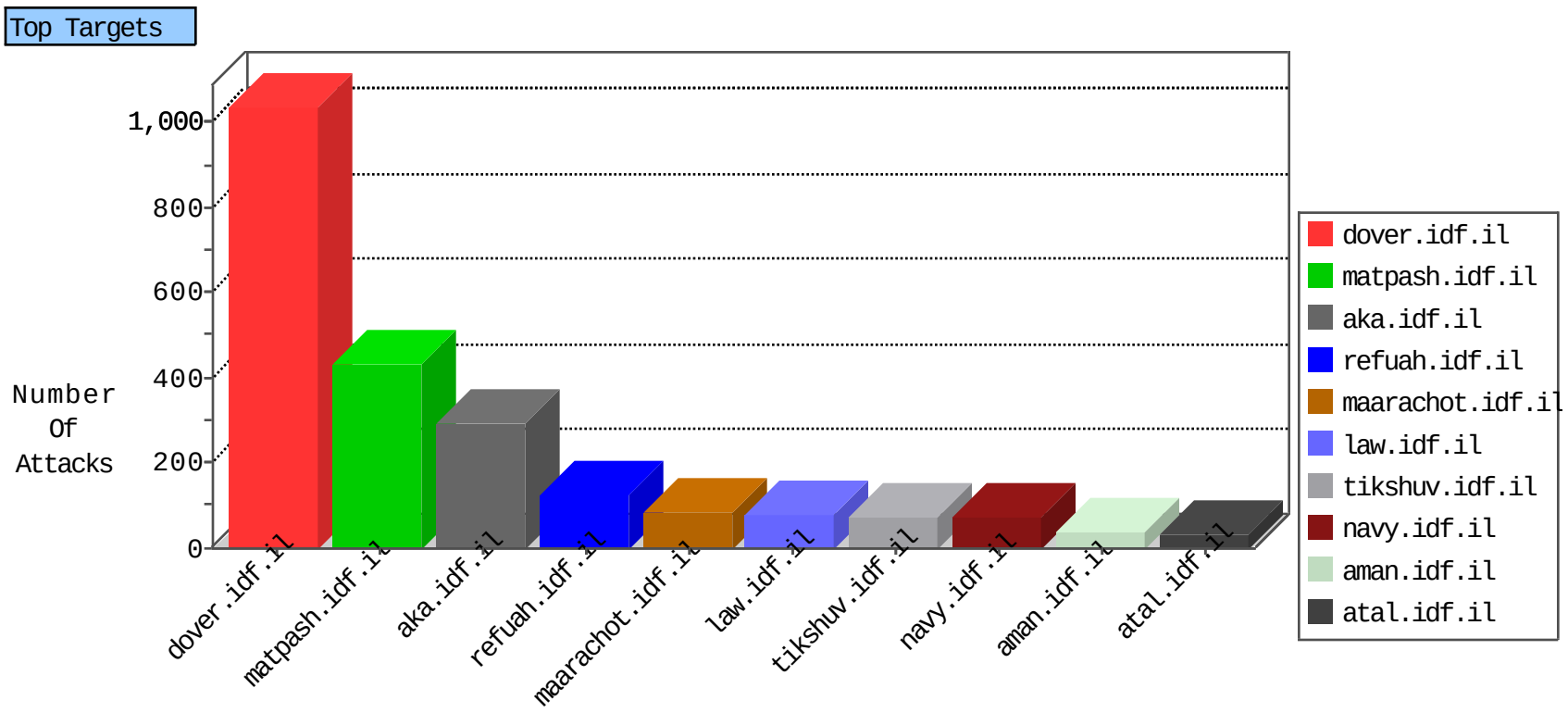
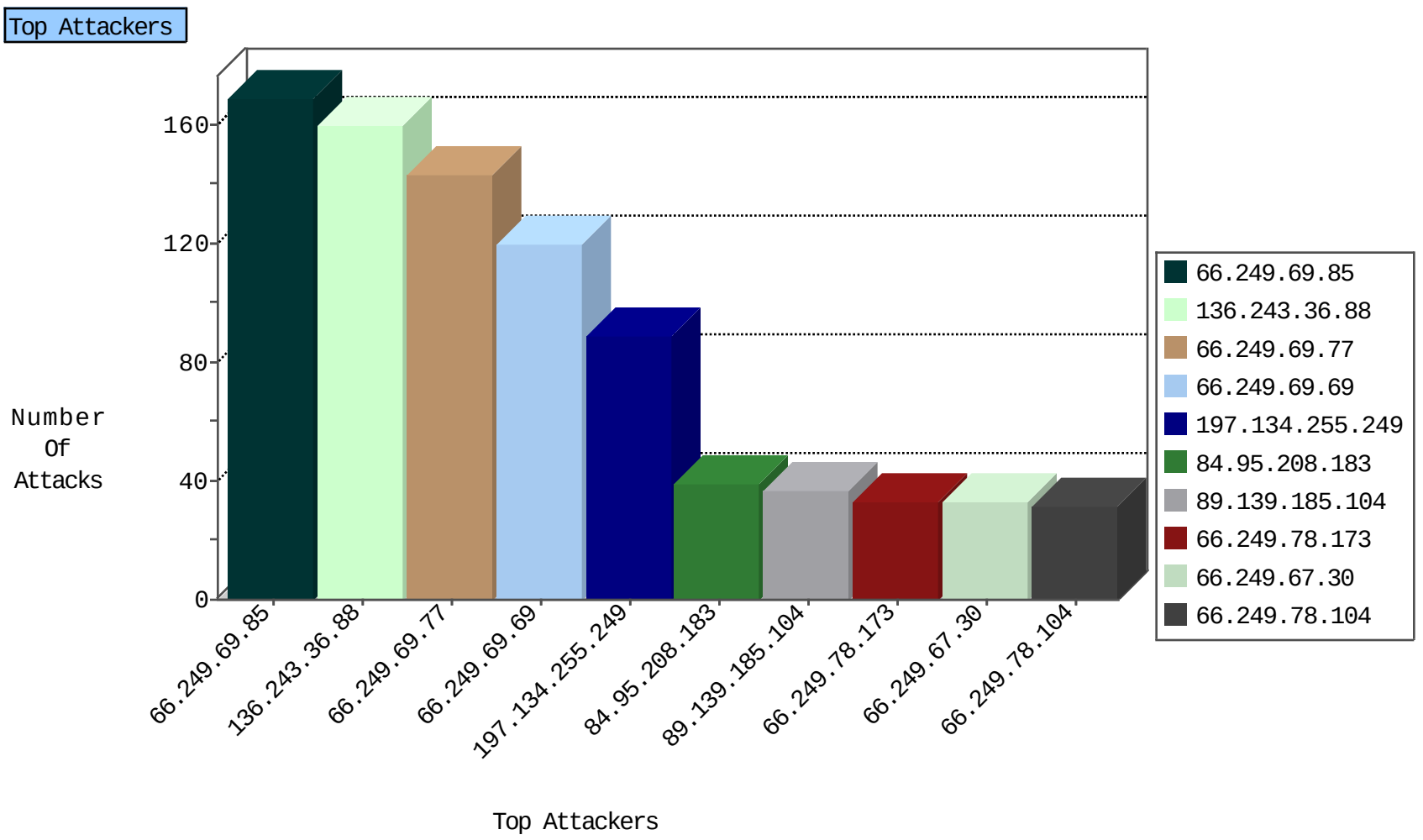
04-11-2015-00:03:09 to 04-11-2015-01:03:09

IDF Under Attack
04-11-2015-00:03:09

Top Targets



Top Attackers



04-11-2015-00:03:09 to 04-11-2015-01:03:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.120	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	431
220.181.108.96	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	372
79.181.96.218	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	234
149.78.6.214	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	196
66.249.69.85	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	169
66.249.69.77	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	142
66.249.69.69	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	117
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	33
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	33
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	31
66.249.67.108	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	27
66.249.78.160	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	26
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	24
66.249.69.87	United States	147.237.0.34	tikshuv.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	19
66.249.69.95	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	18
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	17
66.249.69.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	17
66.249.67.14	United States	147.237.76.86	navy.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
66.249.78.174	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	16
66.249.67.116	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	14
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	14
66.249.78.167	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	14
66.249.69.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	13
66.249.69.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.69.105	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	12
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	12
66.249.78.60	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	12
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	11
66.249.67.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	11
66.249.69.93	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.78.86	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	11
66.249.93.242	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.69.79	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	9
66.249.67.100	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	9
66.249.78.236	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	9
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	9
66.249.69.109	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.69.89	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	8
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	8
66.249.78.242	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	8
66.249.67.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	7
66.249.67.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	7
66.249.69.62	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	6
109.186.154.185	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
66.249.89.105	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
66.249.69.97	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	5
66.249.93.245	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

04-11-2015-00:03:09 to 04-11-2015-01:03:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
37.130.227.133	United Kingdom	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	2
165.215.209.15	United States	147.237.77.216	dover.idf.il	14511: HTTP: Win32/Oliga Fake User Agent	Permit	1
41.47.77.232	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.117.239.121	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
88.182.94.184	France	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
37.26.146.225	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-11-2015-00:03:09 to 04-11-2015-01:03:09

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	7
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
208.80.155.146	United States	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	2
109.67.81.70	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.29.81.223	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.163	Japan	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
128.199.254.26	Singapore	147.237.72.166	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
43.255.191.163	Japan	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
101.226.2.99	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.163	Japan	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
222.186.34.242	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
101.226.2.99	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
91.217.90.49	Ukraine	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
222.186.34.242	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1

04-11-2015-00:03:09 to 04-11-2015-01:03:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
136.243.36.88	Germany	147.237.72.166	aka.idf.il	SAM rule	drop	drop	159
197.134.255.249	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	89
84.95.208.183	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
89.139.185.104	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
77.126.237.125	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
212.179.21.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
2.54.130.97	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
46.19.85.238	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
155.201.35.153	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
46.19.85.177	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
62.219.154.139	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
79.182.126.92	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
79.180.19.188	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
176.61.121.186	Ireland	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
77.127.91.107	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
109.65.112.210	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
79.179.126.122	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
157.55.39.114	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
62.219.154.129	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
109.253.140.244	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
62.219.154.133	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
54.234.145.80	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
134.191.232.70	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
109.186.154.185	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
157.55.39.114	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
80.246.133.199	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
79.176.104.190	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
212.25.102.182	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
157.55.39.42	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
5.29.46.18	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
201.6.219.71	Brazil	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
79.180.123.43	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
157.55.39.42	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
46.116.252.164	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
109.253.138.224	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
31.193.51.59	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
184.33.59.160	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
157.55.39.6	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
85.65.185.11	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
134.191.232.71	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
104.173.222.159		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6

04-11-2015-00:03:09 to 04-11-2015-01:03:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
65.49.17.2	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 65.49.17.2	Block	5
46.117.24.91	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/5/	Block	3
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
5.29.81.223	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
84.94.47.91	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/payslips.aspx	None	1
5.79.16.135	United Kingdom	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
93.173.244.22	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
46.117.24.91	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.117.24.91	Block	1
207.46.13.82	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/homefront/magen1.stm	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1125-2.stm	Block	1
104.131.217.26		147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Untraceable SSL Sessions from 104.131.217.26 (Unknown Server Certificate)	None	1
104.131.217.26		147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
46.117.30.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	1
77.125.87.134	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/	Block	1
109.66.146.233	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$txtSearch in www.aka.idf.il/main/sachar/	None	1
46.119.120.118	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/+	Block	1

04-11-2015-00:03:09 to 04-11-2015-01:03:09