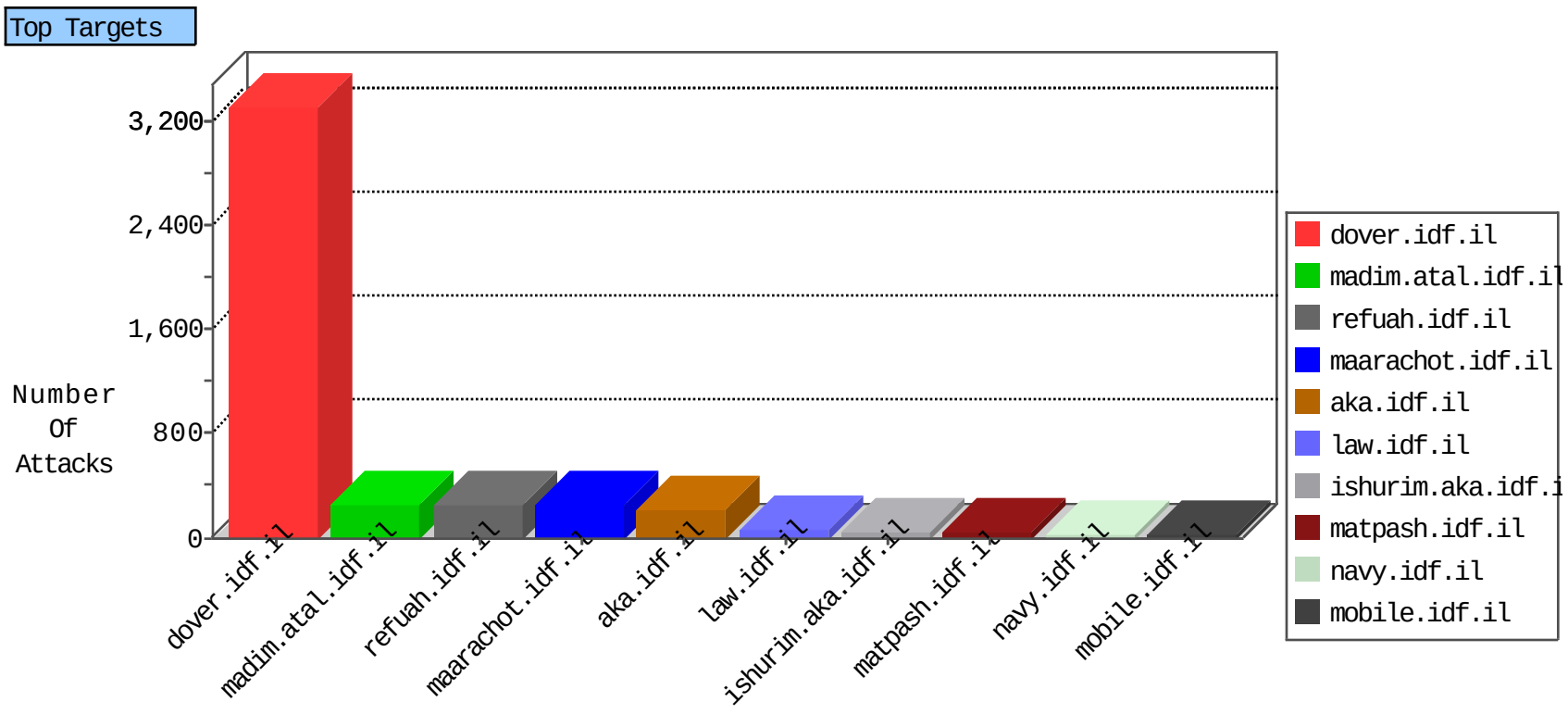
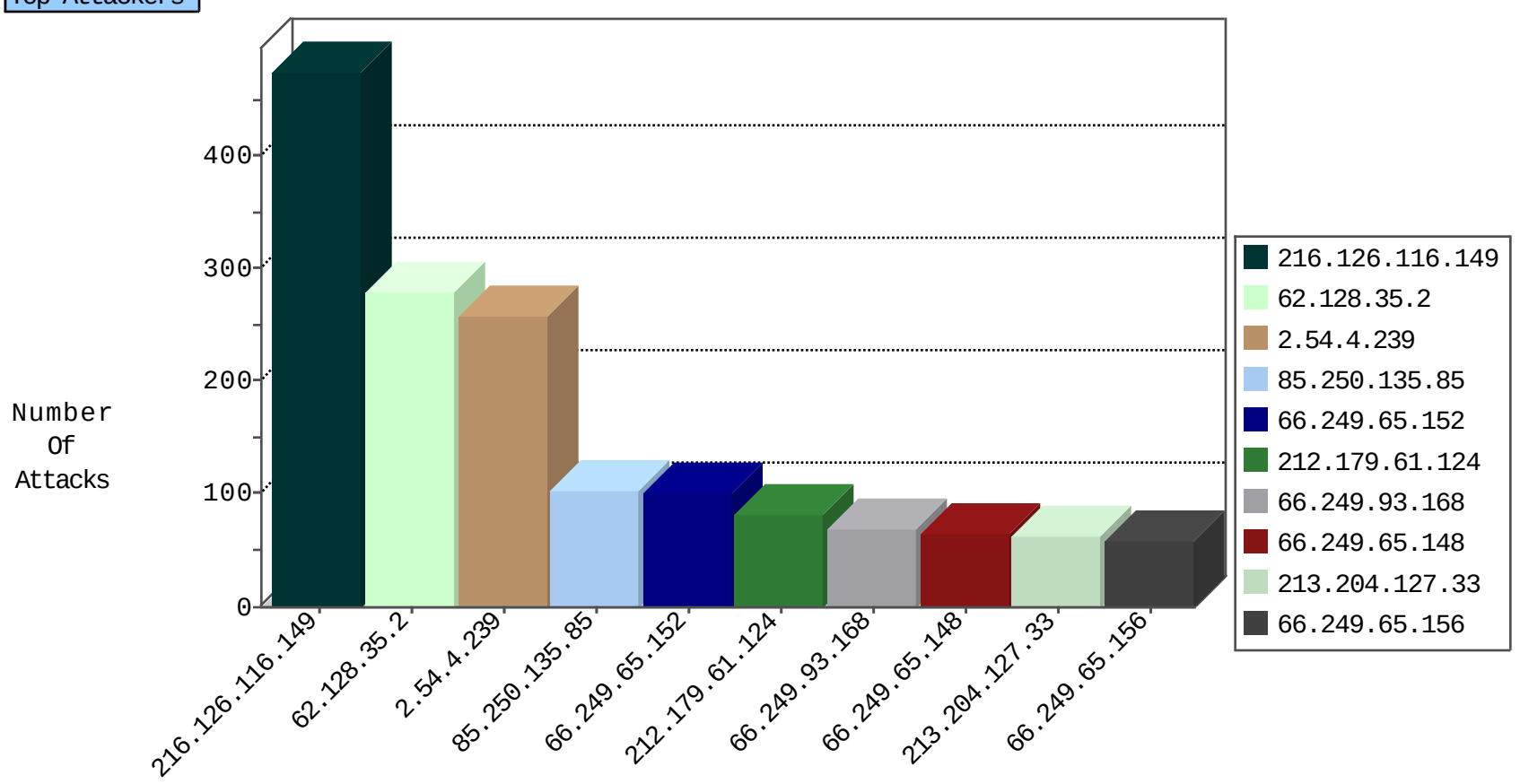
04-13-2015-08:03:07 to 04-13-2015-09:03:07

IDF Under Attack
04-13-2015-08:03:07

Top Targets



Top Attackers



04-13-2015-08:03:07 to 04-13-2015-09:03:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
216.126.116.149	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	16621
77.125.213.222	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2880
213.204.127.33	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2682
79.180.117.24	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2606
162.192.119.52	United States	147.237.8.24	e.lifestyle.idf.il	TCP handshake violation, first packet not syn	drop	619
54.72.0.55	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	579
85.72.40.4	Greece	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	492
132.74.169.209	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	263
199.203.215.1	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	206
46.120.66.22	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	133
66.249.65.152	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	101
66.249.65.148	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	65
66.249.65.156	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	54
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	47
66.249.93.176	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	42
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	40
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	36
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	36
66.249.93.168	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	34
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	28
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	28
66.249.93.172	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	26
66.249.67.100	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	24
220.181.108.141	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	18
82.102.141.255	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	18
66.249.67.108	United States	147.237.77.74	law.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	16
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	14
66.249.78.242	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	12
66.249.73.217	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.73.244	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	11
66.249.78.190	United States	147.237.77.176	matpash.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
66.249.78.167	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	11
66.249.73.140	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
66.249.78.134	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	10
66.249.73.132	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.67.116	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	9
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	9
66.249.80.75	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	9
66.249.89.103	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	8
66.249.80.83	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	8
66.249.93.245	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	8
66.249.64.88	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	8
66.249.78.127	United States	147.237.0.34	tikshuv.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	7
66.249.93.239	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	6

04-13-2015-08:03:07 to 04-13-2015-09:03:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
81.218.251.251	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	4
85.25.43.94	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.13	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
132.66.236.170	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
213.57.214.141	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1

04-13-2015-08:03:07 to 04-13-2015-09:03:07

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	2
46.120.50.92	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.250.135.85	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
221.235.188.212	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
62.128.35.2	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
58.20.54.249	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
125.5.16.195	Philippines	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	1
113.105.167.113	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
113.105.167.113	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
113.105.167.113	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
113.59.33.61	China	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
107.178.214.66	United States	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -f -sS	1
221.235.188.212	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
82.80.153.251	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
221.235.188.212	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
125.5.16.195	Philippines	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.20.54.249	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
125.5.16.195	Philippines	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
113.105.167.113	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
113.105.167.113	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
113.105.167.113	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
107.178.214.66	United States	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1
221.235.188.212	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1

04-13-2015-08:03:07 to 04-13-2015-09:03:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
216.126.116.149	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	427
62.128.35.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	279
85.250.135.85	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	103
212.179.61.124	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	82
213.204.127.33	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	57
115.158.155.192	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	56
89.138.218.49	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	53
46.19.86.162	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
109.253.140.136	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
72.224.135.19	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
109.253.129.201	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
81.218.251.251	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
149.88.56.124	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
109.253.131.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
82.80.153.251	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
109.253.140.174	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
109.253.157.20	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
2.54.176.149	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
176.12.139.212	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
194.90.169.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
80.246.140.89	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
176.12.144.157	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
46.19.85.95	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
91.135.102.161	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
185.4.253.19	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
212.28.230.202	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
67.188.228.161	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
146.185.60.138	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
89.139.183.55	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
94.159.206.238	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
109.253.147.53	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
98.249.39.132	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
157.55.39.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
109.64.7.57	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
37.26.146.209	Israel	147.237.77.243	mobile.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	15
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
157.55.39.6	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
2.54.35.6	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
81.218.80.174	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
46.19.85.101	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
46.19.86.49	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
109.253.140.120	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
83.254.176.167	Sweden	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
77.125.114.0	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
79.177.206.48	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
176.12.143.87	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.4.239	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.4.239	Block	257
87.69.126.204	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	6
80.246.130.117	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	5
109.64.7.57	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
37.26.147.194	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
197.221.14.85	South Africa	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
109.64.7.57	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/scripts/css3pie.htc	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
37.26.147.199	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
80.246.140.89	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
5.135.182.230	France	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
216.69.245.101	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
138.134.102.16	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//milnet	Block	1
62.219.13.180	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
31.168.230.194	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$txtMisparTeuda in www.aka.idf.il/main/sachar/	None	1
212.143.124.199	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.228.96.20	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.145.24	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.179.9.64	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
46.19.86.49	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
109.186.147.59	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/sachar/registrationwizard/register.aspx parameter	None	1
217.69.136.208	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/idf_in_pictures/2003/june/10.stm	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/default.aspx	None	1
157.55.39.171	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
62.219.139.24	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
212.179.4.21	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	1
85.64.57.129	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$txtMisparIshi in www.aka.idf.il/main/sachar/	None	1
176.12.145.185	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.86.110	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
119.127.99.205	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
93.152.203.167	Bulgaria	147.237.76.30	himush.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1
207.46.13.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/0505-4.stm	Block	1
157.55.39.172	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.64.41.59	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
213.151.53.59	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
87.69.25.136	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
80.246.130.210	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
176.12.146.196	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.86.184	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	1
132.70.66.14	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/miluim/login.aspx	None	1
93.152.203.167	Bulgaria	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
5.135.182.230	France	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
207.46.13.103	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
82.102.136.67	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
176.12.139.141	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.176.131.178	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.142.83.65	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.64.110.66	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/registrationwizard/undefined	Block	1
216.69.245.101	United States	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1

04-13-2015-08:03:07 to 04-13-2015-09:03:07