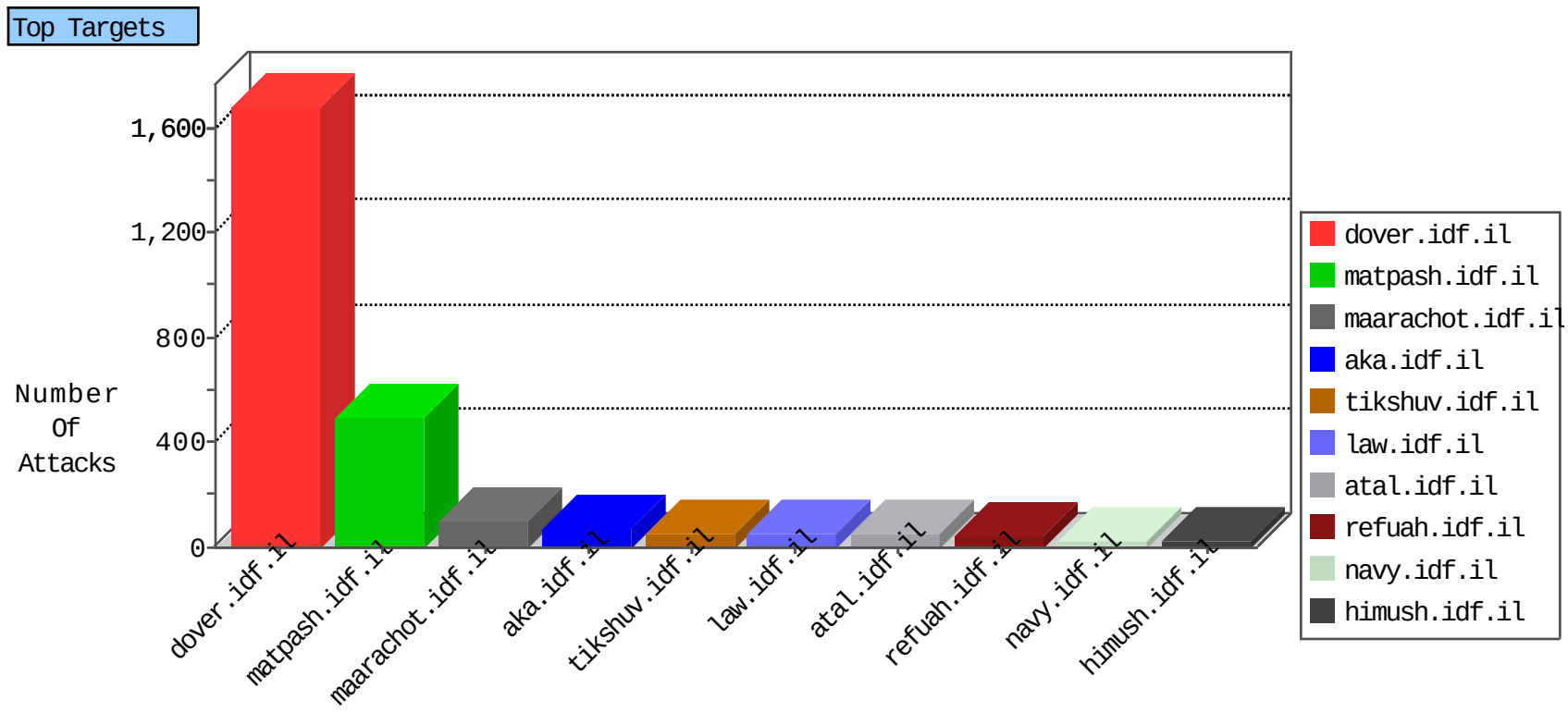
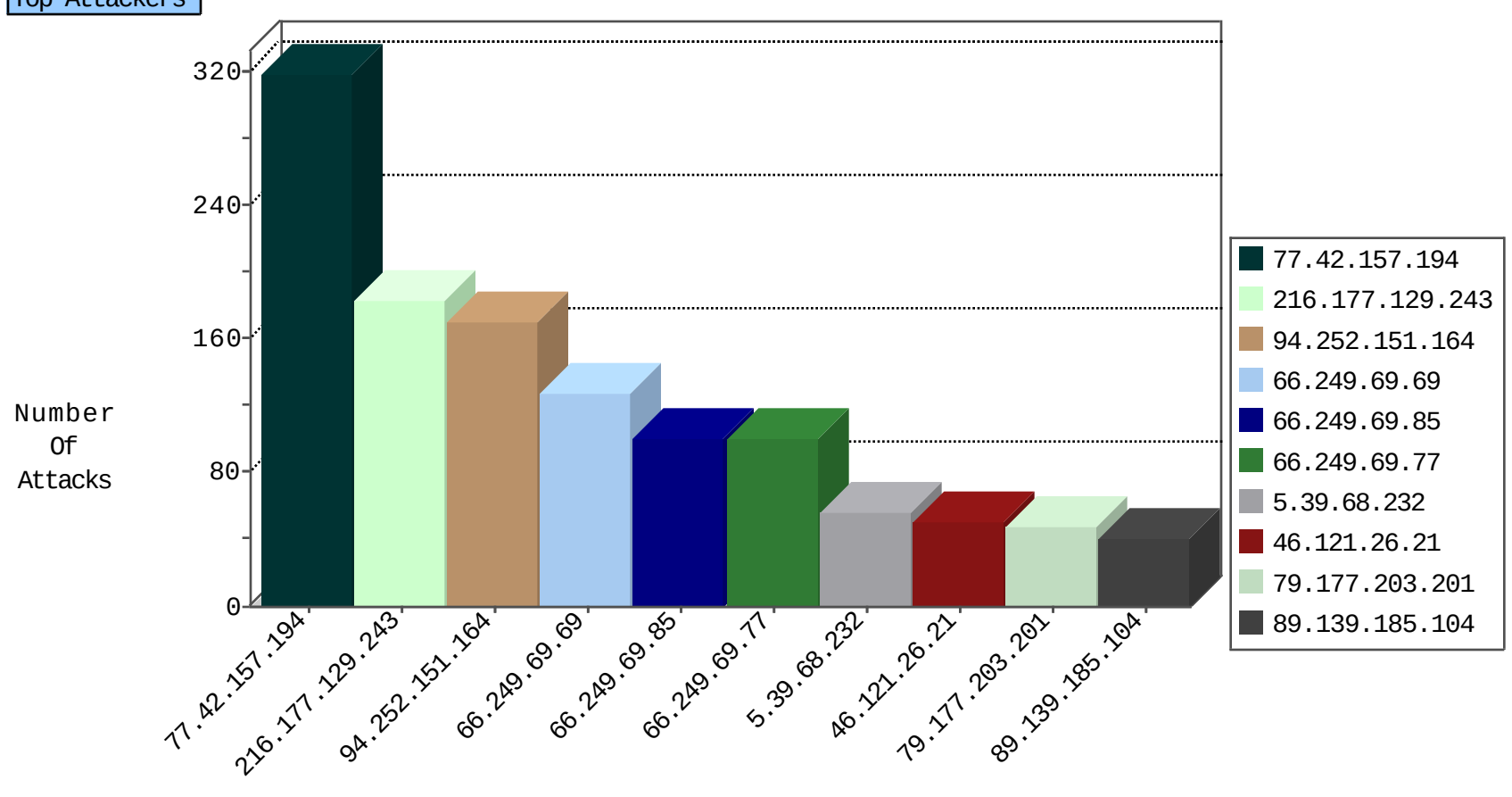
04-11-2015-10:03:02 to 04-11-2015-11:03:02

IDF Under Attack
04-11-2015-10:03:02

Top Targets



Top Attackers



04-11-2015-10:03:02 to 04-11-2015-11:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.69.69	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	123
66.249.69.85	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	101
66.249.69.77	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	100
66.249.93.204	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	29
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	27
66.249.69.95	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	23
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	20
66.249.93.208	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	17
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	16
66.249.67.108	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	15
66.249.67.107	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	14
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	13
66.249.78.86	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	13
66.249.69.79	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	13
66.249.78.93	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	13
66.249.69.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	11
66.249.69.128	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	10
66.249.69.101	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	9
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	9
66.249.93.131	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	9
66.249.69.34	United States	147.237.72.166	aka.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	8
66.249.69.105	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
66.249.67.116	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	7
66.249.67.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	7
66.249.93.238	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	7
66.249.67.99	United States	147.237.76.30	himush.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	6
66.249.89.103	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
66.249.67.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	5
66.249.89.101	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4
66.249.69.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	4
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	4
66.249.93.235	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	4
66.249.78.148	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	4
66.249.78.79	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	4
66.249.93.200	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	4
66.249.64.6	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	4
66.249.78.60	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	4
66.249.89.105	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4
66.249.69.61	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	4
66.249.78.67	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	4
66.249.67.100	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	3
66.249.64.146	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3
66.249.69.109	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	3
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	3
66.249.64.59	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	2

04-11-2015-10:03:02 to 04-11-2015-11:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.121.26.21	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.222	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-11-2015-10:03:02 to 04-11-2015-11:03:02

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	20
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
37.142.160.15	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.125.127.77	Austria	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
61.160.224.130	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
222.69.94.13	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 2048	1
222.69.94.13	China	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1
94.43.85.2	Georgia	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
94.43.85.2	Georgia	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
85.125.127.77	Austria	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.64	China	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
222.69.94.13	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -f -sS	1
222.69.94.13	China	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -f -sS	1
94.102.56.231	Netherlands	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
94.43.85.2	Georgia	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1

04-11-2015-10:03:02 to 04-11-2015-11:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
77.42.157.194	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	319
216.177.129.243	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	183
94.252.151.164	Syrian Arab Republic	147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	monitor	81
94.252.151.164	Syrian Arab Republic	147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	alert	65
5.39.68.232	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	56
46.121.26.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
79.177.203.201	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
89.139.185.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
92.249.206.89	Hungary	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
178.8.93.180	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
46.19.85.35	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
84.109.102.51	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
77.125.98.90	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
46.121.106.127	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
166.137.126.20	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
176.12.144.244	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
5.246.127.71	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
62.201.211.78	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
37.26.147.162	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
37.211.12.28	Qatar	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
37.201.194.47	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
74.6.254.113	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
109.67.111.43	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
174.61.196.158	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
77.125.208.137	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
46.116.159.158	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
107.167.102.132	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
85.64.84.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
213.57.37.213	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
37.202.117.36	Jordan	147.237.77.216	dover.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	11
46.19.85.222	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
157.55.39.6	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
94.252.151.164	Syrian Arab Republic	147.237.77.176	matpash.idf.il	Response out of state	Block HTTP Non Compliant	monitor	10
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
157.55.39.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
82.166.81.221	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
37.202.117.36	Jordan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
82.166.118.226	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
84.228.205.198	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
157.55.39.114	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
79.176.96.235	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
94.249.19.199	Jordan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6

04-11-2015-10:03:02 to 04-11-2015-11:03:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
94.252.151.164	Syrian Arab Republic	147.237.77.176	matpash.idf.il	Multiple Abnormally Long Request from 94.252.151.164	Block	10
85.250.184.63	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	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
157.55.39.6	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.6	Block	2
157.55.39.172	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	2
46.19.85.35	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	2
180.76.4.185	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.65.200.37	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/home.aspx	None	1
46.116.242.220	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
109.253.130.91	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim	Block	1
31.168.68.51	Israel	147.237.72.166	aka.idf.il	Unknown Parameter q861 in www.aka.idf.il/main/giyus/login.aspx	None	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unknown Parameter sig2 in www.aka.idf.il/main/giyus/general.aspx	None	1
46.117.1.151	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
188.165.15.241	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/involvment/english/main_index.stm	Block	1
109.253.139.250	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.114	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.114	Block	1
87.123.75.102	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
54.215.88.171	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	1
79.176.217.216	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
37.201.194.47	Germany	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
94.252.151.164	Syrian Arab Republic	147.237.77.176	matpash.idf.il	Abnormally Long Request URL	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
157.55.39.42	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.42	Block	1
85.65.68.20	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	1

04-11-2015-10:03:02 to 04-11-2015-11:03:02