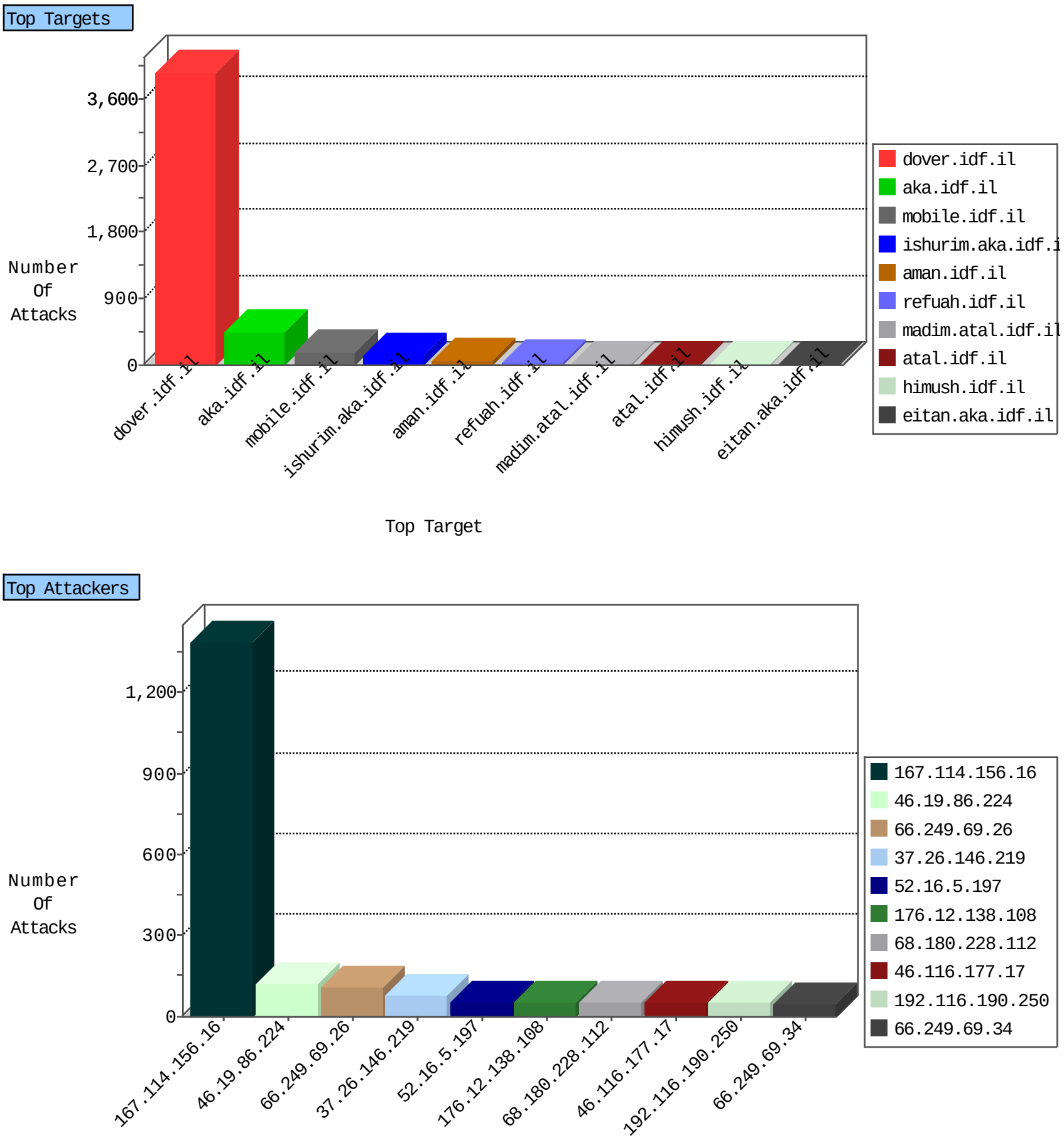
12-31-2015-15:04:05 to 12-31-2015-16:04:05

IDF Under Attack Daily Report



12-31-2015-15:04:05 to 12-31-2015-16:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3476
0.0.0.0		147.237.77.216	dover.idf.il	DOSS-SSL-ClearText	drop	3
173.195.0.22	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
173.195.0.21	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

12-31-2015-15:04:05 to 12-31-2015-16:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-31-2015-15:04:05 to 12-31-2015-16:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.113	147.237.0.34	Ukraine	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
80.178.136.74	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.64.177	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1
109.253.157.11	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
88.204.187.90	147.237.72.14	Kazakstan	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
80.82.64.177	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
5.28.152.169	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

12-31-2015-15:04:05 to 12-31-2015-16:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.224	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	123
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
213.57.134.92	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	35
176.13.19.109	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
213.55.107.230	Ethiopia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
5.22.129.126	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
109.253.213.204	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
109.253.199.54	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
2.54.144.199	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.183.68.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
213.57.131.247	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
46.19.85.245	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
213.57.131.247	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
80.246.137.165	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
54.241.198.78	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
5.102.254.254	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
66.249.64.163	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
94.230.86.185	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
5.102.254.18	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
80.178.100.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.198.164	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
109.253.211.141	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.139	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.81.65.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.232.21.105	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.121.89.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.196.163	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.17.178	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.170	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.196.163	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.17.178	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.146.219	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.229.39.193	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.220	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.32.87	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
67.55.90.132	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
213.57.131.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
37.26.148.193	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
176.13.18.206	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.12.91	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
207.232.21.105	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
37.26.148.194	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
85.64.118.41	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
94.230.86.165	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.57.139.82	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
213.8.122.115	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.69.26	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	108
37.26.146.219	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	67
52.16.5.197	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	55
176.12.138.108	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	54
68.180.228.112	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	50
46.116.177.17	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	50
192.116.190.250	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	50
66.249.69.34	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	44
176.12.138.10	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	42
66.249.69.42	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	41
46.19.86.105	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	38
149.78.51.52	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	36
212.179.21.194	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	36
157.55.39.227	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	34
80.246.136.222	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	30
5.102.213.212	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	30
5.22.130.171	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	30
80.246.136.92	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	30
176.106.41.125	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	30
176.13.18.181	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	30
109.253.218.146	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	26
185.32.179.72	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	25
46.19.86.97	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	24
176.13.18.221	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	24
46.19.86.81	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	24
176.13.3.154	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	23
50.87.144.145	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	22
212.235.98.139	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	21
91.208.139.250	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	20
192.249.66.247	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	20
79.183.104.150	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	18
176.13.10.119	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	18
85.64.22.207	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	18
31.168.192.251	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	18
109.253.144.42	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	18
109.253.196.172	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	16
192.115.130.253	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	16
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	15
176.13.13.220	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	14
193.43.246.250	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	14
37.142.254.97	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	14
109.253.202.186	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	12
149.88.117.64	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	12
37.26.149.156	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	12
2.54.13.159	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	12
149.88.168.7	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	12
185.120.125.40		147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	12
5.102.254.69	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	12
37.26.147.216	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	12
5.22.129.104	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	12

12-31-2015-15:04:05 to 12-31-2015-16:04:05