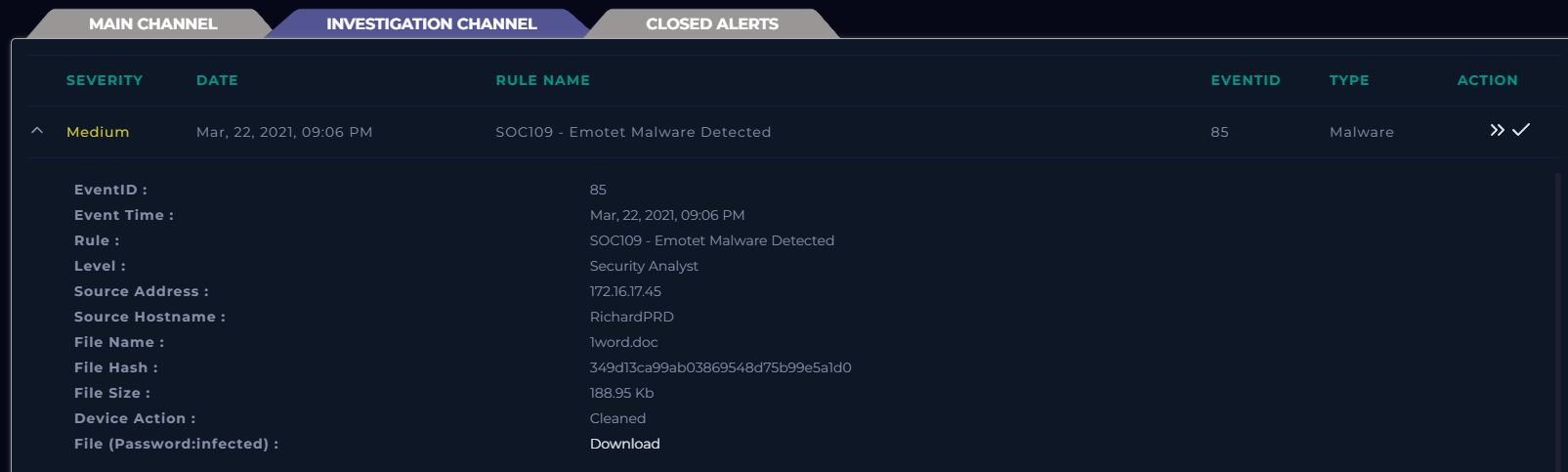
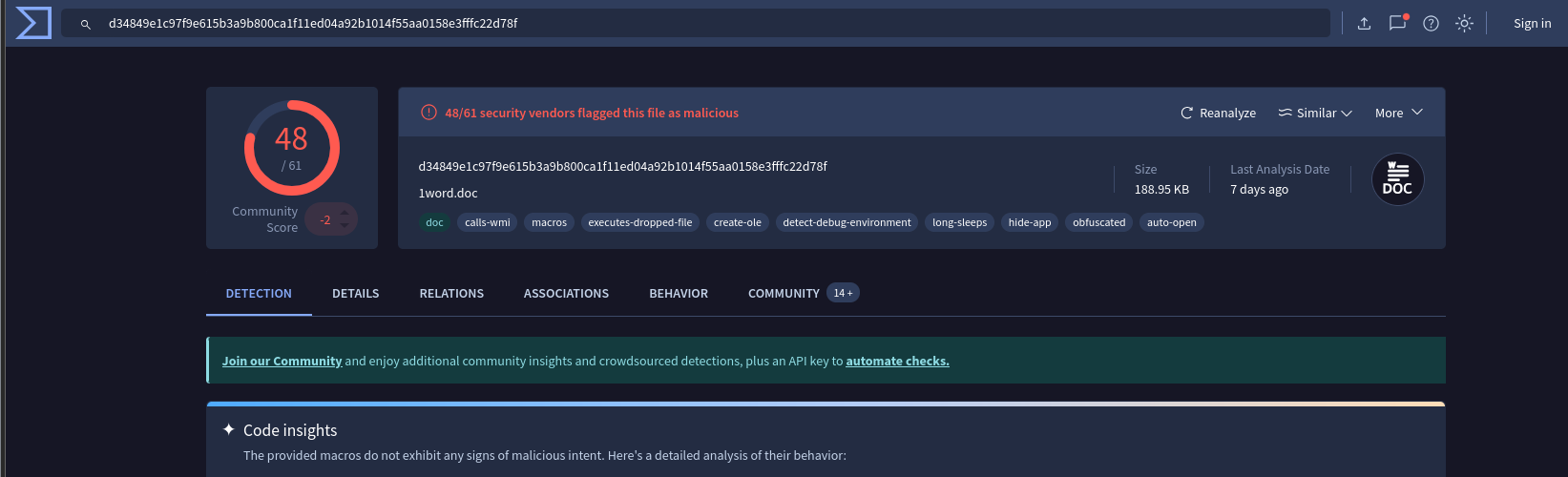
SOC109 - Emotet Malware Detected

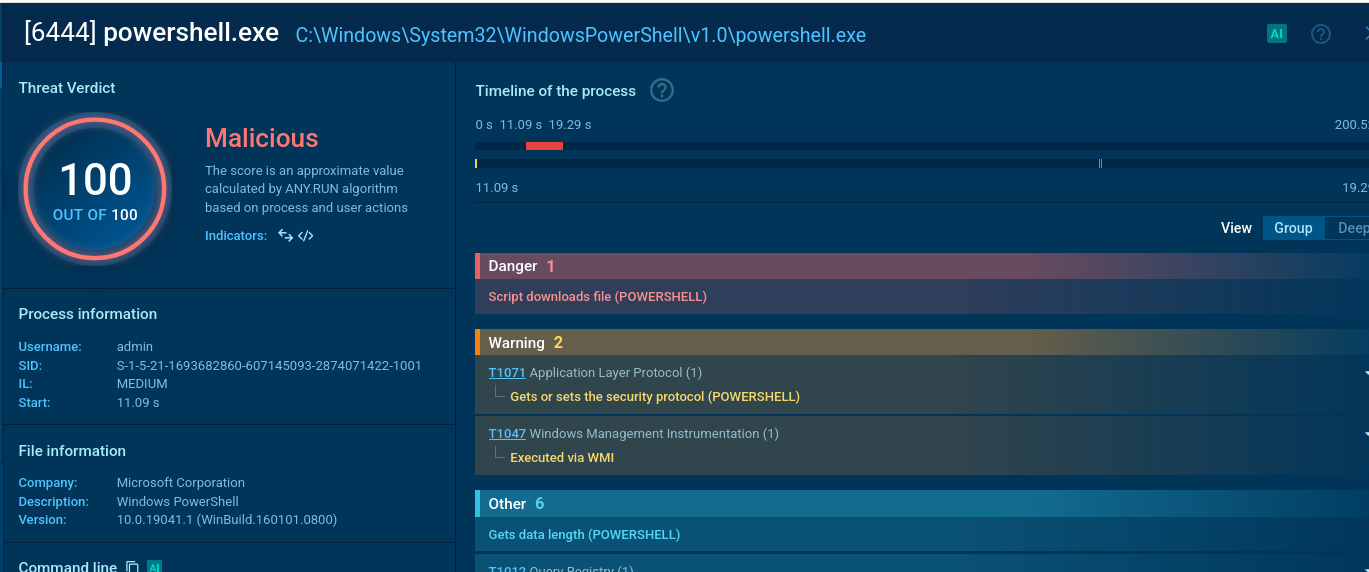
I am going to be creating a playbook on LetsDefend’s “SOC109 - Emotet Malware Detected” alert.



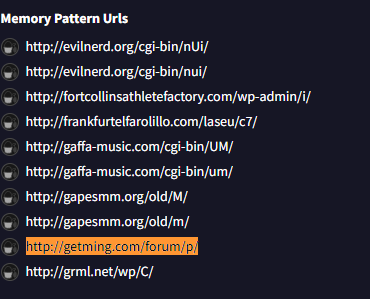
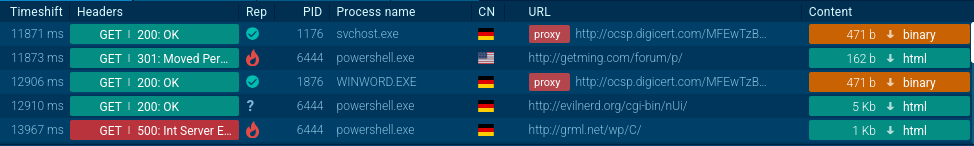
Downloading this file into my Remmux virtual machine, I extract it using the command ‘unzip -P infected 349d13ca99ab03869548d75b99e5a1d0.zip’. Placing the extracted file ‘1word.doc’ into VirusTotal showed a very malicious result.



Running this file on a AnyRun virtual machine gives us more insight on the malicious file. As seen below, the file automatically starts to run powershell commands and causes some automatic internet connections.



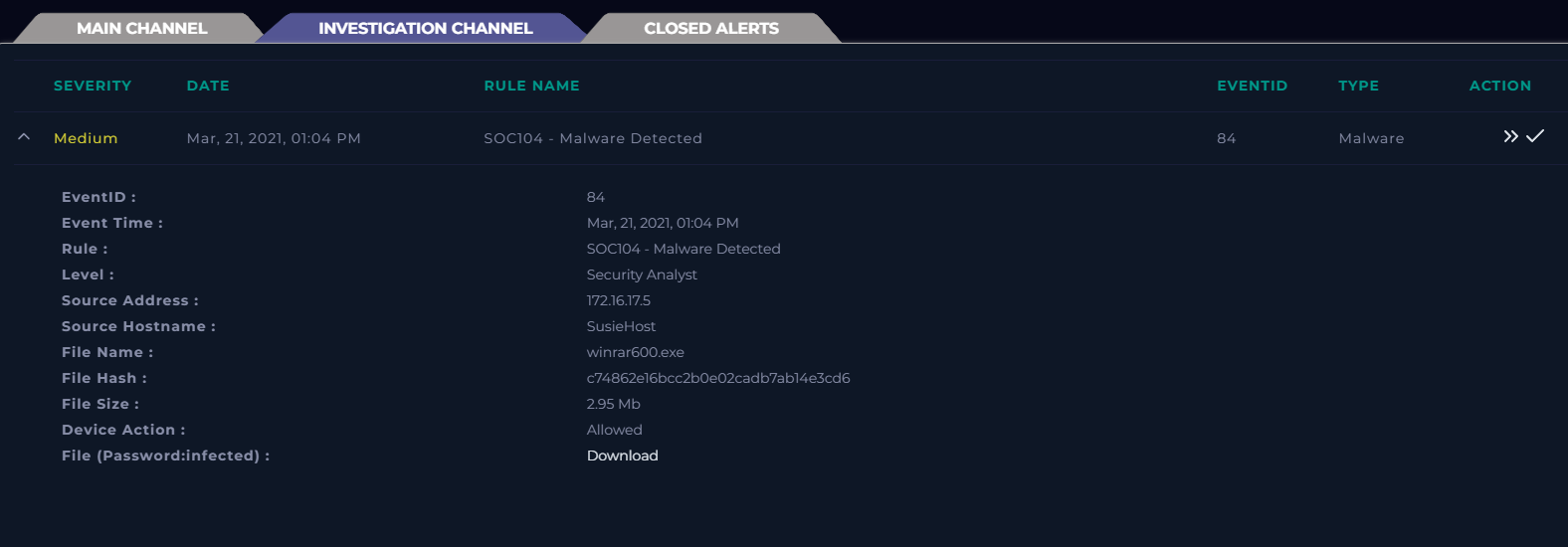
Within the HTTP requests, one low repudiation URL also matches the URLs found in VirusTotal’s analysis (http://getming.com/forum/p/).



When checking RichardPRD endpoint, we see it has already been quarantined. There are no logs available during the time of the alert from Richard’s IP meaning the system successfully cleaned up the malware. No one was able to access the malicious address.

SOC104 - Malware Detected

I am going to be creating a playbook on LetsDefend’s “SOC104 - Malware Detected” alert.



First, I need to check if the affected computer has already been contained or separated from the network. Filtering the endpoint security by the alert’s source address I find that Susie’s host is’nt quarantined.

Second, I will use various tools to analyze the suspicious file sent.

Using WinRar to simulate the suspicious file, opening it I find that its the installer for WinRar file extractor and has no further malicious content leading to be a false positive.



SOC145 - Ransomware Detected

I am going to be creating a playbook on LetsDefend’s alert “SOC145 - Ransomware Detected” . **SOC145 - Ransomware Detected**

