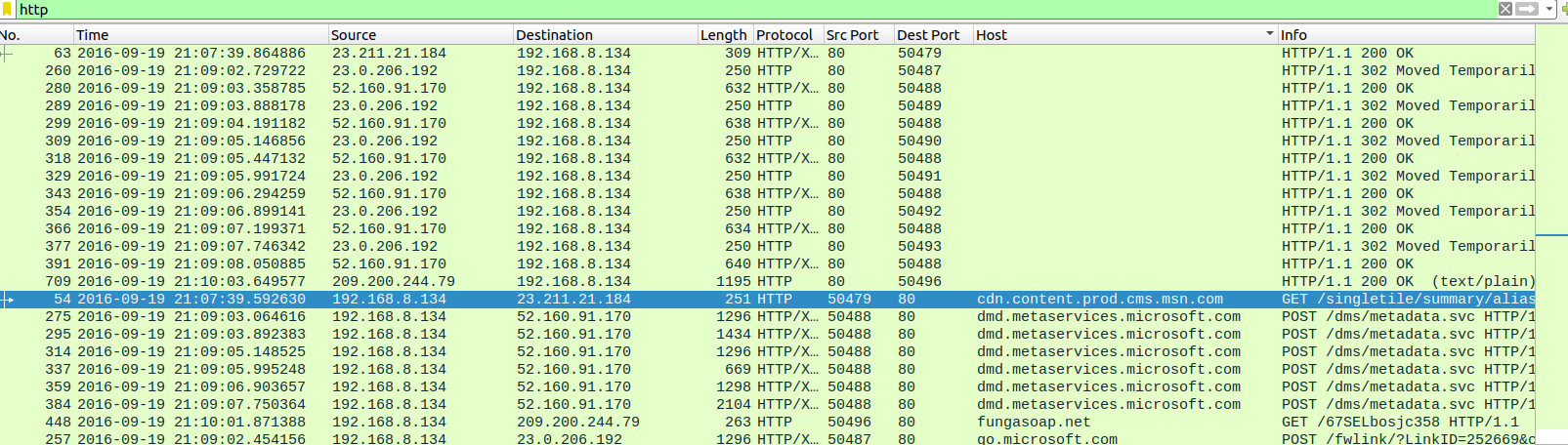
First step in the process, some additional information and cleaning up is taken. Firstly, the time is written in a non-user readable way. Right click on the header with all the column names and select column preferences. For the time column select the time to be UTC. As well as that, port information can also be useful, so they were added in as well. This is done by clicking the green plus button at the bottom of where all the columns are. 2 columns were created and named Src Port, and Dest port, and they were given the value of Src Port (resolved) and Dest port (resolved).



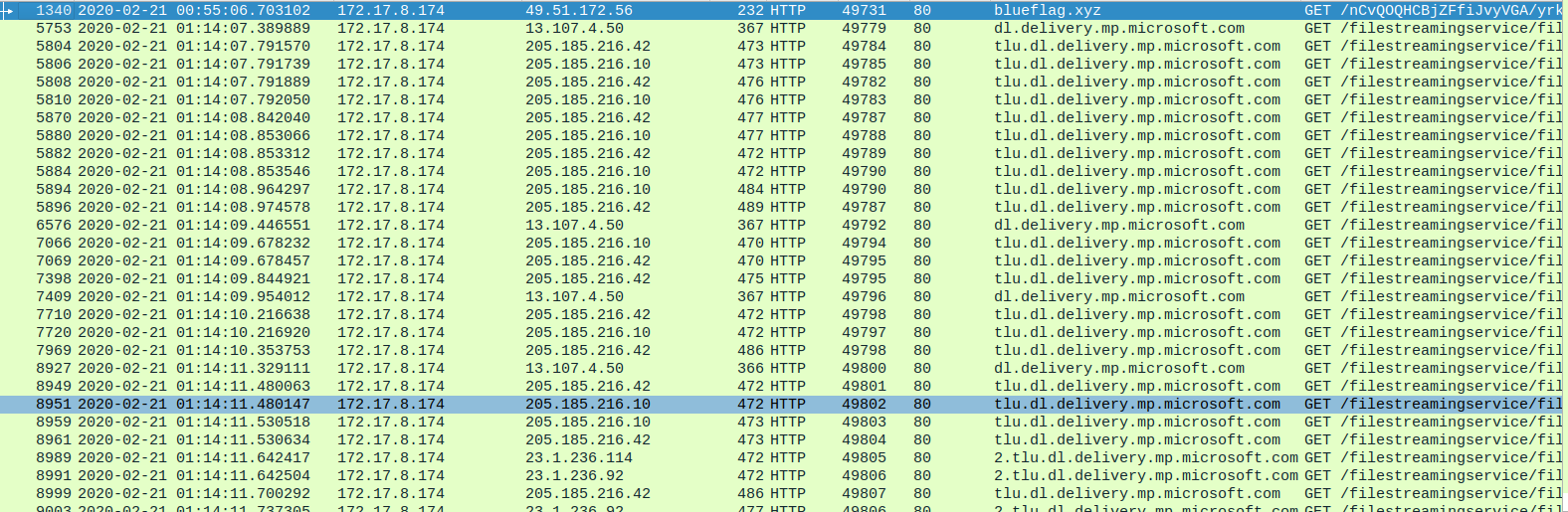
As well as that, a column host was added by clicking on a packet, and on the bottom of the UI, there is a section with more detail on the specific packet. By clicking unto Hypertext transfer Protocol, there is a section called host, right click on that and click add column to add the host to the columns.



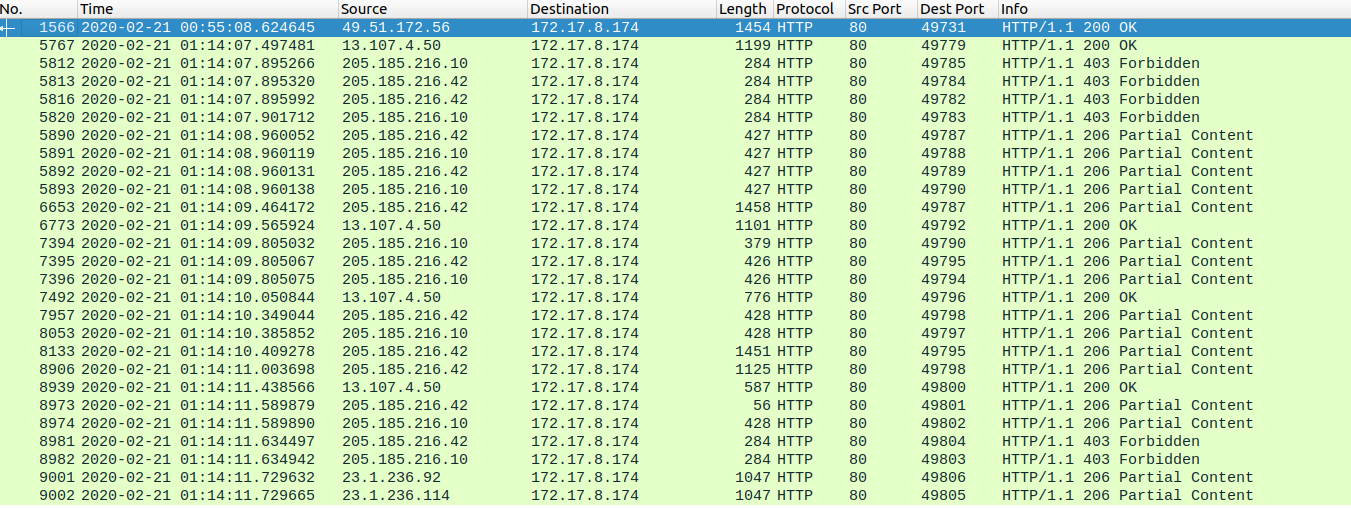
A filter can be applied on the bar just above all the column headings. When examining traffic for malware, HTTP traffic is of great interest, hence the filter applied was to view all HTTP requests and responses.



HTTP requests and responses allows the access to which requests were made, and where were they made to, so if a user downloads something from a website, it can be tracked what was downloaded, when and where. This can be used for further analysis to check if anything requested, then received contained any suspicious malware and from which host / website had provided the malware. The requests were first examined by applying the filter http.request

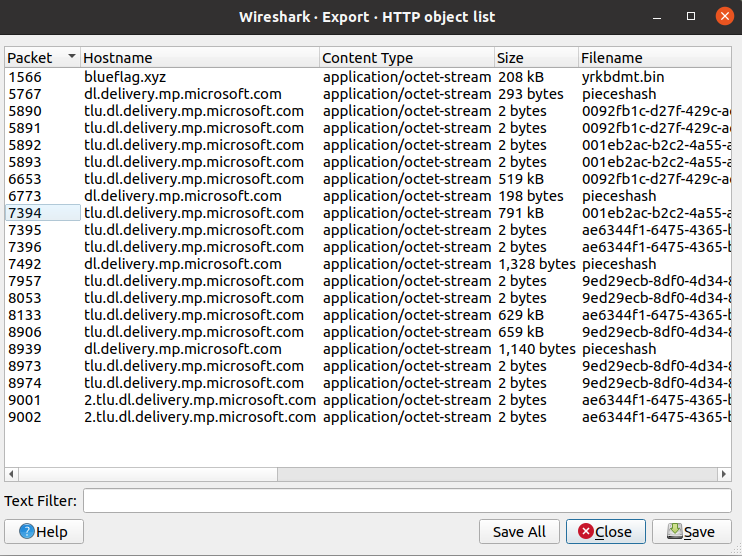


From this example, all the requests made can be seen. There are several GET requests trying to fetch data from the website /filestreamingservice/files. These were all made on 21/02/2020 at 1.14am within seconds of each other, possibly indicating multiple requests were needed to retrieve a single file or piece of data. The responses can be seen using http.response as the filter.

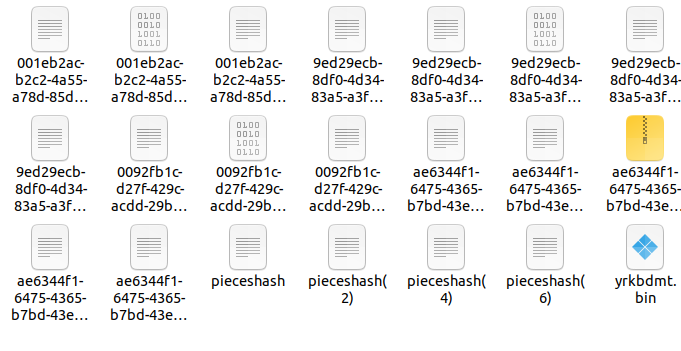


From this several resources requested came back fine, however there are some cases were the error 403 Forbidden is returned, indicating that this user was requesting a file/website or resource that they are not allowed to have access to. As well as that a success response code of 206 Partial Content was also retuned, indicating that a requested resource of a set range, indicated in the header was successfully returned.

All these responses that have succeeded can be extracted by clicking on File, then export objects, then HTTP, and clicking save all can get all these resources in a chosen directory. From them on analysis can be done on those files and resources for analysis.



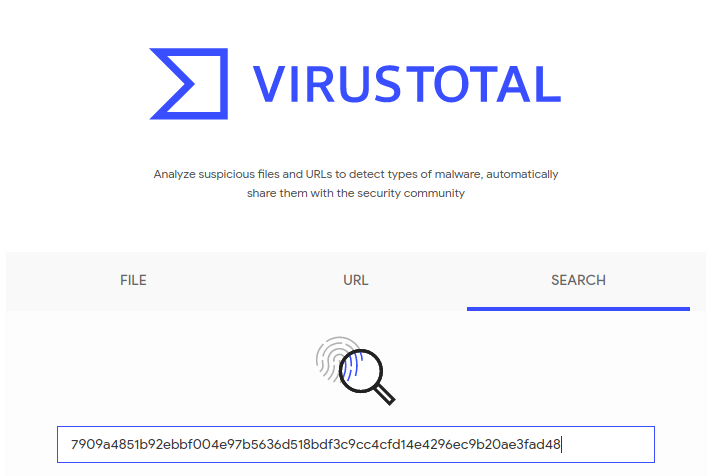
A way of analysis is using a website Virustotal.com. it requires the file’s hash code / checksum which can acquired using the command “sha256sum” on the file. Down below is a list of all the files that have been extracted using the export in Wireshark.

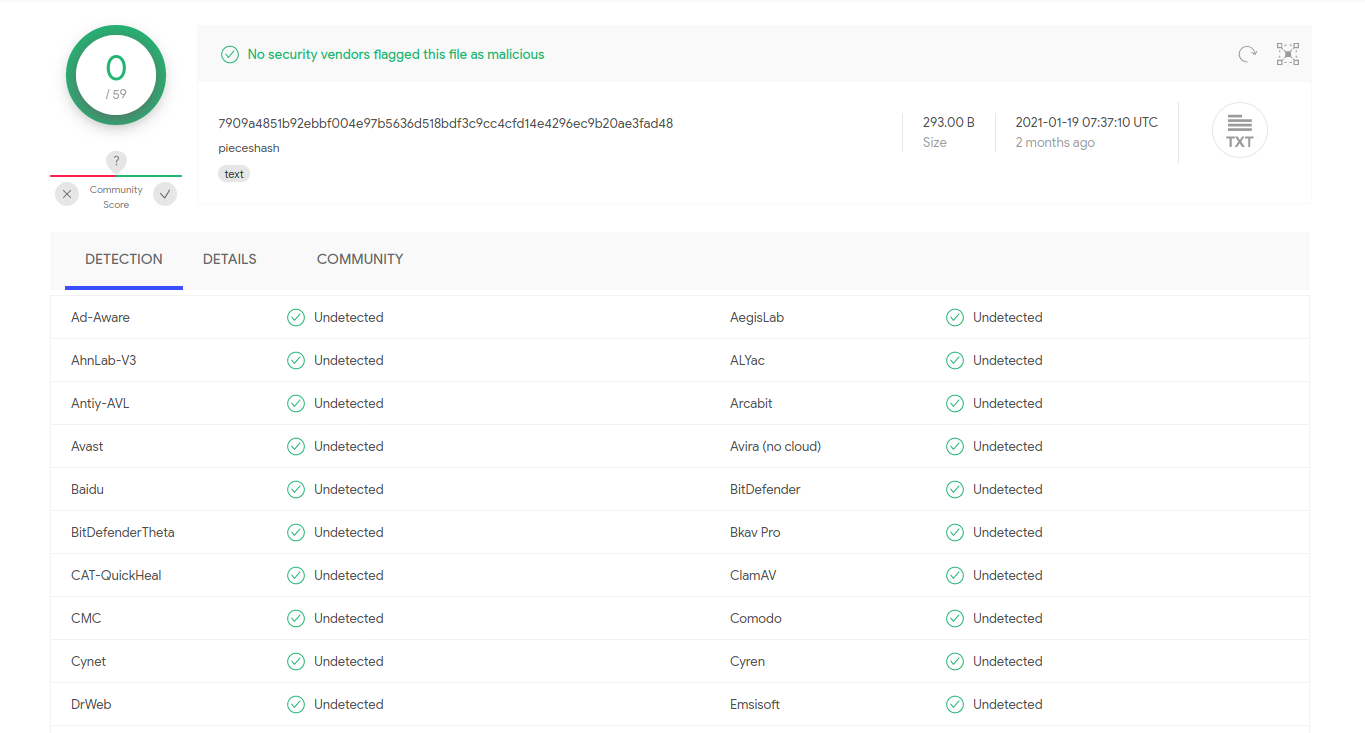


For this case, the first file examined is one of the files that got a OK response, instead of the Partial Content responses. These are the files called pieceshash and ykrbdmt.bin. when the sha256sum is applied in pieceshash a checksum is provided, which can be provided to the website Virustotal.com, by going to the search tab and then Virustotal.com will provide for analysis of any malware.







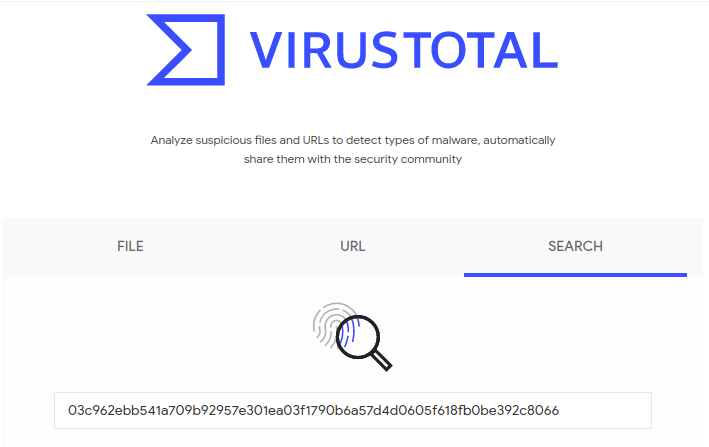


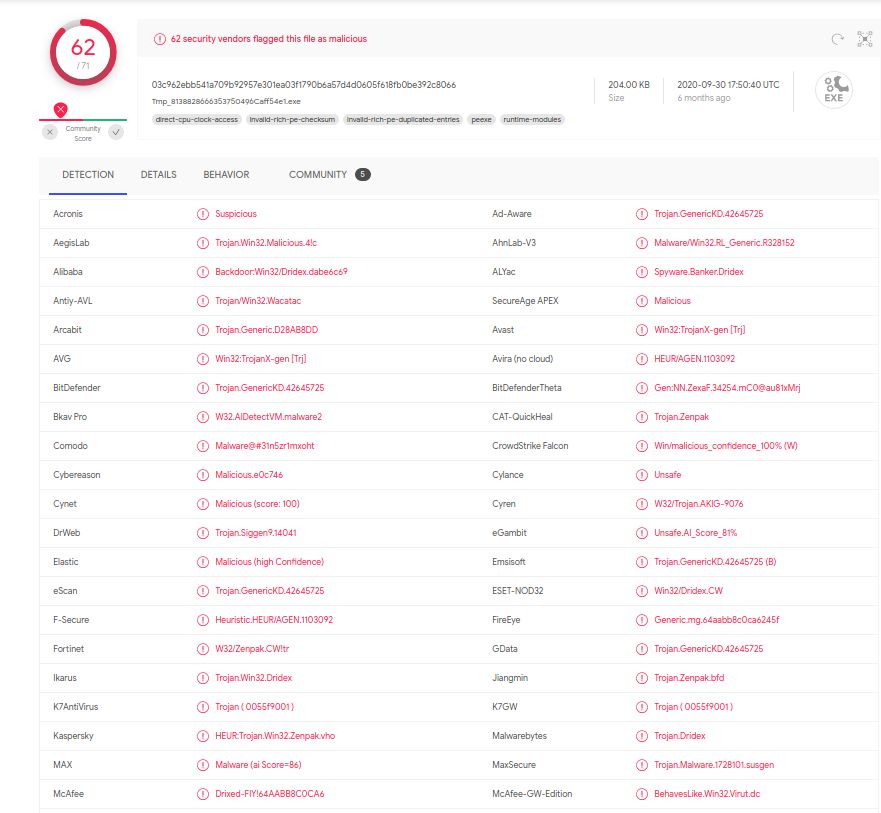
The Virustotal.com results show that the file pieceshash passes all security checks, and it has detected no suspicious or malicious content within this file. The file pieceshash can then be assumed to be harmless and requires no further investigation.

Now the next file to be examined is a bin file yrkbdmt.bin, and the same process is repeated by getting it’s checksum and applying it to the Virustotal search.









As can be seen, several vendors have flagged this file as Malicious and harmful. Further investigation is needed to examine this file and it’s source. With this method, any network traffic can be examined so it can be detected for malware.

This came from this response shown below. This can be seen by filtering http.response and clicking export objects, when clicking on the corrupted file yrkbdmt.bin, this response gets highlighted



This was the request made to it, which can be seen when filtering back to http.requests. it can be seen that the host that provided that file is blueflag.xyz, that’s different from all the other hosts which are all coming from the domain Microsoft.com. We know that the host that provided the infected file came from the host 49.51.172.56. This may need to warrant further investigation.

