

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.

The screenshot shows the VirusTotal Intelligence interface. The search term 'TeslaCrypt' is entered in the search bar. Below the search bar, it indicates '1000+ files found'. Three files are listed in the results table:

File	Ratio	First sub.	Last sub.	Times sub.	Sources	Size
b550f1da64ffeb2ff22933baafc8cf21f3686e3edbb0ba4a2363b551f28435f01802e1977c046379eb66c41ea265062b email	17 / 57	2017-03-31 12:28:11	2017-03-31 12:28:11	1	1	2.7 KB
9aa2bdecdd2c6ccdd3d5b792d4db5302f63c0667a5f3289aa47b36a55d0248c8aeea39c180cc144997efa14212f7c976d email	18 / 56	2017-03-31 12:25:20	2017-03-31 12:25:20	1	1	4.3 KB
03b7da6a7803c0722399608bf7f320af375eabca09ea7e869b22746d031a13f271934614b9bdea466078954c989ea0d email	18 / 57	2017-03-31 12:24:12	2017-03-31 12:24:12	1	1	2.7 KB

Below the file list, the network traffic details for the selected file are shown. The traffic is filtered by 'TCP · 11' and 'UDP · 12'. The table shows the following columns: Address A, Port A, Address B, Port B, Packets, Bytes, Packets A → B, Bytes A → B, Packets B → A, Bytes B → A, Rel Start, Duration, Bits/s A → B, and Bits/s B → A. Red arrows point to the 'TCP · 11' and 'UDP · 12' filters and the 'Bits/s B → A' column.

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 image shows two screenshots from the VirusTotal Intelligence platform. The top screenshot displays search results for the query "positives:0 type:peexe behavior:".php" sources:3+". It lists four files with their hashes, ratios (all 0/61 or 0/62), submission dates, and sizes. The bottom screenshot shows the "File information" page for a selected file, with the "Behaviour" tab selected and the "Network traffic PCAP" option highlighted.

VirusTotal Intelligence Search Results

Search query: `positives:0 type:peexe behavior:".php" sources:3+`

144 files found

File	Ratio	First sub.	Last sub.	Times sub.	Sources	Size
2c030f0bd3ee509bebea3ac5c82703860852852f86e87d4c28db40695d9fdc99edcc3a5e01af88929d649b73c321d06f peexe overlay signed via-tor	0 / 61	2017-03-15 09:24:04	2017-03-31 12:57:32	62	62	7.7 MB
3fe8df96a09a4d2cad3e91be0309df9fa49e7f53f1805e6e9c0f53abeb1cfe951abe694c2b0fc62630128da54c82ae07 peexe	0 / 61	2013-08-04 11:00:01	2017-03-30 20:49:21	4	3	278.5 KB
548145c057940cf69f2ccf422a91ce7612bb183f91dc3e9af844acfc700d5a97ed300df443dedb5d62eeaa4960c44715 peexe signed upx overlay	0 / 62	2015-02-10 20:53:33	2017-03-30 05:16:17	3	3	9.3 MB
f8f2e2edd79cccdcff6879e6c1aee6db8ead44f5849547da0b0d90719827b208	0 / 61	2016-01-14	2017-03-30	3	3	3.7 MB

File information

Identification Details Content Analyses Submissions ITW **Behaviour** Comments

[Full JSON report](#) [Network traffic PCAP](#)

Opened files

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