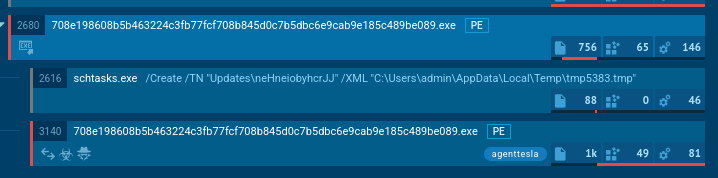
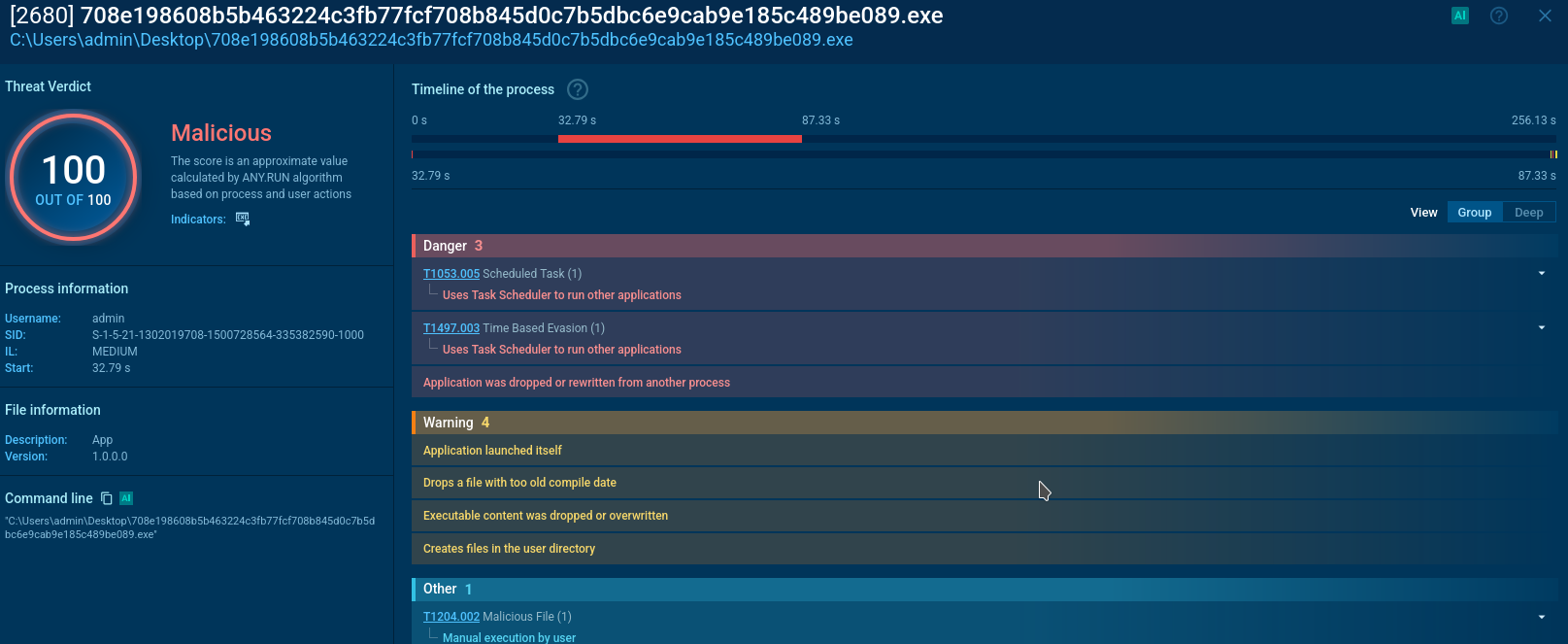
In this lab I will be anaylising the malware including the hash 80b51e872031a2befeb9a0a13e6fc480 provided by the site [AbuseCH](https://bazaar.abuse.ch/sample/708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089/). This will be done dynamically by a simulation on the site [Anyrun](https://any.run/).

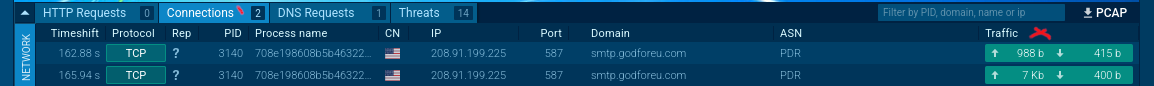
Creating a windows seven virtual machine downloaded with the malicious software, I extracted and ran the malicious software. After a few minutes, I read the report and found the malware ran with two child processes.



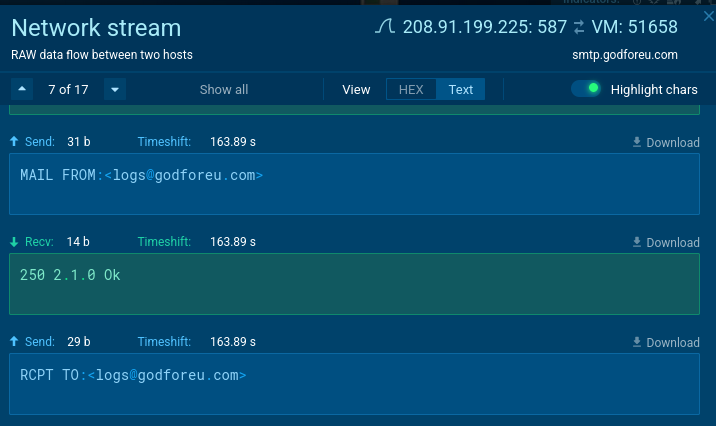
Within the parent proces ID 2680, we see the malicious software rated at 100/100.



Within the connections tab, I can analyze the raw network traffic and convert it from hexadecimal to plaintext.



With this traffic data, I am able to find where the malware is sending the stolen mail server data to was logs@godforeu..com.



I can also find the password the malware used by seeing the line before it was authorised, TzhrI1B6NHNrOndf. However, this password looks like it’s encoded in base64. Decoding it using [CyberChef](https://gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)&input=VHpockkxQjZOSE5yT25kZg) we find that the text version of the password is O8k#Pz4sk:w\_.

