

Splunk ES Investigation by Robert Russ

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

Remote Desktop Network
Bruteforce

--

--

--

Notable

Today, 9:08 AM

Undetermined

Network

Description:

This search looks for RDP application network traffic and filters any source/destination pair generating more than twice the standard deviation of the average traffic.

Additional Fields

Value	Action
Annotations	T1021
	DE.AE
	Delivery
	Ryuk Ransomware
	Reconnaissance
	CIS 12
	PR.IP
	CIS 16
	CIS 9
	SamSam Ransomware
	PR.AC
	T1021.001

Related Investigations:

Currently not investigated.

Correlation Search:

[ESCU - Remote Desktop Network Bruteforce - Rule](#)

History:

[View all review activity for this Notable Event](#)

Adaptive Responses:

Response	Mode	Time
Risk Analysis	saved	2023-07-18T09:08:00-040
Notable	saved	2023-07-18T09:07:59-040

[View Adaptive Response Invocations](#)

Next Steps:

Annotation Framework

analytic_story

cis20

kill_chain_phases

mitre_attack

nist

Destination

Risk Score

Severity

Source

125

125

high

0

No

Event Details:

event_id

FC5EF1EF-0E6E-4C54-902C-4CB2803883E5@@@notable@@@a83b2638ca45905df6254ba91b800fd2

event_hash

a83b2638ca45905df6254ba91b800fd2

eventtype

modnotable_results

notable

Short ID

[Create Short ID](#)

-----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 environment.

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.

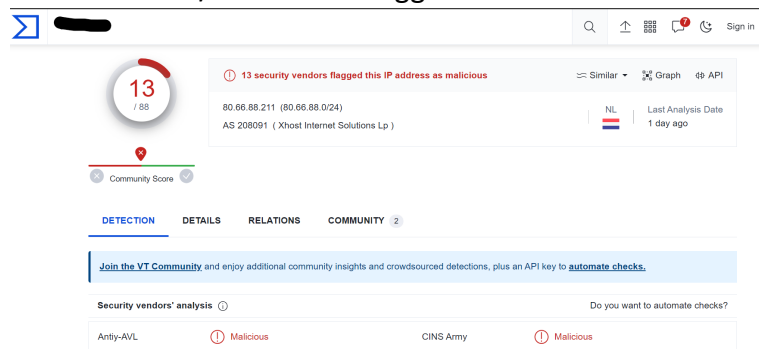
Port(s):

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

AbuseIPDB » 80.66.88.211



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-----

