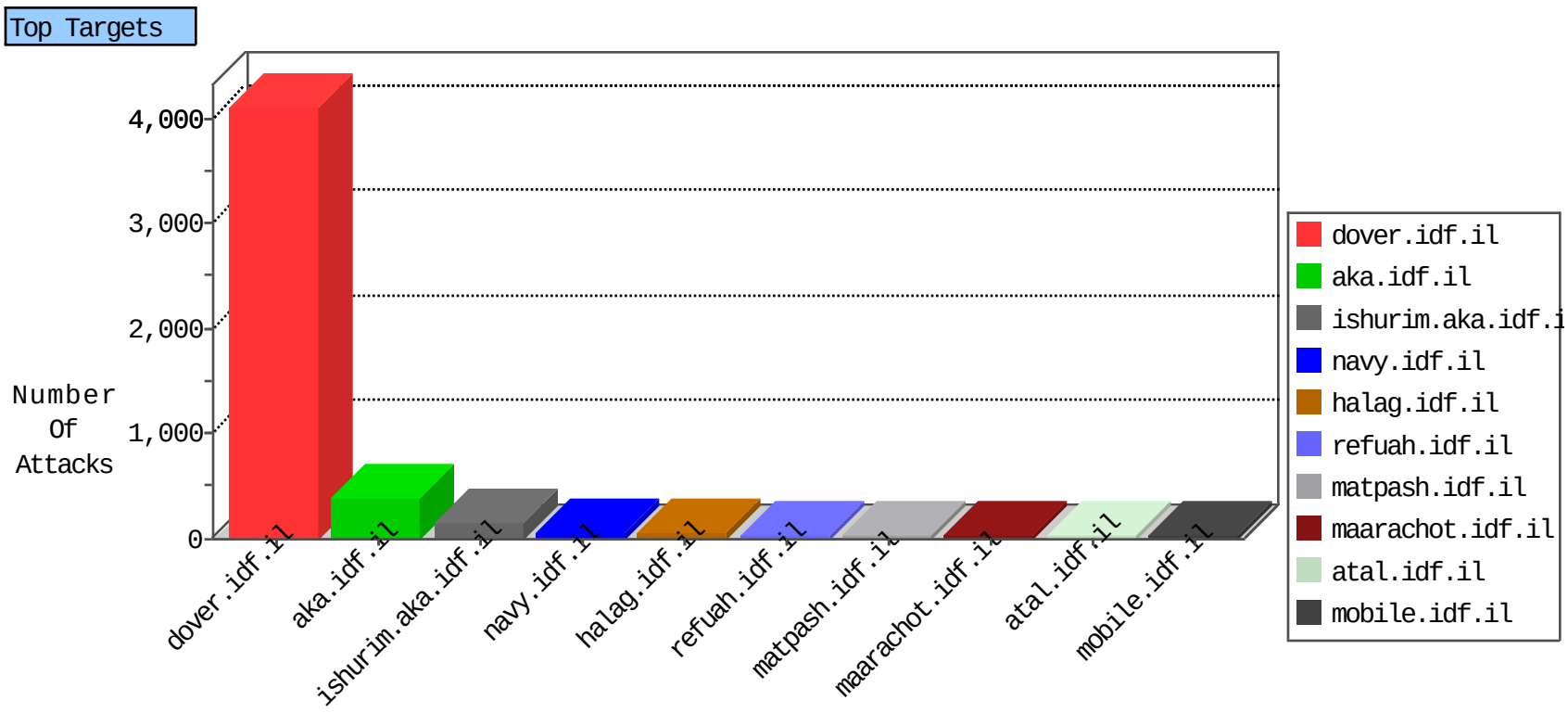
10-23-2015-09:04:07 to 10-23-2015-10:04:07

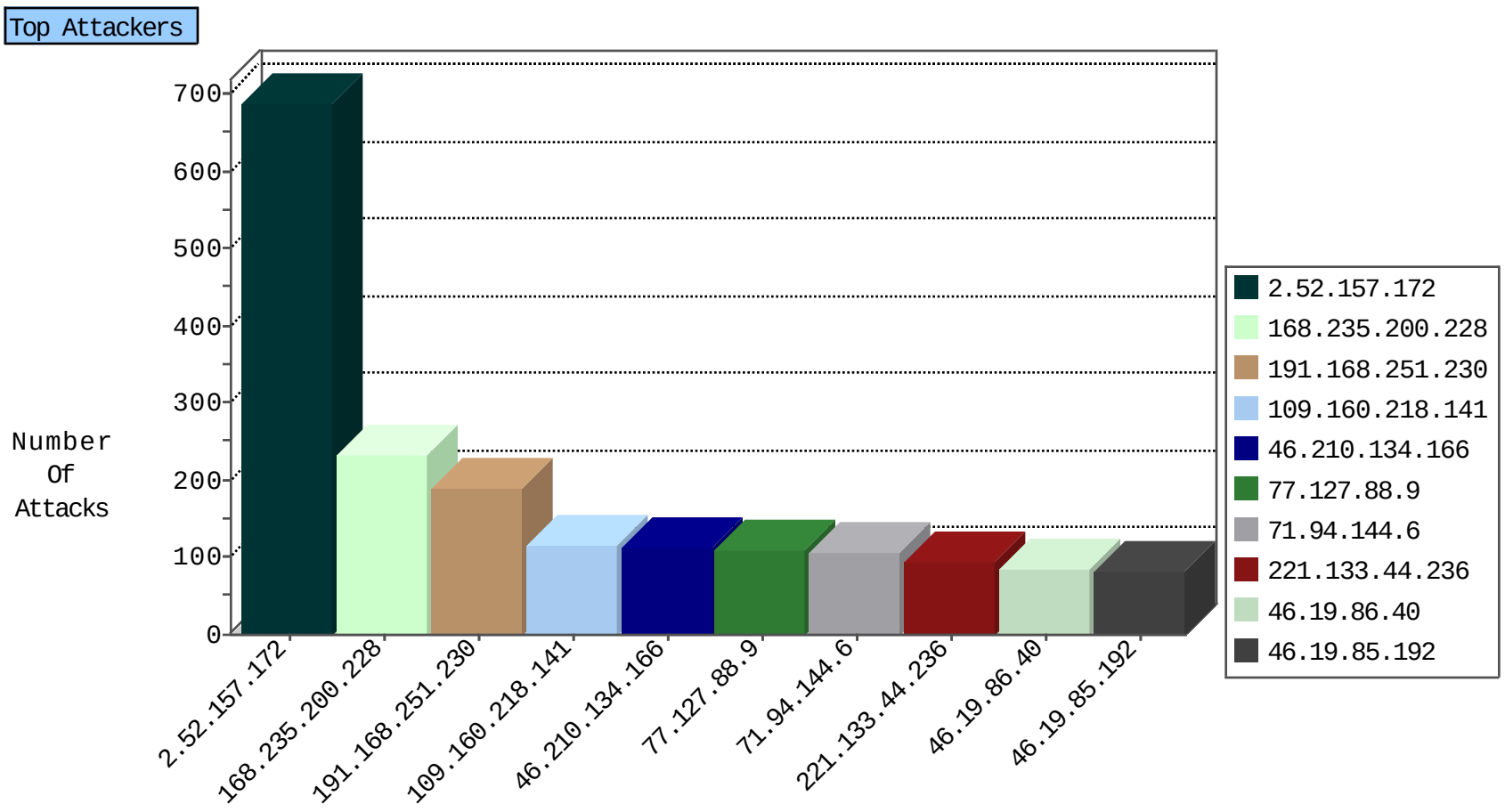
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-23-2015-09:04:07 to 10-23-2015-10:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.158	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3185
109.160.218.141	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	259
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	91
5.29.107.130	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	33
195.101.137.28	France	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
62.219.144.81	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	24
79.183.228.155	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
109.65.48.110	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
79.183.228.155	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	9
46.19.85.16	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
93.172.16.98	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
114.121.237.151	Indonesia	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
2.54.176.168	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
5.29.93.32	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.121.135.198	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.85.126	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.12.139.124	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
64.233.172.162	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
2.54.145.251	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
87.68.52.172	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
2.54.32.45	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
84.228.11.173	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
37.26.149.240	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.12.151.23	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.85.243	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
220.255.193.82	Singapore	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
109.67.103.242	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
222.186.56.42	China	147.237.0.200	m4u.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
2.52.183.107	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
185.32.179.84	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
142.54.172.109	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	drop	1
37.26.148.154	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
142.54.172.110	United States	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
142.54.172.98	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	drop	1
31.210.187.244	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
142.54.174.66	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	drop	1
2.52.157.172	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
176.13.3.147	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
142.54.172.100	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	drop	1
89.248.172.98	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
37.26.147.187	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
173.208.168.164	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1

10-23-2015-09:04:07 to 10-23-2015-10:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-23-2015-09:04:07 to 10-23-2015-10:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	9
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
64.233.172.163	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
46.148.20.22	147.237.76.31	Lithuania	nakchal.idf.il	ET WEB_SERVER Muieblackcat scanner	1
37.143.82.50	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
37.143.82.50	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -f -sS	1
182.19.252.249	147.237.0.17	Singapore	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
182.19.252.249	147.237.0.17	Singapore	m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
37.143.82.50	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
182.19.252.249	147.237.0.17	Singapore	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
121.226.211.138	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

10-23-2015-09:04:07 to 10-23-2015-10:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.52.157.172	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	648
168.235.200.228	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	232
191.168.251.230	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	189
77.127.88.9	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	108
71.94.144.6	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	106
46.210.134.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	96
221.133.44.236	Malaysia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	93
46.19.86.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
5.29.93.32	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	73
85.64.33.215	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
46.19.85.192	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
46.19.86.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
2.54.49.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
80.179.16.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
77.158.88.42	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
132.70.66.10	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	32
195.101.137.28	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
79.176.113.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
176.13.19.146	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
46.19.85.143	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	27
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
188.247.77.88	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
213.57.132.86	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	25
37.142.211.138	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	24
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
77.158.88.41	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
37.26.149.240	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
89.139.50.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
192.99.12.99	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
183.79.220.208	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
46.116.127.83	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
5.29.107.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
2.52.183.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
109.65.48.110	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
109.186.185.89	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
151.80.31.115	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
85.27.200.33	Denmark	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
37.142.185.198	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
213.57.141.237	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18

10-23-2015-09:04:07 to 10-23-2015-10:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
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
91.200.203.20	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim/resources/images/body/images/main.jpg	Block	42
183.79.220.208	Japan	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
176.13.21.102	Israel	147.237.0.17	m.my-kosher-kravi .idf.il	Distributed Illegal Parameter Encoding	None	27
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/scriptresource.axd	Block	14
192.99.12.99	Canada	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/usercontrols/headerupper/	Block	14
93.220.117.201	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/×’×™×•×¡	Block	14
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	14
37.26.148.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	14
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1599-14855-he/dover.aspx	Block	14
207.46.13.35	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/edim/fund/×³Ö³Æ’Ö¶â€™Ö³â€šÖ²Â¯Ö³Æ’×’â,¬ÂšÖ³â€šÖ²Â¿Ö³Æ’×’â,¬ÂšÖ³â€šÖ²Â½×³Ö³Æ’Ö¶â€™Ö³â€šÖ²Â¯Ö³Æ’×’â,¬ÂšÖ³â€šÖ²Â¿Ö³Æ’×’â,¬ÂšÖ³â€šÖ²Â½×³Â§×³Ö³Æ’Ö¶â€™Ö³â€šÖ²Â¯Ö³Æ’×’â,¬ÂšÖ³â€šÖ²Â¿Ö³Æ’×’â,¬ÂšÖ³â€šÖ²Â½×³Ö³Æ’Ö¶â€™Ö³â€šÖ²Â¯Ö³Æ’×’â,¬ÂšÖ³â€šÖ²Â¿Ö³Æ’×’â,¬ÂšÖ³â€šÖ²Â½	Block	14
2.54.0.73	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 2.54.0.73 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	14
141.212.122.160	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	14
46.19.85.143	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
85.130.208.225	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx	None	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-16552-en/dover.aspx-title=for	Block	14
217.194.203.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
2.54.0.73	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	14
149.78.218.83	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	14
74.82.47.3	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	14
46.116.179.151	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	14
188.143.232.10	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation fromDate in www.cogat.idf.il/901-en/cogat.aspx	Block	14
89.138.199.205	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	14
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	14
2.54.0.73	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
157.55.39.13	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	14
79.176.34.128	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	14
46.116.179.151	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/rss.aspx	Block	14
188.143.232.26	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1283-en/dover.aspx	Block	14
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	14
37.26.147.204	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
176.12.139.230	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
80.246.136.238	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14

10-23-2015-09:04:07 to 10-23-2015-10:04:07