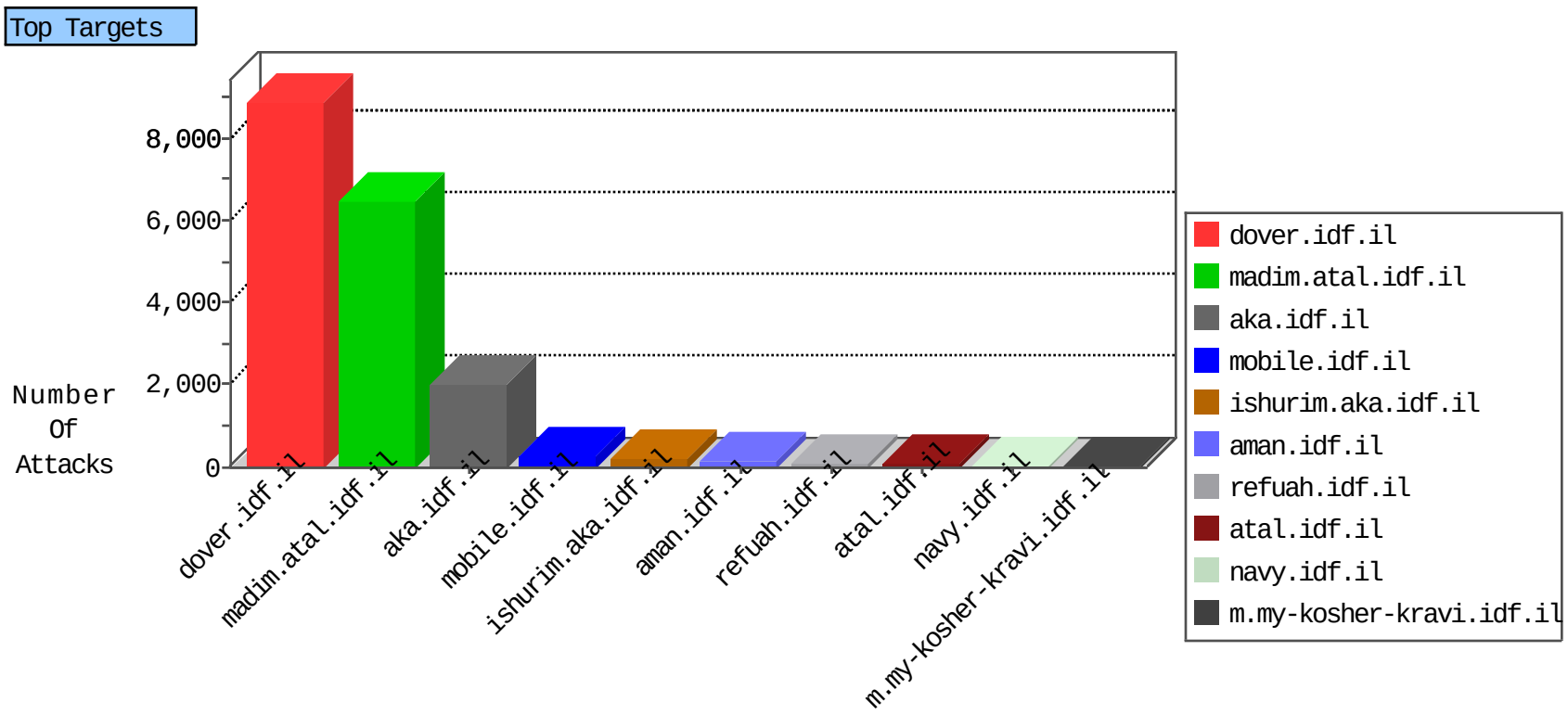
10-26-2015-18:04:03 to 10-26-2015-19:04:03

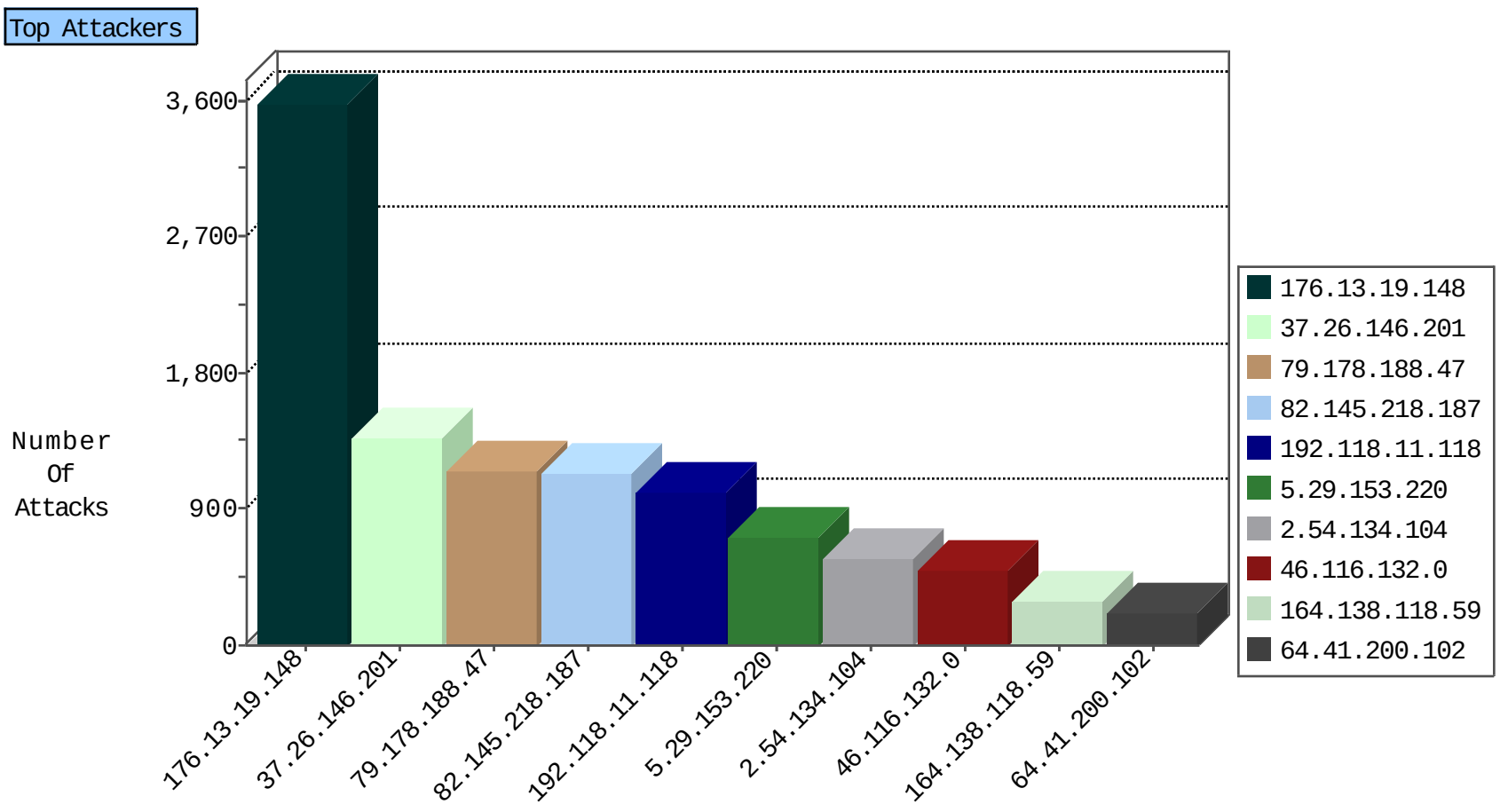
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-26-2015-18:04:03 to 10-26-2015-19:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.153.220	Israel	147.237.72.166	aka.idf.il	TCP Scan (vertical)	drop	3567
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	329
46.19.86.115	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	49
84.228.220.18	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	36
79.179.58.24	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
85.64.199.23	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
46.19.86.233	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	22
199.203.226.21	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
31.154.91.53	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	19
164.138.117.131	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
193.169.70.101	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	17
2.54.143.228	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
37.26.148.166	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	14
176.12.136.110	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	14
95.86.69.116	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
84.228.124.20	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
84.228.100.180	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	10
77.127.108.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
2.54.11.155	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
81.218.2.118	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
217.165.14.180	United Arab Emirates	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
82.145.218.187	Europe	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
37.26.147.172	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
85.65.0.239	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
77.125.90.24	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
2.54.11.155	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
77.125.90.24	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
2.54.11.155	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
80.246.136.95	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
77.125.155.181	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
212.76.110.176	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.53.57	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
93.173.235.62	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.13.18.248	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
95.86.88.45	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
84.109.225.50	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.178.136.84	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
159.0.245.244	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.86.33	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.44.117.139	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
37.60.43.40	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.116.132.0	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
37.142.68.59	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
185.51.221.20	Iraq	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
5.156.240.196	Romania	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
84.228.55.84	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
213.151.58.74	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
77.125.162.51	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
10.0.0.2		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
176.13.16.250	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
54.187.55.213	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3

10-26-2015-18:04:03 to 10-26-2015-19:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.138.17.205	France	147.237.76.38	e.e.meitav.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

10-26-2015-18:04:03 to 10-26-2015-19:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	**Signature**	**Count**

10-26-2015-18:04:03 to 10-26-2015-19:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.178.188.47	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1148
82.145.218.187	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1130
2.54.134.104	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	578
164.138.118.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	286
94.159.159.23	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	132
185.51.221.63	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	124
185.51.221.222	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	122
185.51.221.20	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	121
2.54.141.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	118
185.51.221.66	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	105
46.19.86.7	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	96
37.26.149.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	94
94.202.247.202	United Arab Emirates	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	85
63.116.61.253	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	85
188.51.113.203	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	83
108.59.63.94	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	82
85.64.19.154	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	80
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	73
46.19.86.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
46.19.86.18	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
178.164.137.183	Hungary	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
123.237.167.151	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
5.29.112.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
46.19.86.34	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
81.218.2.118	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
46.19.86.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
176.228.136.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
88.249.49.44	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
89.138.91.98	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
95.185.75.41	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
17.142.156.109	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
46.19.86.85	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
68.4.93.63	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
93.173.233.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
164.138.127.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
79.177.5.189	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
37.26.146.169	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
37.153.217.4	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
95.86.88.45	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
31.154.91.53	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
173.192.79.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
23.242.215.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26

10-26-2015-18:04:03 to 10-26-2015-19:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.19.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3562
192.118.11.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1008
37.26.146.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	709
37.26.146.201	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.146.201	Block	658
46.116.132.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	490
46.19.86.7	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	56
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	56
149.88.75.68	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	56
46.121.76.237	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	54
84.108.70.140	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	42
85.64.58.227	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	42
79.183.38.15	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	42
85.64.58.227	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	42
84.108.70.140	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	42
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	28
46.210.237.246	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	28
213.57.157.76	Israel	147.237.72.156	aman.idf.il	PHP Attempt	Block	28
149.88.141.151	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	28
46.210.237.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	28
64.41.200.102	United States	147.237.77.243	mobile.idf.il	Multiple Untraceable SSL Sessions from 64.41.200.102 (Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE))	None	28
213.57.157.76	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/ajax/updatestatus.php	Block	28
149.88.141.151	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	28
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
5.29.38.138	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	28
178.164.137.183	Hungary	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx	Block	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
149.88.141.151	Israel	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	14
64.41.200.102	United States	147.237.77.243	mobile.idf.il	Multiple Untraceable SSL Sessions from 64.41.200.102 (Unsupported Legacy SSL Version)	None	14
64.41.200.102	United States	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 64.41.200.102 (Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE))	None	14
185.95.104.226		147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/wp-content/plugins/index.php	Block	14
79.180.54.112	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	14
66.249.75.16	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	14
46.19.85.160	Israel	147.237.72.166	aka.idf.il	Malformed URL	Block	14
176.110.50.229	Ukraine	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	14
109.67.67.118	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/resource/userfollowresource/create/	Block	14
64.41.200.102	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unsupported Legacy SSL Version	None	14
5.141.228.1	Russian Federation	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	14
84.111.100.139	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	14
62.90.219.66	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	14
212.76.96.235	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
46.19.86.49	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	14
183.88.78.238	Thailand	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	14
68.180.230.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	14
149.88.141.151	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/ajax/updatestatus.php	Block	14
64.41.200.102	United States	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Unsupported Cipher	None	14
64.41.200.102	United States	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 64.41.200.102 (Unsupported Cipher)	None	14
2.52.171.202	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
89.22.50.55	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
188.138.17.205	France	147.237.77.235	sviva.idf.il	Unauthorized URL Access to 147.237.77.235/	Block	14
79.183.35.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	14

10-26-2015-18:04:03 to 10-26-2015-19:04:03