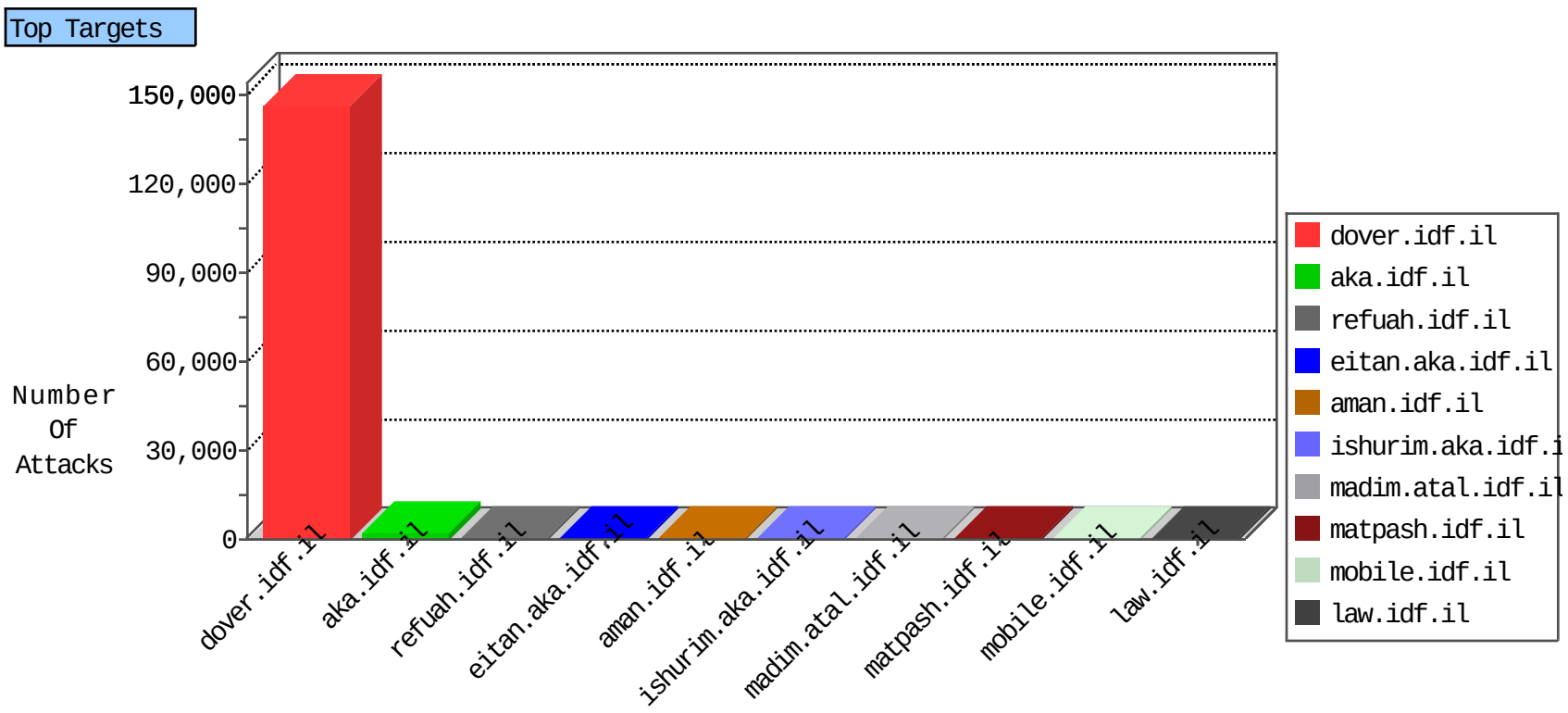
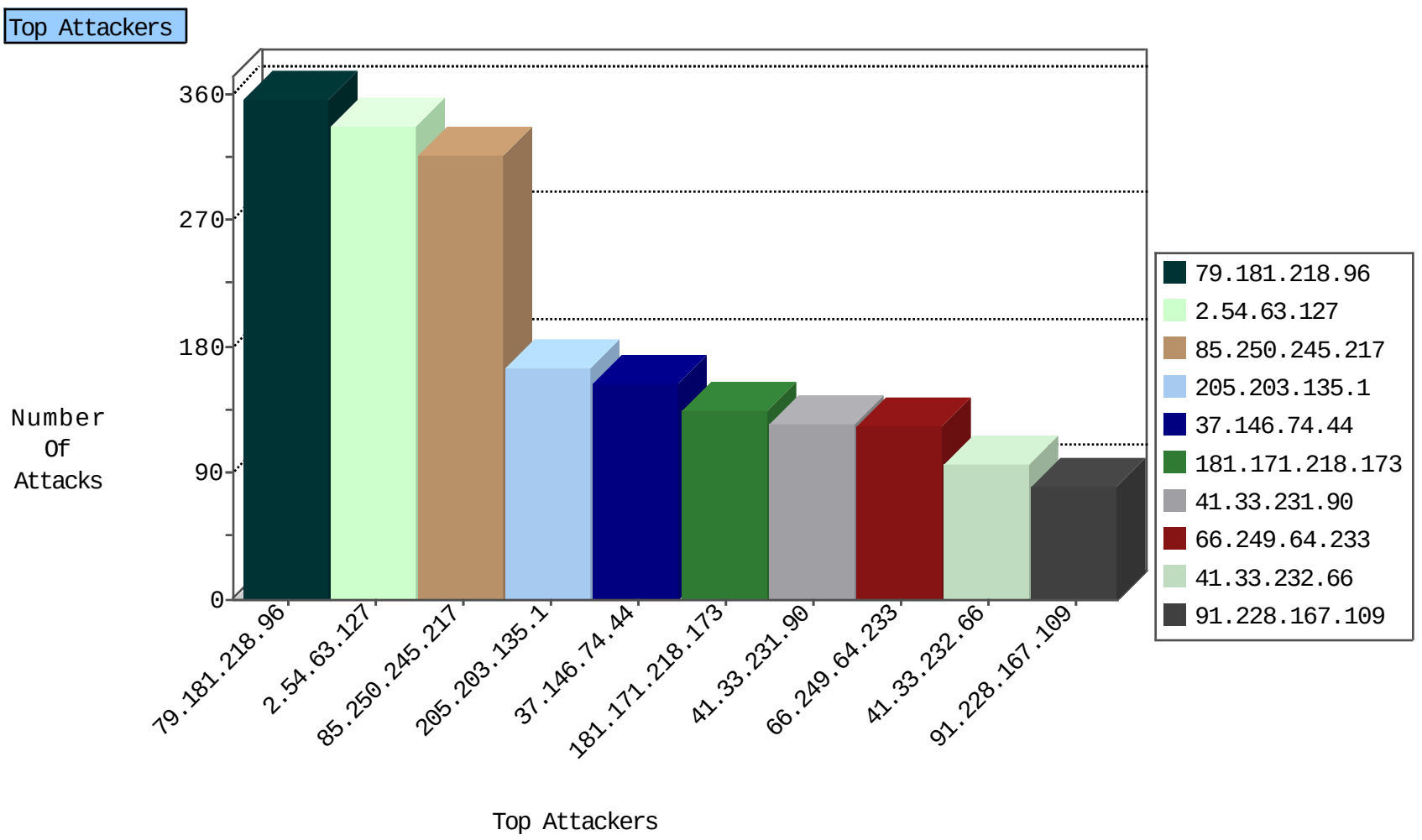
11-12-2015-20:04:09 to 11-12-2015-21:04:09

IDF Under Attack
Daily Report

Top Targets



Top Attackers



11-12-2015-20:04:09 to 11-12-2015-21:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
126.152.164.218	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5990
173.232.44.97	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5808
187.91.144.87	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5732
222.137.129.41	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2999
223.11.70.127	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2885
2.228.23.5	Italy	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2668
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	990
183.160.248.60	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	412
201.52.72.117	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	185
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	174
66.249.67.27	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	146
39.117.211.62	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	98
198.189.230.3	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	38
219.204.55.105	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	37
211.206.245.96	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33
68.11.219.85	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	33
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	21
46.19.85.248	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
79.179.138.108	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
84.95.146.31	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
79.182.204.166	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
71.206.44.84	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	4
98.170.241.5	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
192.168.0.105		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
79.176.138.22	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
77.240.74.79	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
31.168.218.41	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
108.59.69.121	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
91.228.127.198	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
72.23.175.37	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
83.233.213.17	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
31.208.2.106	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
83.233.151.4	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
178.248.26.92	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
69.6.166.118	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
216.237.69.15	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.160.209.80	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
95.127.176.54	Spain	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
209.40.160.60	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
24.97.75.102	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
78.33.218.62	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
162.255.124.50	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
63.248.157.91	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
94.135.203.22	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
201.176.157.91	Argentina	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
2.54.2.162	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
75.56.57.31	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
199.27.232.36	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
72.42.94.90	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

11-12-2015-20:04:09 to 11-12-2015-21:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.125.145.42	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
188.165.15.233	France	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	5
173.0.139.152	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
188.165.15.132	France	147.237.77.176	matpash.idf.il	C228: HTTP: AhrefBot crawler	Block	2
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

11-12-2015-20:04:09 to 11-12-2015-21:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
173.0.139.152	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	10
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	3
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2

11-12-2015-20:04:09 to 11-12-2015-21:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.181.218.96	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	338
2.54.63.127	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	333
85.250.245.217	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	295
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	164
37.146.74.44	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	154
181.171.218.173	Argentina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	135
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	93
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	93
91.228.167.109	Slovakia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	81
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
108.2.147.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
92.90.17.23	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
91.228.167.130	Slovakia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
46.19.85.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	61
70.199.75.108	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
207.179.136.203	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
79.178.155.81	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
192.3.24.227	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
41.218.171.201	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
37.26.146.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
141.0.11.173	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
158.130.0.242	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
62.57.245.247	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
209.239.121.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
5.29.175.165	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	38
91.58.224.191	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
132.3.29.81	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
132.3.29.79	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
132.3.29.80	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
5.29.175.165	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	35
148.240.174.247	Mexico	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
157.55.39.166	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
40.77.167.56	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
37.26.148.161	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
2.219.217.53	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
185.58.201.28	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
37.26.149.128	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
66.249.64.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
132.3.29.81	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
104.240.225.86		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30

11-12-2015-20:04:09 to 11-12-2015-21:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.26.64	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 2.54.26.64	Block	29
176.13.23.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
2.54.11.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
87.68.20.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.54.63.127	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.63.127	Block	5
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
77.125.145.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
176.12.148.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.181.107.37	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/	Block	3
185.32.179.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.229.29.167	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ufi/reaction/	Block	2
46.121.107.41	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
46.19.85.5	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.243	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/edim/fund/×³×ŸÂ¿Â½×³×ŸÂ¿Â½×³Â§×³×ŸÂ¿Â½×³×ŸÂ¿Â½	Block	1
79.176.34.193	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	1
87.69.146.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/updateuserdetails.aspx	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2065-he/cogat.aspx	Block	1
66.249.69.81	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1451-he/atal.aspx	Block	1
222.84.5.155	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/wp-content/plugins/login-wall-ysqow/login_wall.php	Block	1
84.108.234.99	Israel	147.237.72.166	aka.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	1
46.19.85.201	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method %22%2C%22%22%2C1447354364%2C%22https%3A%2F%2Fwww.google.co.il%2F%22%5D; in URL _pk_id.20.8afc=d17f4406def2ae12.1447354364.1.1447354364.1447354364.	Block	1
79.183.185.231	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.237.138.202	Czech Republic	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /	Block	1
31.154.94.6	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.130.9	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
85.250.245.217	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.78.153	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.11.58	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.80.143.233	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
209.88.157.118	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
46.19.85.107	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
157.55.39.244	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.178.105.76	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
5.22.131.177	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.138.1.120	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.idf.il/1038-en/dover.aspx	Block	1
69.41.14.130	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/960.css	Block	1
66.249.69.85	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.69.85	Block	1
84.111.224.245	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.179.96.90	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.12.149.223	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
78.133.219.163	Poland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.146.177	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
109.65.188.83	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
82.166.22.10	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training/catalog.asp	Block	1
212.76.96.132	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20207-he/dover.aspx&sa=u&ved=0cakqfjaaahukewjsvumcwovjahvcwbqkhwfgads&usg=afqjcnhtryxgio9uiefyzaoy9k0bdjboyq	Block	1
46.19.85.201	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
173.252.90.245	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

11-12-2015-20:04:09 to 11-12-2015-21:04:09