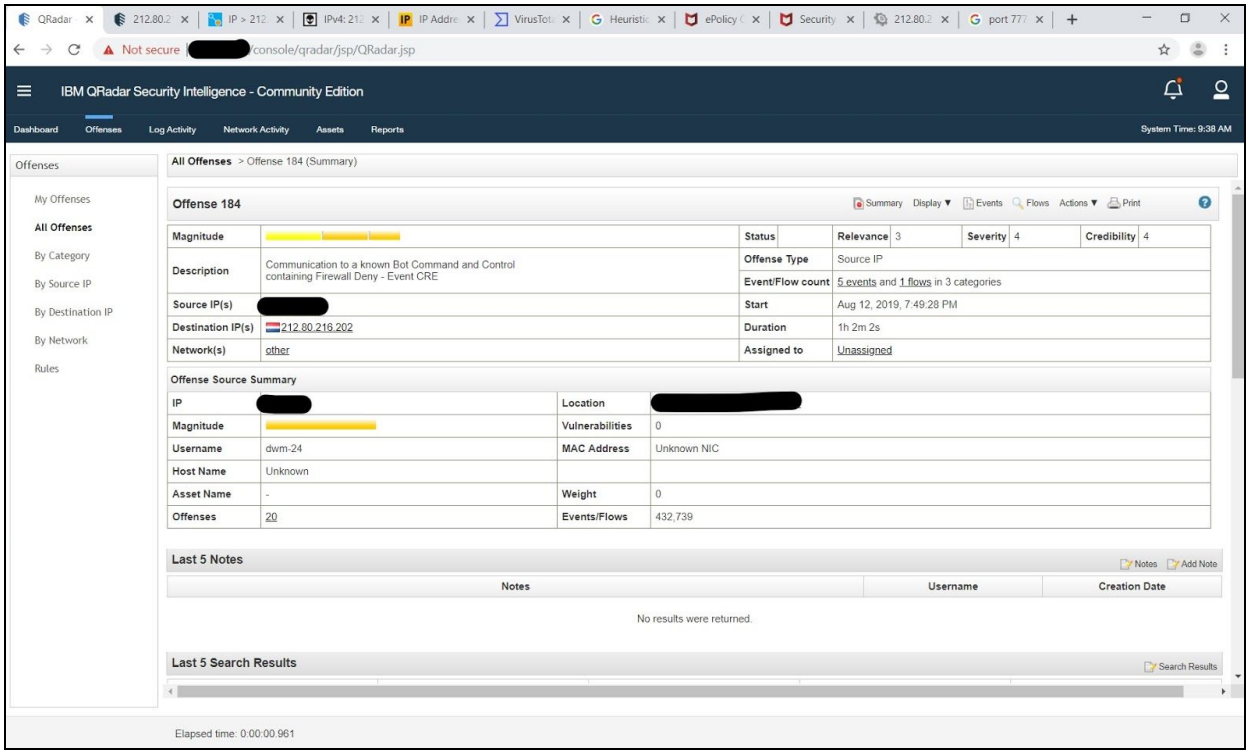
INCIDENT REPORT

As part of our training at SOC Experts, an offense generated by IBM QRadar was analysed. The report of the same is as follows-

INFORMATION OBTAINED:

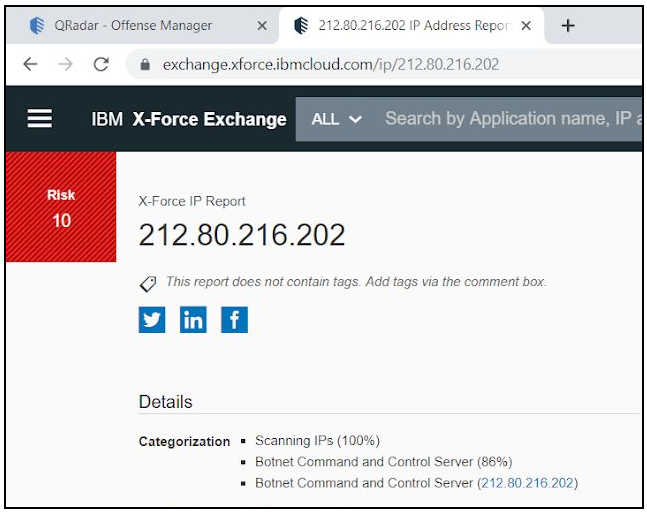


- Offense ID- 184.
- Offense description- **Communication to a known Bot Command and Control containing Firewall deny-Event CRE.**
- It was identified to be outbound traffic.
- Source IP address- xx.xx.xx.xx (Active Directory).
- Destination IP address- 212.80.216.202 (Country-Netherlands).
- Number of events = 5.
- Number of flows = 1.
- Flow activity (total bytes) = 152 bytes.
- Destination port- 7777.
- Log source- Firewall (pfSense).
- Action- Firewall deny.
- Time of occurence- Aug 12, 2019, 7:49:28 PM.
- Reported time- Aug 15, 2019, 8:33:00 AM.

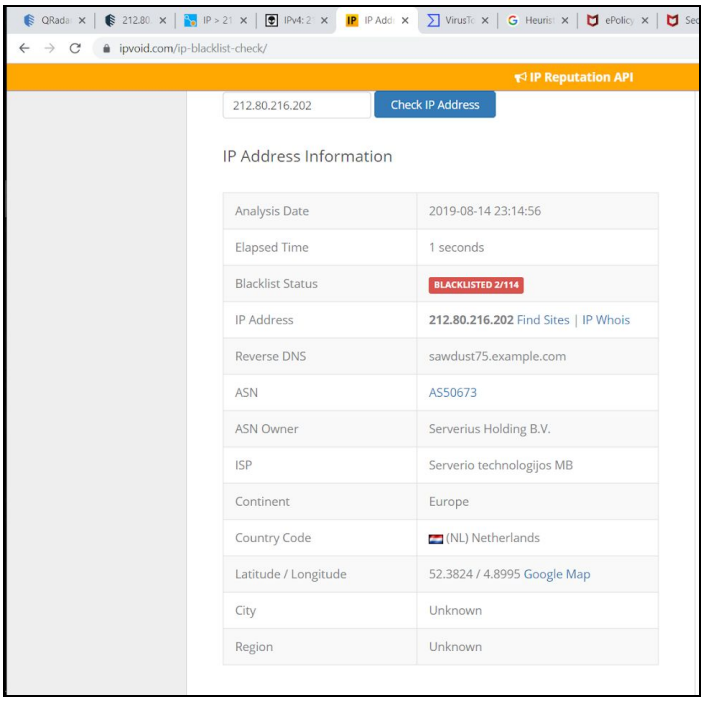
ANALYSIS:

Analysis was performed using various online tools and platforms in order to find the details of the destination IP address 212.80.216.202 (the supposed Command and Control server).

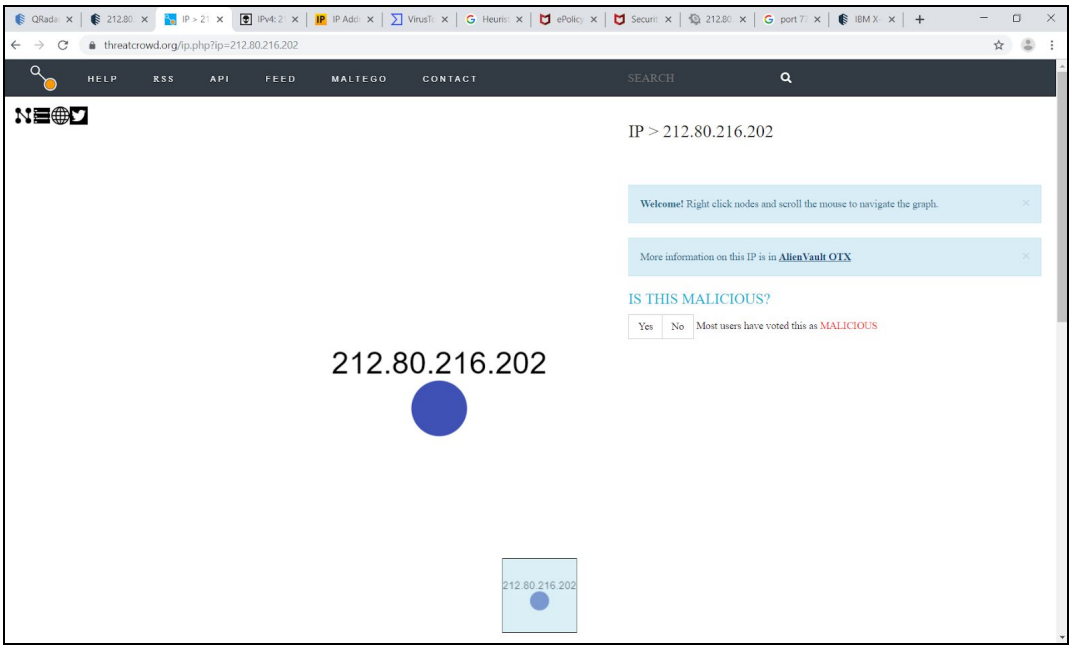
- **IBM X-Force Exchange:** The X-Force IP report stated the following:
    1. Risk = 10.
    2. Categorization- **Botnet Command and Control server.**



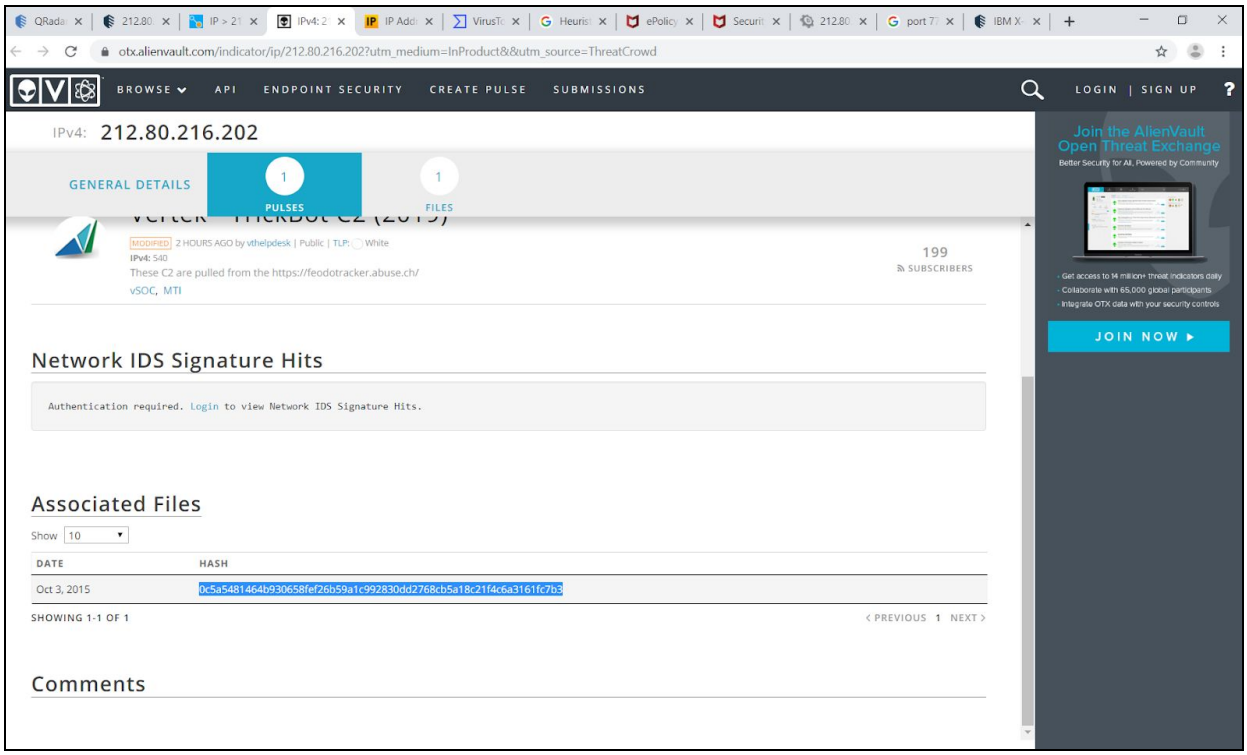
- **IPvoid:** The IP Blacklist Check indicated that the Blacklist status is 2/114.



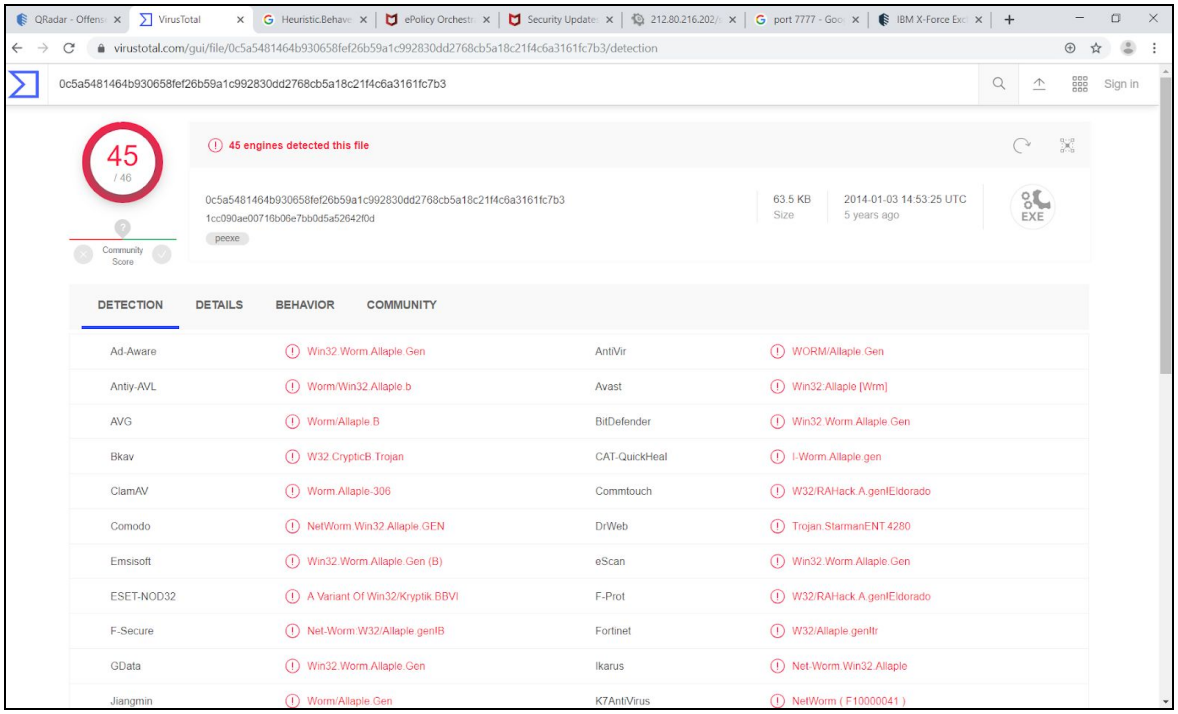
- **Threatcrowd:** It stated the IP address as **malicious**.

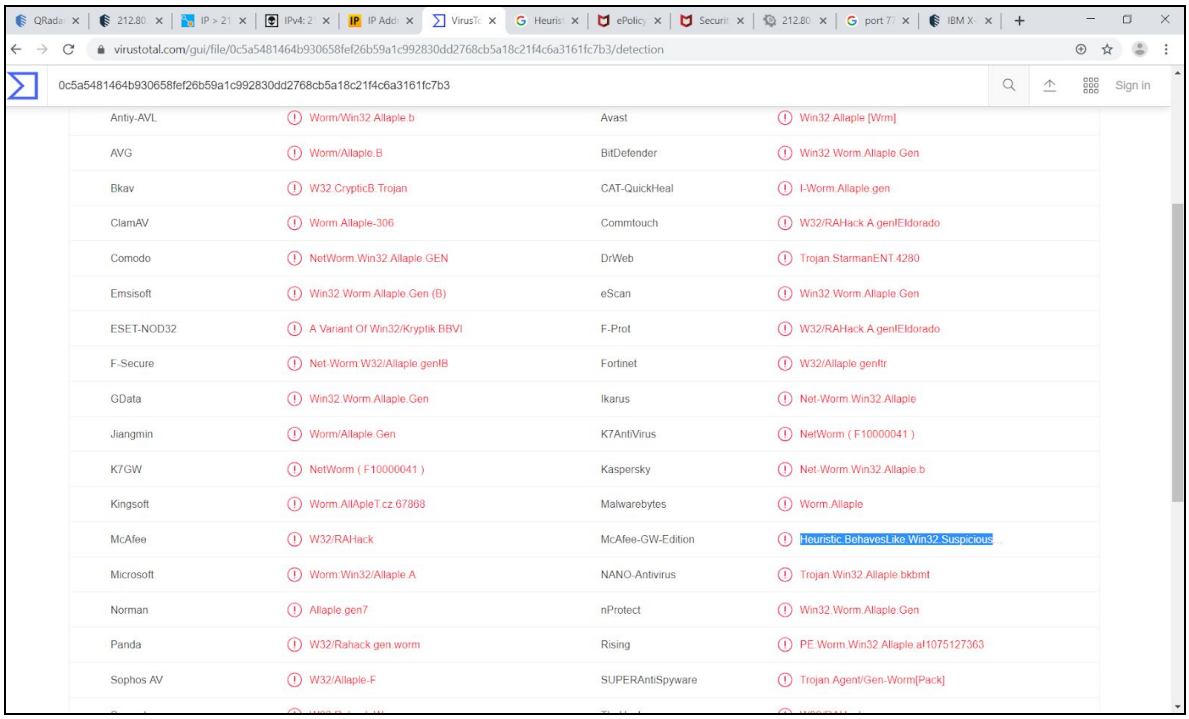


- **AlienVault OTX:** It displayed the file hash of the associated file.

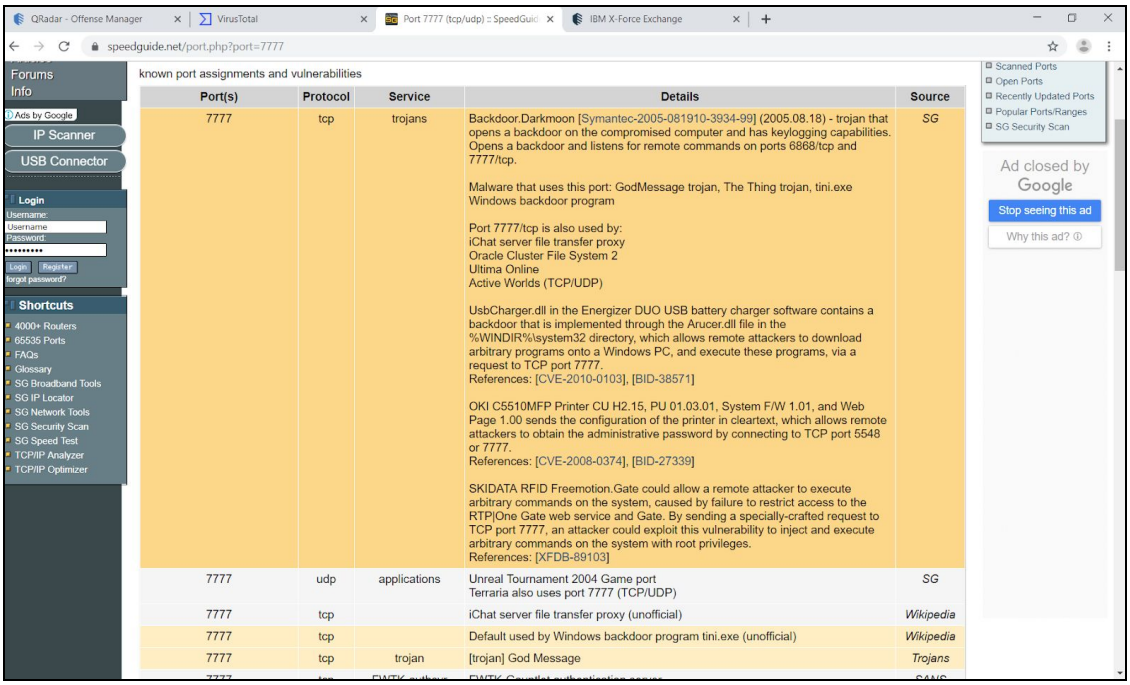


- **VirusTotal:** The file hash obtained in the previous step was then verified with VirusTotal. It was detected to be malicious by 45 out of 46 engines, among which, McAfee-GW-Edition stated it as **Heuristic.BehavesLike.Win32.Suspicious-BAY.G**(a broad classification of files that appear to have **trojan**-like features).

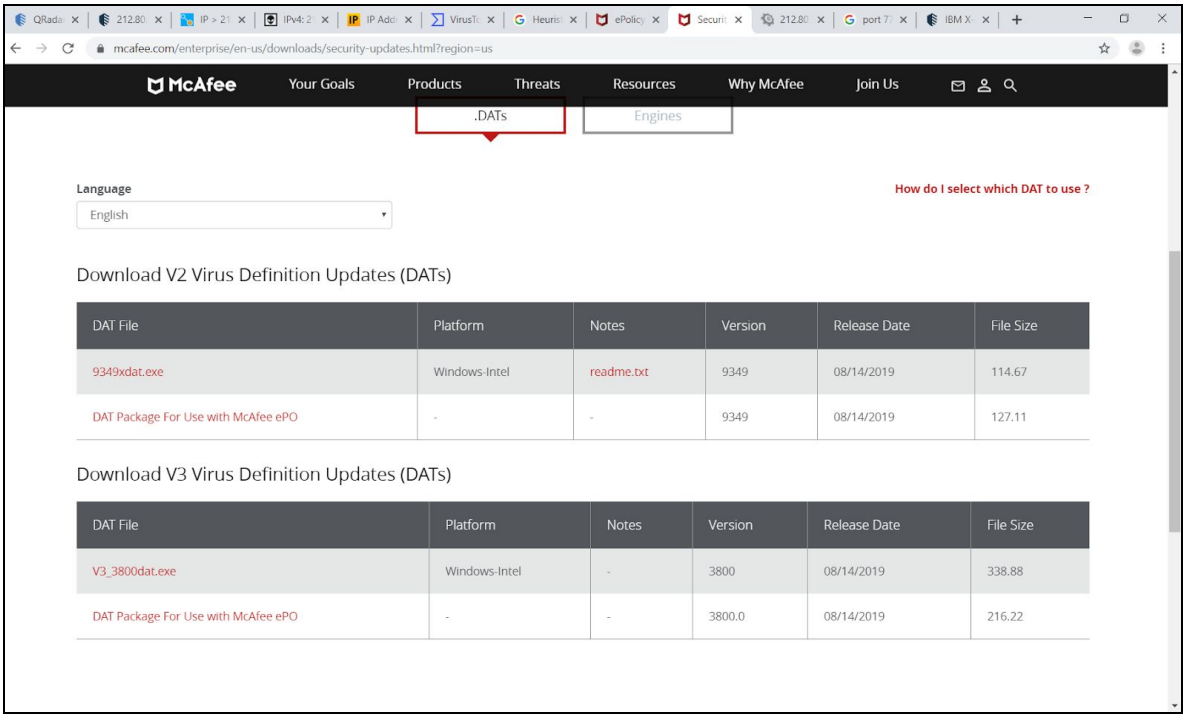


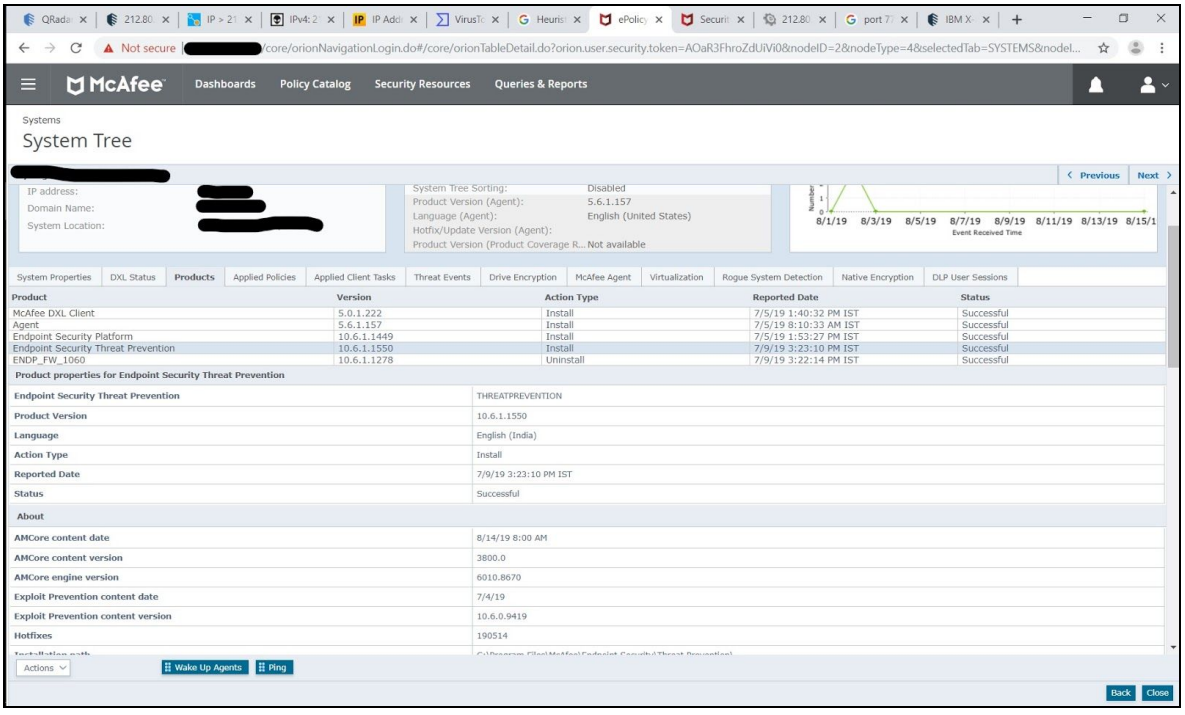


- **Speedguide:** The port used for communication (7777) was found to have services related to **trojans**.



- It was then checked if the latest signatures were available for the discovered malware. Since the antivirus software is responsible for preventing malware activity, it was verified if the Active Directory's Antivirus signature was up-to-date. It was found in McAfee ePO that the AM Core version of the Active Directory was up-to-date.





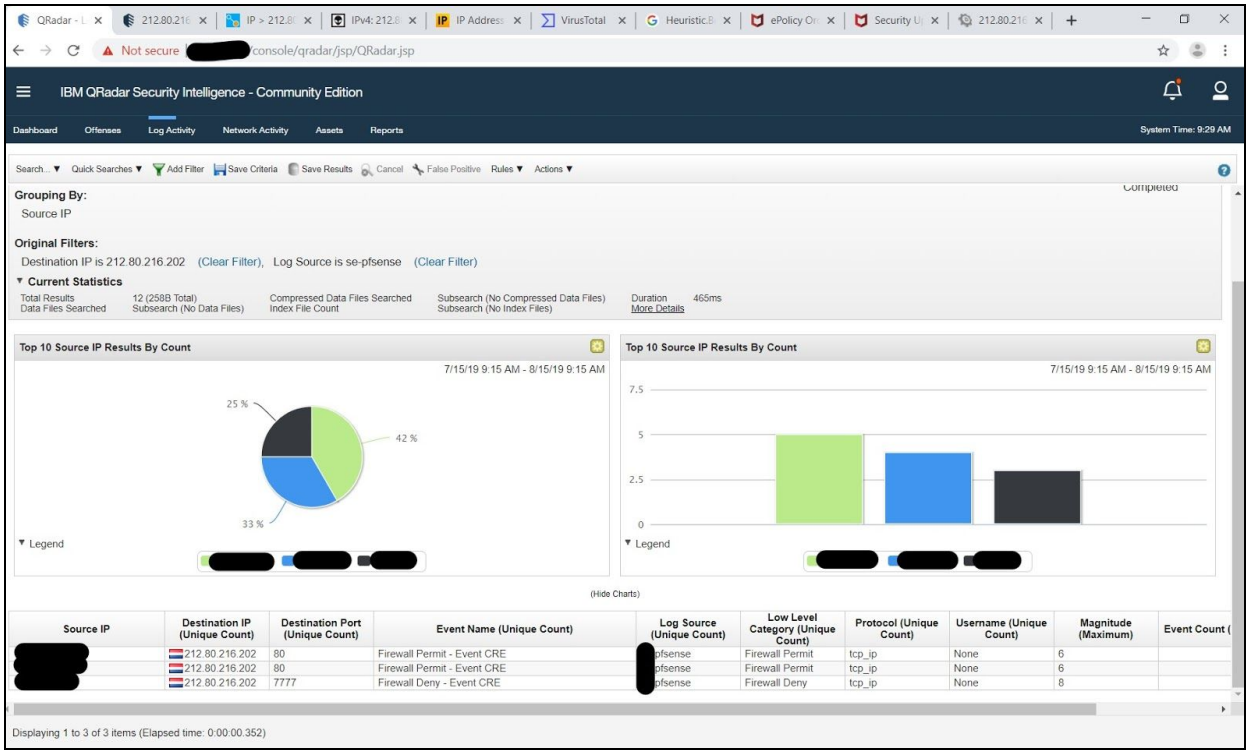
- The event still remained suspicious since it was the Active Directory that was involved in the communication with a command and control server. Therefore, the activity of the Active Directory, 30min-1hr prior to the offense trigger, was checked, but nothing suspicious was encountered.

- Then it was verified if the malicious IP address has ever tried to communicate with the network using the following filters in IBM QRadar:
    1. Log source- pfSense.
    2. Source IP- 212.80.216.202.

  No results were returned.

- Then it was verified if any other device in the network has communicated with the command and control server using the following filters in IBM QRadar:
    1. Log source- pfSense.
    2. Destination IP- 212.80.216.202.
    3. Display/group by- Source IP

  Results indicated that 2 other devices have communicated with the command and control server. Although the event was a Firewall permit, it wasn't found to be critical since the communication occurred on port 80 (just web traffic).



CONCLUSION:

Since the traffic was blocked by the firewall, no further malicious activity occurred. The incident of a device in the network communicating with a command and control server hadn't happened earlier, therefore, not a lot of information could be obtained. But if it does occur again, packet capture must be done and a deep dive analysis has to be performed.

Report by-
Srijana JC.