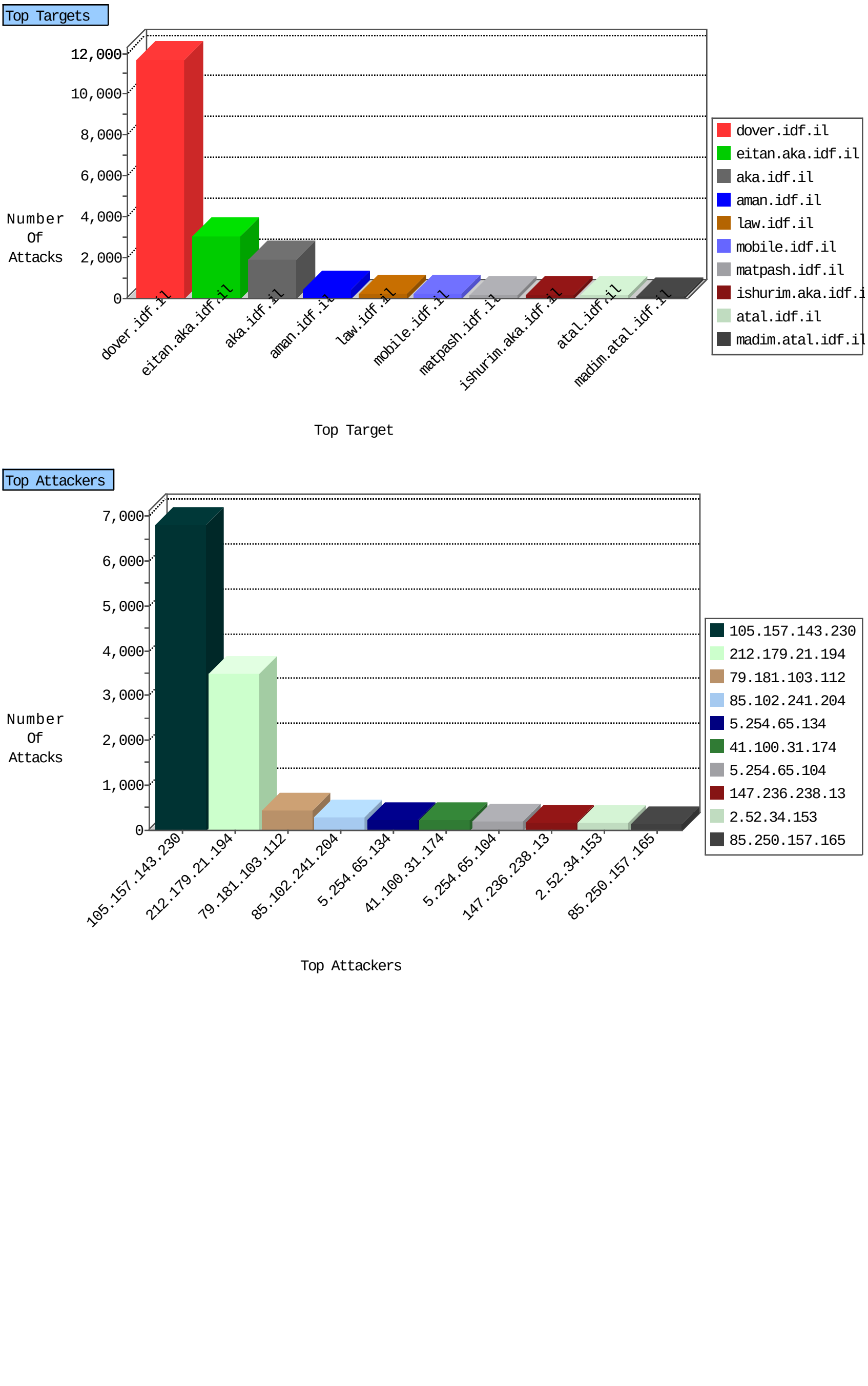
10-29-2015-13:04:07 to 10-29-2015-14:04:07

IDF Under Attack Daily Report



10-29-2015-13:04:07 to 10-29-2015-14:04:07

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	340
79.177.157.33	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	52
109.67.108.108	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	34
2.54.56.61	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	32
194.149.247.24	Germany	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	31
109.64.210.116	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
37.26.146.135	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	30
2.54.51.152	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
2.54.181.47	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	24
185.32.179.55	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
85.102.241.204	Turkey	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
185.32.179.11	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	16
37.26.148.174	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	16
176.13.22.230	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
46.116.206.159	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
177.68.5.229	Brazil	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
132.66.40.116	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
46.19.85.169	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	11
85.102.241.204	Turkey	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
132.68.26.53	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
46.19.86.100	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
5.254.65.134	Romania	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
37.26.146.236	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
85.102.241.204	Turkey	147.237.77.216	dover.idf.il	Web-etc/passwd-Dir-Traversal	dest-reset	10
37.26.146.236	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
85.65.129.103	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
184.163.16.94	Canada	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
80.246.140.247	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	8
46.120.92.244	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
2.54.163.162	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
37.26.149.182	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
2.54.33.225	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
212.25.102.63	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
85.102.241.204	Turkey	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
194.149.247.24	Germany	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
176.13.9.253	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	6
46.19.86.119	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	6
149.78.206.109	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
82.81.33.56	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
5.102.254.174	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
46.210.215.146	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5
212.25.85.234	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.16.239	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
185.40.192.78	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
5.29.195.98	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
46.19.86.154	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.13.9.253	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
80.246.136.134	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	5

10-29-2015-13:04:07 to 10-29-2015-14:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.102.241.204	Turkey	147.237.77.216	dover.idf.il	2809: HTTP: IIS TRACK Method	Block	2
192.115.252.2	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
85.102.241.204	Turkey	147.237.77.216	dover.idf.il	3909: HTTP: Cross Site Scripting (Alert function)	Block	1
115.42.137.250	Singapore	147.237.77.216	dover.idf.il	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	1

10-29-2015-13:04:07 to 10-29-2015-14:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
85.102.241.204	147.237.77.216	Turkey	dover.idf.il	SERVER-WEBAPP client negative Content-Length attempt	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
79.181.38.176	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.102.241.204	147.237.77.216	Turkey	dover.idf.il	SERVER-WEBAPP PHP-CGI remote file include attempt	1
77.125.248.50	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.102.241.204	147.237.77.216	Turkey	dover.idf.il	GPL EXPLOIT php.cgi access	1
37.142.174.186	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.102.241.204	147.237.77.216	Turkey	dover.idf.il	ET WEB_SERVER safe_mode PHP config option in uri	1
37.26.149.219	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.102.241.204	147.237.77.216	Turkey	dover.idf.il	ET WEB_SERVER disable_functions PHP config option in uri	1
2.54.161.123	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.102.241.204	147.237.77.216	Turkey	dover.idf.il	ET WEB_SERVER allow_url_include PHP config option in uri	1
85.65.129.103	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.248	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
109.160.172.104	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.175.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.126.161.202	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.102.241.204	147.237.77.216	Turkey	dover.idf.il	SERVER-APACHE Apache SSI error page cross-site scripting	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
85.102.241.204	147.237.77.216	Turkey	dover.idf.il	ET WEB_SERVER suhosin.simulation PHP config option in uri	1
37.26.149.223	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.102.241.204	147.237.77.216	Turkey	dover.idf.il	ET WEB_SERVER open_basedir PHP config option in uri	1
5.254.65.134	147.237.77.216	Romania	dover.idf.il	portscan: TCP Distributed Portscan	1
85.102.241.204	147.237.77.216	Turkey	dover.idf.il	ET WEB_SERVER auto_prepend_file PHP config option in uri	1
85.102.241.204	147.237.77.216	Turkey	dover.idf.il	ET SCAN Apache mod_proxy Reverse Proxy Exposure 2	1
84.111.114.40	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
163.53.247.3	147.237.72.166	Macau	aka.idf.il	ET SCAN NMAP -sS window 1024	1
80.74.125.21	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.102.241.204	147.237.77.216	Turkey	dover.idf.il	SERVER-WEBAPP php.cgi access	1

10-29-2015-13:04:07 to 10-29-2015-14:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
105.157.143.230	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6205
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	355
85.102.241.204	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	204
2.52.34.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	175
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	103
5.254.65.104	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	78
46.28.109.163	Czech Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	73
5.254.65.134	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
37.26.146.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
173.220.141.227	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
46.120.196.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
132.64.9.118	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
2.54.167.104	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38
81.215.214.181	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
2.54.138.28	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
105.157.143.230	Morocco	147.237.77.216	dover.idf.il	drop		drop	34
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
77.57.181.13	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
185.40.192.78	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
79.180.203.51	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
46.19.85.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.160.149.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
77.125.139.27	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
132.68.26.53	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
188.225.171.198	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
212.25.102.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
2.54.168.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
2.54.138.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
66.249.82.94	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
66.249.64.195	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
192.115.252.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
46.19.85.169	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
80.246.136.134	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
84.94.96.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
209.112.242.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
46.19.86.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
37.142.113.168	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17

10-29-2015-13:04:07 to 10-29-2015-14:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 212.179.21.194	Block	2985
105.157.143.230	Morocco	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 105.157.143.230	Block	557
79.181.103.112	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	225
79.181.103.112	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	219
147.236.238.13	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	135
41.100.31.174	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.100.31.174	Block	135
5.254.65.134	Romania	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.254.65.134	Block	105
2.52.191.7	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	90
85.250.157.165	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	75
5.254.65.204	Romania	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/navy/html/toolfs.asp	Block	75
85.250.157.165	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	75
66.249.64.200	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.200	Block	60
192.117.176.130	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized HTTP Method	Block	60
32.211.76.83	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	59
192.117.176.130	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 192.117.176.130	Block	45
79.178.23.41	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/ajax/updatestatus.php	Block	45
188.225.171.74	Palestinian Territory Occupied	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/657-he/patzar.aspx	Block	45
147.236.238.13	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/4/	Block	45
79.180.15.61	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	45
212.179.21.194	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	45
79.178.23.41	Israel	147.237.72.156	aman.idf.il	PHP Attempt	Block	45
212.179.21.194	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/6/size338x0/1686.jpg	Block	30
66.249.64.195	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.195	Block	30
93.174.93.218	Netherlands	147.237.77.74	law.idf.il	Multiple Illegal Byte Code Character in Method from 93.174.93.218	Block	30
5.254.65.104	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation d in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	30
80.246.139.116	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	30
41.100.31.174	Algeria	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 41.100.31.174	Block	30
5.254.65.134	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation d in www.idf.il/webresource.axd	Block	30
2.52.6.73	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	30
66.249.69.51	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	30
93.174.93.218	Netherlands	147.237.77.74	law.idf.il	Multiple NULL Character in Method from 93.174.93.218	Block	30
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	30
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.190	Block	30
149.88.113.61	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 149.88.113.61	Block	30
5.29.46.33	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	30
85.65.220.87	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	30
149.88.113.61	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	30
5.29.46.33	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	30
46.19.85.73	Israel	147.237.77.176	matpash.idf.il	Distributed Unknown HTTP Request Method	Block	30
62.90.221.127	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/moblie	Block	15
176.13.16.182	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	15
5.254.65.104	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation Language in www.idf.il/shared/ajax/getemergencybanner.aspx	Block	15
2.54.23.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	15
67.55.87.68	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	15
46.19.85.73	Israel	147.237.77.176	matpash.idf.il	Multiple Malformed URL from 46.19.85.73	Block	15
41.100.31.174	Algeria	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	15
66.249.64.238	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/shared/usercontrols/navmenu/	Block	15
5.254.65.134	Romania	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	15
85.102.241.204	Turkey	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	15
66.249.64.165	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	15

10-29-2015-13:04:07 to 10-29-2015-14:04:07