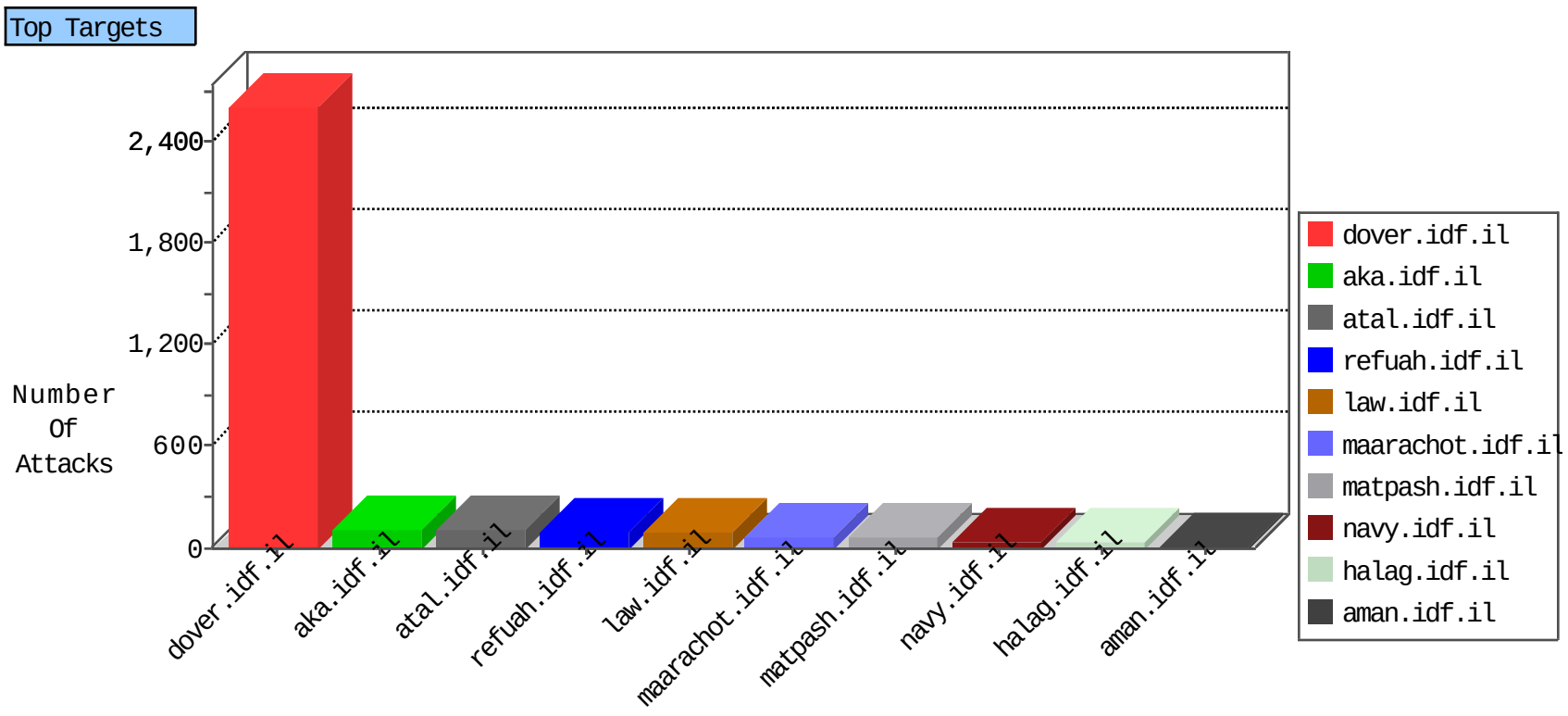
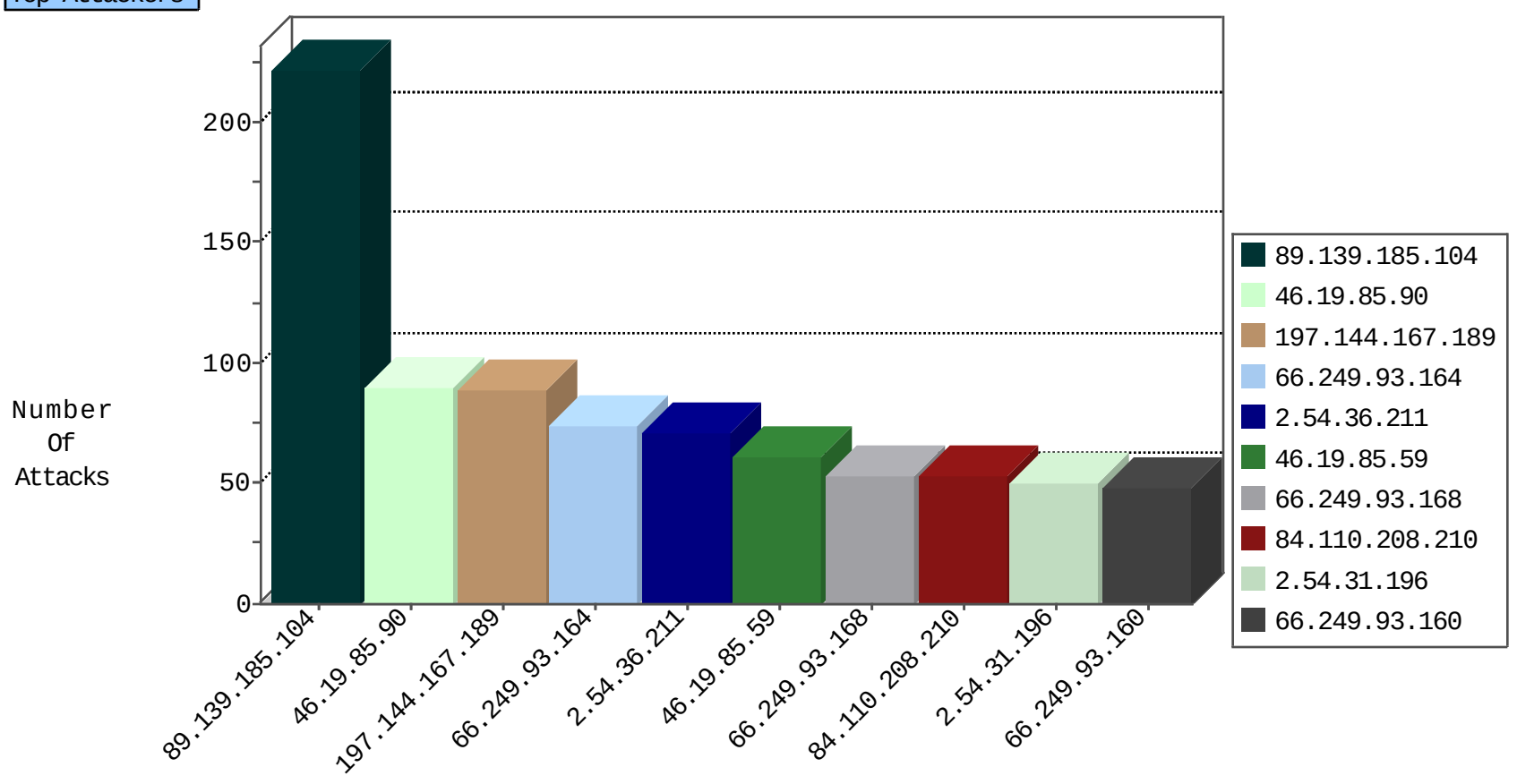
04-10-2015-13:03:06 to 04-10-2015-14:03:06

IDF Under Attack
04-10-2015-13:03:06

Top Targets



Top Attackers



04-10-2015-13:03:06 to 04-10-2015-14:03:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
31.186.228.62	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1345
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	74
197.135.2.191	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	66
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	53
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	48
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	40
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	29
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	26
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	24
66.249.69.128	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	22
66.249.78.79	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	22
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	21
66.249.78.93	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	19
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	19
66.249.93.243	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	18
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	17
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	14
66.249.78.89	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	14
66.249.78.86	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	13
66.249.78.22	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	13
66.249.78.29	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	12
66.249.69.16	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	12
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	12
66.249.93.242	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	11
41.69.250.123	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	11
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	11
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	11
66.249.69.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
66.249.82.202	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	9
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	9
66.249.78.15	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	8
66.249.78.82	United States	147.237.77.74	law.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	7
79.181.26.132	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
66.249.69.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.65.200	United States	147.237.0.19	madim.atal.idf.il	Block_Ip_Web_In	drop	6
66.249.64.129	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	6
66.249.93.240	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	6
66.249.69.93	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5
66.249.64.14	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	5
66.249.78.74	United States	147.237.77.233	atal.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
66.249.64.187	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	5
66.249.64.132	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	4
66.249.78.18	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	4
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	4
66.249.64.151	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	4
66.249.64.10	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	4
66.249.78.96	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	4

04-10-2015-13:03:06 to 04-10-2015-14:03:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
146.148.27.238		147.237.77.74	law.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	11
146.148.27.238		147.237.77.74	law.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	11
197.144.167.189	Morocco	147.237.77.216	dover.idf.il	5380: HTTP: Full-Width / Half-Width Unicode URI Evasion	Permit	5
109.64.9.223	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
149.88.97.233	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
2.54.159.200	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.19.85.225	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	1
85.250.136.203	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.0.15	kosher-kravi.idf.i	DVRep_B-N_60_100	Block	1
2.52.31.184	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1

04-10-2015-13:03:06 to 04-10-2015-14:03:06

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
146.148.27.238		147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	2
2.54.51.229	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.246.130.211	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.66	China	147.237.0.33	idf.il	ET SCAN Potential VNC Scan 5800-5820	1
31.7.57.198	Switzerland	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.170	Japan	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.130		147.237.77.170	maarachot.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.170	Japan	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.170	Japan	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
43.255.191.170	Japan	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.0.35	akaws.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
43.255.191.170	Japan	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.130		147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.170	Japan	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
95.219.86.3	Romania	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.170	Japan	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.170	Japan	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.72.217	e.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
43.255.191.170	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1

04-10-2015-13:03:06 to 04-10-2015-14:03:06

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	222
46.19.85.90	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	90
197.144.167.189	Morocco	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	82
2.54.36.211	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	71
46.19.85.59	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	61
84.110.208.210	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	53
2.54.31.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
95.219.86.3	Romania	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	47
82.166.20.29	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
41.69.250.123	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
82.80.164.113	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
2.54.180.3	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
93.168.186.184	Romania	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
109.64.1.73	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
109.253.133.115	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
2.52.142.128	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
154.68.53.89	Cote D'Ivoire	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
109.253.157.238	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.136.227	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
197.135.2.191	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
109.253.139.160	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
176.12.141.191	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
192.117.13.46	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
81.218.14.201	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
80.246.130.222	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
132.74.30.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
176.12.144.66	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
109.253.128.38	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
85.65.95.157	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
217.55.226.37	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
85.250.136.203	Israel	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	18
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
46.116.32.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
2.54.137.184	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
93.168.120.93	Romania	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
109.253.158.9	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
62.128.48.50	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
157.55.39.114	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
37.142.200.69	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
46.116.166.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
109.67.25.161	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
84.228.144.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
176.12.142.103	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12

04-10-2015-13:03:06 to 04-10-2015-14:03:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
122.58.54.84	New Zealand	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	2
109.66.139.2	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
146.148.27.238		147.237.77.74	law.idf.il	PHP Attempt	Block	2
217.12.204.117	Ukraine	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 217.12.204.117	Block	2
2.54.180.3	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	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
109.64.1.73	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.86.164	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
104.131.193.203		147.237.72.156	aman.idf.il	Unauthorized Method HEAD for /	Block	1
77.126.118.183	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
5.79.16.135	United Kingdom	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
216.245.198.66	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
85.250.136.203	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
54.172.196.207	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
104.131.193.203		147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /	Block	1
79.176.217.216	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
37.26.147.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
109.186.147.76	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
92.205.39.135	Germany	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.34	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper/	Block	1
157.55.39.172	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
104.131.193.203		147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /	Block	1
79.178.63.82	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
37.142.86.74	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
217.12.204.117	Ukraine	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/1072-he/shared/usercontrols/headerupper/	Block	1
109.253.145.127	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
101.22.191.97	China	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 101.22.191.97	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
184.168.27.42	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
104.131.193.203		147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	1
79.182.128.4	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$btnSubmit.x in www.aka.idf.il/main/sachar/	None	1
46.19.85.33	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
217.69.133.226	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
109.253.147.104	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
101.22.191.97	China	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/6/266.pdf/trackback/	Block	1
5.29.176.186	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	1
188.165.15.241	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.241	Block	1
79.183.180.242	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1

04-10-2015-13:03:06 to 04-10-2015-14:03:06