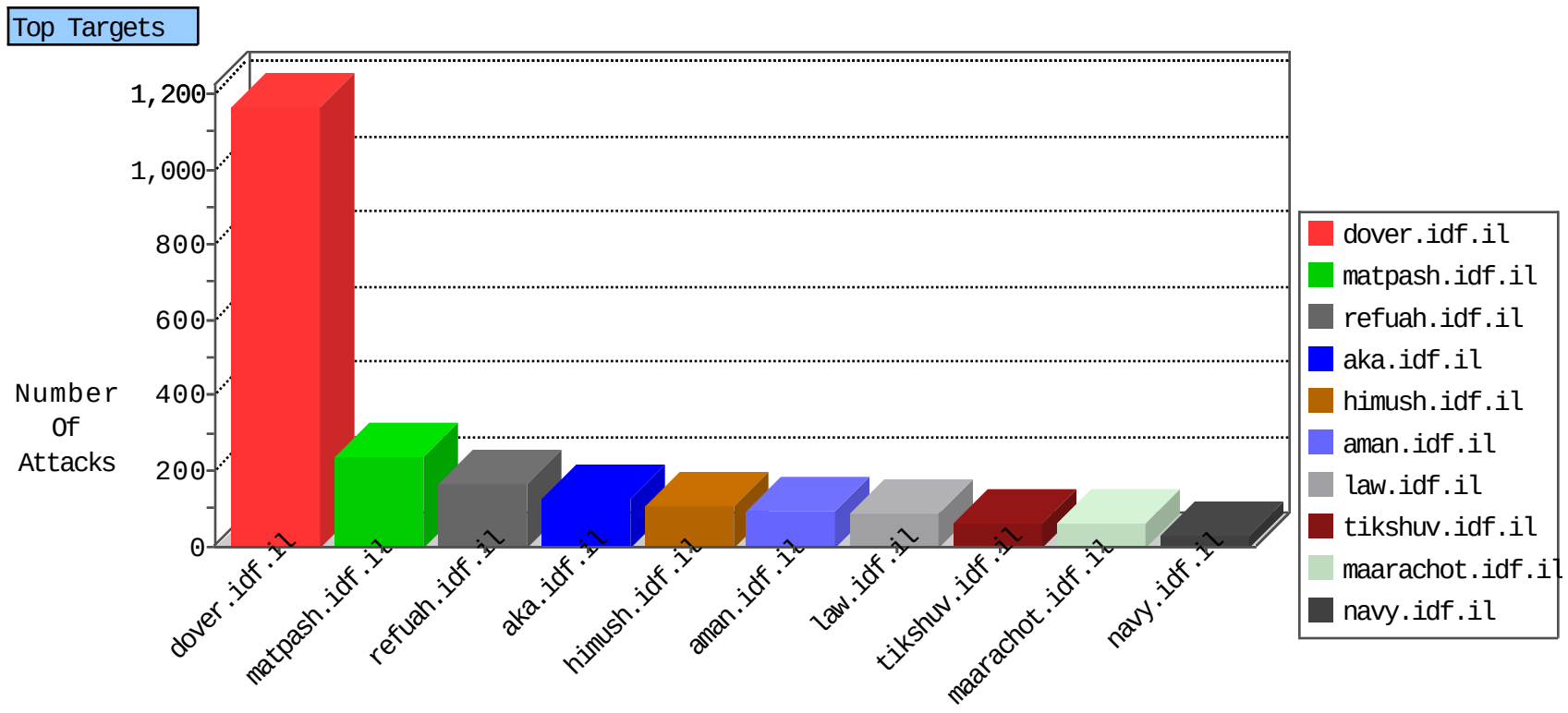
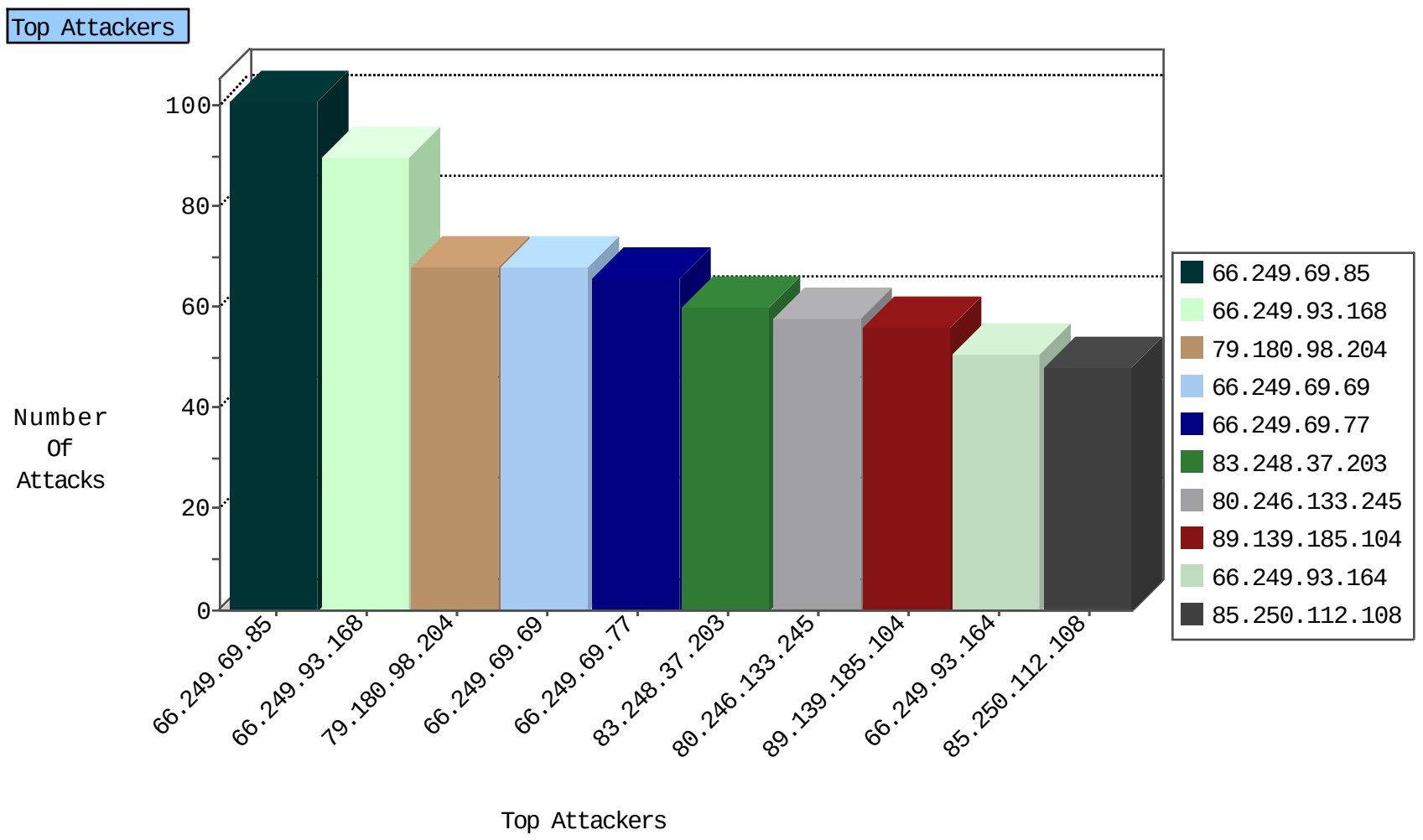
04-11-2015-15:03:04 to 04-11-2015-16:03:04

IDF Under Attack
04-11-2015-15:03:04

Top Targets



Top Attackers



04-11-2015-15:03:04 to 04-11-2015-16:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
79.180.98.204	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	838
213.204.101.34	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	288
66.249.69.85	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	101
84.110.60.143	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	78
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	69
66.249.69.69	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	68
66.249.69.77	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	66
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	51
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	31
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	31
66.249.69.87	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	27
66.249.67.99	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	25
66.249.67.107	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	25
66.249.67.108	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	25
66.249.67.115	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	24
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	23
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	22
66.249.93.168	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	21
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	18
66.249.93.172	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	18
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	17
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	17
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	16
66.249.69.93	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	14
66.249.67.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	14
66.249.78.174	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	14
66.249.67.100	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	13
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	13
66.249.67.116	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	12
66.249.67.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	12
66.249.67.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	11
66.249.69.95	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	10
66.249.93.176	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	9
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	9
66.249.78.167	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	8
66.249.78.160	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	8
66.249.69.79	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	7
66.249.78.60	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	7
66.249.78.248	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	7
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	7
66.249.69.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
82.102.141.250	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	6
66.249.78.93	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	6
66.249.78.134	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	6
66.249.93.204	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	5
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	5
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	5
66.249.69.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5
66.249.78.141	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	5
66.249.69.105	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	4

04-11-2015-15:03:04 to 04-11-2015-16:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
74.208.173.18	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
89.139.185.104	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
5.29.197.57	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
41.107.196.128	Algeria	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
213.57.34.54	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
80.246.139.100	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
2.54.190.158	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-11-2015-15:03:04 to 04-11-2015-16:03:04

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
218.77.79.43	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.130	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
206.117.7.4	United States	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
58.20.54.249	China	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
110.173.177.37	India	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 4096	1
101.226.2.99	China	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 4096	1
91.231.192.149	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
61.240.144.67	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.130	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
208.80.155.146	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
60.18.162.244	China	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
110.173.177.37	India	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
101.226.2.99	China	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
83.248.37.203	Sweden	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.67	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1

04-11-2015-15:03:04 to 04-11-2015-16:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
89.139.185.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	54
85.250.112.108	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
83.248.37.203	Sweden	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	47
46.19.85.168	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
80.246.133.245	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.144.15	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
49.98.139.92	Japan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
80.246.133.245	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
85.65.101.18	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
82.166.130.46	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
37.39.83.42	Kuwait	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
46.19.86.130	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
46.117.102.80	Israel	147.237.76.30	himush.idf.il	Invalid ACK number	Bad TCP sequence	monitor	18
211.30.236.90	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
213.204.101.34	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
85.65.32.11	Israel	147.237.0.34	tikshuv.idf.i	Invalid ACK number	Bad TCP sequence	monitor	14
149.78.176.225	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
94.249.78.24	Jordan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
157.55.39.114	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
79.179.63.160	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	13
46.117.102.80	Israel	147.237.76.30	himush.idf.il	Invalid ACK number	Bad TCP sequence	alert	13
157.55.39.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
84.108.120.132	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
89.138.72.165	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
64.233.172.155	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
73.213.111.189	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
109.253.139.230	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
77.127.246.205	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
157.55.39.6	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
46.117.44.170	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
77.125.116.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
37.142.10.254	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.117.102.80	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
220.255.1.24	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
220.255.1.62	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
79.183.198.204	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
83.248.37.203	Sweden	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
83.248.37.203	Sweden	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	5
93.172.131.96	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
188.120.133.91	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
46.121.244.146	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.86.220	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
208.80.155.146	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
79.181.50.3	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4

04-11-2015-15:03:04 to 04-11-2015-16:03:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.9.214	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
46.4.68.142	Germany	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 46.4.68.142	Block	3
173.93.238.175	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 173.93.238.175	Block	3
79.177.194.48	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.172	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
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	2
149.78.152.221	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	2
37.142.13.18	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.42	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.42	Block	1
84.109.36.206	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
207.46.13.79	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.186.145.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
79.179.63.160	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 79.179.63.160	Block	1
157.55.39.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/info06.stm	Block	1
84.228.201.216	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/tfasim.aspx	None	1
207.46.13.82	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/april/15.stm	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/home.asp/info.asp	Block	1
111.252.211.64	Taiwan	147.237.77.216	dover.idf.il	Unknown HTTP Request Method COOK in URL www.idf.il/1116-en/dover.aspx	Block	1
79.182.13.219	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
46.4.68.142	Germany	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/templates/homepage/404.aspx	Block	1
173.93.238.175	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm	Block	1
157.55.39.55	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
85.65.35.108	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/miluim/login.aspx	None	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Unknown Parameter m in www.aka.idf.il/main/drushim/drushim/general.aspx	None	1
125.25.12.245	Thailand	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
79.182.129.47	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
46.117.83.50	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
89.139.10.48	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
73.213.111.189	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
157.55.39.153	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/navy/flotilla2.stm	Block	1
84.108.210.49	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
188.120.148.136	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
46.121.244.146	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/chamatz/miktzoa/default.asp	None	1
109.186.145.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1

04-11-2015-15:03:04 to 04-11-2015-16:03:04