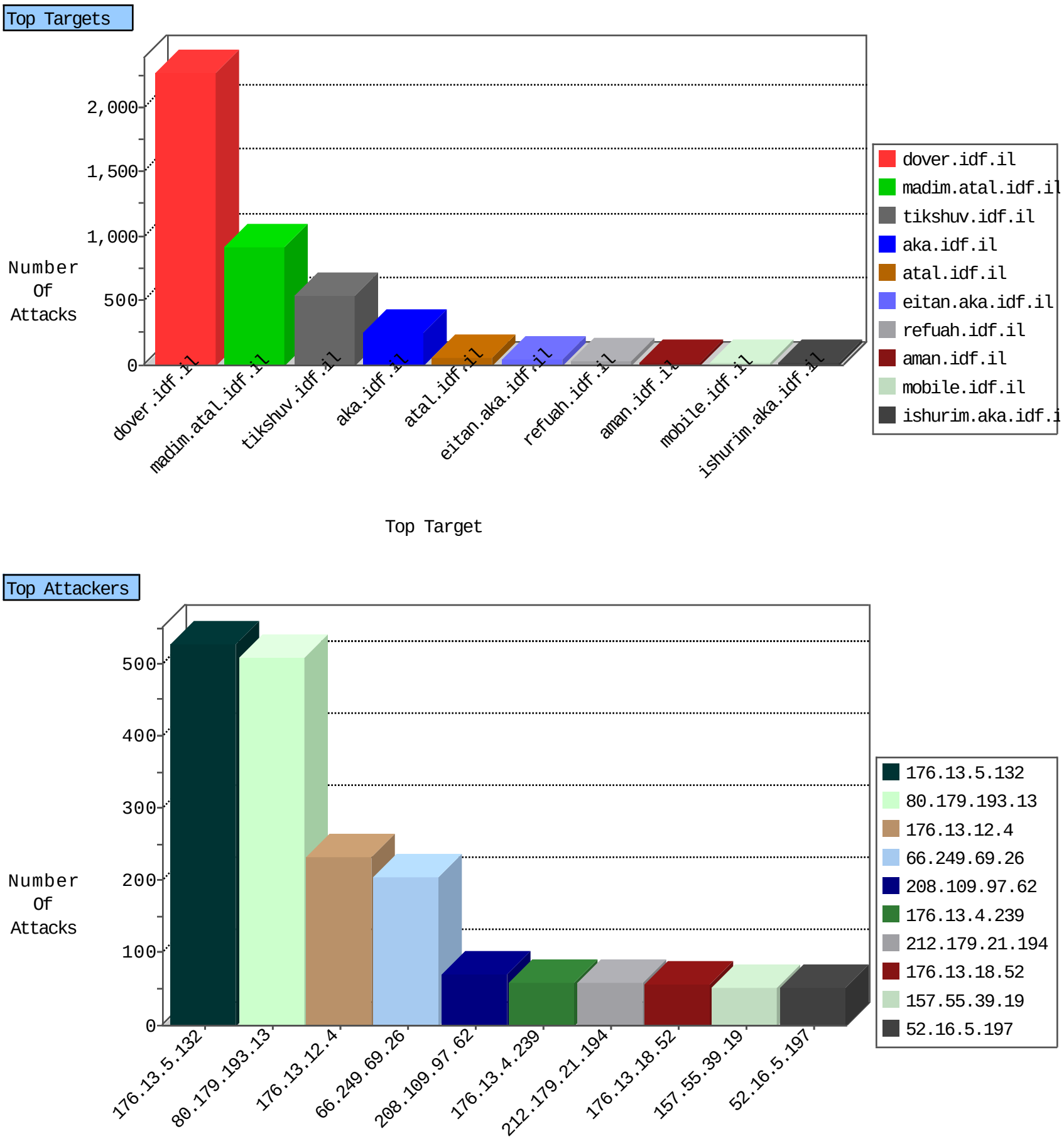
02-14-2016-15:04:07 to 02-14-2016-16:04:07

IDF Under Attack Daily Report



02-14-2016-15:04:07 to 02-14-2016-16:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.46.189	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
115.239.228.10	China	147.237.0.34	tikshuv.idf.il	Frk_Under_Attack_Con_Http	drop	2
185.130.5.224		147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
177.9.17.85	Brazil	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
115.239.228.10	China	147.237.0.34	tikshuv.idf.il	Frk_Purple_Con_Limit_Http	drop	1
185.94.111.1		147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
176.13.5.132	Israel	147.237.0.19	madim.atal.idf.il	DOSS-SSL-ClearText	drop	1

02-14-2016-15:04:07 to 02-14-2016-16:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.19.35	Israel	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
198.20.87.98	United States	147.237.76.38	e.e.meitav.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

02-14-2016-15:04:07 to 02-14-2016-16:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
94.188.248.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
84.108.48.190	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.203.167	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
125.89.70.205	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
91.135.102.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.48.140	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
69.197.145.242	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
2.54.10.155	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-14-2016-15:04:07 to 02-14-2016-16:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.121.82.102	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
79.182.203.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
185.5.223.192	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
195.160.242.40	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
195.160.242.40	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
138.134.192.10	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
84.108.40.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
84.94.123.10	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
208.109.97.62	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
2.54.152.130	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
84.108.40.253	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	7
171.100.231.35	Thailand	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.253.204.87	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
80.246.137.68	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.204.87	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.41.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.222.177	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
195.190.19.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.232	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.200.205.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.15.229	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
176.13.20.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.98.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.142.235	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
31.210.186.46	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.143.227.174	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.199.104.146	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.143.227.174	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
159.203.123.37	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
185.120.125.37		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
217.132.240.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.36.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.233	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.166.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.235.37.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.118.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.110		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.160.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.87.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.137.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.8.124.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.232.12.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.211.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.179.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-14-2016-15:04:07 to 02-14-2016-16:04:07

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
109.65.15.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.187.70	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.52.140.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.179.193.13	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	508
176.13.5.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	272
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	203
176.13.5.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	127
176.13.12.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	120
176.13.12.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	111
176.13.5.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
208.109.97.62	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	62
176.13.4.239	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	60
176.13.18.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	54
52.16.5.197	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	51
157.55.39.19	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	51
2.52.14.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
2.54.30.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
207.46.13.174	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	44
52.33.66.29	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	43
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	41
40.77.167.100	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	38
157.55.39.147	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	33
2.54.142.126	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	27
50.87.144.145	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
46.19.85.84	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
176.13.5.132	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
192.118.27.253	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
192.249.66.247	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	23
185.32.179.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
31.168.3.188	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	22
31.168.169.122	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	20
84.108.237.203	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	20
82.166.93.193	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	20
46.116.230.52	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	19
109.253.204.164	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	19
2.54.14.76	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
93.173.233.135	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
37.26.148.167	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
62.219.118.135	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	17
217.132.135.178	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	16
84.94.159.95	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
212.117.137.146	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
62.90.235.67	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
82.166.233.145	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
109.65.15.229	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
81.241.113.31	Belgium	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
46.116.162.172	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
213.151.35.213	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
2.52.162.106	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
2.52.48.94	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
84.95.5.90	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
2.54.4.254	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12

02-14-2016-15:04:07 to 02-14-2016-16:04:07