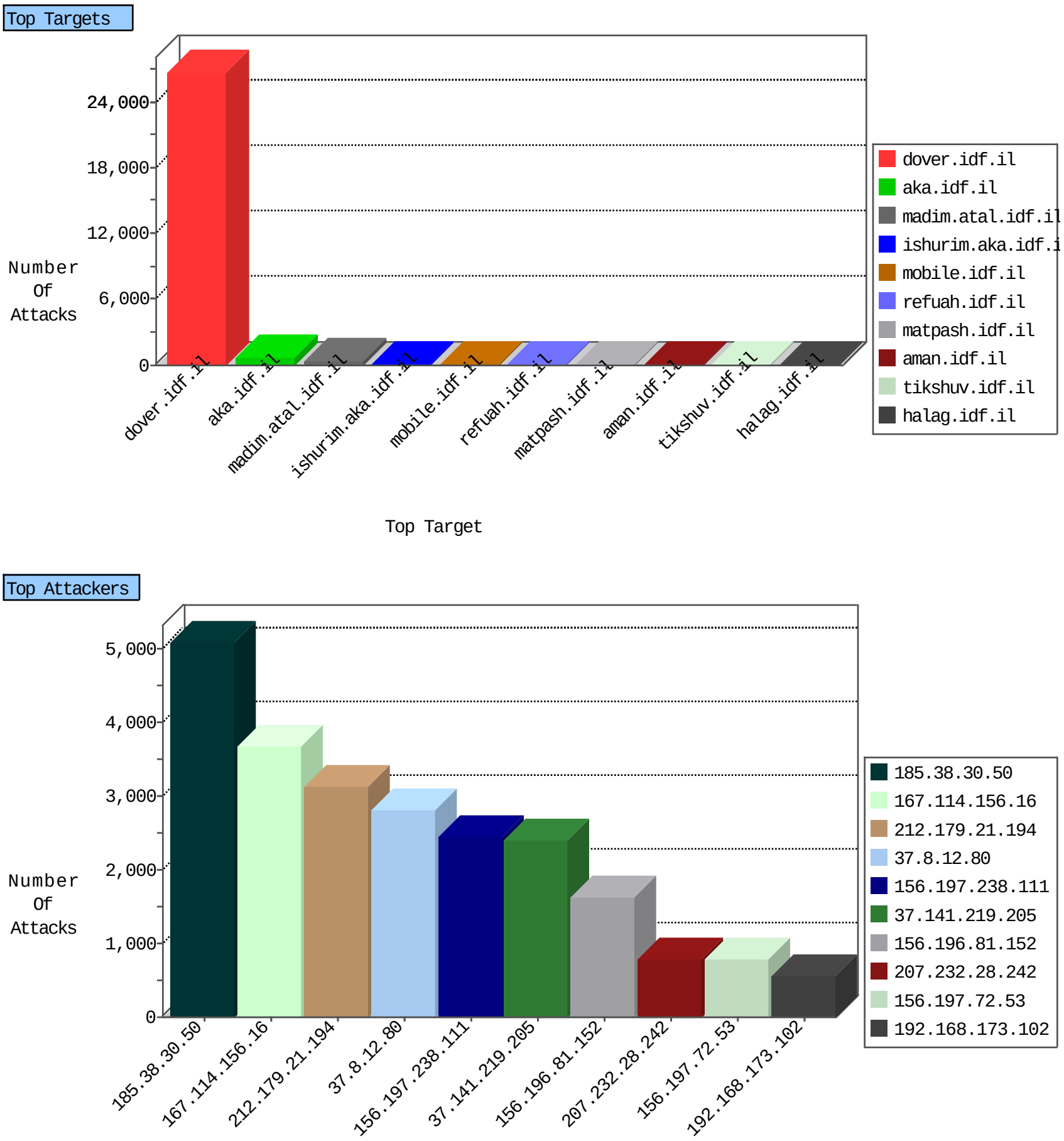
04-07-2016-15:04:01 to 04-07-2016-16:04:01

IDF Under Attack Daily Report



04-07-2016-15:04:01 to 04-07-2016-16:04:01

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	Block_Ip_Web_In	drop	3664
37.239.68.12	Iraq	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2673
37.8.12.80	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1330
212.179.21.194	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	857
38.95.109.35	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	178
38.95.109.35	United States	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	126
156.197.136.7	Egypt	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	58
37.141.219.205	Saudi Arabia	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	20
80.246.137.199	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
79.141.165.42	Europe	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	13
82.145.219.88	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
158.169.150.4	Belgium	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
37.141.219.205	Saudi Arabia	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
79.177.169.195	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
37.239.68.65	Iraq	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
37.239.68.12	Iraq	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
37.239.68.12	Iraq	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
37.239.68.12	Iraq	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
169.54.233.120	United States	147.237.77.233	atal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
37.141.219.205	Saudi Arabia	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
79.179.184.87	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
37.8.119.61	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
37.239.68.65	Iraq	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
182.52.16.51	Thailand	147.237.76.177	ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
185.103.252.96	Russian Federation	147.237.72.167	ishurim.aka.idf.i	Block_Udp_All_Nets	drop	1
89.187.219.147	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
52.53.222.9	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
169.54.233.120	United States	147.237.77.233	atal.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

04-07-2016-15:04:01 to 04-07-2016-16:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.183.182.139	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
5.29.240.151	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
149.88.213.91	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
213.151.32.163	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
38.95.109.35	United States	147.237.77.216	dover.idf.il	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	2
65.55.210.121	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.135.63.82	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-07-2016-15:04:01 to 04-07-2016-16:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
89.138.57.80	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -sS window 1024	1
62.219.113.121	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.134.107	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.84.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
185.38.30.50	147.237.77.216	Lebanon	dover.idf.il	ET SCAN NMAP -sA (2)	1
165.138.213.4	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
104.232.98.60	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
84.109.229.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
31.168.24.52	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.108.132.58	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
212.235.4.26	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.116.102.73	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
165.138.213.4	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.194.211	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

04-07-2016-15:04:01 to 04-07-2016-16:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.38.30.50	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5102
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3128
156.197.238.111	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2459
37.141.219.205	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1897
156.196.81.152	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1643
37.8.12.80	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1399
207.232.28.242	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	791
156.197.72.53	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	778
156.196.221.133	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	457
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	345
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	313
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	222
176.67.168.195	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	152
37.141.219.205	Saudi Arabia	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	148
37.141.219.205	Saudi Arabia	147.237.77.216	dover.idf.il	drop		drop	116
37.8.12.80	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop		drop	67
156.197.136.7	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
188.247.73.159	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
46.19.85.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
192.116.240.154	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
205.235.33.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
176.13.6.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
5.102.219.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
46.19.85.122	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
213.151.32.163	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
185.3.147.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
82.173.114.35	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
79.180.218.230	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
91.63.111.28	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
84.111.120.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
41.108.105.23	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
66.102.8.238	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
185.32.179.69	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
62.219.164.92	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
109.186.49.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
37.141.219.205	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	19
79.178.212.48	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
84.228.243.103	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.19.86.190	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
185.3.146.218	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
176.12.160.4	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15

04-07-2016-15:04:01 to 04-07-2016-16:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	154
2.53.3.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	101
46.19.85.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	63
46.19.85.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
46.19.86.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
46.19.85.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	9
46.19.85.122	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
176.13.2.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
79.178.212.48	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.69.155.28	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 87.69.155.28	Block	3
79.181.141.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.69.155.28	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 87.69.155.28	Block	3
2.54.160.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.69.155.28	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 87.69.155.28	Block	3
87.69.155.28	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 87.69.155.28	Block	3
87.69.155.28	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 87.69.155.28	Block	2
66.102.8.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.253.157.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.69.155.28	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 87.69.155.28	Block	2
109.253.205.55	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
82.80.129.8	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/mivtza	Block	2
87.69.155.28	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 87.69.155.28	Block	2
66.249.93.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 141.8.132.78	Block	1
87.69.155.28	Israel	147.237.72.166	aka.idf.il	NULL Character in Method]1Á[[#27]],«œ_þ[[#27]]$Ê[[#0]]©¼	Block	1
37.141.219.205	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
216.218.206.66	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
109.67.155.191	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
87.69.155.28	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 87.69.155.28	Block	1
85.130.246.49	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
17.142.156.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
68.68.96.23	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/-ar/بريد	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18247-en/dover.aspx.	Block	1
87.69.155.28	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
37.238.204.96	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
220.255.145.142	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
176.13.2.86	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.69.34	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.69.34	Block	1
85.250.48.27	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
37.8.12.80	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
207.46.13.144	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.maarachot.idf.il/pdf/files/' ×'½¿|' '½¿|'½¿|'½¿|'½¿|'½¿|	Block	1
68.180.229.89	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
141.8.184.13	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	1
89.139.185.86	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
40.77.167.75	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
222.235.67.132	Korea, Republic of	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/joomla.xml	Block	1
176.13.15.140	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1

04-07-2016-15:04:01 to 04-07-2016-16:04:01