Firewall: Permit From a Known Scanning IP: Theory & Playbook

What is a Scanning IP?

> "*Adversaries may perform different forms of active scanning depending on what information they seek to gather. These scans can also be performed in various ways, including using native features of network protocols such as ICMP.[1][2] Information from these scans may reveal opportunities for other forms of reconnaissance (ex: Search Open Websites/Domains or Search Open Technical Databases), establishing operational resources (ex: Develop Capabilities or Obtain Capabilities), and/or initial access (ex: External Remote Services or Exploit Public-Facing Application).*" – Active Scanning, MITRE
>
> Active Scanning, Technique T1595 - Enterprise | MITRE ATT&CK®

MITRE has categorized reconnaissance into three techniques:

- **Focused scanning of a public IP segments**, that may be allocated to and organization by a block, in this technique the attacker focuses on the IP's that belong to the organization, looking for **externally exposed services** such as websites, databases or external remote services.
  See T1595.001.

  It can also assist you to be familiar with two associated terminologies, known as | VERTICAL SCANNING | and -HORIZONTAL SCANNING- .

  Vertical Scanning refers to a single IP being scanned for multiple ports, that might reveal an open service on one of the ports.

  Horizontal Scanning refers to a scan against a group of IPs for a single port, mostly to discover if an endpoint is running a specific service associated with the port.

- **Vulnerability Scanning** refers to obtaining information about existence of a known vulnerability on an exposed service, this is mostly done by obtaining the name and version of an exposed service through server banners or other network artifacts (for instance, see Wappalyzer), and correlating them to a CVE database.
  See T1595.002.
- **Wordlist Scanning** refers to probing the infrastructure using a focused bruteforce dictionary, against, for example a sub-domain name, or website directories (See DirBuster), in order to identify the existence of some content, and it's availability to the attacker.
  See T1595.003.

What Is A Firewall Permit?

Most packets that are sent towards and endpoint on non operating port are blocked, but if there is a service running on some IP address, let's say a Website on IP 216.58.212.206, on port 443. We will receive a firewall permit, and the endpoint will try to establish an HTTPS session.

Receiving a firewall permit by a known scanning IP is the way the scanning IP achieves service discovery.

What IP is considered a Scanning IP?

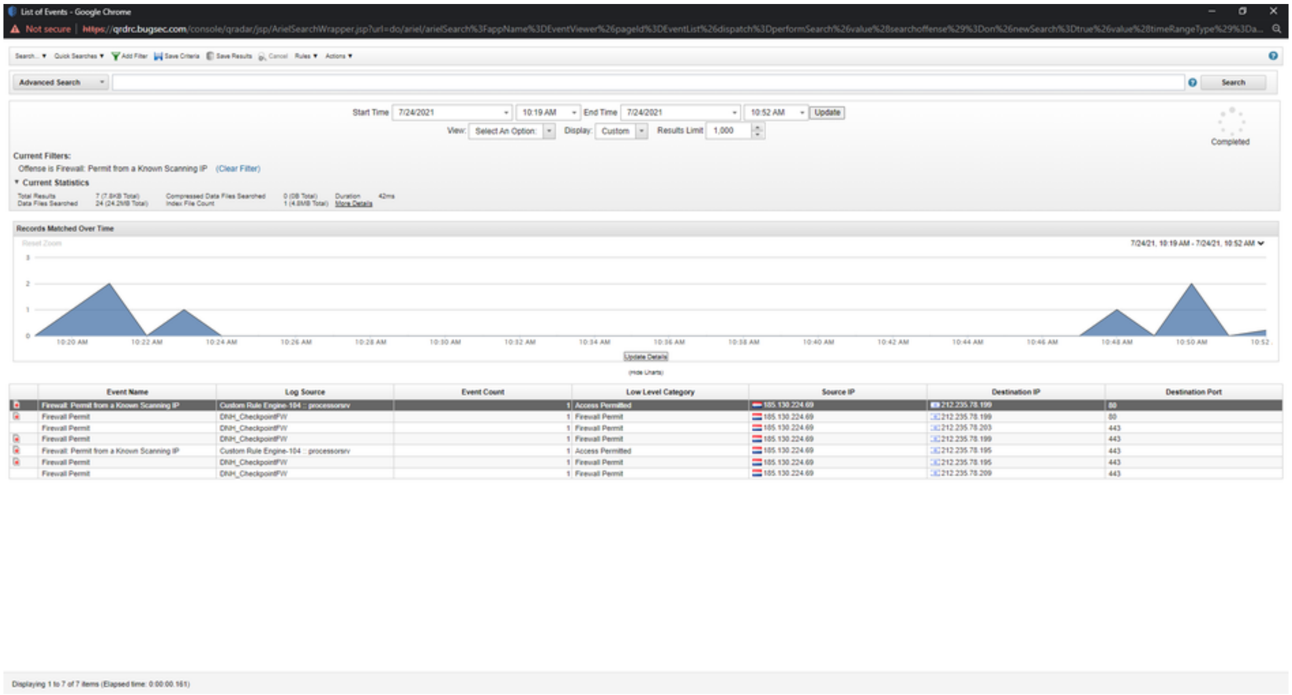
QRadar default ruleset reports a ***"Permit from a Known Scanning IP",*** if it Detects more than 1000 firewall deny attempts from a single source to a single destination with 1 firewall permit within 5 minutes.

No “False Positive”s

Nobody normally normally try connect and be denied 1000 times in 5 minutes

The First Step of Investigation: IBM QRadar SIEM Analysis (Example)

Let us observe the event list associated with an “Firewall: Permit from a known scanning IP”:


List of Events - Google Chrome
Not secure
https://qrdrc.bugsec.com/console/qradar/jsp/ArielSearchWrapper.jsp?url=do/ariel/arielSearch%3FappName%3DEventViewer%26pageId%3DEventList%26dispatch%3DperformSearch%26value%28searchoffense%29%3Don%26newSearch%3Dtrue%26value%28timeRangeType%29%3Da...
Search...
Quick Searches
Add Filter
Save Criteria
Save Results
Cancel
Rules
Actions
Advanced Search
Search
Update
Completed
Records Matched Over Time
Reset Zoom
7/24/21, 10:19 AM - 7/24/21, 10:52 AM
3
2
1
0
10:20 AM
10:22 AM
10:24 AM
10:26 AM
10:28 AM
10:30 AM
10:32 AM
10:34 AM
10:36 AM
10:38 AM
10:40 AM
10:42 AM
10:44 AM
10:46 AM
10:48 AM
10:50 AM
10:52
Update Details
(Hide Charts)

Start Time 7/24/2021 10:19 AM End Time 7/24/2021 10:52 AM

View: Select An Option: Display: Custom Results Limit 1,000

Current Filters:

Offense is Firewall: Permit from a Known Scanning IP (Clear Filter)

Current Statistics

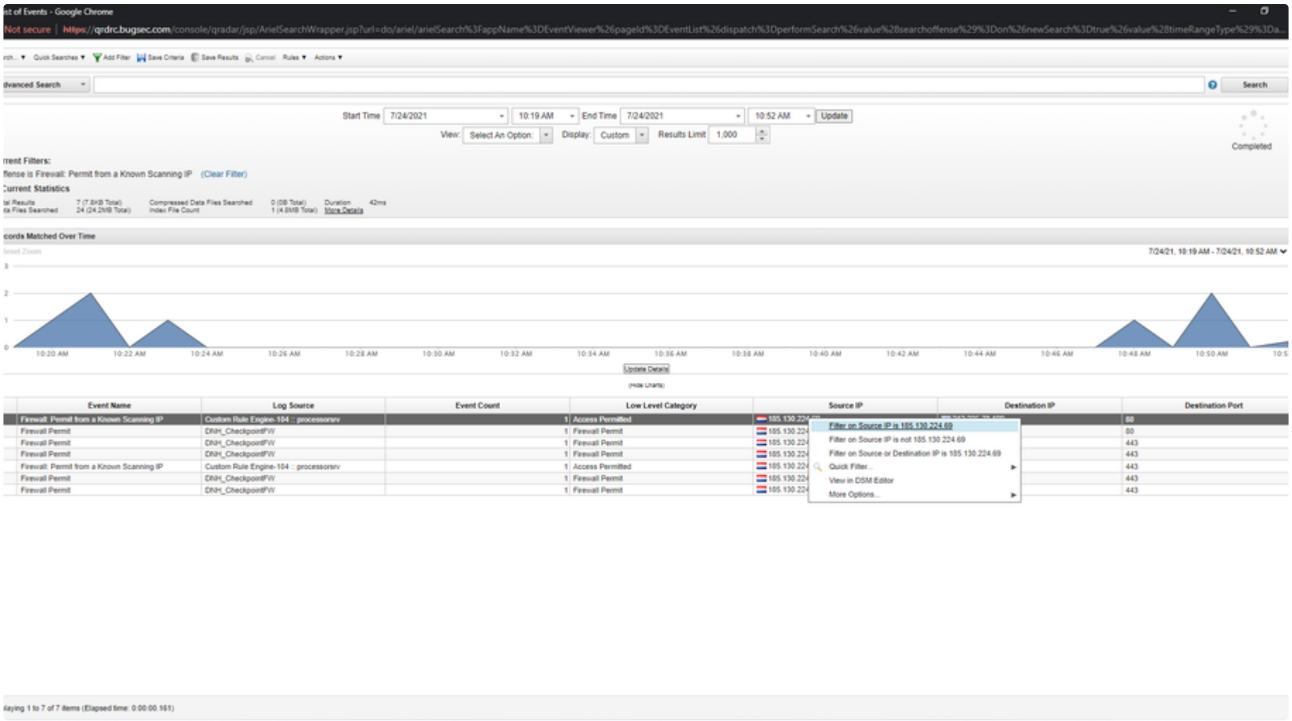
Total Results	7 (7.8KB Total)	Compressed Data Files Searched	0 (0B Total)	Duration	42ms
Data Files Searched	24 (24.2MB Total)	Index File Count	1 (4.8MB Total)	More Details	

Event Name	Log Source	Event Count	Low Level Category	Source IP	Destination IP	Destination Port
Firewall: Permit from a Known Scanning IP	Custom Rule Engine-104 :: processorsrv	1	Access Permitted	185.130.224.69	212.235.78.199	80
Firewall Permit	DNH_CheckpointFW	1	Firewall Permit	185.130.224.69	212.235.78.199	80
Firewall Permit	DNH_CheckpointFW	1	Firewall Permit	185.130.224.69	212.235.78.203	443
Firewall Permit	DNH_CheckpointFW	1	Firewall Permit	185.130.224.69	212.235.78.199	443
Firewall: Permit from a Known Scanning IP	Custom Rule Engine-104 :: processorsrv	1	Access Permitted	185.130.224.69	212.235.78.195	443
Firewall Permit	DNH_CheckpointFW	1	Firewall Permit	185.130.224.69	212.235.78.195	443
Firewall Permit	DNH_CheckpointFW	1	Firewall Permit	185.130.224.69	212.235.78.209	443

Displaying 1 to 7 of 7 items (Elapsed time: 0:00:00.161)

Once we open the event list in the offense in QRadar we can see that three addresses got firewall permits on two ports, but what was the nature of the scan?

Let’s filter on the source IP:



ist of Events - Google Chrome

Not secure | https://qrdrc.bugsec.com/console/qradar/jsp/ArielSearchWrapper.jsp?url=do/ariel/arielSearch%3FappName%3DEventViewer%26pageId%3DEventList%26dispatch%3DperformSearch%26value%28searchoffense%29%3Don%26newSearch%3Dtrue%26value%28timeRangeType%29%3Da...

rch... ▼ Quick Searches ▼ Add Filter Save Criteria Save Results Cancel Rules ▼ Actions ▼
dvanced Search
Search
Completed

Start Time 7/24/2021 10:19 AM End Time 7/24/2021 10:52 AM Update

View: Select An Option: Display: Custom Results Limit 1,000

rrent Filters:

ffense is Firewall: Permit from a Known Scanning IP (Clear Filter)

Current Statistics

tal Results	7 (7.8KB Total)	Compressed Data Files Searched	0 (0B Total)	Duration	42ms
ta Files Searched	24 (24.2MB Total)	Index File Count	1 (4.8MB Total)	More Details	

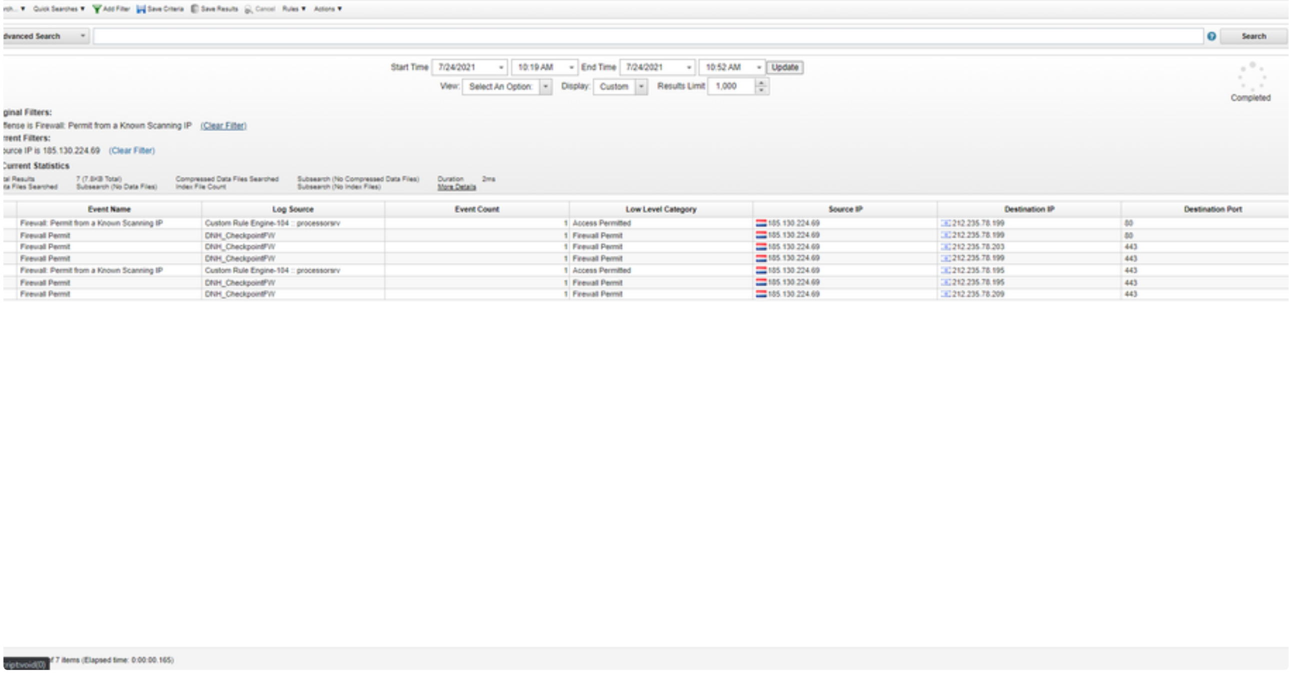
cords Matched Over Time

Event Name	Log Source	Event Count	Low Level Category	Source IP	Destination IP	Destination Port
Firewall: Permit from a Known Scanning IP	Custom Rule Engine-104 :: processorsrv	1	Access Permitted	185.130.224		80
Firewall Permit	DNH_CheckpointFW	1	Firewall Permit	185.130.224		80
Firewall Permit	DNH_CheckpointFW	1	Firewall Permit	185.130.224		443
Firewall Permit	DNH_CheckpointFW	1	Firewall Permit	185.130.224		443
Firewall: Permit from a Known Scanning IP	Custom Rule Engine-104 :: processorsrv	1	Access Permitted	185.130.224		443
Firewall Permit	DNH_CheckpointFW	1	Firewall Permit	185.130.224		443
Firewall Permit	DNH_CheckpointFW	1	Firewall Permit	185.130.224		443

Filter on Source IP is 185.130.224.69
Filter on Source IP is not 185.130.224.69
Filter on Source or Destination IP is 185.130.224.69
Quick Filter...
View in DSM Editor
More Options...

laying 1 to 7 of 7 items (Elapsed time: 0:00:00.161)

And clear “Offense is Firewall: Permit from a Known Scanning IP” Filter:



rch... ▼ Quick Searches ▼ Add Filter Save Criteria Save Results Cancel Rules ▼ Actions ▼
dvanced Search
Search
Completed

Start Time 7/24/2021 10:19 AM End Time 7/24/2021 10:52 AM Update

View: Select An Option: Display: Custom Results Limit 1,000

ginal Filters:

ffense is Firewall: Permit from a Known Scanning IP (Clear Filter)

rrent Filters:

ource IP is 185.130.224.69 (Clear Filter)

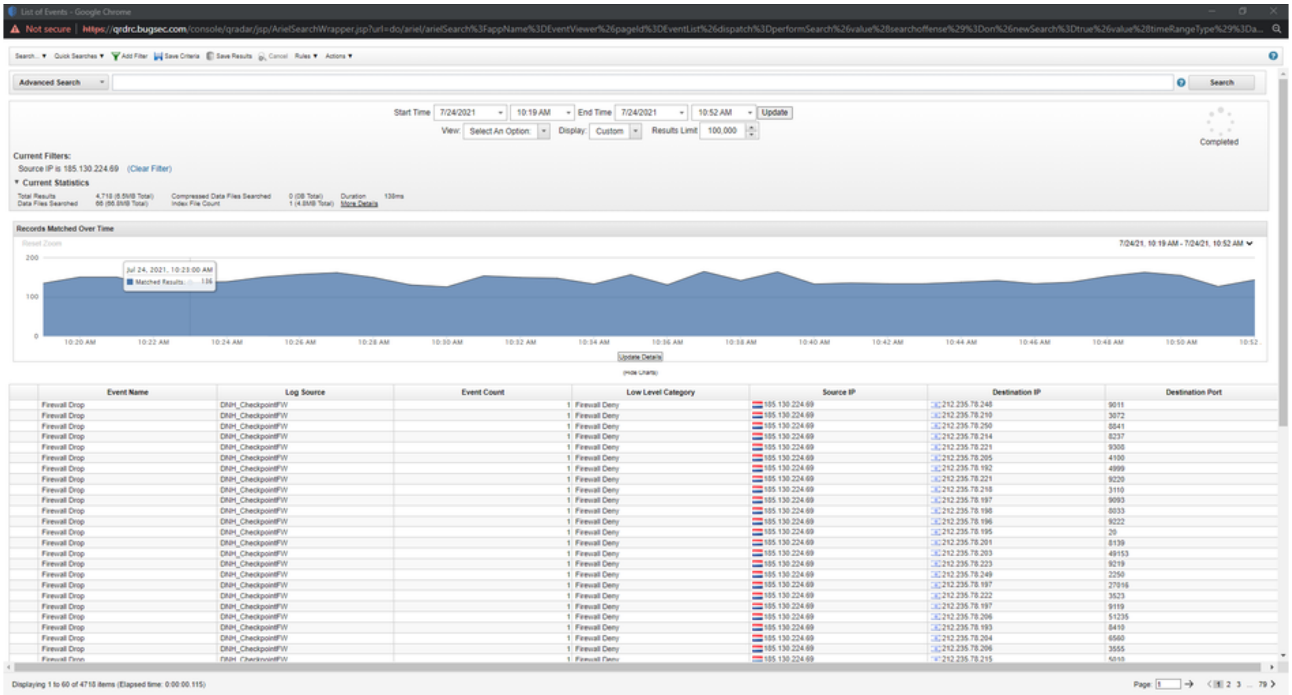
Current Statistics

tal Results	7 (7.8KB Total)	Compressed Data Files Searched	Subsearch (No Compressed Data Files)	Duration	2ms
ta Files Searched	Subsearch (No Data Files)	Index File Count	Subsearch (No Index Files)	More Details	

Event Name	Log Source	Event Count	Low Level Category	Source IP	Destination IP	Destination Port
Firewall: Permit from a Known Scanning IP	Custom Rule Engine-104 :: processorsrv	1	Access Permitted	185.130.224.69	212.235.78.199	80
Firewall Permit	DNH_CheckpointFW	1	Firewall Permit	185.130.224.69	212.235.78.199	80
Firewall Permit	DNH_CheckpointFW	1	Firewall Permit	185.130.224.69	212.235.78.203	443
Firewall Permit	DNH_CheckpointFW	1	Firewall Permit	185.130.224.69	212.235.78.199	443
Firewall: Permit from a Known Scanning IP	Custom Rule Engine-104 :: processorsrv	1	Access Permitted	185.130.224.69	212.235.78.195	443
Firewall Permit	DNH_CheckpointFW	1	Firewall Permit	185.130.224.69	212.235.78.195	443
Firewall Permit	DNH_CheckpointFW	1	Firewall Permit	185.130.224.69	212.235.78.209	443

riptvoid(0) f 7 items (Elapsed time: 0:00:00.165)

Now we can see 4718 events that indicate that there was a scanning process:


List of Events - Google Chrome
Not secure | https://qrdrc.bugsec.com/console/qradar/jsp/ArielSearchWrapper.jsp?url=do/ariel/arielSearch%3FappName%3DEventViewer%26pageId%3DEventList%26dispatch%3DperformSearch%26value%28searchoffense%29%3Don%26newSearch%3Dtrue%26value%28timeRangeType%29%3Da...
Search... ▾
Quick Searches ▾
Add Filter
Save Criteria
Save Results
Cancel
Rules ▾
Actions ▾
Advanced Search
Search
Update
Completed
Records Matched Over Time
Reset Zoom
7/24/21, 10:19 AM - 7/24/21, 10:52 AM
200
100
0
Jul 24, 2021, 10:23:00 AM
Matched Results: 136
10:20 AM
10:22 AM
10:24 AM
10:26 AM
10:28 AM
10:30 AM
10:32 AM
10:34 AM
10:36 AM
10:38 AM
10:40 AM
10:42 AM
10:44 AM
10:46 AM
10:48 AM
10:50 AM
10:52
Update Details
(Hide Charts)

Start Time 7/24/2021 10:19 AM End Time 7/24/2021 10:52 AM

View: Select An Option: Display: Custom Results Limit 100,000

Current Filters:

Source IP is 185.130.224.69 (Clear Filter)

▾ Current Statistics

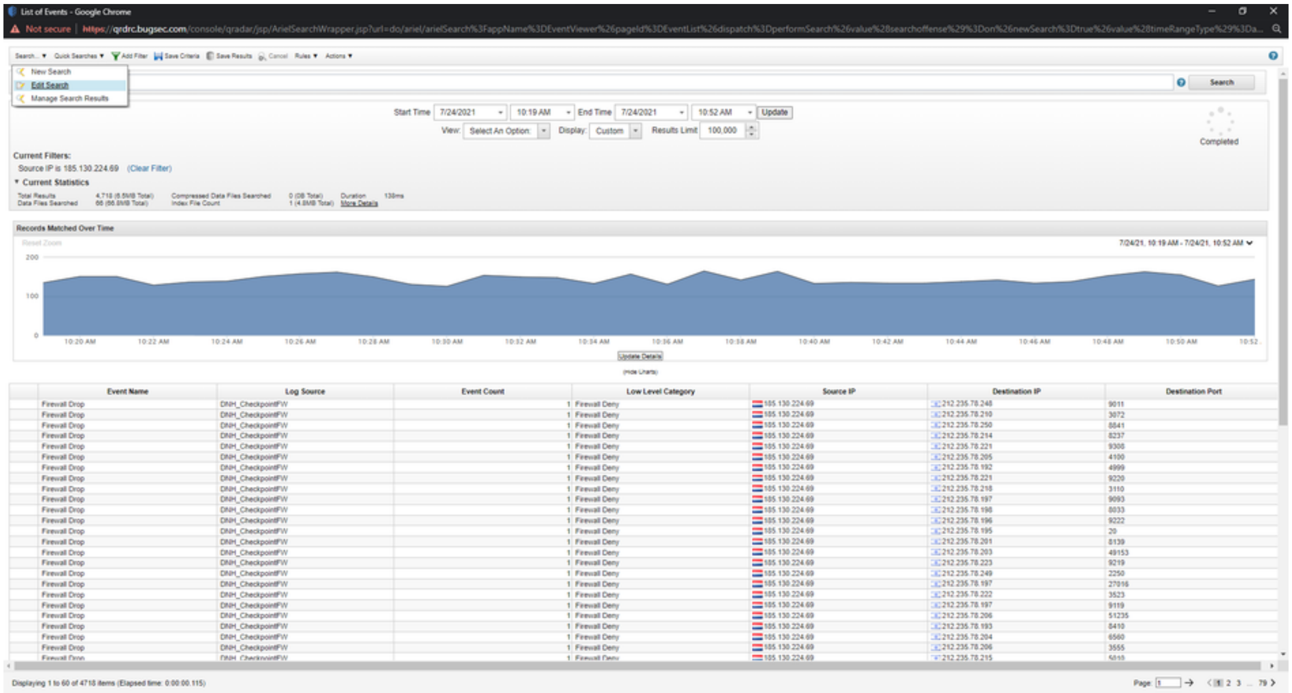
Total Results	4,718 (6.5MB Total)	Compressed Data Files Searched	0 (0B Total)	Duration	139ms
Data Files Searched	66 (66.8MB Total)	Index File Count	1 (4.8MB Total)	More Details	

Event Name	Log Source	Event Count	Low Level Category	Source IP	Destination IP	Destination Port
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.248	9011
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.210	3072
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.250	8841
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.214	8237
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.221	9308
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.205	4100
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.192	4999
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.221	9220
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.218	3110
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.197	9093
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.198	8033
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.196	9222
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.195	20
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.201	8139
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.203	49153
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.223	9219
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.249	2250
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.197	27016
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.222	3523
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.197	9119
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.206	51235
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.193	8410
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.204	6560
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.206	3555
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.215	5010

Displaying 1 to 60 of 4718 items (Elapsed time: 0:00:00.115)

Page: 1 → ‹ 1 2 3 ... 79 ›

We can see that the destination IP’s repeat themselves. We can edit the search:



List of Events - Google Chrome

Not secure | https://qrdrc.bugsec.com/console/qradar/jsp/ArielSearchWrapper.jsp?url=do/ariel/arielSearch%3FappName%3DEventViewer%26pageId%3DEventList%26dispatch%3DperformSearch%26value%28searchoffense%29%3Don%26newSearch%3Dtrue%26value%28timeRangeType%29%3Da...

Start Time 7/24/2021 10:19 AM End Time 7/24/2021 10:52 AM

View: Select An Option: Display: Custom Results Limit 100,000

Current Filters:

Source IP is 185.130.224.69 (Clear Filter)

▾ Current Statistics

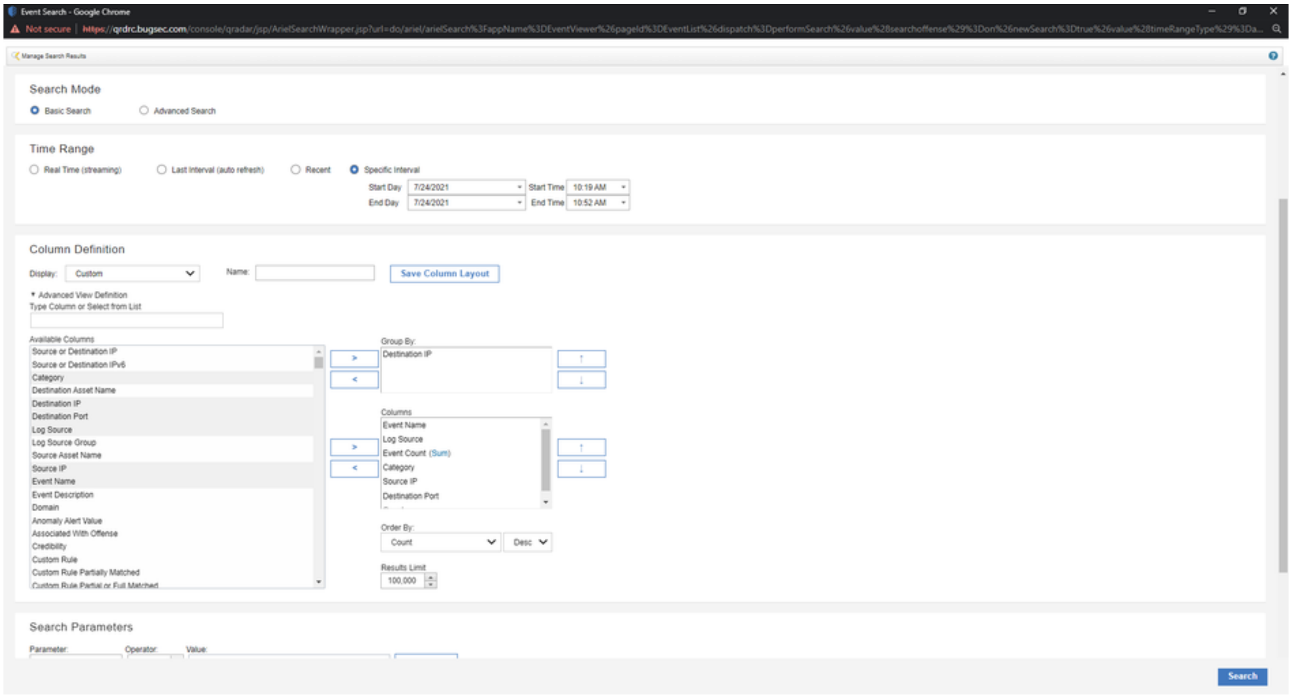
Total Results	4,718 (6.5MB Total)	Compressed Data Files Searched	0 (0B Total)	Duration	139ms
Data Files Searched	66 (66.8MB Total)	Index File Count	1 (4.8MB Total)	More Details	

Event Name	Log Source	Event Count	Low Level Category	Source IP	Destination IP	Destination Port
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.248	9011
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.210	3072
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.250	8841
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.214	8237
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.221	9308
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.205	4100
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.192	4999
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.221	9220
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.218	3110
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.197	9093
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.198	8033
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.196	9222
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.195	20
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.201	8139
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.203	49153
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.223	9219
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.249	2250
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.197	27016
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.222	3523
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.197	9119
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.206	51235
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.193	8410
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.204	6560
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.206	3555
Firewall Drop	DNH_CheckpointFW	1	Firewall Deny	185.130.224.69	212.235.78.215	5010

Displaying 1 to 60 of 4718 items (Elapsed time: 0:00:00.115)

Page: 1 → ‹ 1 2 3 ... 79 ›

And choose to group by Destination IP, by removing it from the “Column” list and adding it to the “Group By” list:


Event Search - Google Chrome
Not secure | https://qrdrc.bugsec.com/console/qradar/jsp/ArielSearchWrapper.jsp?url=do/ariel/arielSearch%3FappName%3DEventViewer%26pageId%3DEventList%26dispatch%3DperformSearch%26value%28searchOffense%29%3Don%26newSearch%3Dtrue%26value%28timeRangeType%29%3Da...
Manage Search Results
Save Column Layout
Search

Search Mode

● Basic Search ○ Advanced Search

Time Range

○ Real Time (streaming) ○ Last Interval (auto refresh) ○ Recent ● Specific Interval

Start Day: 7/24/2021 Start Time: 10:19 AM

End Day: 7/24/2021 End Time: 10:52 AM

Column Definition

Display: Custom Name:

▾ Advanced View Definition

Type Column or Select from List

Available Columns: Source or Destination IP, Source or Destination IPv6, Category, Destination Asset Name, Destination IP, Destination Port, Log Source, Log Source Group, Source Asset Name, Source IP, Event Name, Event Description, Domain, Anomaly Alert Value, Associated With Offense, Credibility, Custom Rule, Custom Rule Partially Matched, Custom Rule Partial or Full Matched

Group By: Destination IP

Columns: Event Name, Log Source, Event Count (Sum), Category, Source IP, Destination Port

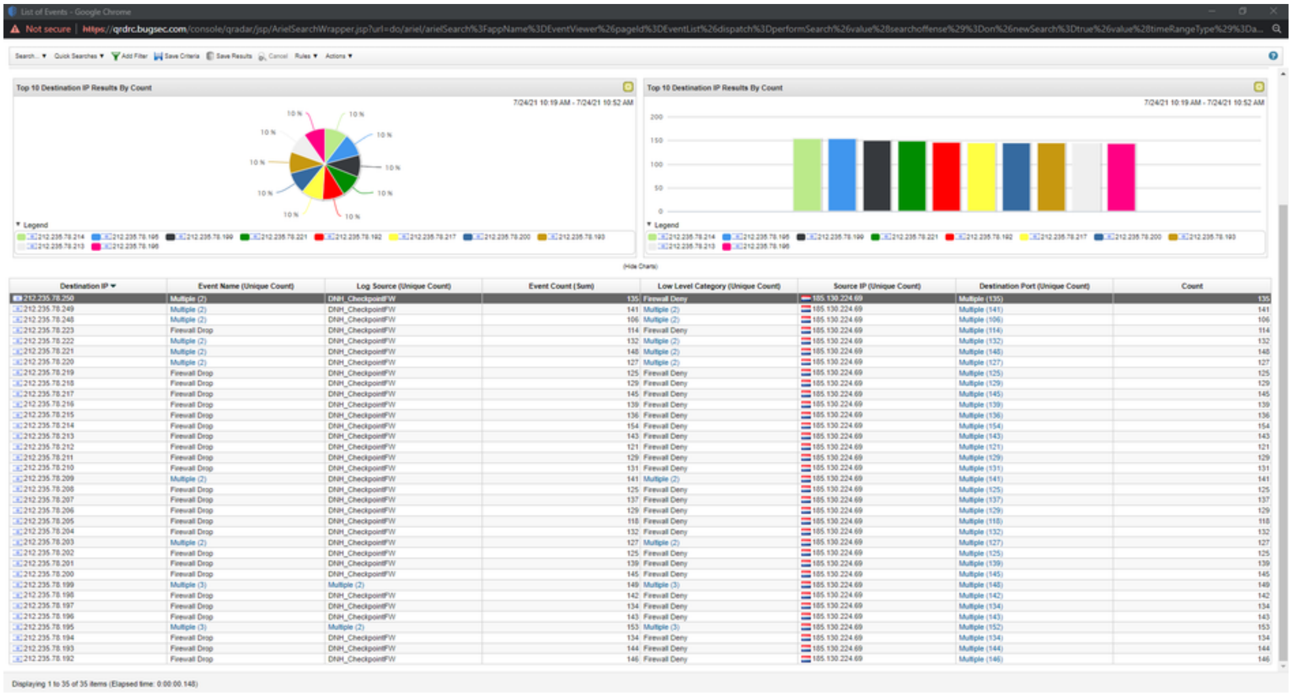
Order By: Count Desc

Results Limit: 100,000

Search Parameters

Parameter: Operator: Value:

Finally we can sortlist by the “Destination IP” column:


List of Events - Google Chrome
Not secure | https://qrdrc.bugsec.com/console/qradar/jsp/ArielSearchWrapper.jsp?url=do/ariel/arielSearch%3FappName%3DEventViewer%26pageId%3DEventList%26dispatch%3DperformSearch%26value%28searchOffense%29%3Don%26newSearch%3Dtrue%26value%28timeRangeType%29%3Da...
Search... ▾ Quick Searches ▾ Add Filter Save Criteria Save Results Cancel Rules ▾ Actions ▾
Top 10 Destination IP Results By Count
7/24/21 10:19 AM - 7/24/21 10:52 AM
10 %
10 %
10 %
10 %
10 %
10 %
10 %
10 %
10 %
10 %
Top 10 Destination IP Results By Count
7/24/21 10:19 AM - 7/24/21 10:52 AM
200
150
100
50
0
▾ Legend
212.235.78.214
212.235.78.195
212.235.78.199
212.235.78.221
212.235.78.192
212.235.78.217
212.235.78.200
212.235.78.193
212.235.78.213
212.235.78.196
(Hide Charts)

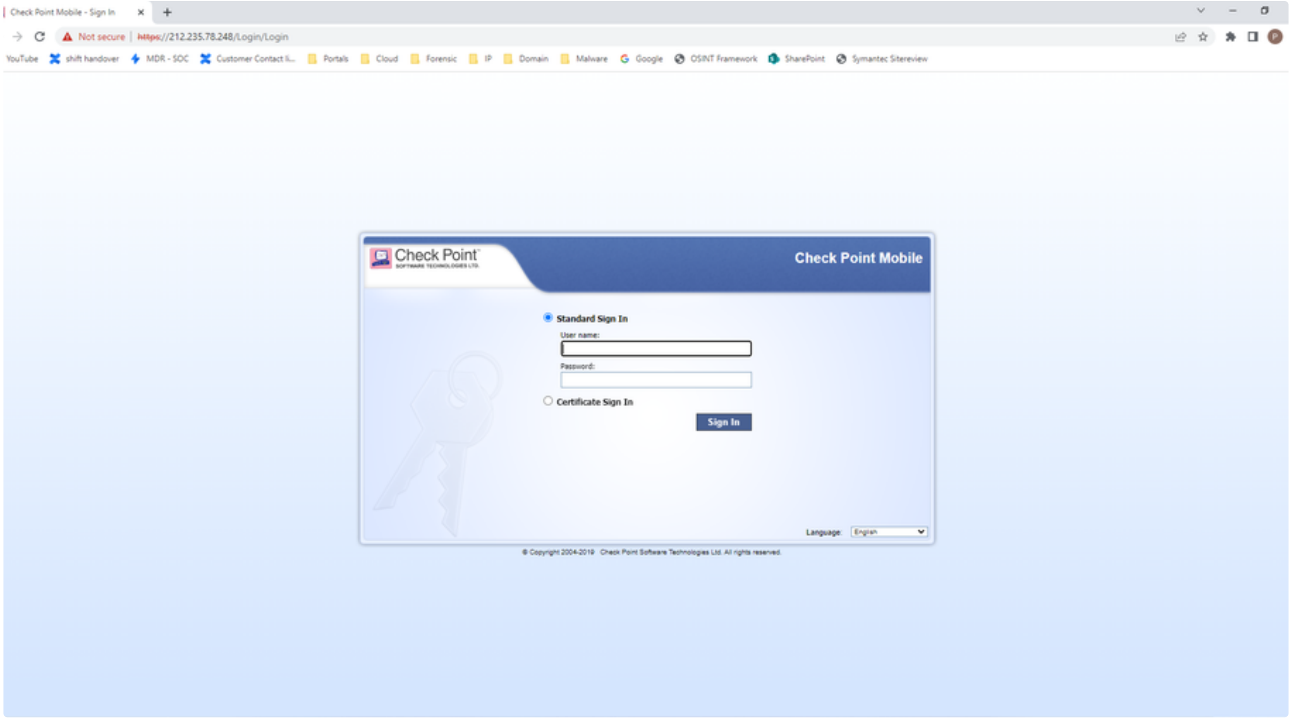
Destination IP ▾	Event Name (Unique Count)	Log Source (Unique Count)	Event Count (Sum)	Low Level Category (Unique Count)	Source IP (Unique Count)	Destination Port (Unique Count)	Count
212.235.78.250	Multiple (2)	DNH_CheckpointFW	135	Firewall Deny	185.130.224.69	Multiple (135)	135
212.235.78.249	Multiple (2)	DNH_CheckpointFW	141	Multiple (2)	185.130.224.69	Multiple (141)	141
212.235.78.248	Multiple (2)	DNH_CheckpointFW	106	Multiple (2)	185.130.224.69	Multiple (106)	106
212.235.78.223	Firewall Drop	DNH_CheckpointFW	114	Firewall Deny	185.130.224.69	Multiple (114)	114
212.235.78.222	Multiple (2)	DNH_CheckpointFW	132	Multiple (2)	185.130.224.69	Multiple (132)	132
212.235.78.221	Multiple (2)	DNH_CheckpointFW	148	Multiple (2)	185.130.224.69	Multiple (148)	148
212.235.78.220	Multiple (2)	DNH_CheckpointFW	127	Multiple (2)	185.130.224.69	Multiple (127)	127
212.235.78.219	Firewall Drop	DNH_CheckpointFW	125	Firewall Deny	185.130.224.69	Multiple (125)	125
212.235.78.218	Firewall Drop	DNH_CheckpointFW	129	Firewall Deny	185.130.224.69	Multiple (129)	129
212.235.78.217	Firewall Drop	DNH_CheckpointFW	145	Firewall Deny	185.130.224.69	Multiple (145)	145
212.235.78.216	Firewall Drop	DNH_CheckpointFW	139	Firewall Deny	185.130.224.69	Multiple (139)	139
212.235.78.215	Firewall Drop	DNH_CheckpointFW	136	Firewall Deny	185.130.224.69	Multiple (136)	136
212.235.78.214	Firewall Drop	DNH_CheckpointFW	154	Firewall Deny	185.130.224.69	Multiple (154)	154
212.235.78.213	Firewall Drop	DNH_CheckpointFW	143	Firewall Deny	185.130.224.69	Multiple (143)	143
212.235.78.212	Firewall Drop	DNH_CheckpointFW	121	Firewall Deny	185.130.224.69	Multiple (121)	121
212.235.78.211	Firewall Drop	DNH_CheckpointFW	129	Firewall Deny	185.130.224.69	Multiple (129)	129
212.235.78.210	Firewall Drop	DNH_CheckpointFW	131	Firewall Deny	185.130.224.69	Multiple (131)	131
212.235.78.209	Multiple (2)	DNH_CheckpointFW	141	Multiple (2)	185.130.224.69	Multiple (141)	141
212.235.78.208	Firewall Drop	DNH_CheckpointFW	125	Firewall Deny	185.130.224.69	Multiple (125)	125
212.235.78.207	Firewall Drop	DNH_CheckpointFW	137	Firewall Deny	185.130.224.69	Multiple (137)	137
212.235.78.206	Firewall Drop	DNH_CheckpointFW	129	Firewall Deny	185.130.224.69	Multiple (129)	129
212.235.78.205	Firewall Drop	DNH_CheckpointFW	118	Firewall Deny	185.130.224.69	Multiple (118)	118
212.235.78.204	Firewall Drop	DNH_CheckpointFW	132	Firewall Deny	185.130.224.69	Multiple (132)	132
212.235.78.203	Multiple (2)	DNH_CheckpointFW	127	Multiple (2)	185.130.224.69	Multiple (127)	127
212.235.78.202	Firewall Drop	DNH_CheckpointFW	125	Firewall Deny	185.130.224.69	Multiple (125)	125
212.235.78.201	Firewall Drop	DNH_CheckpointFW	139	Firewall Deny	185.130.224.69	Multiple (139)	139
212.235.78.200	Firewall Drop	DNH_CheckpointFW	145	Firewall Deny	185.130.224.69	Multiple (145)	145
212.235.78.199	Multiple (3)	Multiple (2)	149	Multiple (3)	185.130.224.69	Multiple (148)	149
212.235.78.198	Firewall Drop	DNH_CheckpointFW	142	Firewall Deny	185.130.224.69	Multiple (142)	142
212.235.78.197	Firewall Drop	DNH_CheckpointFW	134	Firewall Deny	185.130.224.69	Multiple (134)	134
212.235.78.196	Firewall Drop	DNH_CheckpointFW	143	Firewall Deny	185.130.224.69	Multiple (143)	143
212.235.78.195	Multiple (3)	Multiple (2)	153	Multiple (3)	185.130.224.69	Multiple (152)	153
212.235.78.194	Firewall Drop	DNH_CheckpointFW	134	Firewall Deny	185.130.224.69	Multiple (134)	134
212.235.78.193	Firewall Drop	DNH_CheckpointFW	144	Firewall Deny	185.130.224.69	Multiple (144)	144
212.235.78.192	Firewall Drop	DNH_CheckpointFW	146	Firewall Deny	185.130.224.69	Multiple (146)	146

Displaying 1 to 35 of 35 items (Elapsed time: 0:00:00.148)

We can see now that the segment 212.235.78.192-212.235.78.250 was vertically scanned for about ~140 different ports.

The only firewall permits we’ve got are for ports 80, 443 - indicating website discovery.

If we try to access https://212.235.78.248:443 IP, we will get comapany's checkpoint portal:

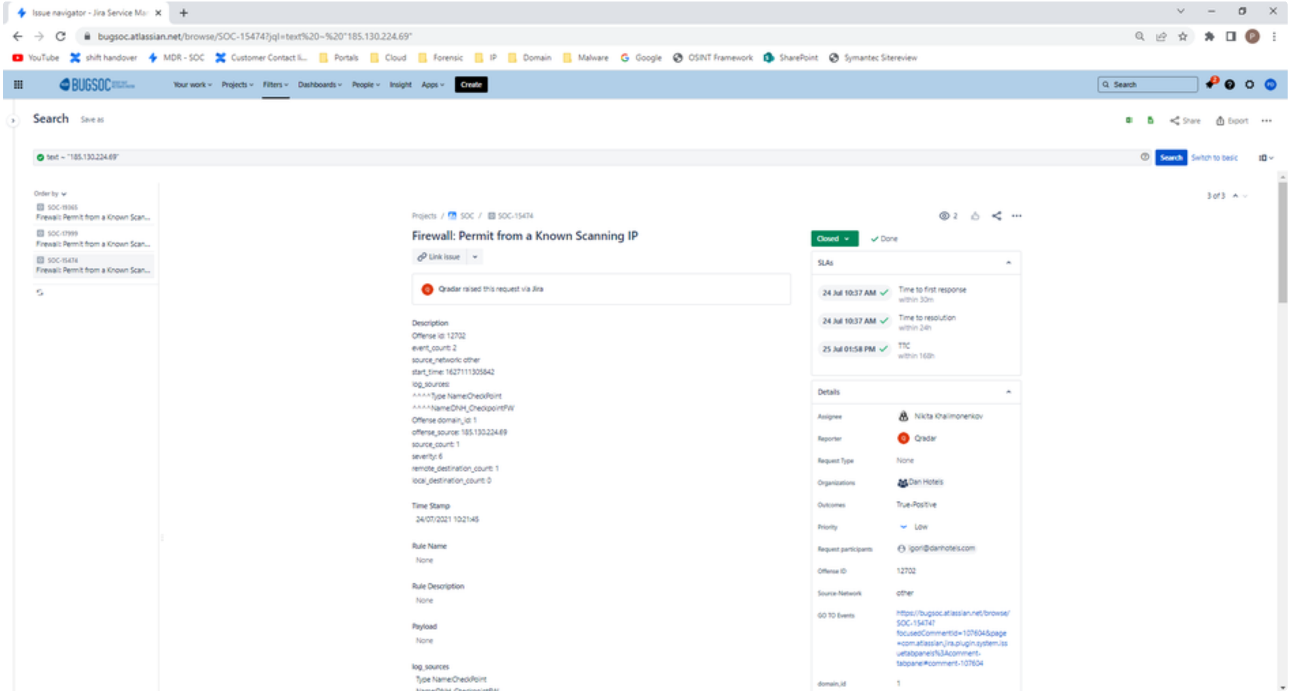


It is important to sort and organize the events in IBM QRadar, widening the timespan before the firewall permit to understand the following:

- Was there a specific segment of IP's that was scanned? Then the scan is vertical, was the attacker trying to reveal what services rely behind those endpoints? Are there known exploits on those services? Can the computer be attacked?
- Was there a specific list of ports against many IP's? What services use those ports? Was the attacker looking for exploits against specific services?

Step 2: Scanner IP Reputation - First JIRA, then Web

The next obvious step is to check the scanner IP reputation. But first let's search our database. Searching Jira for the scanner IP, reveals that it has scanned Dan Hotels, as well as SkyBox and Kali, and everyone ended up blocking it.



text ~ "185.130.224.69"

SOC-19365 Firewall: Permit from a Known Scan...
SOC-17999 Firewall: Permit from a Known Scan...
SOC-15474 Firewall: Permit from a Known Scan...

Projects / SOC / SOC-15474

Firewall: Permit from a Known Scanning IP

Qradar raised this request via Jira

Description
Offense id: 12702
event_count: 2
source_network: other
start_time: 1627111305842
log_sources:
^^^^Type Name:CheckPoint
^^^^Name:DNH_CheckpointFW
Offense domain_id: 1
offense_source: 185.130.224.69
source_count: 1
severity: 6
remote_destination_count: 1
local_destination_count: 0

Time Stamp
24/07/2021 10:21:45

Rule Name
None

Rule Description
None

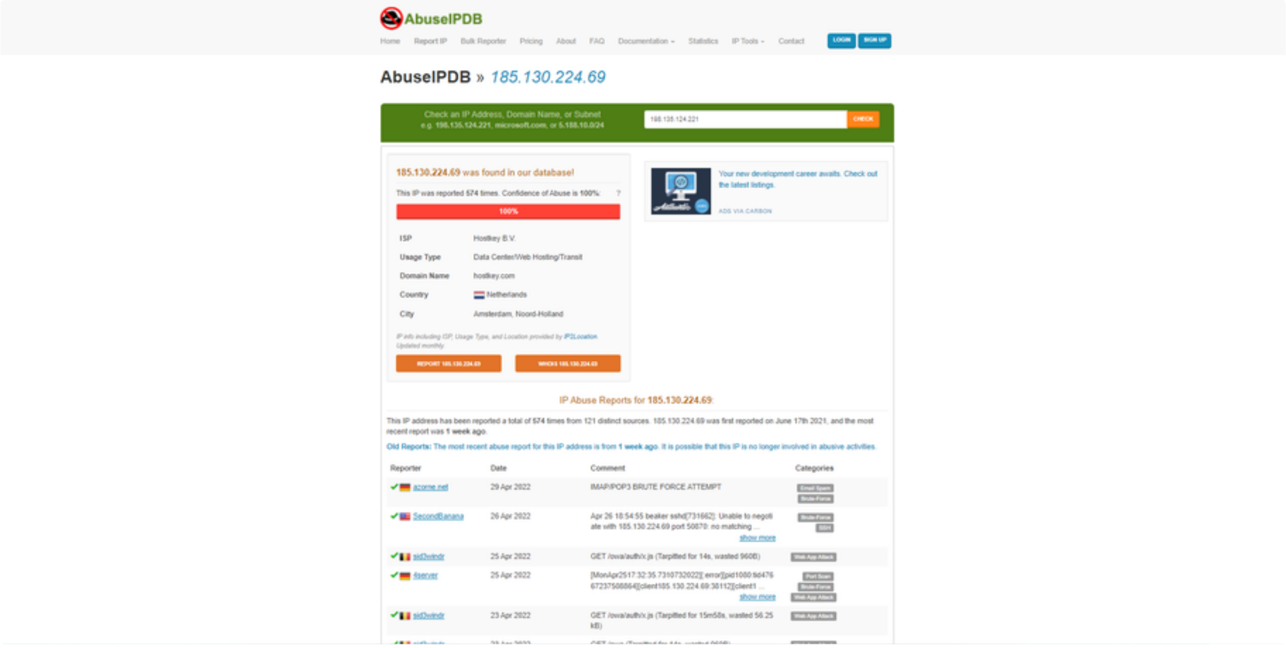
Payload
None

log_sources
Type Name:CheckPoint

24 Jul 10:37 AM ✓	Time to first response within 30m
24 Jul 10:37 AM ✓	Time to resolution within 24h
25 Jul 01:58 PM ✓	TTC within 168h

Assignee	Nikita Khalimonenkov
Reporter	Qradar
Request Type	None
Organizations	Dan Hotels
Outcomes	True-Positive
Priority	Low
Request participants	igori@danhotels.com
Offense ID	12702
Source-Network	other
GO TO Events	https://bugsoc.atlassian.net/browse/SOC-15474?focusedCommentId=107604&page=com.atlassian.jira.plugin.system.issuetabpanels%3Acomment-tabpanel#comment-107604
domain_id	1

After consulting Jira, we can go on the web, and find more evidence of IP’s suspected reputation, for example 185.130.224.69 | Hostkey B.V. | AbuseIPDB :



AbuseIPDB » 185.130.224.69

Check an IP Address, Domain Name, or Subnet
e.g. 198.135.124.221, microsoft.com, or 5.188.10.0/24

198.135.124.221

185.130.224.69 was found in our database!

This IP was reported 574 times. Confidence of Abuse is 100%:

ISP	Hostkey B.V.
Usage Type	Data Center/Web Hosting/Transit
Domain Name	hostkey.com
Country	Netherlands
City	Amsterdam, Noord-Holland

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

IP Abuse Reports for 185.130.224.69:

This IP address has been reported a total of 574 times from 121 distinct sources. 185.130.224.69 was first reported on June 17th 2021, and the most recent report was 1 week ago.

Old Reports: The most recent abuse report for this IP address is from 1 week ago. It is possible that this IP is no longer involved in abusive activities.

Reporter	Date	Comment	Categories
✓ azorne.net	29 Apr 2022	IMAP/POP3 BRUTE FORCE ATTEMPT	Email Spam Brute-Force
✓ SecondBanana	26 Apr 2022	Apr 26 18:54:55 beaker sshd[731662]: Unable to negotiate with 185.130.224.69 port 50870: no matching ... show more	Brute-Force SSH
✓ sid3windr	25 Apr 2022	GET /owa/auth/x.js (Tarpitted for 14s, wasted 960B)	Web App Attack
✓ 4server	25 Apr 2022	[MonApr2517:32:35.7310732022][:error][pid1080:tid47667237508864][client185.130.224.69:38112][client1 ... show more	Port Scan Brute-Force Web App Attack
✓ sid3windr	23 Apr 2022	GET /owa/auth/x.js (Tarpitted for 15m58s, wasted 56.25 kB)	Web App Attack

On AbuseIPDB - IP address abuse reports - Making the Internet safer, one IP at a time we can see the number of reports against this source, as well as community’s comments.

After this step we can already organize the data from QRadar regarding which addresses got permit, and bring supporting evidence to recommend and block the IP.

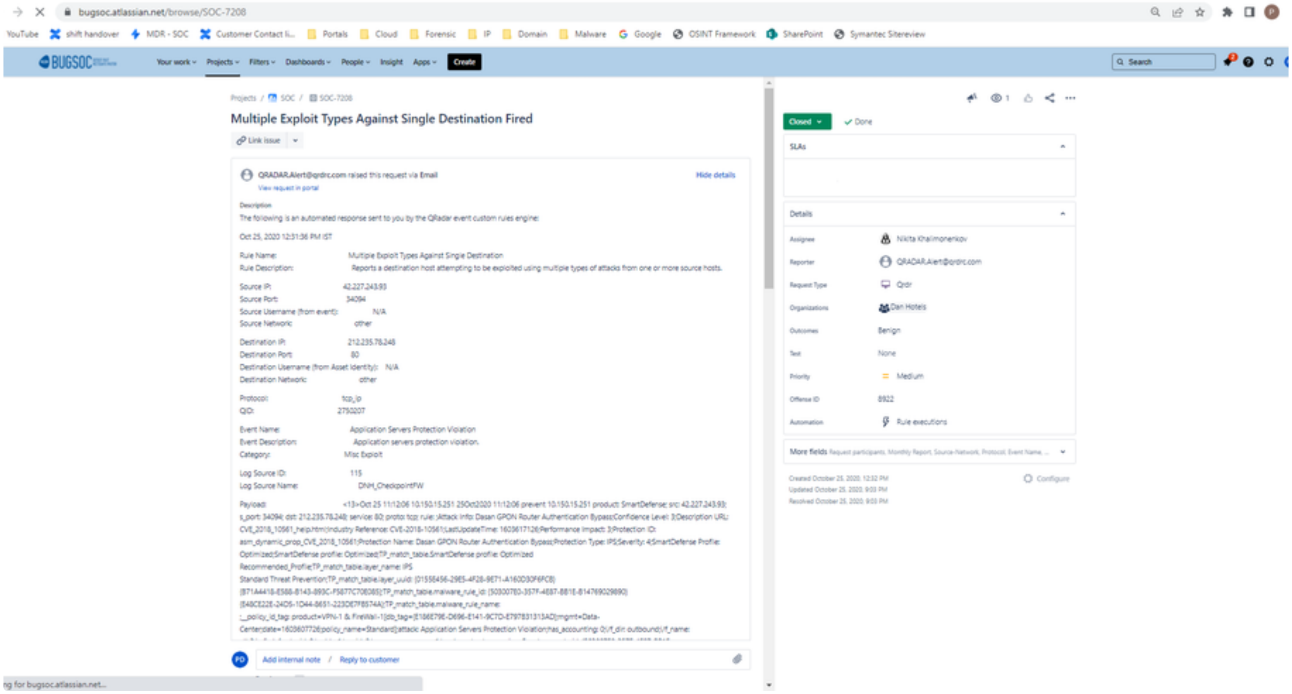
The Playbook: Recommended Investigation Steps

- Open the event list in IBM QRadar

- Remove the “User”, “Magnitude”, “Source Port” Columns from the advanced search, change the number of results to 100,000, and press “Search”
- Document all the permit destination IP’s and destination ports in the ticket
    - Search what services operate on each port
- If there is only one permitted Source IP, filter on It, else do the following instruction for each IP separately
- Widen the search to future time
- Clear the “Offense is Firewall: Permit from a Known Scanning IP” filter
- Try to use “Edit Search” to group by destination IPs or destination ports
- Feel free to do any other QRadar “magic” to try and figure out the nature of the scan
- Search Jira for the scanning IP(s)
- Search AbuseIPDB - IP address abuse reports - Making the Internet safer, one IP at a time, VirusTotal, IBM X-Force Exchange for IP’s reputation, and document it in the ticket.
- If you have access to clients EDR, search the scanning IP in it’s portal
- If possible, search the scanned IP’s that got permit in Jira to see if any attack was launched against the client in the time you did your investigation, see “Extra” below.

Extra: Let’s Search Jira for Scanned Addresses

If we search Jira for the CheckPoint’s Portal we can find a ticket reporting multiple Web Attack’s against the scanned address:



Multiple Exploit Types Against Single Destination Fired

QRADAR.Alert@qrdrc.com raised this request via Email

Description

The following is an automated response sent to you by the QRadar event custom rules engine:

Oct 25, 2020 12:31:36 PM IST

```
Rule Name:                 Multiple Exploit Types Against Single Destination
Rule Description:           Reports a destination host attempting to be exploited using multiple types of attacks from one or more source hosts.

Source IP:                42.227.243.93
Source Port:               34094
Source Username (from event):         N/A
Source Network:              other

Destination IP:              212.235.78.248
Destination Port:              80
Destination Username (from Asset Identity):   N/A
Destination Network:              other

Protocol:                 tcp_ip
QID:                    2750207

Event Name:                Application Servers Protection Violation
Event Description:           Application servers protection violation.
Category:                 Misc Exploit

Log Source ID:               115
Log Source Name:               DNH_CheckpointFW

Payload:                  <13>Oct 25 11:12:06 10.150.15.251 25Oct2020 11:12:06 prevent 10.150.15.251 product: SmartDefense; src: 42.227.243.93;
s_port: 34094; dst: 212.235.78.248; service: 80; proto: tcp; rule: ;Attack Info: Dasan GPON Router Authentication Bypass;Confidence Level: 3;Description URL:
CVE_2018_10561_help.htm;Industry Reference: CVE-2018-10561;LastUpdateTime: 1603617126;Performance Impact: 3;Protection ID:
asm_dynamic_prop_CVE_2018_10561;Protection Name: Dasan GPON Router Authentication Bypass;Protection Type: IPS;Severity: 4;SmartDefense Profile:
Optimized;SmartDefense profile: Optimized;TP_match_table.SmartDefense profile: Optimized
Recommended_Profile;TP_match_table.layer_name: IPS
Standard Threat Prevention;TP_match_table.layer_uuid: {01558456-29E5-4F28-9E71-A160D30F6FC8}
{B71A4418-E588-8143-893C-F5877C70E085};TP_match_table.malware_rule_id: {503007E0-357F-4E87-881E-814769029890}
{E48CE22E-24D5-1D44-8651-223DE7FB574A};TP_match_table.malware_rule_name:
;__policy_id_tag: product=VPN-1 & FireWall-1[db_tag={E186E79E-D696-E141-9C7D-E797B31313AD};mgmt=Data-
Center;date=1603607726;policy_name=Standard];attack: Application Servers Protection Violation;has_accounting: 0;i/f_dir: outbound;i/f_name:
```

Details

Assignee	Nikita Khalimonenkov
Reporter	QRADAR.Alert@qrdrc.com
Request Type	Qrdr
Organizations	Dan Hotels
Outcomes	Benign
Test	None
Priority	Medium
Offense ID	8922
Automation	Rule executions

More fields Request participants, Monthly Report, Source-Network, Protocol, Event Name, ...

Created October 25, 2020, 12:32 PM
Updated October 25, 2020, 9:03 PM
Resolved October 25, 2020, 9:03 PM

See: SOC-7208: Multiple Exploit Types Against Single Destination Fired CLOSED .