

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:

The screenshot displays the IBM QRadar Security Intelligence - Community Edition interface. The main content area shows details for Offense 184. The interface includes a navigation menu on the left with options like Dashboard, Offenses, Log Activity, Network Activity, Assets, and Reports. The main area is titled 'All Offenses > Offense 184 (Summary)'. It features a summary table with columns for Magnitude, Status, Relevance, Severity, and Credibility. Below this is a detailed description of the offense, including its type, event/flow count, start time, duration, and assigned status. An 'Offense Source Summary' table provides further details about the source IP, location, vulnerabilities, username, host name, asset name, weight, and the number of offenses and events/flows. At the bottom, there are sections for 'Last 5 Notes' and 'Last 5 Search Results', both of which currently show no results.

Magnitude	Status	Relevance	Severity	Credibility
[Progress Bar]		3	4	4

Offense Type	Source IP
Event/Flow count	5 events and 1 flows in 3 categories
Start	Aug 12, 2019, 7:49:28 PM
Duration	1h 2m 2s
Assigned to	Unassigned

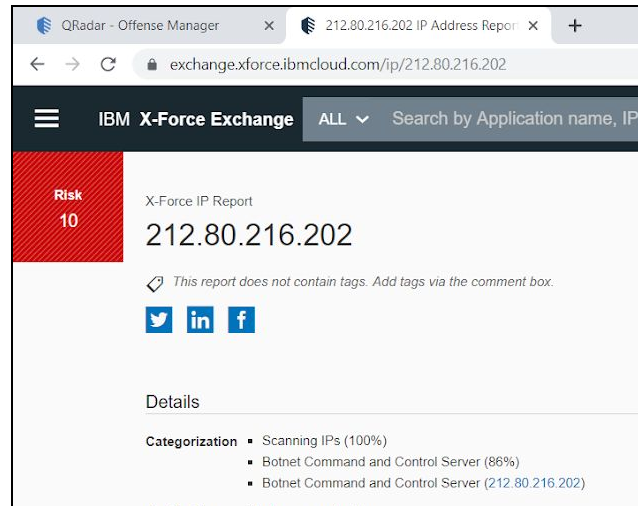
IP	Location
[Redacted]	[Redacted]
Magnitude	Vulnerabilities
[Progress Bar]	0
Username	MAC Address
dwm-24	Unknown NIC
Host Name	Unknown
Asset Name	Weight
-	0
Offenses	Events/Flows
20	432,739

- 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 occurrence- 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).

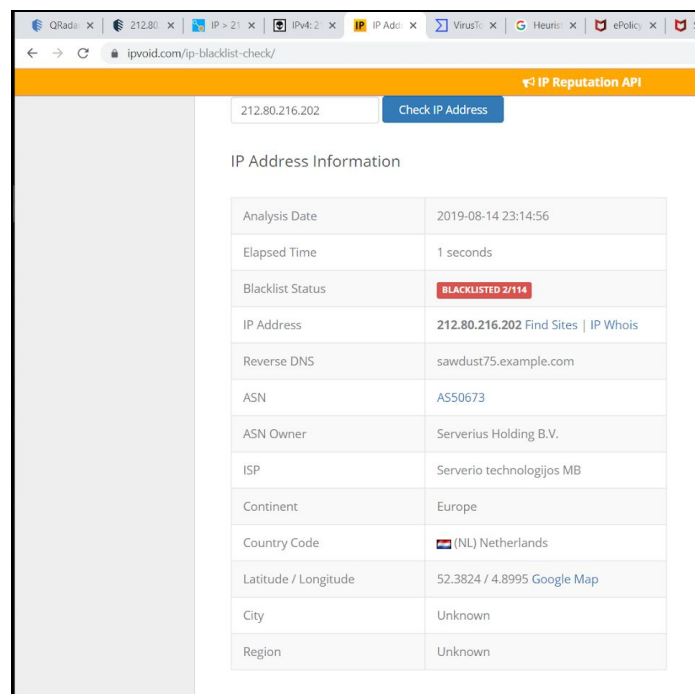
- **IBM X-Force Exchange:** The X-Force IP report stated the following:
 1. Risk = 10.
 2. Categorization- **Botnet Command and Control server.**




The screenshot shows the IBM X-Force Exchange interface. The URL is exchange.xforce.ibmcloud.com/ip/212.80.216.202. The page displays an X-Force IP Report for 212.80.216.202 with a Risk score of 10. Below the risk score, there are social media sharing icons for Twitter, LinkedIn, and Facebook. The 'Details' section shows the following categorization:

- Scanning IPs (100%)
- Botnet Command and Control Server (86%)
- Botnet Command and Control Server (212.80.216.202)

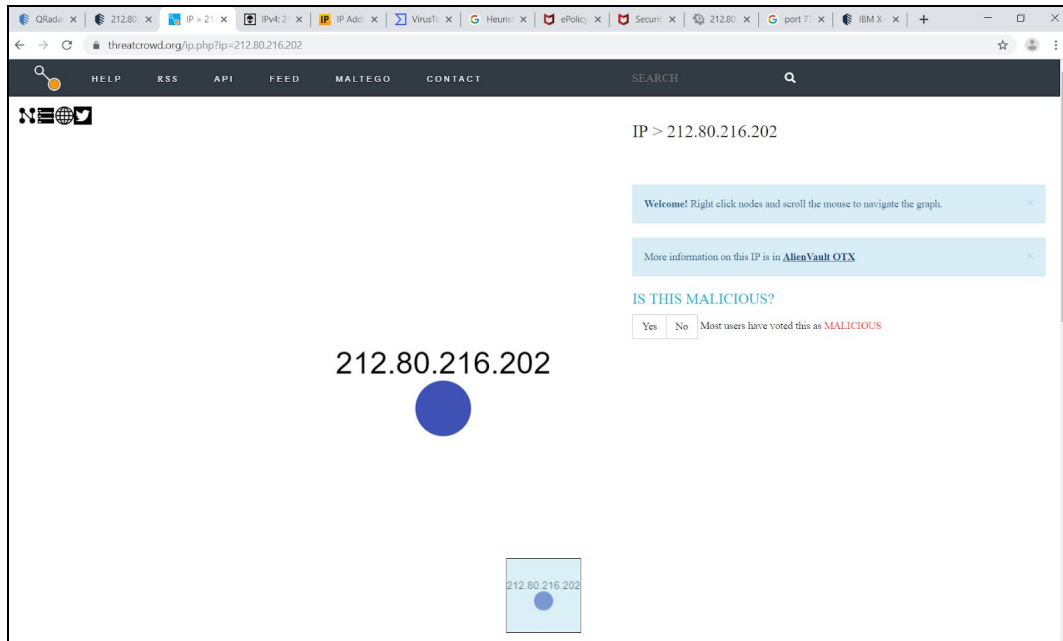
- **IPvoid:** The IP Blacklist Check indicated that the Blacklist status is 2/114.



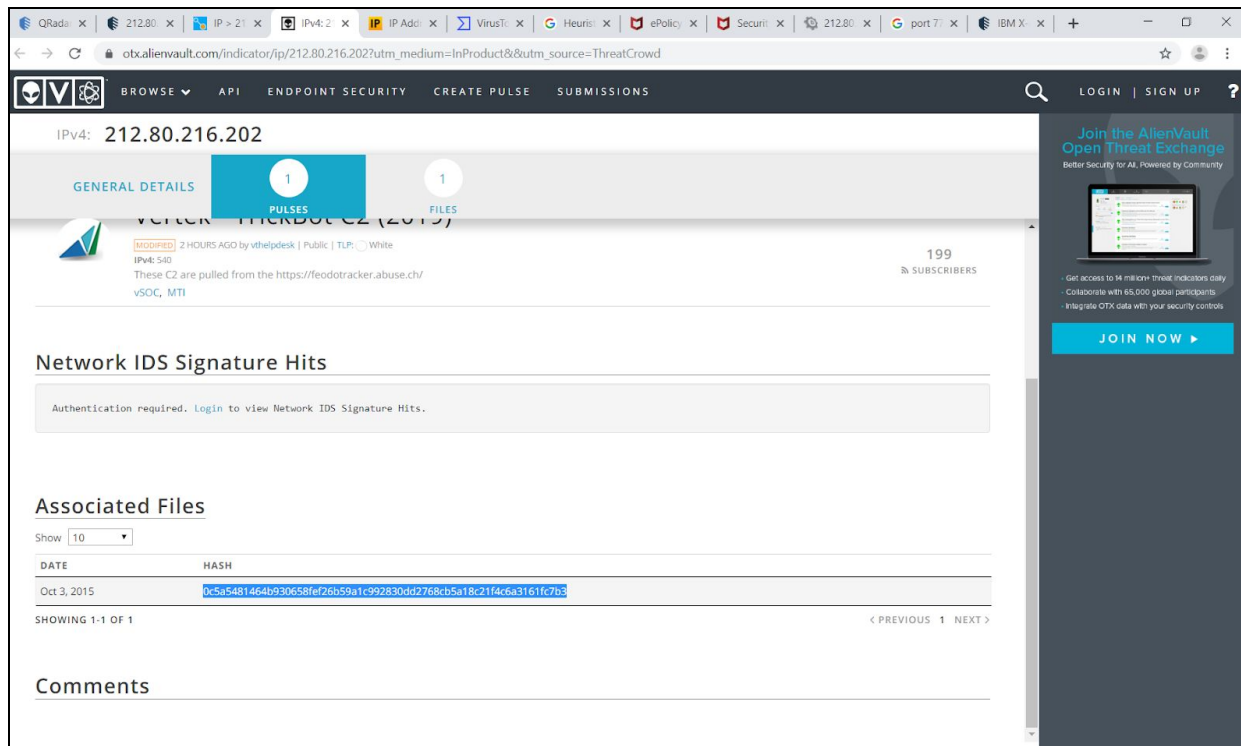
The screenshot shows the IPvoid IP Reputation API interface. The URL is ipvoid.com/ip-blacklist-check/. The page displays the results for the IP address 212.80.216.202. The Blacklist Status is shown as **BLACKLISTED 2/114**. The IP Address Information table is as follows:

Analysis Date	2019-08-14 23:14:56
Elapsed Time	1 seconds
Blacklist Status	BLACKLISTED 2/114
IP Address	212.80.216.202 Find Sites IP Whois
Reverse DNS	sawdust75.example.com
ASN	AS50673
ASN Owner	Serverius Holding B.V.
ISP	Serverio technologijos MB
Continent	Europe
Country Code	 (NL) Netherlands
Latitude / Longitude	52.3824 / 4.8995 Google Map
City	Unknown
Region	Unknown

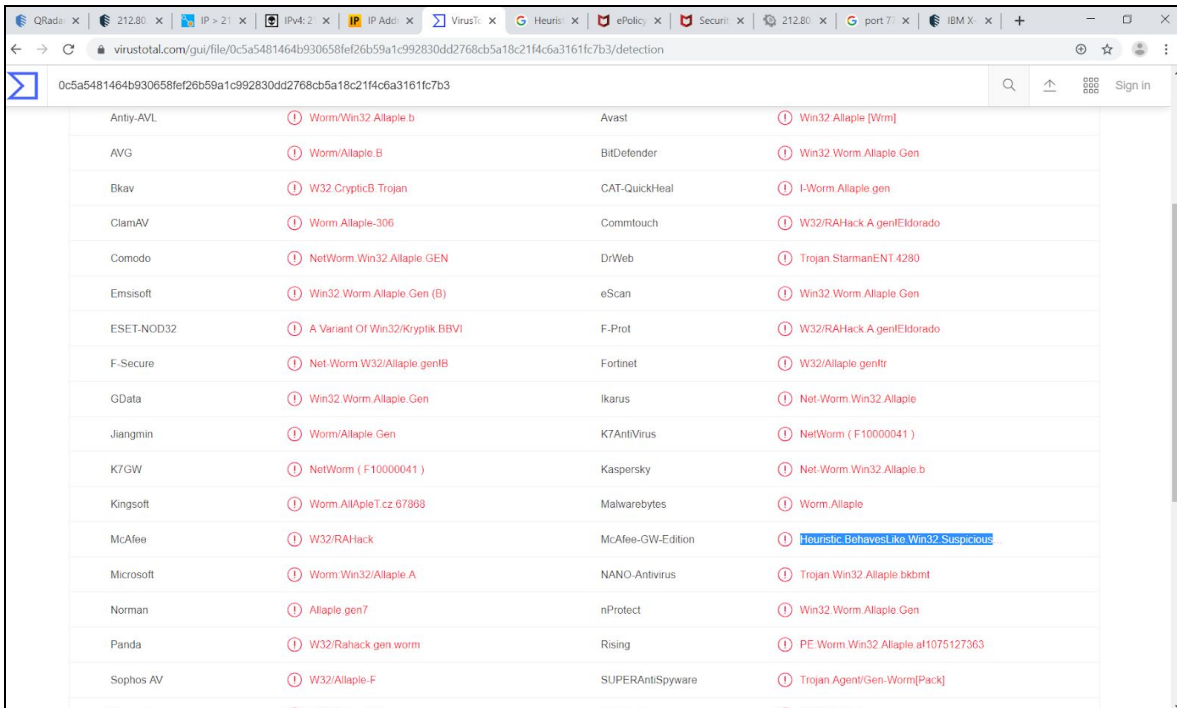
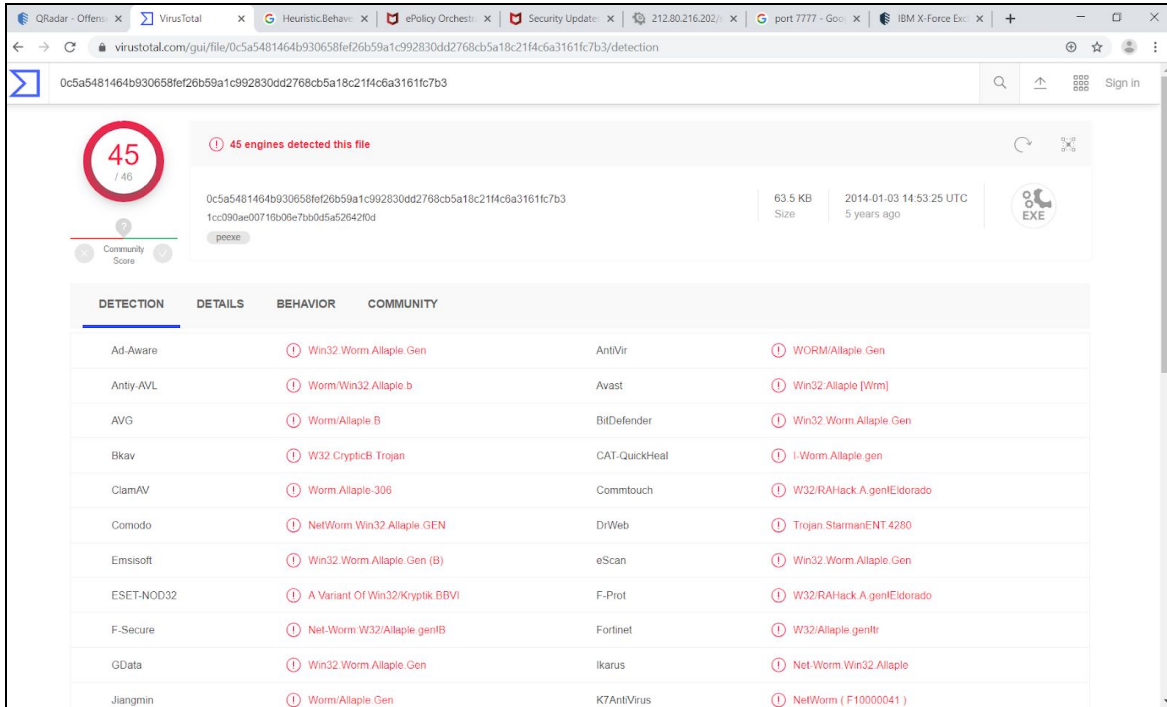
- **Threatcrowd:** It stated the IP address as **malicious**.



- **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**.

known port assignments and vulnerabilities

Port(s)	Protocol	Service	Details	Source
7777	tcp	trojans	<p>Backdoor.Darkmoon [Symantec-2005-081910-3934-99] (2005.08.18) - trojan that opens a backdoor on the compromised computer and has keylogging capabilities. Opens a backdoor and listens for remote commands on ports 6868/tcp and 7777/tcp.</p> <p>Malware that uses this port: GodMessage trojan, The Thing trojan, tini.exe Windows backdoor program</p> <p>Port 7777/tcp is also used by: iChat server file transfer proxy Oracle Cluster File System 2 Ultima Online Active Worlds (TCP/UDP)</p> <p>UsbCharger.dll in the Energizer DUO USB battery charger software contains a backdoor that is implemented through the Arucer.dll file in the %WINDIR%\system32 directory, which allows remote attackers to download arbitrary programs onto a Windows PC, and execute these programs, via a request to TCP port 7777. References: [CVE-2010-0103], [BID-38571]</p> <p>OKI C5510MFP Printer CU H2.15, PU 01.03.01, System F/W 1.01, and Web Page 1.00 sends the configuration of the printer in cleartext, which allows remote attackers to obtain the administrative password by connecting to TCP port 5548 or 7777. References: [CVE-2008-0374], [BID-27339]</p> <p>SKIDATA RFID Froemotion.Gate could allow a remote attacker to execute arbitrary commands on the system, caused by failure to restrict access to the RTPOne Gate web service and Gate. By sending a specially-crafted request to TCP port 7777, an attacker could exploit this vulnerability to inject and execute arbitrary commands on the system with root privileges. References: [XFDB-89103]</p>	SG
7777	udp	applications	Unreal Tournament 2004 Game port Terraria also uses port 7777 (TCP/UDP)	SG
7777	tcp		iChat server file transfer proxy (unofficial)	Wikipedia
7777	tcp		Default used by Windows backdoor program tini.exe (unofficial)	Wikipedia
7777	tcp	trojan	[trojan] God Message	Trojans
7777	tcp			

- 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.

McAfee .DATs Engines

Language: English

How do I select which DAT to use ?

Download V2 Virus Definition Updates (DATs)

DAT File	Platform	Notes	Version	Release Date	File Size
9349xdm.exe	Windows-Intel	readme.txt	9349	08/14/2019	114.67
DAT Package For Use with McAfee ePO	-	-	9349	08/14/2019	127.11

Download V3 Virus Definition Updates (DATs)

DAT File	Platform	Notes	Version	Release Date	File Size
V3_3800dat.exe	Windows-Intel	-	3800	08/14/2019	338.88
DAT Package For Use with McAfee ePO	-	-	3800.0	08/14/2019	216.22

McAfee Dashboards Policy Catalog Security Resources Queries & Reports

System Tree

IP address: [redacted]
 Domain Name: [redacted]
 System Location: [redacted]

System Tree Sorting: Disabled
 Product Version (Agent): 5.6.1.157
 Language (Agent): English (United States)
 Hotfix/Update Version (Agent):
 Product Version (Product Coverage R...): Not available

System Properties DXL Status Products Applied Policies Applied Client Tasks Threat Events Drive Encryption McAfee Agent Virtualization Rogue System Detection Native Encryption DLP User Sessions

Product	Version	Action Type	Reported Date	Status
McAfee DXL Client	5.0.1.222	Install	7/5/19 1:40:32 PM IST	Successful
Agent	5.6.1.157	Install	7/5/19 8:10:33 AM IST	Successful
Endpoint Security Platform	10.6.1.1449	Install	7/5/19 1:53:27 PM IST	Successful
Endpoint Security Threat Prevention	10.6.1.1550	Install	7/9/19 3:23:10 PM IST	Successful
ENDP_FW_1050	10.6.1.1278	Uninstall	7/9/19 3:22:14 PM IST	Successful

Product properties for Endpoint Security Threat Prevention

Endpoint Security Threat Prevention	THREATPREVENTION
Product Version	10.6.1.1550
Language	English (India)
Action Type	Install
Reported Date	7/9/19 3:23:10 PM IST
Status	Successful

About

AMCore content date	8/14/19 8:00 AM
AMCore content version	3800.0
AMCore engine version	6010.8670
Exploit Prevention content date	7/4/19
Exploit Prevention content version	10.6.0.9419
Hotfixes	190514

Actions: Wake Up Agents Ping

- 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).

The screenshot shows the IBM QRadar Security Intelligence interface. The search criteria are: Destination IP is 212.80.216.202 and Log Source is se-pfsense. The current statistics show 12 total results. The pie chart shows the distribution of source IPs: 42% (green), 33% (blue), and 25% (black). The bar chart shows the count of events for each source IP: 5 (green), 4 (blue), and 3 (black).

Source IP	Destination IP (Unique Count)	Destination Port (Unique Count)	Event Name (Unique Count)	Log Source (Unique Count)	Low Level Category (Unique Count)	Protocol (Unique Count)	Username (Unique Count)	Magnitude (Maximum)	Event Count
[Redacted]	212.80.216.202	80	Firewall Permit - Event CRE	pfSense	Firewall Permit	tcp_ip	None	6	
[Redacted]	212.80.216.202	80	Firewall Permit - Event CRE	pfSense	Firewall Permit	tcp_ip	None	6	
[Redacted]	212.80.216.202	7777	Firewall Deny - Event CRE	pfSense	Firewall Deny	tcp_ip	None	8	

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.