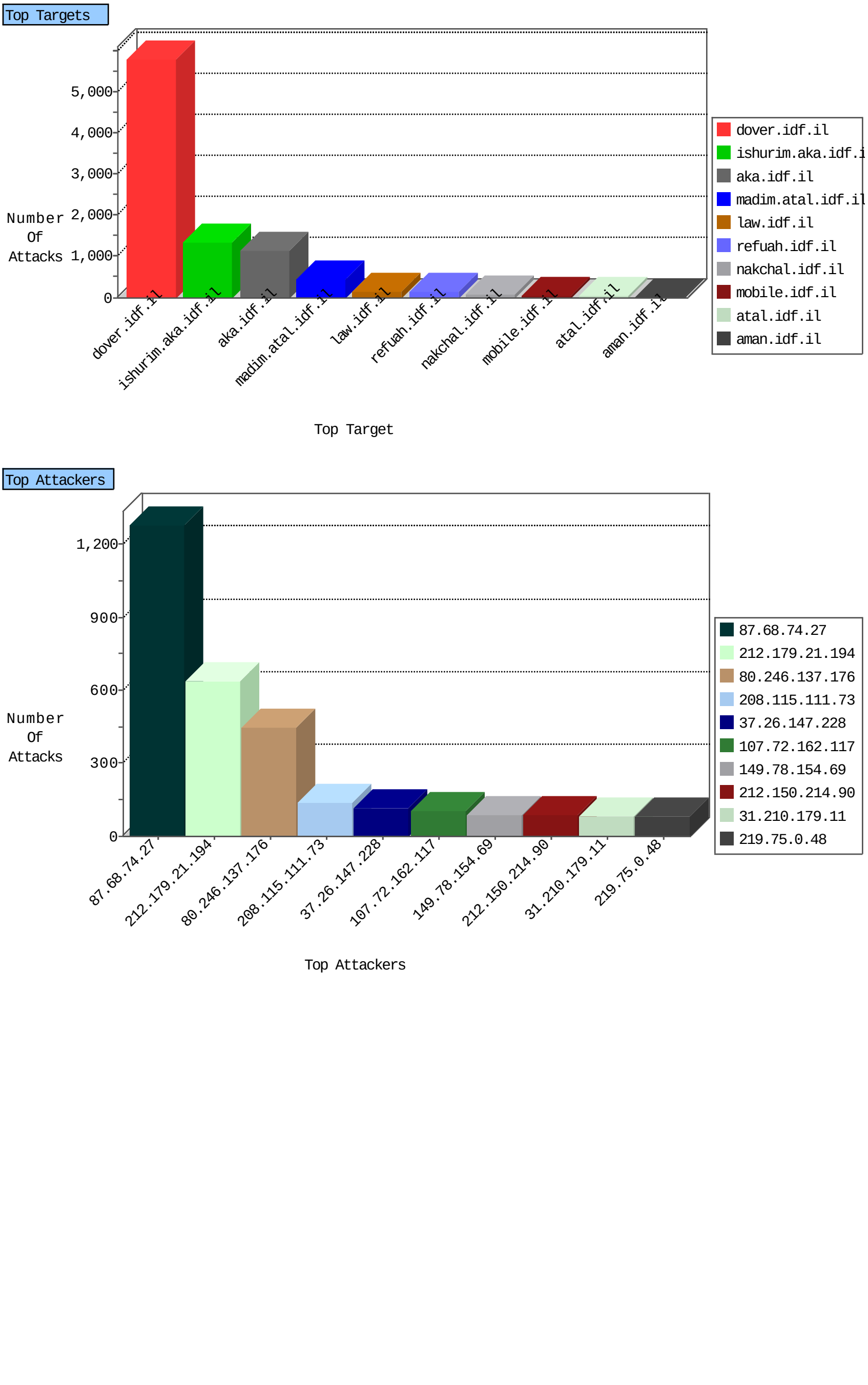
10-18-2015-13:04:01 to 10-18-2015-14:04:01

IDF Under Attack Daily Report



10-18-2015-13:04:01 to 10-18-2015-14:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	364
176.13.19.62	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	72
46.19.85.125	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	68
46.19.85.182	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	53
37.26.147.228	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	48
79.176.182.104	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
82.80.119.226	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
93.157.87.61	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
83.252.230.239	Sweden	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
82.166.22.80	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	23
77.126.69.2	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
166.172.186.228	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
2.54.168.11	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	19
2.54.16.153	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
37.26.146.205	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
79.178.189.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
62.128.45.194	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15
31.168.217.95	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
62.219.99.154	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
81.218.67.58	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	14
84.110.110.66	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	11
79.179.112.107	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
190.31.135.167	Argentina	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
79.178.12.240	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
62.128.45.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
81.218.33.77	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
84.110.110.178	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
94.159.205.146	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
109.186.92.190	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
46.19.86.188	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	9
87.69.207.137	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
84.94.32.197	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
84.108.70.132	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
95.86.96.10	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
192.114.23.208	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	7
176.13.6.163	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
79.179.112.107	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
64.233.172.162	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
192.117.150.233	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
194.56.215.66	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
132.66.34.96	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
147.161.1.68	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
109.67.117.83	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
217.99.255.34	Poland	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
212.143.231.220	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.13.17.117	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
46.19.86.90	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.13.19.62	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
134.191.232.69	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4

10-18-2015-13:04:01 to 10-18-2015-14:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-18-2015-13:04:01 to 10-18-2015-14:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.81.196	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.153	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
185.32.179.63	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
132.72.172.202	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.173.16	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.205.214.104	147.237.77.74	Latvia	law.idf.il	ET SCAN NMAP -sS window 3072	1
24.225.8.5	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
198.58.102.156	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
176.12.146.137	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.66.178.192	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.194	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
79.183.186.48	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

10-18-2015-13:04:01 to 10-18-2015-14:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	612
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	136
107.72.162.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	104
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	87
219.75.0.48	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	76
212.179.42.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
31.210.179.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
37.26.147.228	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
85.181.50.29	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
212.199.57.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
209.95.36.14	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
46.19.85.125	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
212.179.28.34	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
84.108.7.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
87.68.74.27	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
81.218.33.77	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
212.150.214.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	43
212.150.214.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	42
213.151.59.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
212.117.136.8	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
80.178.136.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
77.126.69.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
81.242.88.144	Belgium	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
194.56.215.66	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
213.8.94.216	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
64.233.172.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
46.19.86.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
85.250.75.110	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
81.17.31.224	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
37.26.147.130	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
147.161.1.68	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
64.233.172.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
62.128.45.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
157.55.39.214	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
79.183.99.87	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
5.28.158.206	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	21
132.71.108.120	Israel	147.237.76.31	nakchal.idf.i	drop	First packet isn't SYN	drop	21
37.26.148.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21

10-18-2015-13:04:01 to 10-18-2015-14:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.68.74.27	Israel	147.237.72.167	ishurim.aka.idf.il	Too Many of the Same Response Code (404) in Session from 87.68.74.27	Block	1222
80.246.137.176	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.137.176	Block	437
68.180.230.97	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-he	Block	78
138.134.102.16	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	52
85.65.193.69	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	39
82.166.97.42	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/894-he/refuah.aspx -	Block	39
15.203.178.12	France	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	26
213.8.99.123	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	26
213.57.82.130	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	26
213.151.37.68	Israel	147.237.77.74	law.idf.il	Parameter Type Violation SearchText in www.law.idf.il/163-6639-he/patzar.aspx	Block	26
199.16.156.126	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 199.16.156.126	Block	26
62.90.147.145	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	13
132.66.34.96	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
46.19.85.115	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
80.246.130.82	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	13
176.12.149.157	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
46.116.102.106	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
88.73.30.179	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
37.26.147.228	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
79.179.102.230	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
2.54.133.101	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
207.46.13.127	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
66.102.9.101	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	13
85.250.31.60	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	13
46.19.85.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
31.168.239.231	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	13
80.246.136.3	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
176.13.9.7	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
69.171.230.117	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/sip_storage/files/4/size220x0/1744.jpg	Block	13
46.120.8.100	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	13
93.173.45.104	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
84.94.202.244	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	13
37.187.157.108	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	13
79.181.58.56	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam/main/home	Block	13
2.54.144.19	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	13
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation docId in tikshuv.idf.il/site/story.aspx	Block	13
149.88.112.251	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	13
85.250.154.235	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
46.19.85.201	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	13
31.210.179.11	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	13
213.151.36.20	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
80.246.137.33	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	13
74.82.47.3	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	13
192.118.118.1	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	13
46.120.117.168	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	13
109.64.13.89	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
84.111.226.133	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/tfasim.aspx	None	13
46.19.85.3	Israel	147.237.76.42	refuah.idf.il	Malformed URL	Block	13
79.183.99.87	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	13

10-18-2015-13:04:01 to 10-18-2015-14:04:01