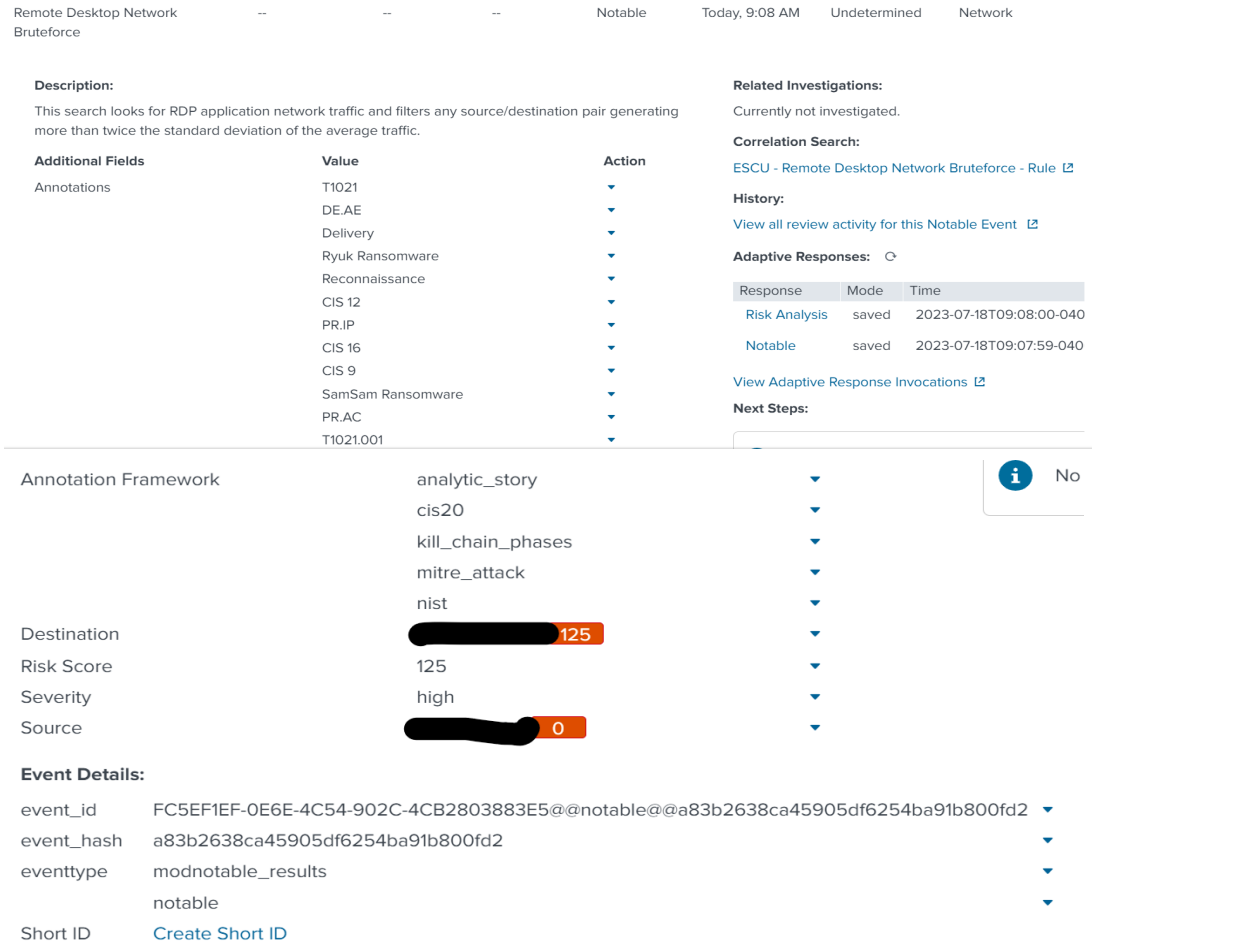
Splunk ES Investigation by Robert Russ

Splunk Alert (For security, there will be information blacked out to protect the environment)



----------**START OF TICKET**----------

Executive summary:

The detection occurred on July 18, 2023 at 9:08 AM. Splunk labeled the detection as Remote Desktop Network Bruteforce.

The rule that was triggered states this search looks for RDP application network traffic and filters any source/destination pair generating more than twice the standard of the average traffic.

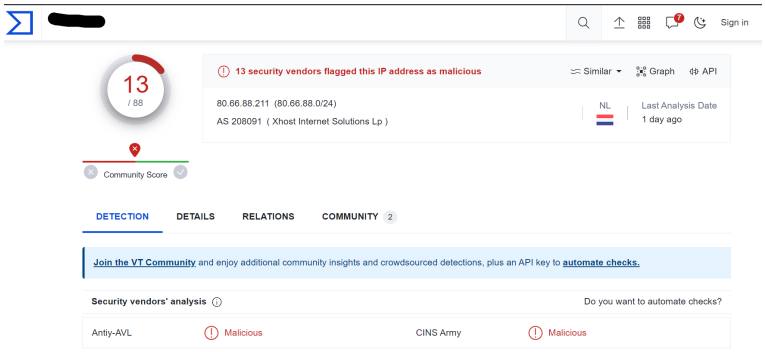
Through the investigation, it was determined the source IP address is malicious. I queried Splunk to check for previous activity to make sure the attacker was not successful in logging into an endpoint in the environment. The query displayed a table of the activity and revealed the firewall blocked the attacker from entering the enviornment.

IP(s):
The source IP is 80.xx.88.2xx and destination IP is the company's public IP address. A threat actor is attempting to bruteforce the network through RDP.

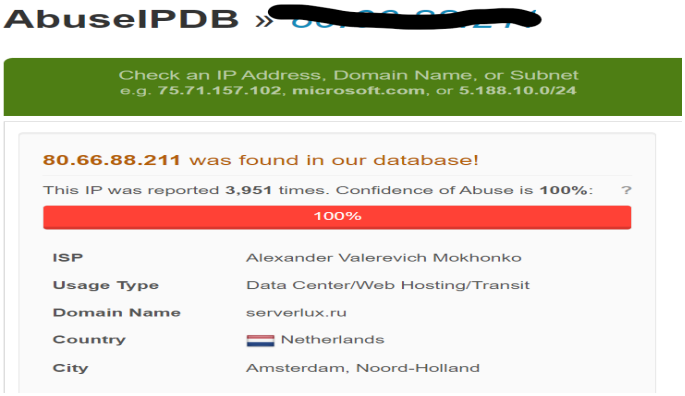
Port(s):
RDP Port 3389

IP Reputation:

Virus total:
- Risk score: 13/88 vendors flagged the source IP as malicious



AbuseIPDB:
- Risk score: 100% confidence of abuse



In the reports, people labeled the source IP address used for Bruteforce attack RDP server and port scanning.

Declaration:
The investigation lead to conclude this detection is a true positive non-issue or it is benign because the firewall blocked the traffic. There is not recommendation at this time.

----------END OF TICKET----------