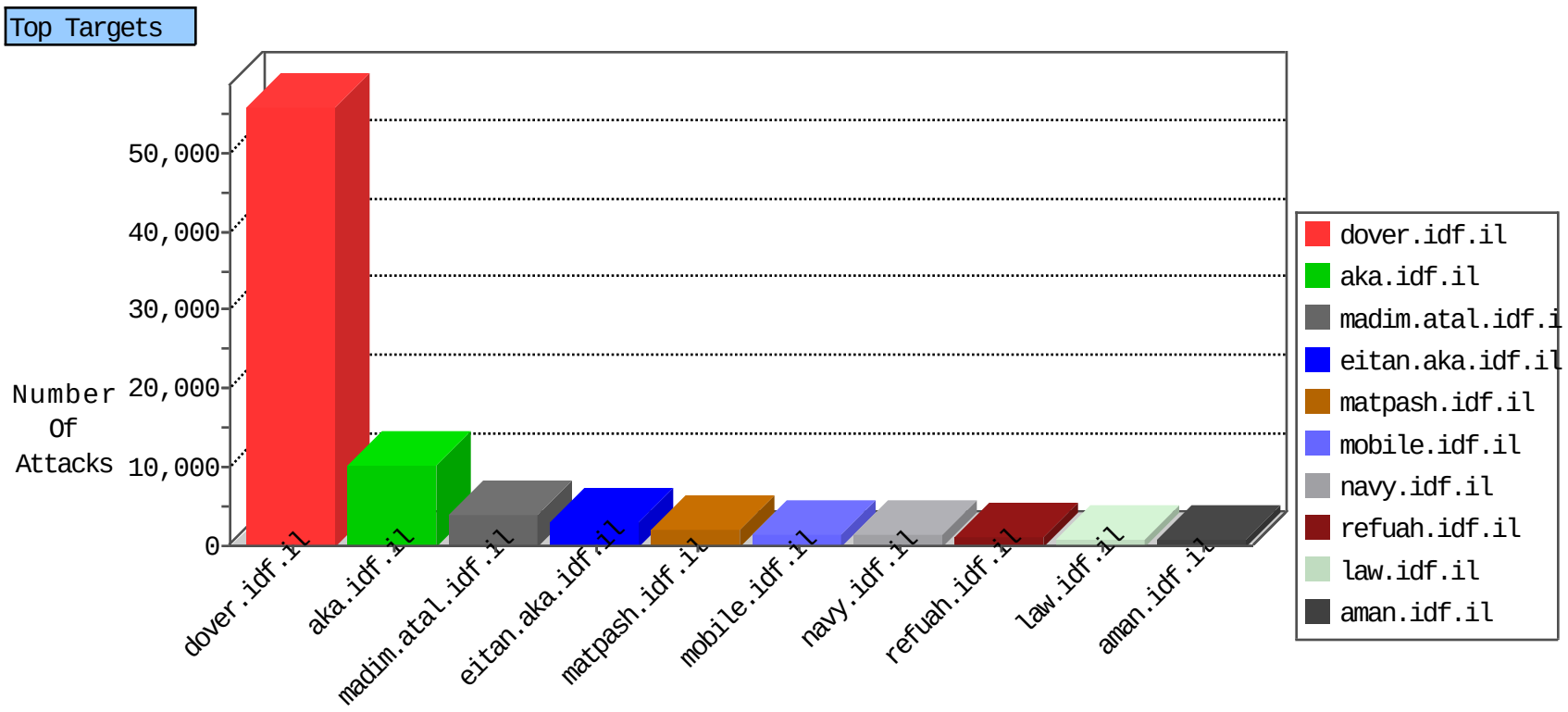
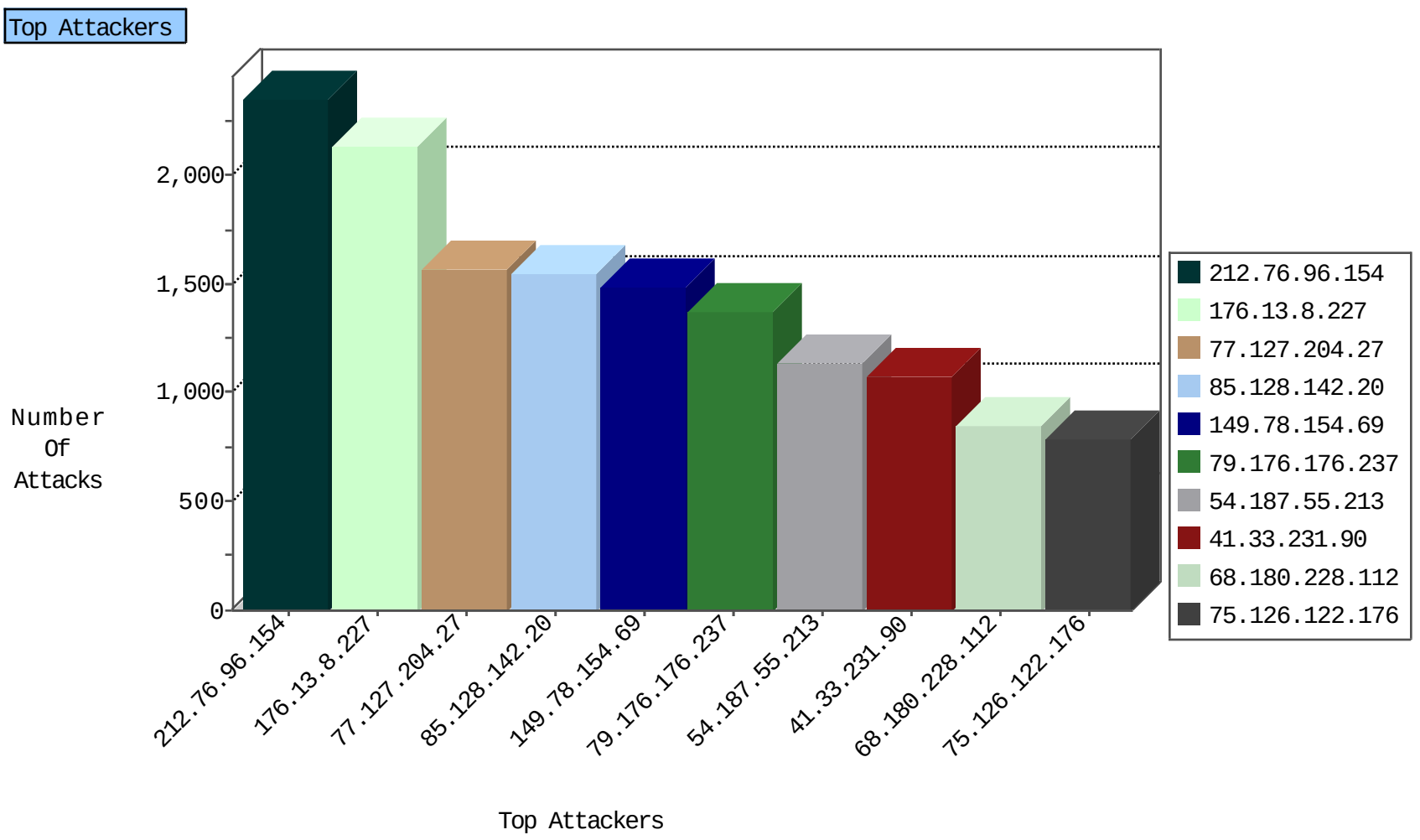
10-05-2015-00:00:03 to 10-06-2015-00:00:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-05-2015-00:00:03 to 10-06-2015-00:00:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.69.34	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	25078
66.249.69.42	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	22009
78.95.235.115	Romania	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	15603
83.250.115.140	Sweden	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10774
84.91.200.66	Portugal	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6528
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3685
66.249.64.102	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	2853
66.249.67.79	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2590
66.249.67.122	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1348
66.249.67.87	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1191
66.249.67.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	495
66.102.9.81	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	491
66.249.67.6	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	426
202.69.240.177	Hong Kong	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	263
66.102.9.91	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	153
66.102.9.101	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	77
66.249.64.235	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	72
5.22.129.175	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	67
37.26.146.176	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	66
84.228.26.51	Israel	147.237.77.243	mobile.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	63
2.54.61.67	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	45
5.22.129.189	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	43
31.210.186.132	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	36
2.54.17.169	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	35
100.100.74.158		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	34
46.19.85.125	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	31
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	29
149.78.18.187	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	29
83.44.150.26	Spain	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	24
10.0.0.1		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	22
62.238.195.85	Netherlands	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	20
109.65.116.157	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
37.26.149.132	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	18
149.202.42.188	Germany	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
79.181.6.101	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15
5.29.252.40	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
84.226.110.21	Switzerland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
2.52.188.233	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	11
46.19.86.72	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	11
192.168.126.166		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
87.68.68.58	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	9
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	9
31.154.91.165	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	8
62.90.94.72	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	8
2.54.29.251	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	8
46.19.86.116	Israel	147.237.72.156	aman.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	8
85.130.207.54	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	8
46.19.86.126	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
37.26.146.234	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	7

10-05-2015-00:00:03 to 10-06-2015-00:00:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.116.235.36	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	10
204.93.156.141	United States	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	5
37.61.201.161	Germany	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
94.102.153.58	United Kingdom	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
213.247.63.11	Netherlands	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
195.140.210.83	Germany	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
213.247.63.11	Netherlands	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
23.91.127.130	United States	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
198.143.164.7	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
23.91.127.130	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
200.59.205.238	Argentina	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
178.210.160.50	Turkey	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
94.73.145.90	Turkey	147.237.0.34	tikshuv.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	3
46.137.81.122	Ireland	147.237.76.86	navy.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	3
37.142.187.6	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
70.114.160.158	United States	147.237.76.86	navy.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	2
77.126.215.181	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
79.180.4.217	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
84.110.109.182	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
74.208.66.220	United States	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	2
23.91.122.62	United States	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	2
204.12.241.170	United States	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
82.145.24.68	Germany	147.237.0.34	tikshuv.idf.il	16797: HTTP: GNU Bash URI Parameter Remote Code Execution Vulnerability	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
23.91.122.62	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
91.121.211.59	France	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
77.126.21.100	Israel	147.237.76.200	eitan.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
94.179.177.69	Ukraine	147.237.77.216	dover.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1
2.91.164.61	Saudi Arabia	147.237.77.216	dover.idf.il	C091: HTTP: Access to - admin.asp	Block	1
82.145.24.68	Germany	147.237.77.216	dover.idf.il	16797: HTTP: GNU Bash URI Parameter Remote Code Execution Vulnerability	Block	1
91.237.221.221	Russian Federation	147.237.77.216	dover.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1
204.93.156.141	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
117.241.208.110	India	147.237.77.216	dover.idf.il	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	1
5.45.73.22	Netherlands	147.237.0.15	kosher-kravi.idf.i	16797: HTTP: GNU Bash URI Parameter Remote Code Execution Vulnerability	Block	1
82.145.24.68	Germany	147.237.77.234	halag.idf.il	16797: HTTP: GNU Bash URI Parameter Remote Code Execution Vulnerability	Block	1
70.114.160.158	United States	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
223.92.122.93	China	147.237.77.74	law.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
206.72.117.72	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1
5.45.73.22	Netherlands	147.237.77.74	law.idf.il	16797: HTTP: GNU Bash URI Parameter Remote Code Execution Vulnerability	Block	1
223.176.62.44	India	147.237.77.205	prisha.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
37.46.39.12	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
201.20.37.106	Brazil	147.237.77.170	maarachot.idf.il	16797: HTTP: GNU Bash URI Parameter Remote Code Execution Vulnerability	Block	1
94.73.145.90	Turkey	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
79.182.120.177	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
206.72.117.72	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
46.137.81.122	Ireland	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
188.165.251.13	France	147.237.76.86	navy.idf.il	16797: HTTP: GNU Bash URI Parameter Remote Code Execution Vulnerability	Block	1
84.229.32.194	Israel	147.237.72.156	aman.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
74.208.66.220	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

10-05-2015-00:00:03 to 10-06-2015-00:00:03

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	118
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	40
46.19.86.210	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	24
109.65.141.99	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	14
66.249.67.122	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	14
200.59.205.238	147.237.72.166	Argentina	aka.idf.il	SQL Injection - Select From	12
94.102.153.58	147.237.72.166	United Kingdom	aka.idf.il	SQL Injection - Select From	12
213.247.63.11	147.237.77.233	Netherlands	atal.idf.il	SQL Injection - Select From	12
213.247.63.11	147.237.77.74	Netherlands	law.idf.il	SQL Injection - Select From	12
66.249.67.6	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	10
66.249.67.13	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	10
204.93.156.141	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	8
37.26.147.161	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	8
23.91.127.130	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
74.208.66.220	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	6
94.73.145.90	147.237.0.34	Turkey	tikshuv.idf.il	SQL Injection - Select From	6
178.210.160.50	147.237.77.74	Turkey	law.idf.il	SQL Injection - Select From	6
46.137.81.122	147.237.76.86	Ireland	navy.idf.il	SQL Injection - Select From	6
195.140.210.83	147.237.77.233	Germany	atal.idf.il	SQL Injection - Select From	6
198.143.164.7	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
23.91.127.130	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	6
37.61.201.161	147.237.77.74	Germany	law.idf.il	SQL Injection - Select From	6
23.91.122.62	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	5
66.249.67.79	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	5
70.114.160.158	147.237.76.86	United States	navy.idf.il	SQL Injection - Select From	5
182.100.67.4	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	4
31.184.242.17	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	4
66.249.78.137	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	4
182.100.67.4	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	4
182.100.67.4	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	4
182.100.67.4	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	3
66.249.67.67	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
182.100.67.4	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	2
82.117.208.243	147.237.72.167		ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	2
46.19.85.15	147.237.77.216	Israel	dover.idf.il	ET SCAN NMAP -sA (2)	2
193.107.17.72	147.237.76.177	Seychelles	ncore.idf.il	ET SCAN NMAP -sS window 1024	2
199.203.59.121	147.237.77.61	Israel	e.cogat.idf.il	ET SCAN Potential SSH Scan	2
61.94.145.124	147.237.77.212	Indonesia	e.dover.idf.il	ET SCAN Potential SSH Scan	2
182.100.67.4	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	2
116.110.81.253	147.237.8.27	Vietnam	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	2
182.100.67.4	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
116.110.81.253	147.237.0.33	Vietnam	idf.il	ET SCAN Potential SSH Scan	2
199.203.59.121	147.237.72.14	Israel	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
182.100.67.4	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	2
66.249.93.200	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
182.100.67.4	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	2
66.249.67.91	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
208.123.65.20	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	2
182.100.67.4	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	2
218.87.111.117	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	2

10-05-2015-00:00:03 to 10-06-2015-00:00:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.76.96.154	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2356
85.128.142.20	Poland	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1540
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1483
79.176.176.237	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1378
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1130
70.26.59.159	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	740
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	610
77.127.204.27	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	588
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	501
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	492
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	490
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	489
46.19.85.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	481
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	476
89.108.144.114	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	446
77.126.21.100	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	435
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	414
79.177.151.183	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	405
149.88.88.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	362
66.249.69.42	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	358
66.249.69.26	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	336
89.138.220.185	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	330
66.249.69.34	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	326
81.17.31.214	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	305
77.125.75.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	304
2.54.138.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	302
199.200.25.52	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	298
109.64.13.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	291
2.54.45.51	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	290
37.26.146.161	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	282
81.214.196.212	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	281
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	273
77.126.37.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	246
213.151.51.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	239
37.8.43.72	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	238
37.236.104.36	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	236
52.0.53.79	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	220
77.126.233.181	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	219
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	214
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	214
109.66.113.149	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	207
70.162.126.16	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	203
85.64.133.121	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	203
109.66.105.189	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	196
85.91.84.254	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	195
66.249.64.178	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	194
66.249.64.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	190
166.137.126.123	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	190
157.55.39.55	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	185
207.46.13.166	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	185

10-05-2015-00:00:03 to 10-06-2015-00:00:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.8.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2141
77.127.204.27	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 77.127.204.27	Block	966
176.12.145.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	704
87.68.250.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	539
75.126.122.176	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	462
46.19.86.105	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.105	Block	440
31.154.145.40	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	418
75.126.122.176	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	330
72.9.148.10	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	242
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	209
46.117.184.2	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.117.184.2	Block	187
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	164
37.142.64.64	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Email in mobile.idf.il/sachar/createaccount	Block	143
188.76.156.172	Spain	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 188.76.156.172	Block	132
149.88.227.152	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 149.88.227.152	Block	132
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.42	Block	132
31.154.145.40	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	127
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.173	Block	110
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.178	Block	110
2.91.164.61	Saudi Arabia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 2.91.164.61	Block	88
66.249.69.34	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.34	Block	88
66.249.79.25	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	88
46.229.164.99	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.229.164.99	Block	77
81.17.31.214	Switzerland	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	77
176.106.227.209	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	77
46.229.164.98	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.229.164.98	Block	66
77.125.162.162	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	66
178.150.15.158	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	66
2.91.164.61	Saudi Arabia	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 2.91.164.61	Block	55
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	55
178.150.15.158	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 178.150.15.158	Block	55
173.236.176.119	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 173.236.176.119	Block	55
46.19.85.66	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	55
46.120.184.9	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.120.184.9	Block	55
66.249.64.154	Israel	147.237.76.147	chinuch.aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	55
46.19.85.66	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	55
184.106.66.76	United States	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 184.106.66.76	Block	55
2.91.164.61	Saudi Arabia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	55
74.208.16.114	United States	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 74.208.16.114	Block	44
79.176.170.187	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	44
79.178.214.152	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	44
66.249.64.154	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	44
157.55.39.20	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	44
109.64.182.235	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	44
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	44
109.65.116.157	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	44
109.160.142.20	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.160.142.20	Block	44
77.126.166.204	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	44
66.249.79.25	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	33
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/5/size220x0/17175.jpg	Block	33

10-05-2015-00:00:03 to 10-06-2015-00:00:03