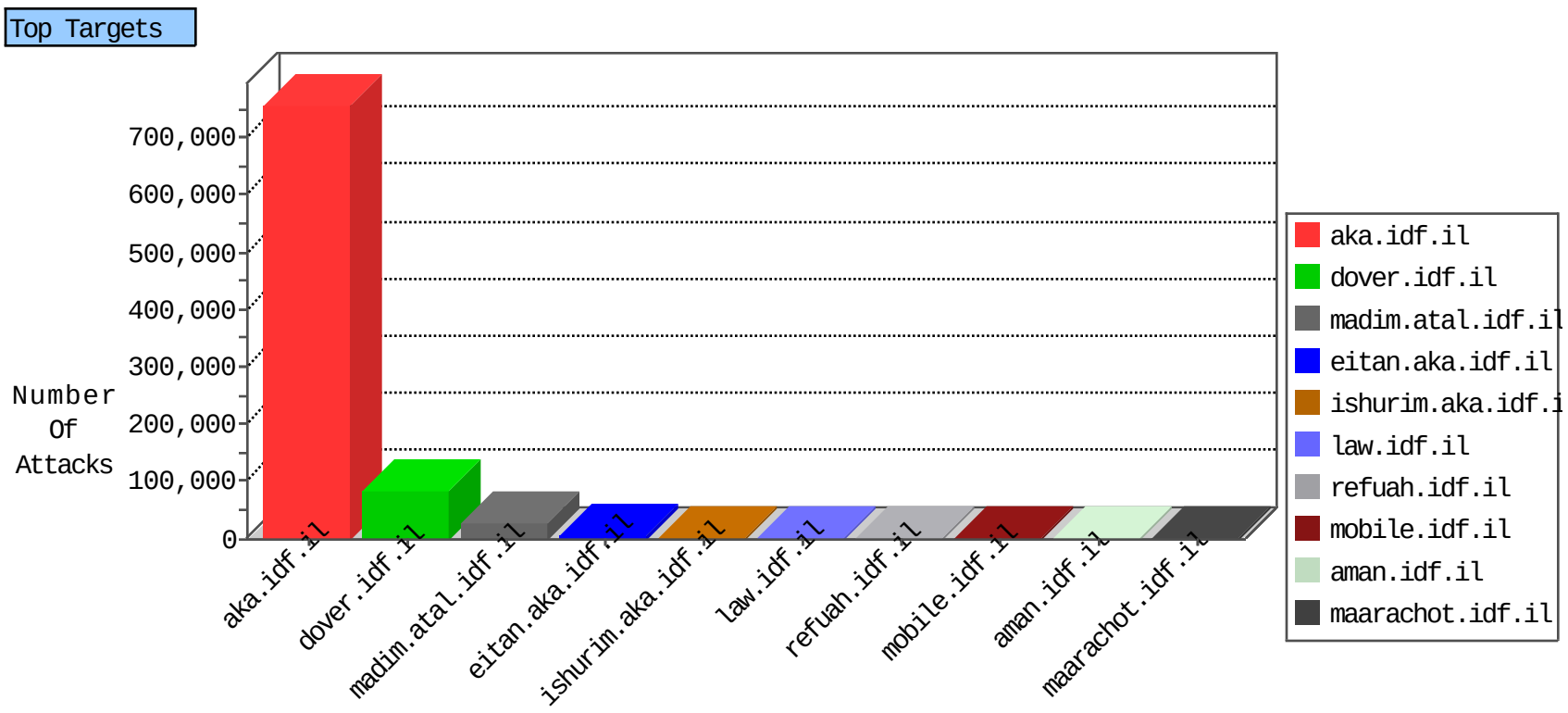
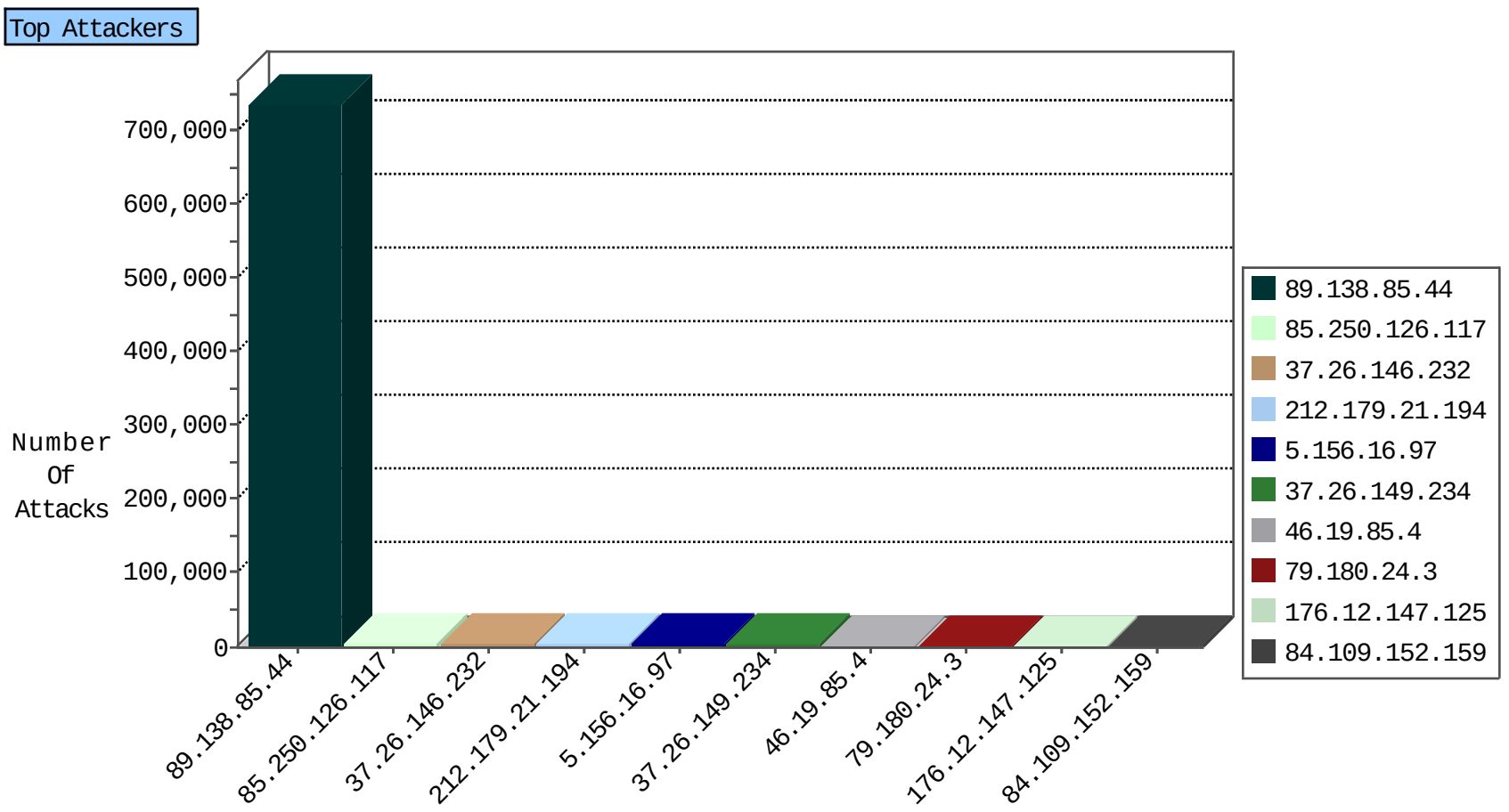
09-24-2015-00:00:03 to 09-25-2015-00:00:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-24-2015-00:00:03 to 09-25-2015-00:00:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.9	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	7388
66.249.78.160	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	6947
66.249.78.146	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4702
192.249.64.249	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3293
65.222.202.204	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2651
66.249.78.2	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1331
66.249.78.153	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1039
5.156.16.97	Romania	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	825
66.249.67.6	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	433
66.249.78.254	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	426
147.235.236.1	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	271
66.249.67.65	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	209
80.246.136.84	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	159
5.28.157.76	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	150
79.176.1.56	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	148
168.235.198.171	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	146
77.126.175.125	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	137
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	137
82.80.222.116	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	124
2.54.191.185	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	111
46.120.184.9	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	110
2.54.31.217	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	108
46.116.112.108	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	103
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	102
37.26.149.151	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	94
80.246.136.132	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	93
46.19.86.230	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	91
46.19.85.148	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	85
176.12.146.26	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	85
176.12.150.243	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	82
109.67.103.167	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	80
37.26.146.232	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	79
2.54.182.226	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	79
46.19.85.78	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	74
37.26.148.251	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	72
46.19.86.208	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	70
185.32.179.19	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	70
80.246.139.232	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	70
79.177.160.247	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	69
46.121.102.202	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	67
185.32.179.125	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	66
46.19.86.109	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	57
80.246.139.41	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	56
46.116.105.114	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	56
132.66.46.94	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	53
37.26.146.208	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	52
95.86.77.67	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	51
2.52.63.156	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	51
80.246.139.78	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	48
109.67.192.192	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	46

09-24-2015-00:00:03 to 09-25-2015-00:00:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.251.252	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	36
81.218.48.37	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	10
212.97.133.140	Denmark	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	7
81.218.155.169	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
213.179.60.10	United Kingdom	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
189.38.90.189	Brazil	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
178.210.160.50	Turkey	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
8.8.246.60	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
216.201.148.210	United States	147.237.77.233	atal.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	4
89.185.247.72	Czech Republic	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
74.84.136.105	United States	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
5.156.16.97	Romania	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	3
31.168.144.217	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
77.242.124.2	Netherlands	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	3
176.228.178.161	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
132.76.50.5	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
109.66.11.139	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
217.132.196.79	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
93.172.6.133	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
204.93.197.45	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	2
23.99.3.151	United States	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	2
106.38.241.118	China	147.237.77.233	atal.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
95.86.115.93	Israel	147.237.77.216	dover.idf.il	C091: HTTP: Access to - admin.asp	Block	1
204.102.229.130	United States	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
89.138.85.44	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
193.128.60.132	United Kingdom	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
46.19.85.154	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
136.243.5.87	Germany	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
98.142.212.37	United States	147.237.77.216	dover.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1
78.46.174.197	Germany	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
211.59.8.170	Korea, Republic of	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
182.184.69.100	Pakistan	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
14.176.3.232	Vietnam	147.237.77.74	law.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1
109.67.146.245	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
193.201.224.8	Ukraine	147.237.77.216	dover.idf.il	C1000196: HTTP: Block admin login to gov.il sites ?q=user	Block	1
62.210.225.135	France	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1
162.210.196.129	United States	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
106.38.241.118	China	147.237.76.42	refuah.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
183.80.159.188	Vietnam	147.237.77.216	dover.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1
23.99.3.101	United States	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1
128.69.42.161	Russian Federation	147.237.8.45	e.eitan.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1
62.210.225.135	France	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
173.48.141.204	United States	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
106.38.241.118	China	147.237.77.176	matpash.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
212.97.133.140	Denmark	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
188.116.38.101	Poland	147.237.77.216	dover.idf.il	C076: HTTP: Access to - action=... (General)	Block	1
128.69.42.161	Russian Federation	147.237.77.243	mobile.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1
95.52.37.173	Russian Federation	147.237.77.216	dover.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1
204.93.197.45	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

09-24-2015-00:00:03 to 09-25-2015-00:00:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	61
46.19.85.232	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	44
189.38.90.189	147.237.77.233	Brazil	atal.idf.il	SQL Injection - Select From	13
89.185.247.72	147.237.77.74	Czech Republic	law.idf.il	SQL Injection - Select From	12
213.179.60.10	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	12
206.72.113.4	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	10
212.97.133.140	147.237.76.42	Denmark	refuah.idf.il	SQL Injection - Select From	10
62.210.225.135	147.237.72.166	France	aka.idf.il	SQL Injection - Select From	9
204.93.197.45	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	9
74.84.136.105	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	7
66.249.78.160	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	6
178.210.160.50	147.237.77.233	Turkey	atal.idf.il	SQL Injection - Select From	6
8.8.246.60	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
216.201.148.210	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
188.165.246.177	147.237.77.216	France	dover.idf.il	SQL Injection - Select From	5
176.13.4.48	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
66.249.93.138	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	4
80.246.133.58	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
66.249.67.13	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
23.99.3.101	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	3
94.102.49.102	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN Potential SSH Scan	3
77.242.124.2	147.237.77.216	Netherlands	dover.idf.il	SQL Injection - Select From	3
46.116.24.30	147.237.77.74	Israel	law.idf.il	SERVER-APACHE Apache Byte-Range Filter denial of service attempt	3
59.106.108.116	147.237.77.216	Japan	dover.idf.il	Tehila - Perl LWP with fake user agent	2
103.54.202.74	147.237.77.227		e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.223	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sA (2)	2
106.120.201.115	147.237.77.243	China	mobile.idf.il	GPL SCAN nmap TCP	2
218.87.111.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	2
82.102.228.83	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	2
94.102.49.102	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential SSH Scan	2
218.87.111.117	147.237.8.27	China	e.madim.atal.idf.i	ET SCAN Potential SSH Scan	2
176.13.18.177	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
94.102.49.102	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN Potential SSH Scan	2
80.246.130.6	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
218.87.111.117	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	2
93.174.93.100	147.237.0.15	Netherlands	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	2
66.249.67.65	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
46.19.85.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
218.65.30.23	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2
218.87.111.117	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	2
66.249.67.53	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.178	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
218.87.111.117	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
68.180.228.112	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	2
66.249.64.153	147.237.77.74	United States	law.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)	2
66.249.78.127	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
103.54.202.74	147.237.72.156		aman.idf.il	ET SCAN Potential SSH Scan	2
218.65.30.23	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	2

09-24-2015-00:00:03 to 09-25-2015-00:00:03

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	4719
5.156.16.97	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3603
79.180.24.3	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2514
2.54.6.12	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1268
212.76.117.155	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1251
91.227.71.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1250
212.76.116.152	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1199
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1056
192.116.218.146	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1053
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	773
82.80.64.146	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	650
168.244.5.60	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	644
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	639
192.249.64.249	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	622
2.54.59.147	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	612
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	596
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	595
84.228.29.74	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	582
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	575
66.249.67.53	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	564
66.249.67.59	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	523
66.249.67.65	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	514
89.138.220.185	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	441
80.178.157.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	430
46.19.86.54	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	413
109.67.177.169	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	399
45.219.92.75	Uruguay	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	398
141.0.15.21	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	391
190.31.136.16	Argentina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	379
176.106.226.120	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	372
109.73.15.149	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	360
37.26.148.216	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	347
2.52.172.174	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	345
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	343
95.86.124.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	337
212.25.102.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	324
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	319
80.179.202.13	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	306
82.145.216.152	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	298
65.222.202.204	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	294
204.76.113.54	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	294
95.5.208.244	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	288
109.64.170.210	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
207.241.226.38	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	282
65.222.202.202	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	247
82.80.25.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	243
37.231.145.105	Kuwait	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	238
82.145.211.76	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	233
2.54.44.124	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	231
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	230

09-24-2015-00:00:03 to 09-25-2015-00:00:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.138.85.44	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	696586
89.138.85.44	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	39574
85.250.126.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6155
37.26.146.232	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.146.232	Block	5188
37.26.149.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3524
46.19.85.4	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.4	Block	2954
176.12.147.125	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.147.125	Block	2285
84.109.152.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2270
46.19.86.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1220
176.106.227.142	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.106.227.142	Block	1140
212.235.98.139	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1000
176.13.6.183	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.6.183	Block	859
37.26.149.192	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.149.192	Block	630
176.13.2.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	560
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	490
84.228.41.22	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 84.228.41.22	Block	411
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	360
132.72.64.219	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 132.72.64.219	Block	310
79.182.34.74	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 79.182.34.74	Block	240
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	220
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	220
176.12.143.159	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 176.12.143.159	Block	190
176.13.7.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	190
46.120.184.9	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.120.184.9	Block	180
79.182.175.204	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 79.182.175.204	Block	170
176.13.15.186	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	170
84.108.20.110	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	160
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.65	Block	130
216.113.24.1	Canada	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 216.113.24.1	Block	130
213.8.242.98	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 213.8.242.98	Block	110
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.168	Block	100
79.181.126.48	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 79.181.126.48	Block	90
82.166.22.142	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/www.tikshuv.idf.il	Block	90
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	90
46.19.85.141	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.141	Block	90
46.120.8.100	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	90
66.249.78.153	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	90
190.57.152.98	Ecuador	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 190.57.152.98	Block	90
79.181.126.48	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	77
196.219.163.49	Egypt	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/xmlrpc.php	Block	70
176.13.6.229	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 176.13.6.229	Block	70
77.125.7.229	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/resources/controls/captcha.ashx	Block	70
5.100.249.38	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.100.249.38	Block	70
87.68.167.106	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 87.68.167.106	Block	70
196.219.163.49	Egypt	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	70
82.166.22.206	Israel	147.237.72.167	ishurim.aka.idf.il	Too Many of the Same Response Code (404) in Session from 82.166.22.206	Block	70
89.138.85.44	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 89.138.85.44	Block	60
149.88.42.200	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	60
79.181.126.48	Israel	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	60
95.35.145.135	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtAreaRemarks in m.my-kosher-kravi.idf.il/templates/training/training.aspx	Block	60

09-24-2015-00:00:03 to 09-25-2015-00:00:03