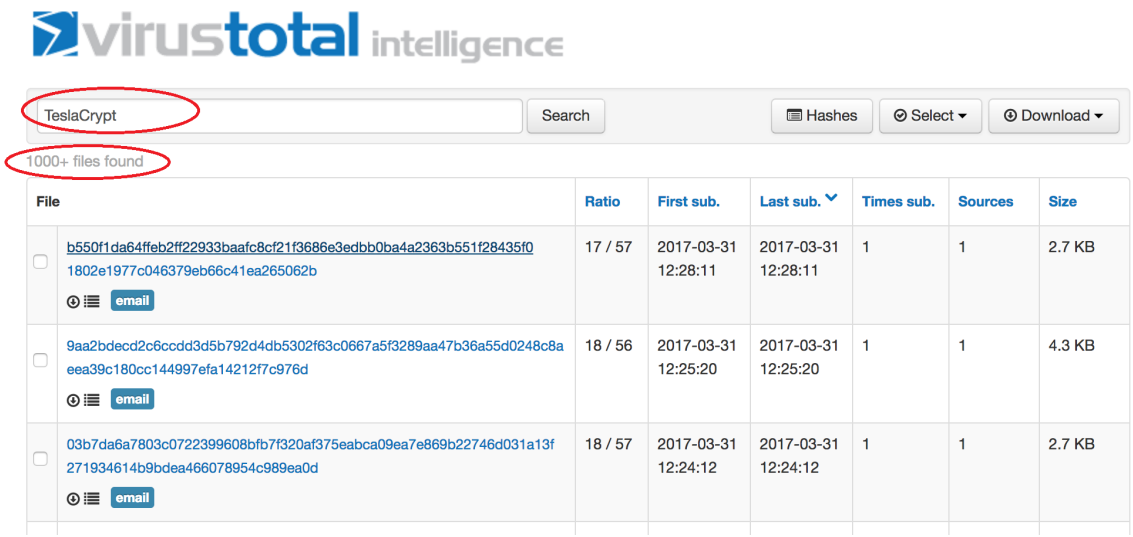
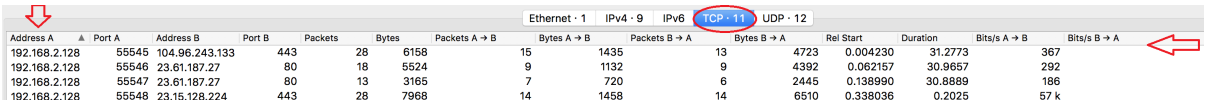
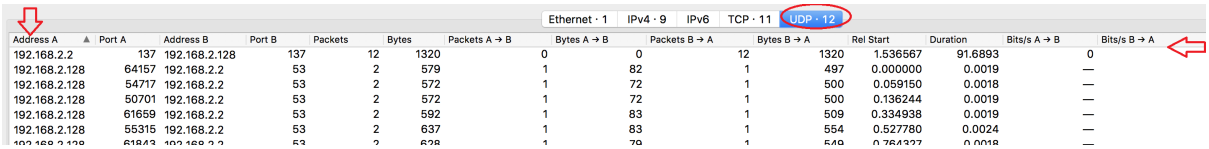
The source of Malware PCAP files

Searching for the specific ransomware families in the Virus Total Intelligence platform we could identify portable executable samples that had a corresponding behavioural analysis network traffic PCAP files. Then we filtered this information using the command lines below, to extract the conversation and related features as shown below.







Extract script

Tshark -q -z conv,tcp -z conv,udp -r "input path\input pcap" >>"output path\familyname.xls"

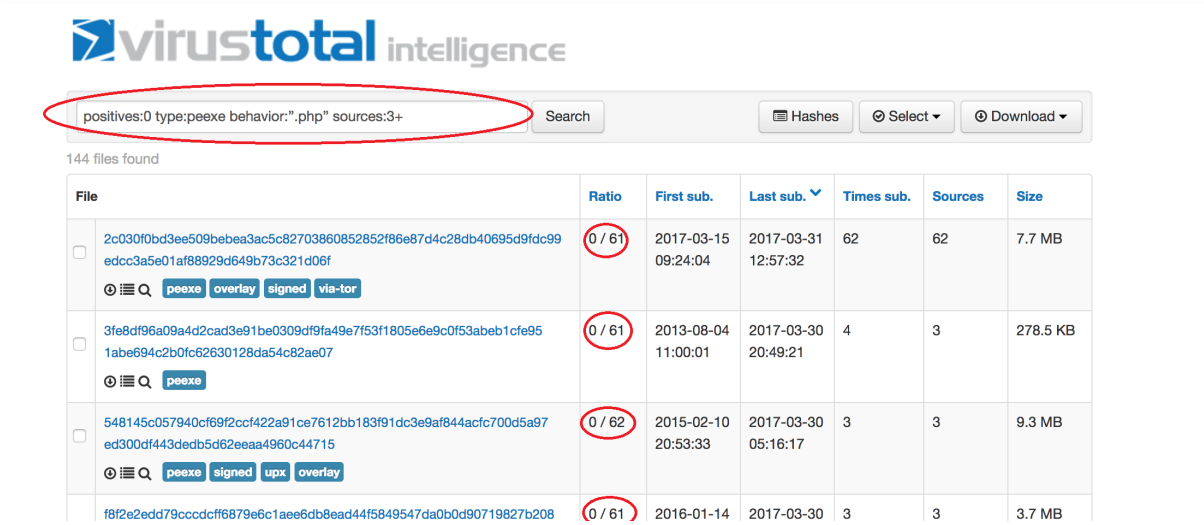
-z conv, tcp	Show TCP statistics
-z conv, udp	Show Udp statistics
-q	To print statistics
-r	Input file
>>	Append date to specified output file

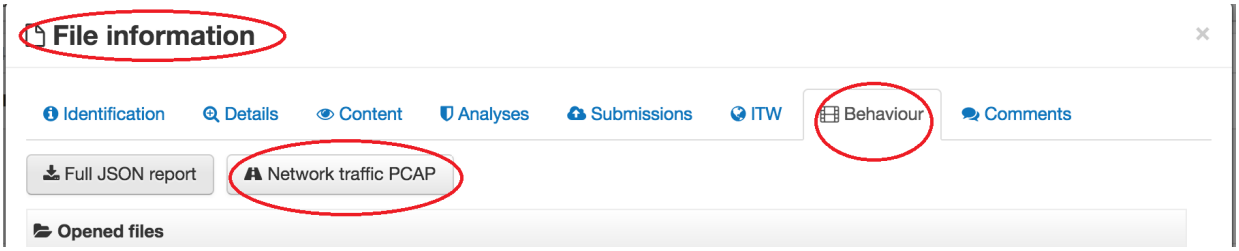
Then, the texts converted to columns using Excel. In addition, of two other columns added for our reference:

1- Protocol for Tcp/Udp conversation
2- Hash to identify which conversation belong to traffic samples.

The source of Goodware PCAP files

We used virus total threat intelligence platform, our search criteria targeted portable executable files that had been submitted at least three times and had zero detections by antivirus engines. The search was applied to several different behavioural report criteria to provide a collection of 264 goodware samples. As you can see below.





The PCAP files downloaded were filtered and features extracted using the same procedures used for malware above.