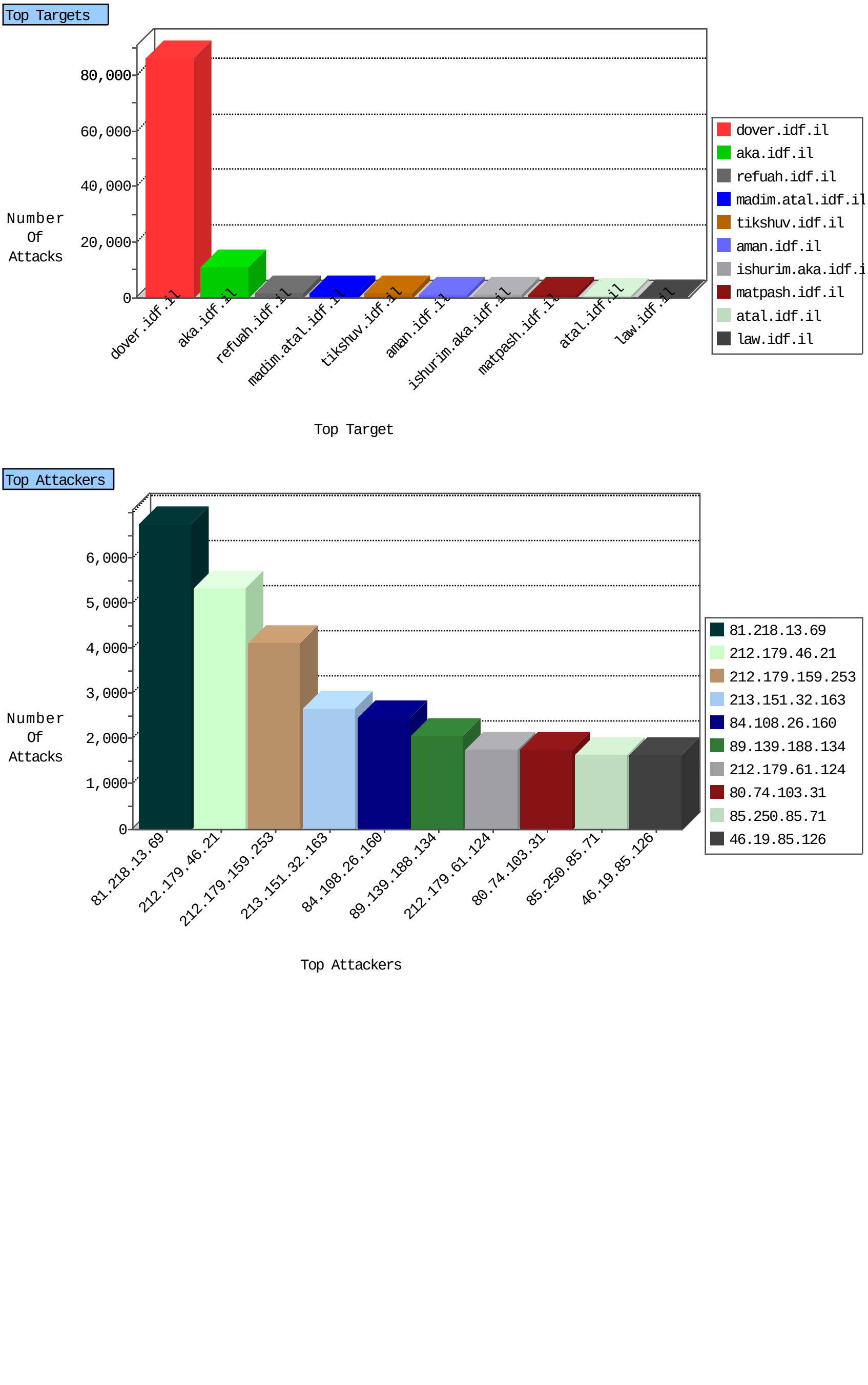
05-26-2015-00:00:02 to 05-27-2015-00:00:02

IDF Under Attack Daily Report



05-26-2015-00:00:02 to 05-27-2015-00:00:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.67.126	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5573
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4325
78.108.161.226	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3060
220.181.108.85	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	2819
31.210.186.143	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	796
79.177.56.200	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	646
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	495
79.178.112.13	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	456
79.176.19.189	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	440
93.172.175.83	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	318
109.253.144.161	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	312
46.19.86.106	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	309
149.78.171.236	United States	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	288
37.142.170.248	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	276
212.179.239.194	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	254
84.108.84.114	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	243
84.228.195.100	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	242
79.176.149.237	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	238
84.229.176.54	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	238
212.179.21.194	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	222
220.181.108.118	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	212
79.180.137.238	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	204
149.78.10.11	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	198
147.235.236.1	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	196
95.86.116.54	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	192
84.108.103.208	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	189
84.229.170.142	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	186
220.181.108.121	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	181
46.121.121.44	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	176
220.181.108.104	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	171
109.186.182.200	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	169
84.110.60.111	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	167
220.181.108.153	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	163
212.199.112.144	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	163
109.67.174.13	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	158
87.69.36.187	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	157
93.173.13.32	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	149
46.116.149.222	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	141
149.88.125.123	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	139
66.249.78.159	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	138
212.179.44.27	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	120
109.65.43.38	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	114
192.115.116.25	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	106
37.142.2.254	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	105
46.19.85.191	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	105
109.66.170.215	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	104
37.142.4.112	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	99
213.8.2.128	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	98
46.19.86.190	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
77.127.19.43	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90

05-26-2015-00:00:02 to 05-27-2015-00:00:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
84.108.26.160	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	2473
84.111.2.144	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	1457
84.108.61.28	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	844
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	779
212.185.61.12	Germany	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	778
84.109.25.246	Israel	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	595
84.109.190.123	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	567
84.94.41.65	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	391
84.108.137.250	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	372
77.125.87.158	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	274
184.173.183.172	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	221
184.173.183.172	United States	147.237.77.233	atal.idf.il	DVRep_P-N_40-59	Permit	201
184.173.183.172	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_P-N_40-59	Permit	129
93.186.16.154	South Africa	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	112
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	111
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	72
212.179.61.124	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	28
87.68.24.92	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	24
46.120.123.228	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	24
89.139.188.134	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	23
193.43.245.250	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	23
84.94.123.179	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	22
193.43.246.250	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	22
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	20
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	20
212.25.102.57	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	18
2.54.140.198	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	18
206.12.10.245	Canada	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	17
31.154.241.34	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	16
93.172.137.250	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	16
46.116.210.160	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	16
46.121.60.65	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	16
37.142.1.172	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	16
192.187.124.251	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	15
109.66.81.237	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	15
80.246.130.247	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	15
84.109.243.141	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	14
149.88.78.117	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	14
79.183.103.32	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	14
79.182.18.193	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	14
93.172.54.219	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	14
84.111.156.183	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	14
5.29.134.238	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	13
82.166.61.181	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	13
79.176.151.243	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	13
79.180.58.97	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	13
183.60.217.62	China	147.237.76.31	nakchal.idf.il	DVRep_P-N_40-59	Permit	13
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
192.117.138.210	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	12
80.246.133.138	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	11

05-26-2015-00:00:02 to 05-27-2015-00:00:02

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.67.15	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	192
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	163
62.90.195.52	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	14
66.249.67.2	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	10
89.139.188.134	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	6
66.249.78.96	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	5
66.249.67.174	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	4
66.249.67.139	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.67.190	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.67.152	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	3
66.249.78.173	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	3
61.240.144.67	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	3
43.255.188.132	Japan	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	3
66.249.67.172	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	3
78.168.18.77	Turkey	147.237.77.216	dover.idf.il	INDICATOR-OBFUSCATION script tag in POST parameters - likely cross-site scripting	3
221.235.189.244	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.121	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.132	Japan	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.67	China	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	2
221.235.189.244	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.132	Japan	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.82	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
221.235.189.244	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.22	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
183.136.216.4	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	2
61.183.128.6	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	2
221.235.189.244	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
61.183.128.6	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	2
91.224.132.118	Russian Federation	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.67.53	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.64	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.132	Japan	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	2
221.235.189.244	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.132	Japan	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.65	China	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.67	China	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.130	Japan	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
221.235.189.244	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.66	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	2
66.102.6.210	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.28	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
221.235.189.244	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.67	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
217.160.165.219	Germany	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
221.235.189.244	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
183.136.216.4	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	2
91.224.132.118	Russian Federation	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.135	Japan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.65	China	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	2

05-26-2015-00:00:02 to 05-27-2015-00:00:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
81.218.13.69	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6766
212.179.46.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5182
212.179.159.253	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4141
213.151.32.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2681
89.139.188.134	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2028
80.74.103.31	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1762
212.179.61.124	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1692
85.250.85.71	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1660
46.19.85.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1655
2.54.16.200	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1584
212.179.21.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1314
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	845
213.57.182.110	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	843
95.86.78.65	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	799
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	795
80.246.133.251	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	757
213.57.9.5	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	636
37.60.41.141	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	561
212.179.61.127	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	560
213.204.103.36	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	521
95.86.72.174	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	502
213.204.104.34	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	447
2.54.186.127	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	414
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	370
213.57.128.231	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	334
37.142.11.62	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	331
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	324
213.8.119.129	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	311
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	308
185.46.214.66	Switzerland	147.237.72.167	ishurim.aka.idf.i	SAM rule	drop	drop	296
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	291
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	286
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	279
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	268
132.71.106.91	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	259
93.173.28.39	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	254
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	245
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	235
192.115.248.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	201
212.76.115.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	200
2.54.166.65	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	195
5.29.18.15	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	193
81.218.251.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	180
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	179
77.125.128.230	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	169
186.188.239.1	Panama	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	169
81.218.251.251	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	167
82.145.216.52	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	165
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	164
192.116.218.146	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	164

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.85.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	504
176.12.149.114	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.149.114	Block	212
87.68.61.252	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 87.68.61.252	Block	137
46.19.86.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	133
109.253.136.128	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.136.128	Block	123
46.19.86.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	122
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	119
46.19.85.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	91
46.19.86.27	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.27	Block	80
37.142.229.136	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.142.229.136	Block	78
85.250.94.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	71
2.54.171.241	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.171.241	Block	65
94.159.207.150	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	65
176.12.137.219	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.137.219	Block	61
212.179.155.129	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	45
109.253.136.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	43
176.12.149.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	35
80.178.157.40	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	33
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	25
109.66.177.225	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 109.66.177.225	Block	22
81.218.207.89	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	17
85.64.182.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
5.102.254.51	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
46.19.85.191	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
2.54.161.86	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	13
85.64.96.118	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	13
109.64.108.185	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12
62.219.142.181	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	12
85.64.85.117	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	11
2.52.173.187	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	10
112.74.75.173	China	147.237.77.176	matpash.idf.il	Multiple Admin Blocking from 112.74.75.173	Block	10
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	10
109.64.166.175	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	10
87.68.62.230	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
212.25.102.57	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/9/71529. jpg	Block	9
212.25.102.57	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/1/71531. jpg	Block	8
84.109.160.31	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
217.194.196.47	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	8
95.86.115.113	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
149.78.226.178	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 149.78.226.178	Block	7
91.200.12.130	Ukraine	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//894-he/chinuch.aspx	Block	6
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	6
85.65.90.15	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
37.60.41.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	6
62.90.159.249	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	6
109.253.130.122	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	6
212.25.102.57	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//sip_storage/files/9/71529. jpg	Block	6
188.120.133.128	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 188.120.133.128	Block	6
109.253.58.232	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	6
37.26.150.249	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	5