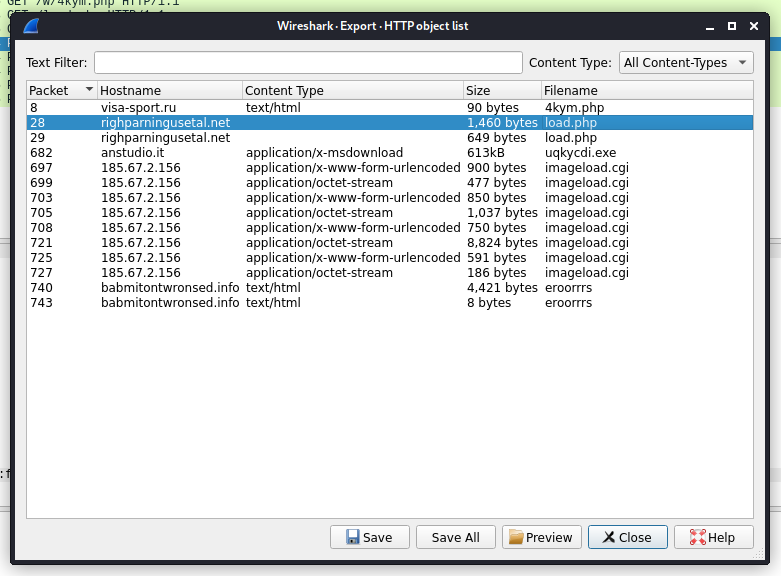
**NETWORK TRAFFIC ANALYSIS**

FILE NAME: mal\_traffic\_1

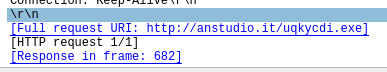
Objects contained:

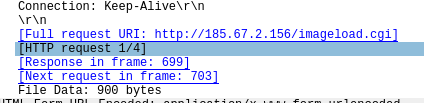


Communicated domains: , Compromised sites

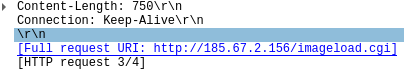










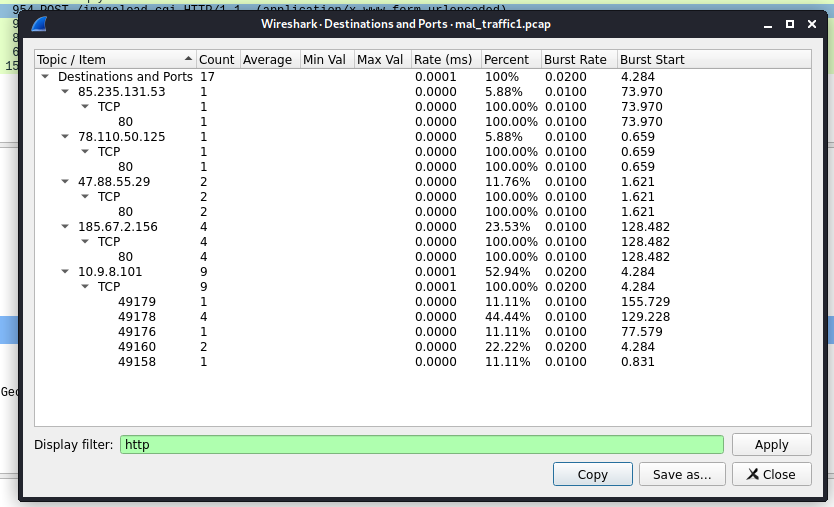






Protocol used : TCP

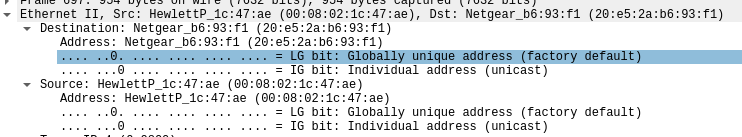
Ports Communicated:



OS the infected host runs: Windows

Ip address of the infected host: 10.9.8.101

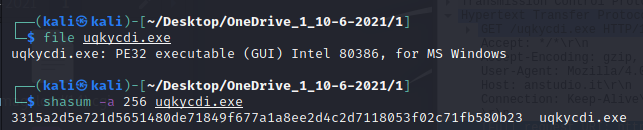
MAC address of the infected host and Host Name:



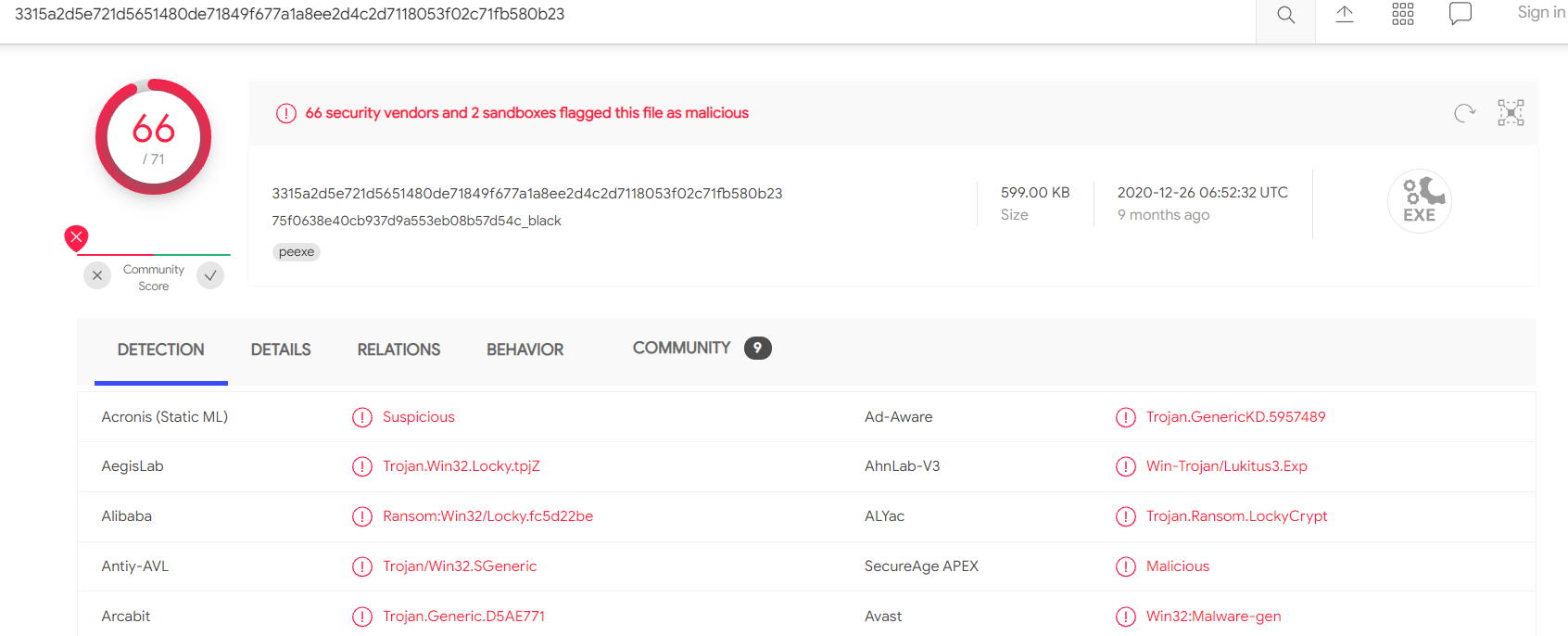
Infected URl containg exe file:

http://anstudio.it/uqkycdi.exe

Generating SHA256 hashes for the exe file

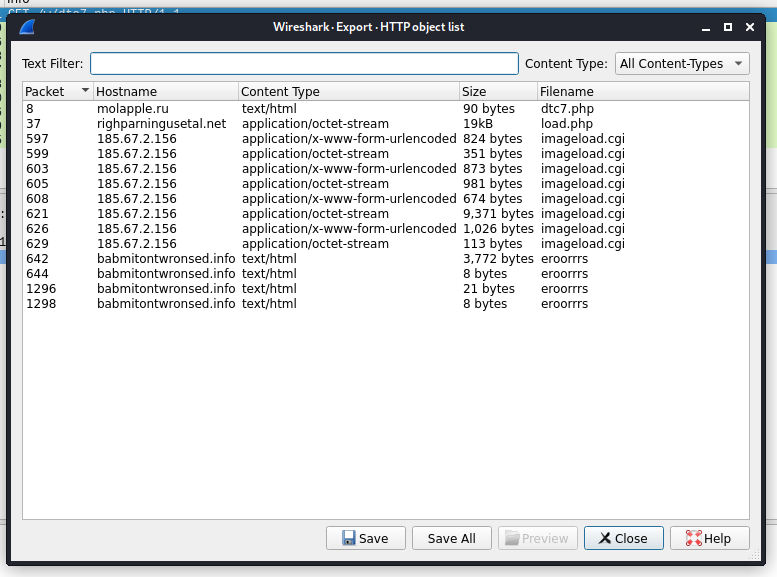


Type of malware: Trojan

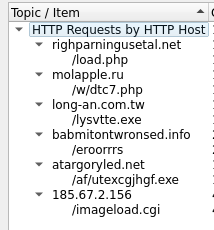


FILE NAME: mal\_traffic\_2

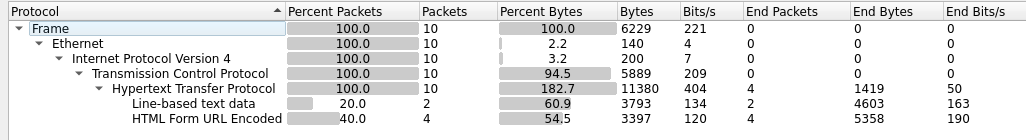
Objects contained:



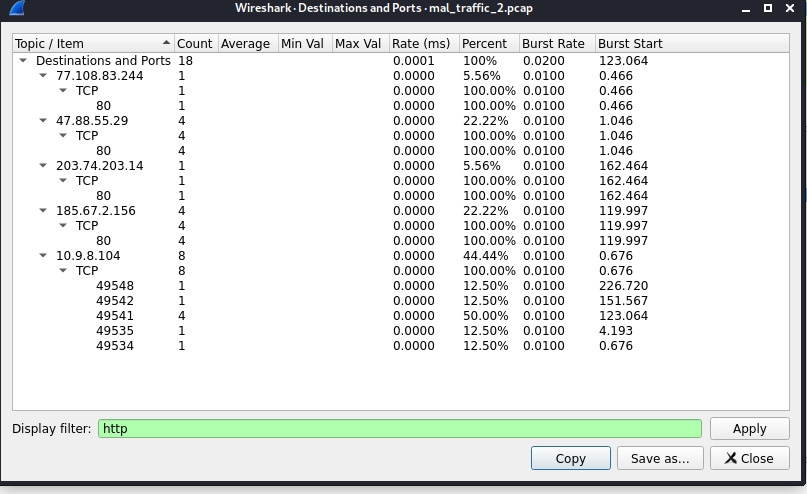
Communicated domains: , Compromised sites:



Protocol used :



Ports Communicated:

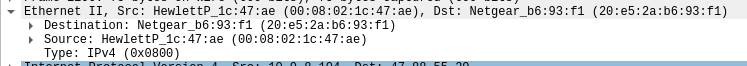


OS the infected host runs: Windows

Ip address of the infected host:



MAC address of the infected host and Host Name:



Infected URl containg exe file:

No exe file in URL, so attack must be done with file with any other format.

Php files containing Trojans.

<http://molapple.ru/w/dtc7.php>

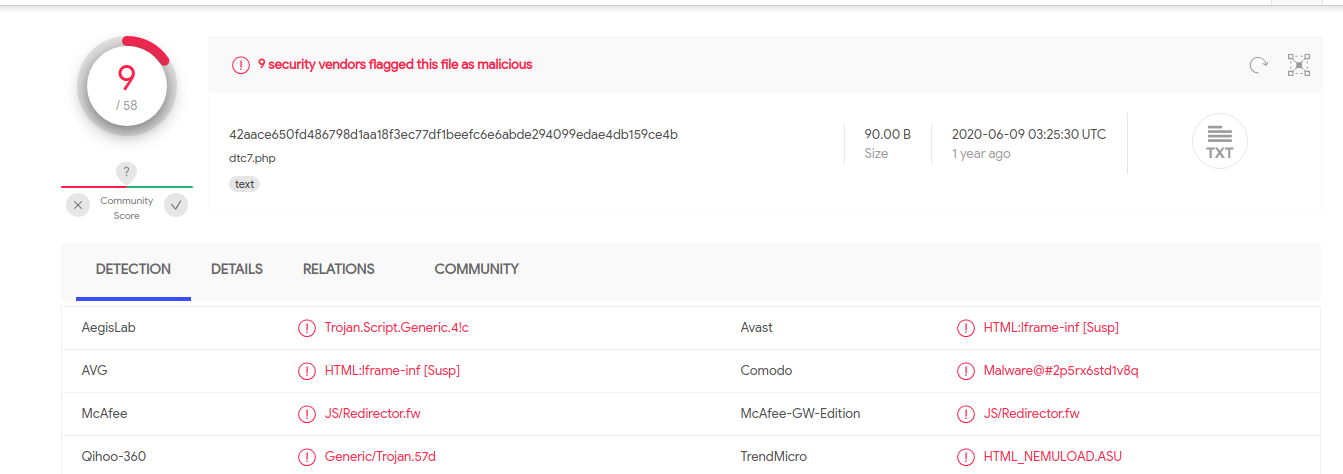
http://righparningusetal.net/load.php

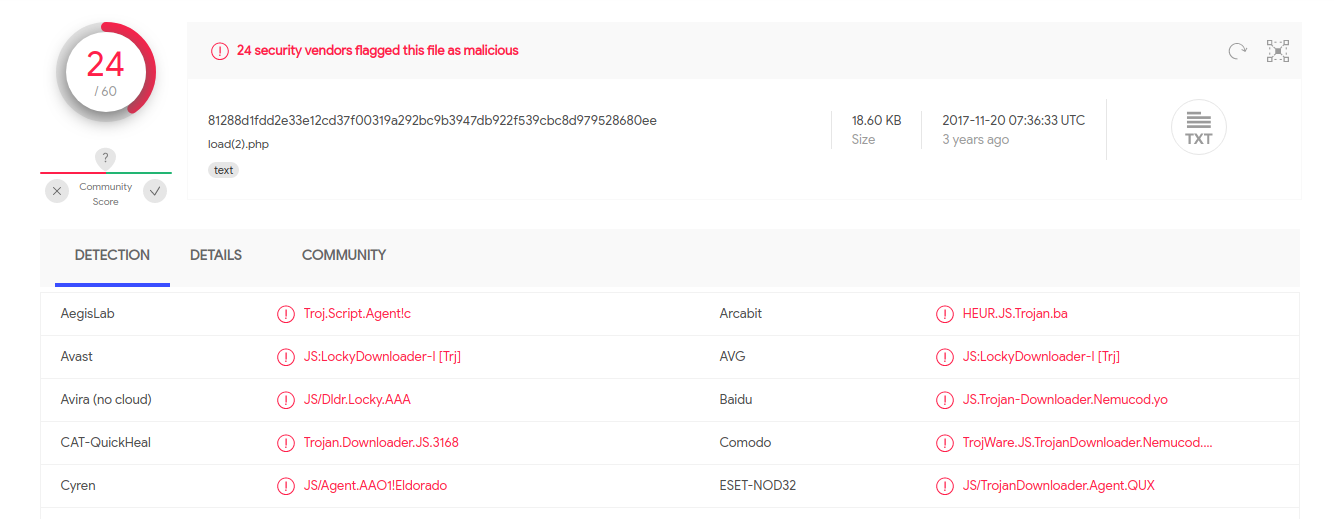
Generating SHA256 hashes for the exe file

No exe file

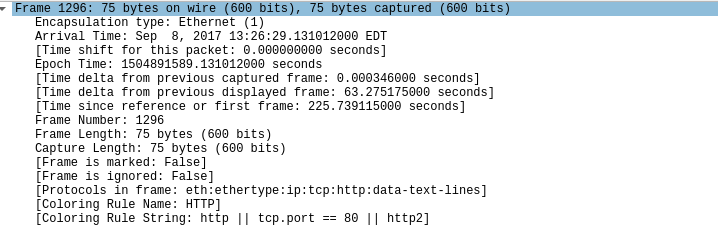
Type of malware:

It’s the php file contain malware, its confirmed by the virus total.



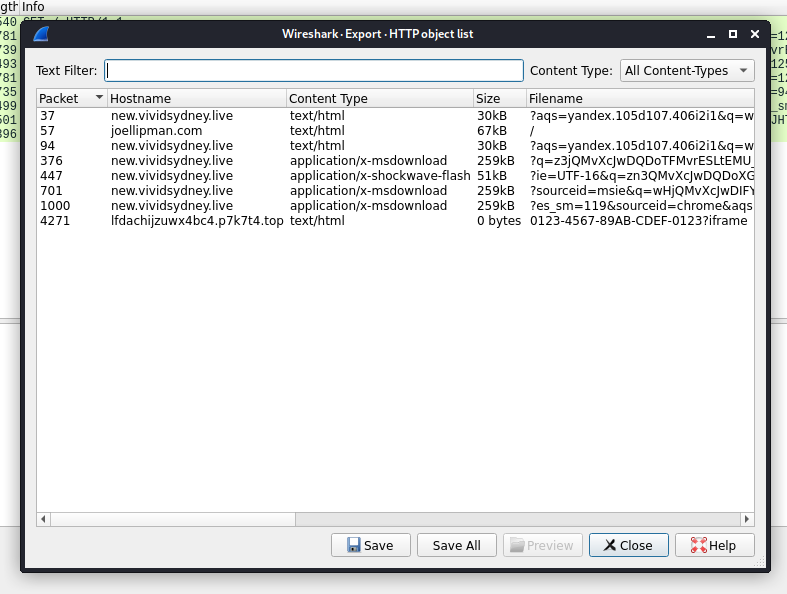


Time and Date of Attack:



FILE NAME: Malwaretraffic\_ransomware.pcap

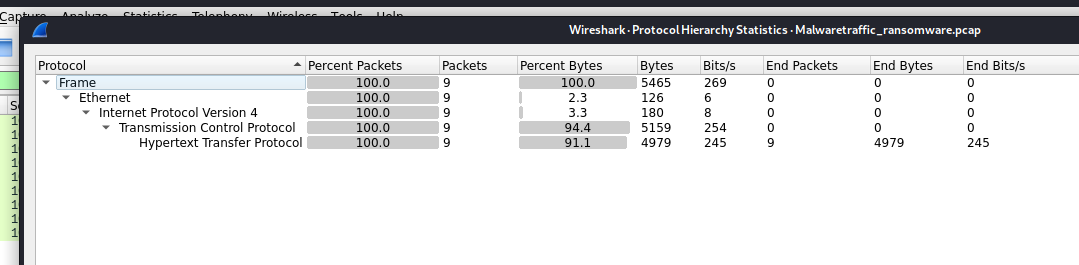
Objects contained:



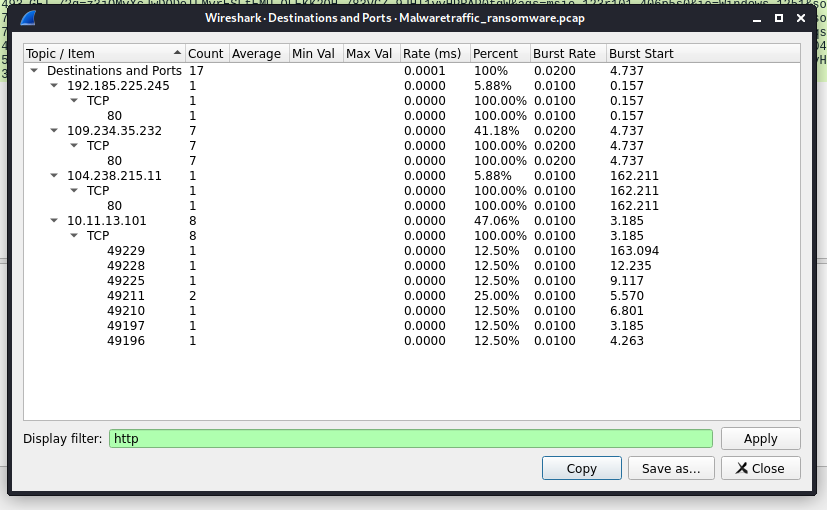
Communicated domains: , Compromised sites:



Protocol used :



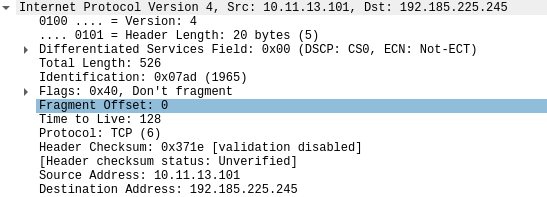
Ports Communicated:



OS the infected host runs:

Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)

Ip address of the infected host:



MAC address of the infected host and Host Name:



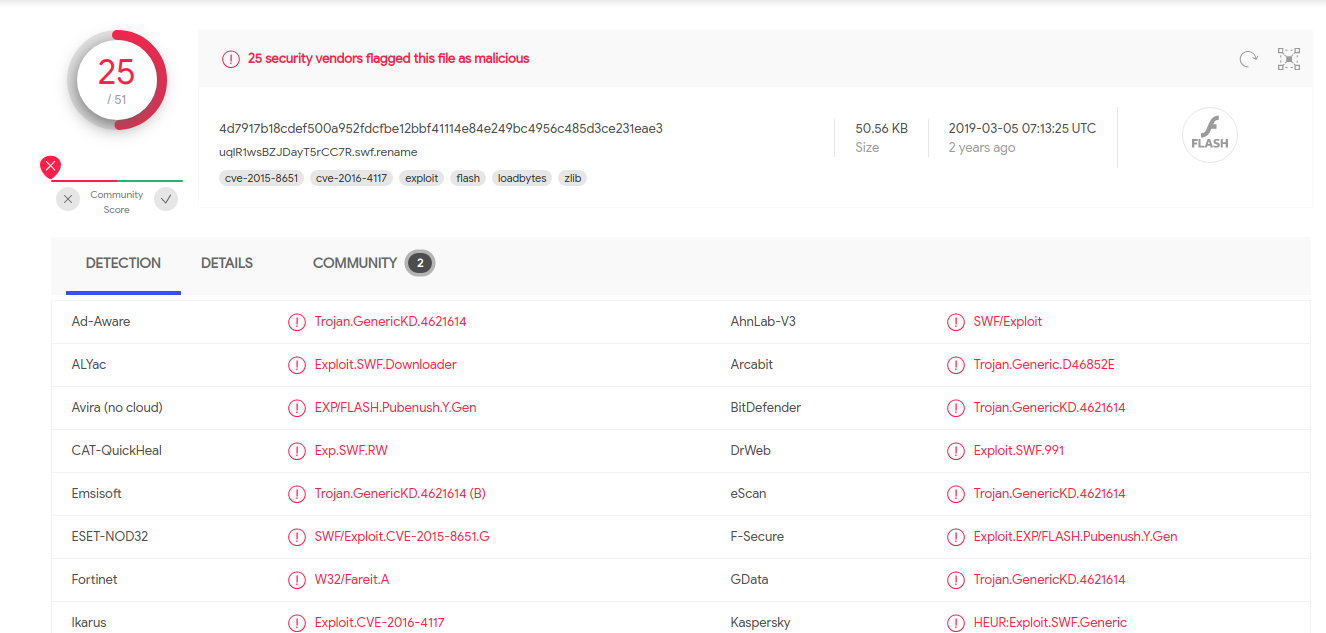
Infected URl containg exe file:

http://new.vividsydney.live/?ie=UTF-16&q=zn3QMvXcJwDQDoXGMvrESLtEMUzQA0KK2OH\_76eyEoH9JHT1vrTUSkrttgWCelz&sourceid=mozilla&es\_sm=94&aqs=mozilla.90e77.406k6m7&oq=Uo6IoLuZTOQK33hOAc1FilYlbA1wRoqr9j0jSm0XOhsLQrBG9YANM\_5alV7l8jg

Generating SHA256 hashes for the exe file:

There is no exe file, but the video file containing the malware

Type of malware:



Time and Date of Attack:

