SEQURETEK
SIMPLIFY SECURITY

IR
Incident Report

Summary

Incident No.	**#93167**	**Client:**	**NEOGROWTH**
Incident Date:	**8/17/2022**	**Incident Time:**	**09:23:08 IST**
Incident Type:	Actionable	**Severity:**	Medium
Event Source:	Amazon	**Event Count:**	54
Category:	Cyber Threat Intelligence	**Specify Others:**	-
Detected on Device	Amazon VPC	**Device IP/Host Name**	**-**

Incident Details

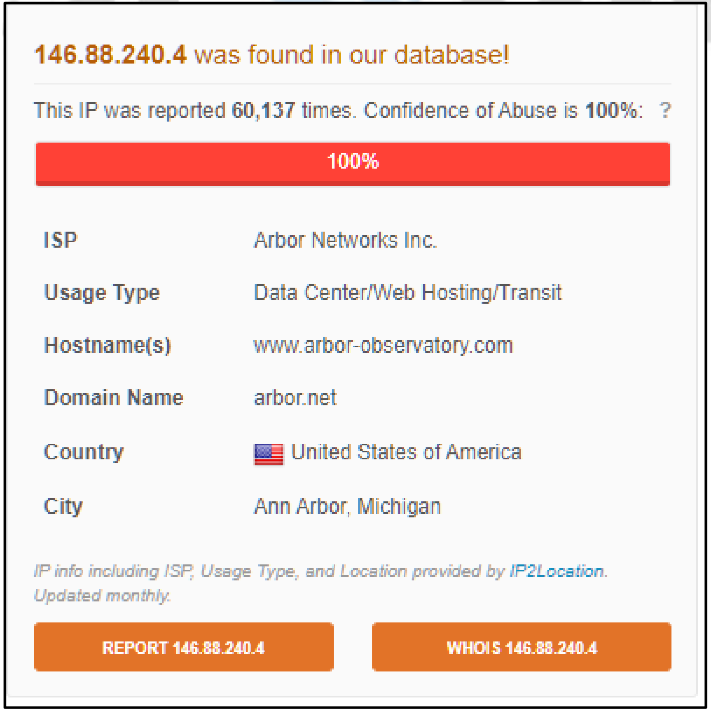
Source Address/Host	Source Country	Source Port	Destination Address/Host	Destination Port	Destination Country
146.88.240.4	**USA**	**Multiple**	**Multiple**	**Multiple**	**Internal**
10.5.1.10	**Internal**	**111**	**146.88.240.4**	**50578**	**USA**
User Name	-				
URL	-				
Incident Description	**1.** Inbound Communication has been observed from the Source IP "**146.88.240.4**" towards Multiple Internal Destination IPs on **Multiple Critical** Ports such as (**17,123,111,137**) for which device action on **Amazon VPC is "Accept**". **2.** Also we have observed Outbound Communication from Internal SourceIP "**10.5.1.10"** towards Destination IP "**146.88.240.4**" and over Port **50578** for which device action on **Amazon VPC is "Accept**". 3. IP "**146.88.240.4**" belongs to "**USA**" and is reported for **Port Scan, Hacking** etc. 4. Please find attached communication details for your reference.				
Associated Risk	1. Communicating with suspicious IP can allow attacker to install malware/Trojan on the targeted system which further can be spread into the whole network. Which can cause to Information Disclosure, Credential Theft and Data leakage 2. **Port 137** is utilized by **NetBIOS Name service**. Enabling NetBIOS services provide access to shared resources like files and printers not only to your				

	network computers but also to anyone across the internet. Therefore it is advisable to block port 137 in the Firewall. 3. **Port 17: Used to receive remote QOTDs**. Used for social engineering attacks, where users receive fake instructions to verify passwords , etc. Disable this port on all hosts. 4. **Port 111** is the **SUN Remote Procedure Call**. It is referred to as a "portmapper" because it provides a directory, or "mapping" between available services and their ports. 5. **Port 123** is used for **NTP server communication.**	
Actionable Points	**Temporary Containment**	1. It is recommended to block the IP "**146.88.240.4**" on all perimeter, if the activity is not authorized.
	Mitigation Steps	1. Regularly update devices with the latest patches to help prevent attacks that exploit vulnerabilities. 2. It is recommended to close the unwanted ports.

Note: All malicious indicators given in the report have been corroborated from Sequretek's Threat Intelligence Feed which has been integrated with the SOC to provide a contextual corelation of any malicious activity.

Threat Intelligence Screenshots:

IP Reputation: (Source:www. abuseipdb.com)



146.88.240.4 was found in our database!

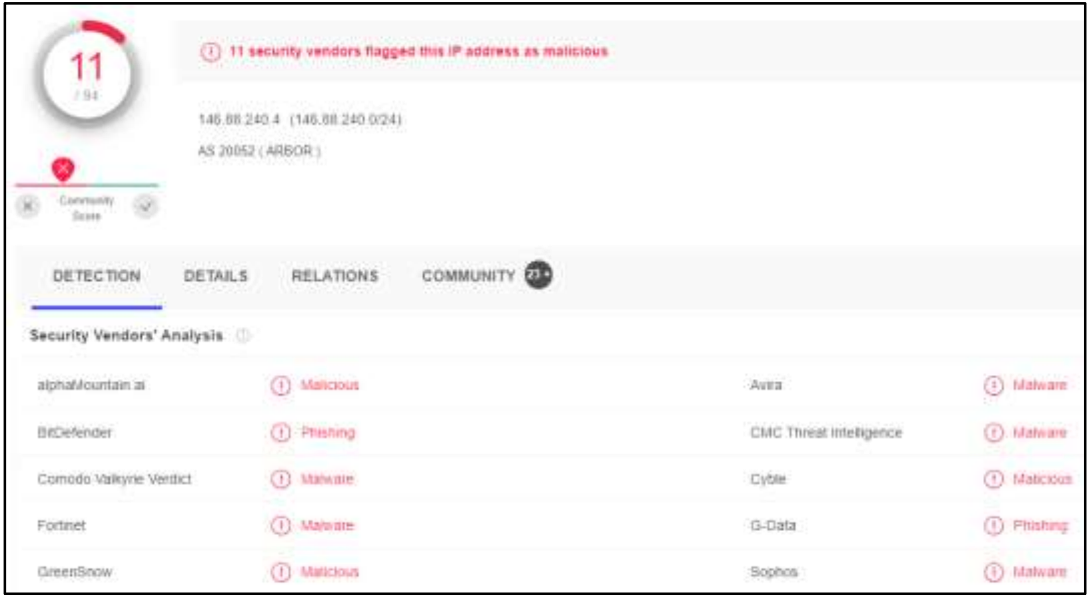
This IP was reported **60,137** times. Confidence of Abuse is **100%**: ?

100%

ISP	Arbor Networks Inc.
Usage Type	Data Center/Web Hosting/Transit
Hostname(s)	www.arbor-observatory.com
Domain Name	arbor.net
Country	United States of America
City	Ann Arbor, Michigan

IP info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly.

Source: (www.virustotal.com)



11 security vendors flagged this IP address as malicious

11
/ 94

Community Score

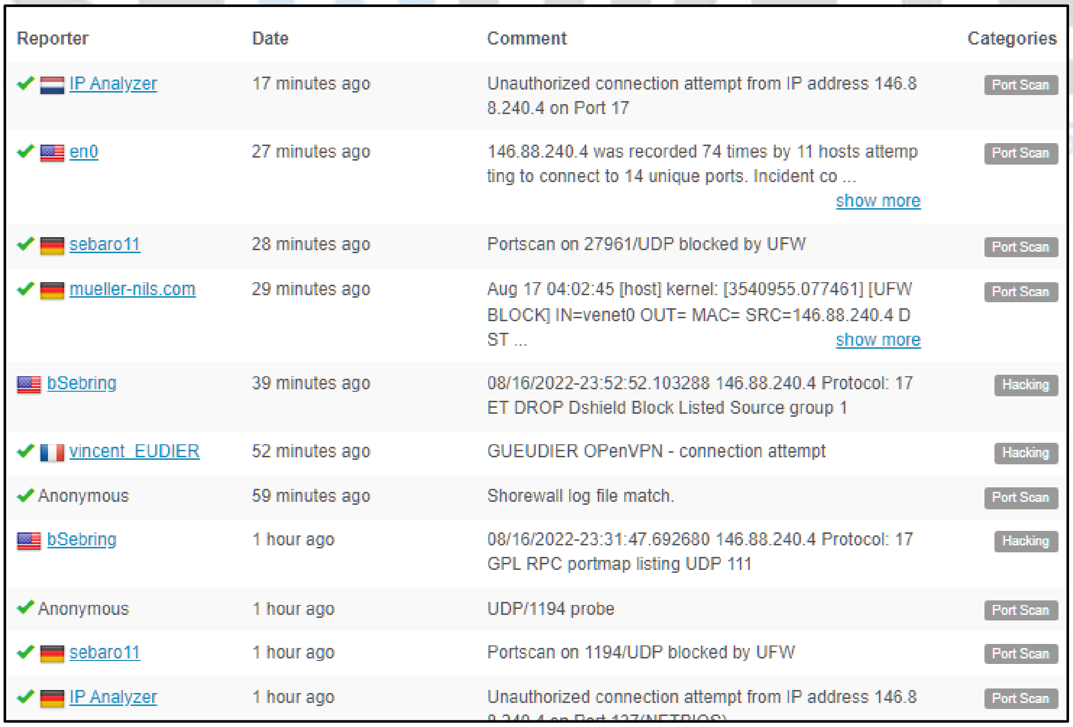
146.88.240.4 (146.88.240.0/24)
AS 20052 (ARBOR)

Security Vendors' Analysis

alphaMountain.ai	Malicious	Avira	Malware
BitDefender	Phishing	CMC Threat Intelligence	Malware
Comodo Valkyrie Verdict	Malware	Cyble	Malicious
Fortinet	Malware	G-Data	Phishing
GreenSnow	Malicious	Sophos	Malware

Recent Activity

Source: (www.abuseipdb.com)



Reporter	Date	Comment	Categories
✓ IP Analyzer	17 minutes ago	Unauthorized connection attempt from IP address 146.88.240.4 on Port 17	Port Scan
✓ en0	27 minutes ago	146.88.240.4 was recorded 74 times by 11 hosts attempting to connect to 14 unique ports. Incident co ... show more	Port Scan
✓ sebaro11	28 minutes ago	Portscan on 27961/UDP blocked by UFW	Port Scan
✓ mueller-nils.com	29 minutes ago	Aug 17 04:02:45 [host] kernel: [3540955.077461] [UFW BLOCK] IN=venet0 OUT= MAC= SRC=146.88.240.4 DST ... show more	Port Scan
bSebring	39 minutes ago	08/16/2022-23:52:52.103288 146.88.240.4 Protocol: 17 ET DROP Dshield Block Listed Source group 1	Hacking
✓ vincent_EUDIER	52 minutes ago	GUEUDIER OPenVPN - connection attempt	Hacking
✓ Anonymous	59 minutes ago	Shorewall log file match.	Port Scan
bSebring	1 hour ago	08/16/2022-23:31:47.692680 146.88.240.4 Protocol: 17 GPL RPC portmap listing UDP 111	Hacking
✓ Anonymous	1 hour ago	UDP/1194 probe	Port Scan
✓ sebaro11	1 hour ago	Portscan on 1194/UDP blocked by UFW	Port Scan
✓ IP Analyzer	1 hour ago	Unauthorized connection attempt from IP address 146.88.240.4 on Port 137(NETBIOS)	Port Scan