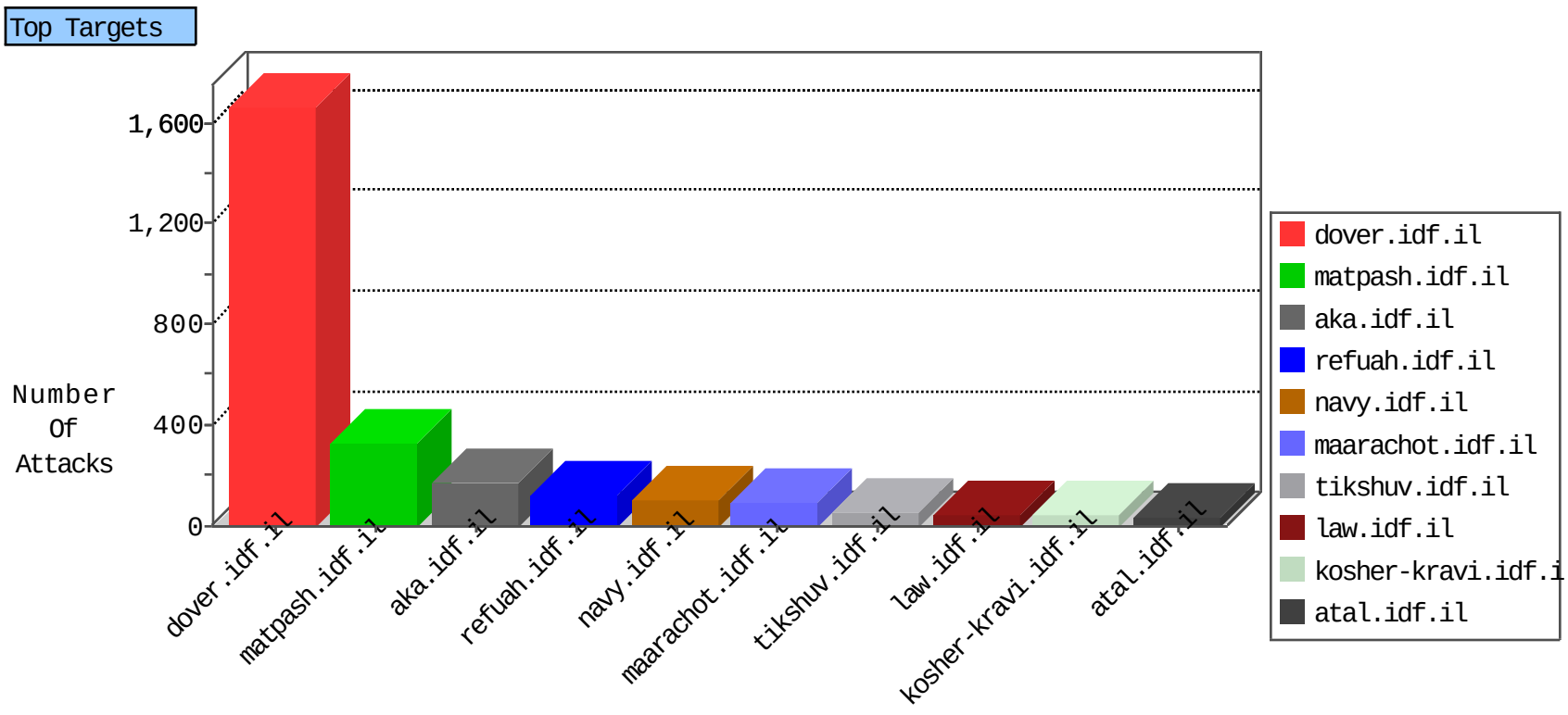
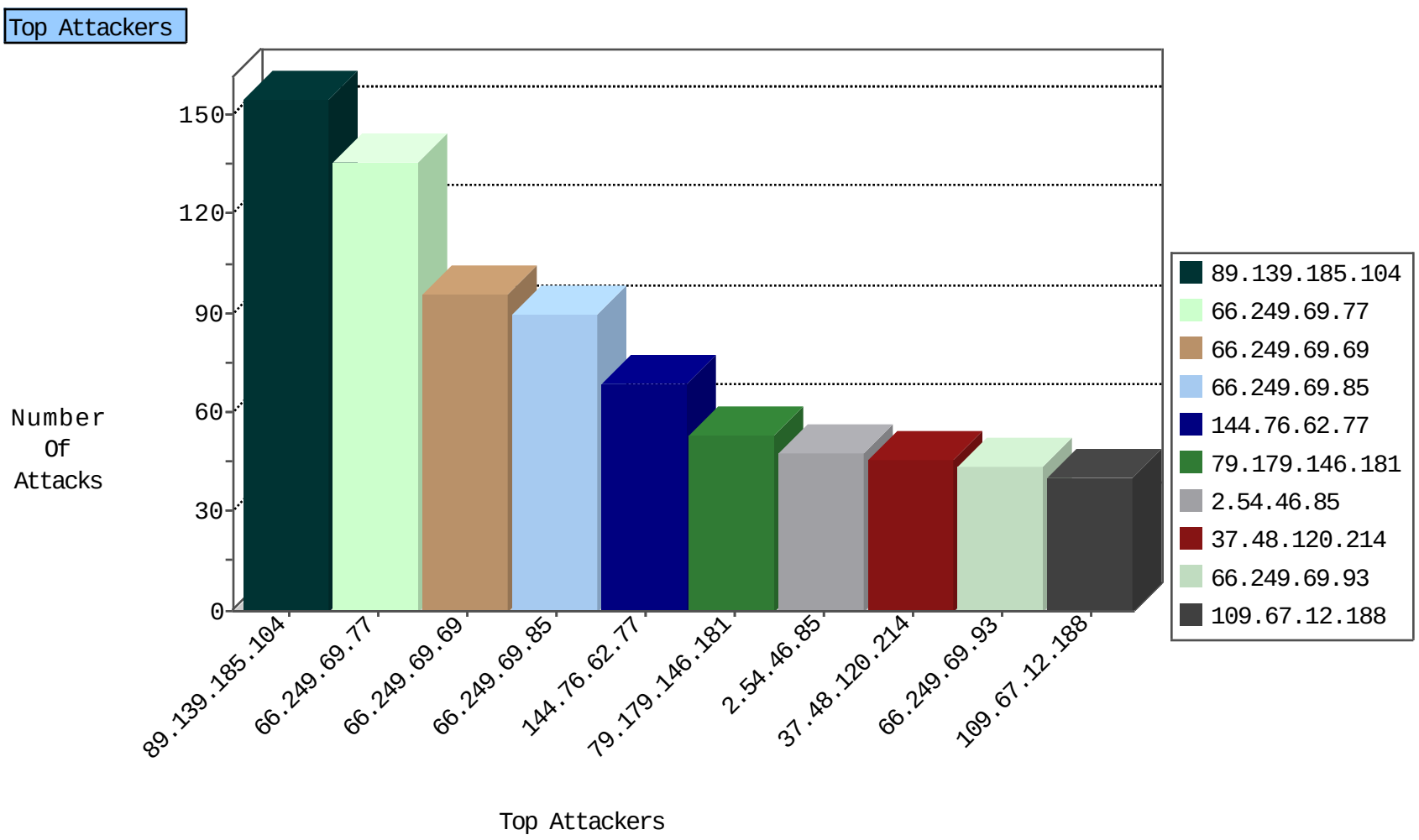
04-11-2015-12:03:07 to 04-11-2015-13:03:07

IDF Under Attack
04-11-2015-12:03:07





04-11-2015-12:03:07 to 04-11-2015-13:03:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
2.52.31.240	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	861
89.139.185.104	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	727
66.249.69.77	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	136
66.249.69.69	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	96
66.249.69.85	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	90
66.249.69.93	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	44
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	30
66.249.69.79	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	27
66.249.69.109	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	27
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	26
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	23
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	21
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	20
66.249.69.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	19
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	18
66.249.78.174	United States	147.237.76.42	refuah.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	16
66.249.69.105	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	16
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	15
66.249.67.155	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	15
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	15
66.249.78.160	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	14
66.249.67.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	14
66.249.78.166	United States	147.237.77.216	dover.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
66.249.67.147	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	13
66.249.69.87	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	12
66.249.64.125	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	12
66.249.78.93	United States	147.237.77.233	atal.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	10
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	10
66.249.69.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.67.115	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	9
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	8
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	8
66.249.78.79	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	8
66.249.69.120	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	7
66.249.69.128	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	7
66.249.93.245	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.64.173	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	6
66.249.69.47	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	6
66.249.67.99	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	6
66.249.67.116	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	5
66.249.67.34	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	5
66.249.69.89	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	5
66.249.64.132	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	5
66.249.78.167	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	5
66.249.64.63	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	4
66.249.67.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	4
66.249.78.134	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	4

04-11-2015-12:03:07 to 04-11-2015-13:03:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
188.23.94.61	Austria	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
37.205.9.131	Slovakia	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
37.205.9.131	Slovakia	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
54.158.192.194	United States	147.237.77.235	sviva.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
91.207.4.22	Ukraine	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	1
93.120.27.62	Romania	147.237.8.24	e.lifestyle.idf	DVRep_B-N_60_100	Block	1

04-11-2015-12:03:07 to 04-11-2015-13:03:07

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	6
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
109.65.160.166	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.76	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.0.19	madim.atal.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 5800-5820	1
113.98.255.48	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
36.72.228.72	Indonesia	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 4096	1
113.98.255.48	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
183.60.106.175	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
107.170.72.219	United States	147.237.77.243	mobile.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
122.228.207.76	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.231	Netherlands	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.231	Netherlands	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
122.228.207.76	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.130	China	147.237.76.42	refuah.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
122.228.207.76	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.130	China	147.237.72.166	aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
113.98.255.48	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
1.217.90.123	Korea, Republic of	147.237.0.35	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.60.106.175	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
183.60.106.175	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.130		147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 3072	1
122.228.207.76	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.231	Netherlands	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1

04-11-2015-12:03:07 to 04-11-2015-13:03:07

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	150
144.76.62.77	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	69
79.179.146.181	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	52
2.54.46.85	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
109.67.12.188	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
46.19.85.57	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
84.229.36.139	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
72.211.238.80	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
79.181.97.50	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
212.179.61.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
87.69.189.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
80.246.133.154	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
188.23.94.61	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
46.121.70.201	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
79.177.203.201	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
176.12.138.58	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
89.139.20.168	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
82.166.27.51	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
80.74.126.107	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
84.229.135.100	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
5.22.129.204	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
84.111.61.133	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	16
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
66.87.65.245	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
82.80.164.249	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
207.46.13.82	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
109.186.167.131	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
80.178.13.172	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
79.179.118.14	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
84.109.113.216	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
189.251.101.17	Mexico	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
37.16.72.139	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
176.12.149.232	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
80.246.133.63	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
46.120.129.112	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
176.12.137.55	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
37.142.166.203	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
157.55.39.114	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
87.68.15.143	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
98.90.10.195	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
193.252.202.185	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
84.118.30.115	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
185.24.79.181	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
85.65.48.126	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	3
81.159.124.2	United Kingdom	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 81.159.124.2	Block	3
207.46.13.79	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
107.170.72.219	United States	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
93.172.86.42	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
207.46.13.82	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/twinse.stm	Block	1
79.181.212.47	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
23.20.72.246	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
149.88.149.117	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
104.131.231.127		147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /	Block	1
84.109.2.215	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/templates/sendtofriend/sendtofriend.aspx	Block	1
188.138.17.205	France	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on 147.237.77.176//	Block	1
68.104.69.237	United States	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/iturim/iturim.aspx	None	1
109.64.52.127	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
104.131.197.175		147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on //	Block	1
217.132.123.40	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
79.182.170.22	Israel	147.237.72.166	aka.idf.il	Unknown Parameter q in www.aka.idf.il/main/giyus/login.aspx	None	1
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
157.55.39.114	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
104.131.231.127		147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /	Block	1
84.228.159.227	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
202.112.50.77	China	147.237.77.216	dover.idf.il	Malformed URL	Block	1
70.167.8.42	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/318-he/sb_item_lev2	Block	1
125.209.235.178	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm	Block	1
104.131.205.116		147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on //	Block	1
217.132.123.40	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
79.182.187.93	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
46.19.85.69	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
162.243.77.186	United States	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on //	Block	1
104.131.231.127		147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	1
202.112.50.77	China	147.237.77.216	dover.idf.il	Unknown HTTP Request Method quit in URL	Block	1
149.78.159.240	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
104.131.205.116		147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on //	Block	1
46.116.206.13	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$employmentStatus in www.aka.idf.il/main/sachar/payslips.aspx	None	1
167.114.64.100	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
107.170.72.219	United States	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on //	Block	1
85.65.138.192	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl71 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
79.179.48.141	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
5.102.204.177	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
149.78.190.25	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
104.131.231.127		147.237.72.156	aman.idf.il	Unauthorized Method HEAD for /	Block	1
82.166.118.105	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.117.148.239	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
180.76.4.109	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1