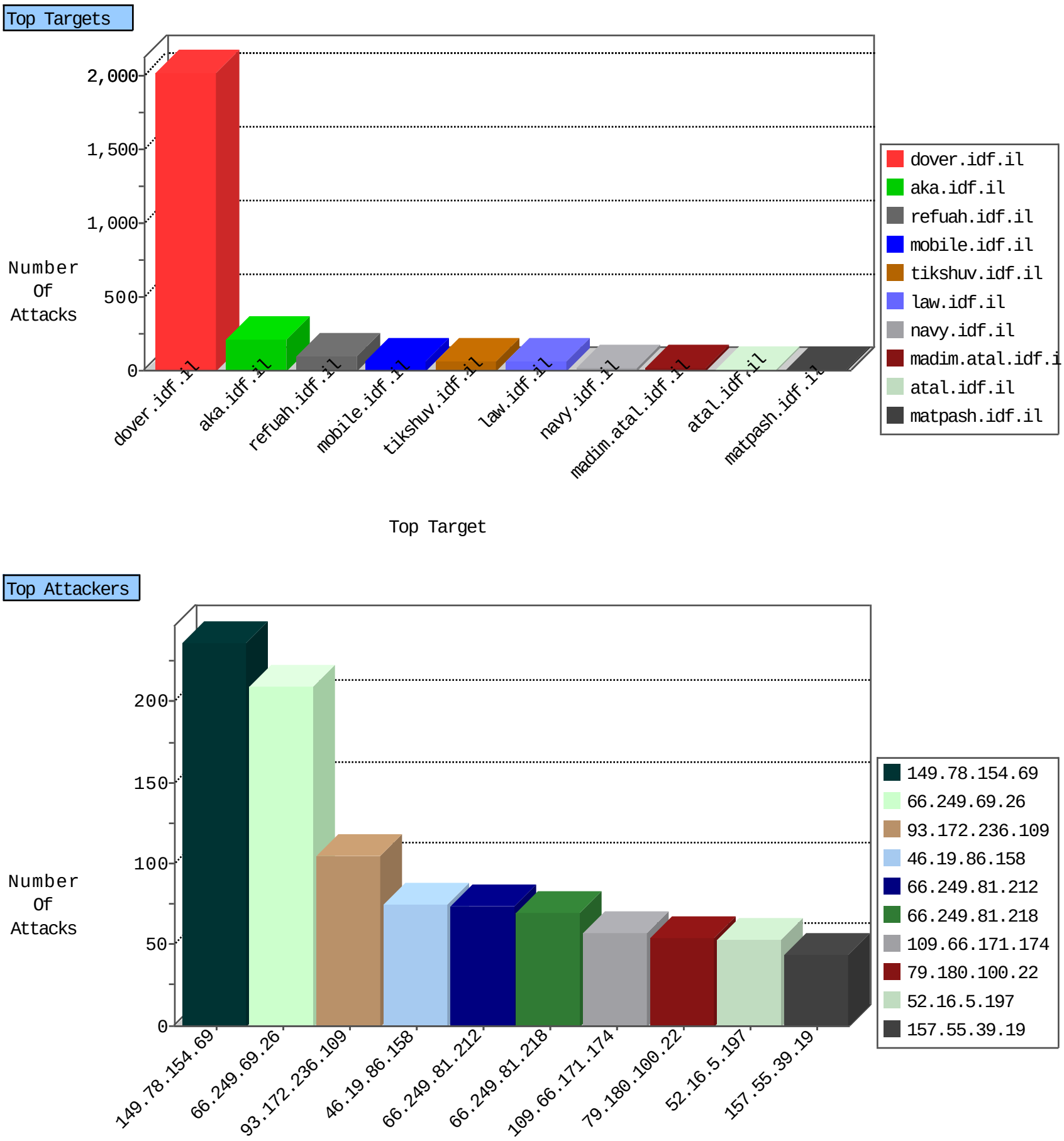
02-13-2016-23:04:08 to 02-14-2016-00:04:08

IDF Under Attack Daily Report



02-13-2016-23:04:08 to 02-14-2016-00:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
115.239.228.10	China	147.237.76.38	e.e.meitav.idf.il	JLM_Under_Attack_Con_Http	drop	2
151.80.109.153	Italy	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1

02-13-2016-23:04:08 to 02-14-2016-00:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.98.3.81	Netherlands	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	2
188.165.15.61	France	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1

02-13-2016-23:04:08 to 02-14-2016-00:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
183.60.48.25	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
61.244.111.77	147.237.76.199	Hong Kong	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.244.111.77	147.237.0.200	Hong Kong	m4u.idf.il	ET SCAN Potential SSH Scan	1
61.244.111.77	147.237.0.19	Hong Kong	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
27.221.10.43	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
183.175.141.214	147.237.0.35	China	akaws.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
183.60.48.25	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.193	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
61.244.111.77	147.237.76.148	Hong Kong	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
61.244.111.77	147.237.0.35	Hong Kong	akaws.idf.il	ET SCAN Potential SSH Scan	1
61.244.111.77	147.237.0.15	Hong Kong	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
1.231.159.189	147.237.76.44	Korea, Republic of	e.refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.60.48.25	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1

02-13-2016-23:04:08 to 02-14-2016-00:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
93.172.236.109	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	76
46.19.86.158	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	75
109.64.10.132	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
37.26.146.217	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
84.111.12.130	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
217.132.41.104	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
208.109.97.62	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
185.3.144.31	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.147.201	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.208.205	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
213.57.145.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
85.64.47.237	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.140	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
24.185.168.76	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.140	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
195.60.232.57	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
185.32.179.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
66.249.66.60	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.102.242.62	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.181.128.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.15.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.137.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.106.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.205.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
109.253.200.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.214.166	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
217.132.41.104	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.182.167.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.144.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.205.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.217.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.24.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.175.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.188.126	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.130.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.117.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.150.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.51.49	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-13-2016-23:04:08 to 02-14-2016-00:04:08

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
109.253.134.152	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
195.239.16.53	Russian Federation	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
31.210.187.112	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	236
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	207
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	74
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	70
109.66.171.174	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	57
79.180.100.22	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 79.180.100.22	Block	54
52.16.5.197	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	53
157.55.39.19	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	44
89.138.66.69	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	40
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	39
89.138.171.64	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	32
79.183.59.157	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	30
208.109.97.62	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	30
93.172.236.109	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
40.77.167.100	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	27
109.186.183.134	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	26
50.87.144.145	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	25
192.249.66.247	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
85.64.154.3	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	23
5.28.144.167	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	22
89.139.234.12	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	20
37.26.149.192	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	19
79.182.13.182	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
46.116.160.92	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
84.228.48.82	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
176.13.1.26	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
89.138.212.197	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
149.78.21.206	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
37.8.81.128	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
2.54.179.243	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
31.210.187.214	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	9
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	9
84.111.189.76	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
37.46.39.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
109.67.105.235	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
109.64.148.41	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
82.205.113.88	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
45.35.64.142		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
109.253.201.93	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
109.67.56.220	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	7
67.141.240.132	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	7
89.139.29.13	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	7
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
24.106.185.35	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.113	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
157.55.39.159	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
85.65.114.110	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
2.54.13.27	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
5.22.135.140	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.228	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6

02-13-2016-23:04:08 to 02-14-2016-00:04:08