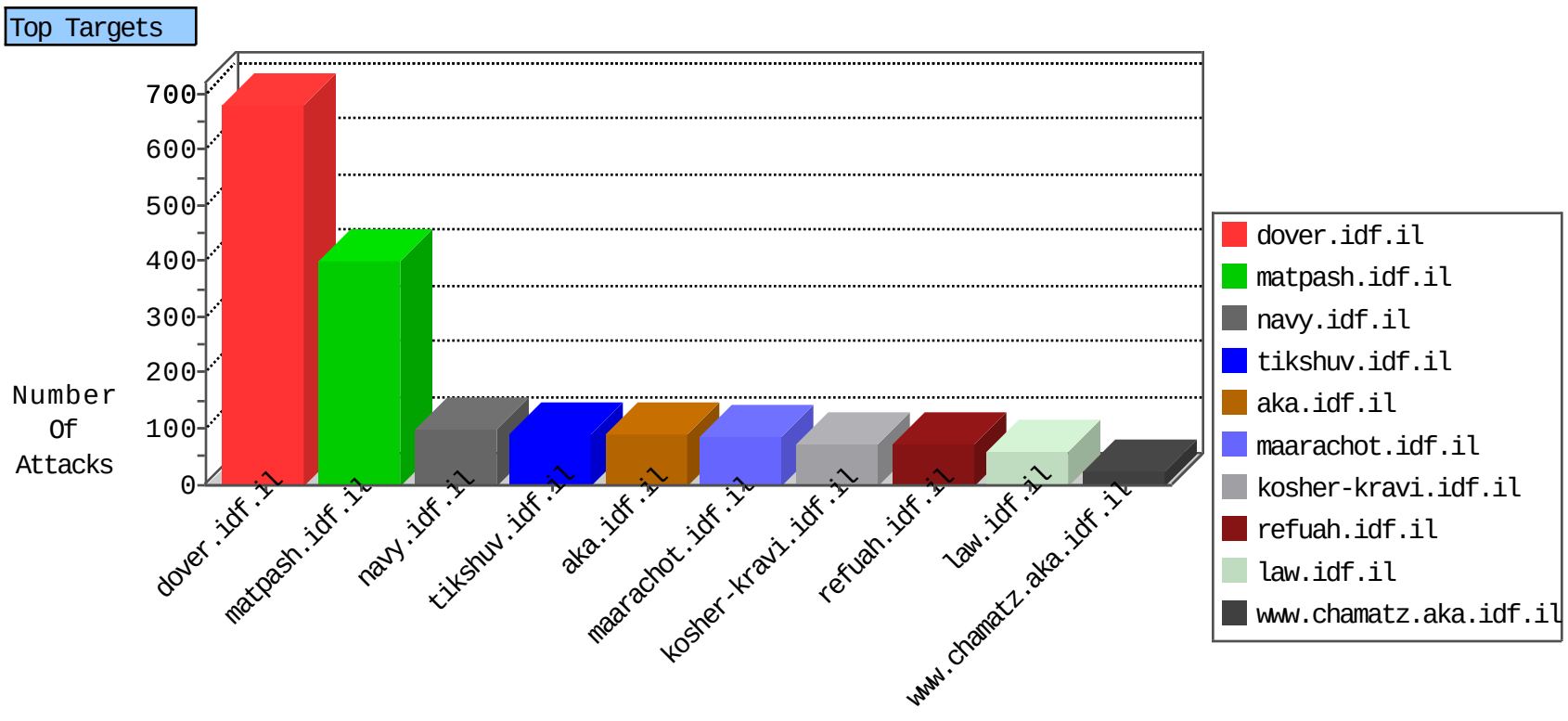
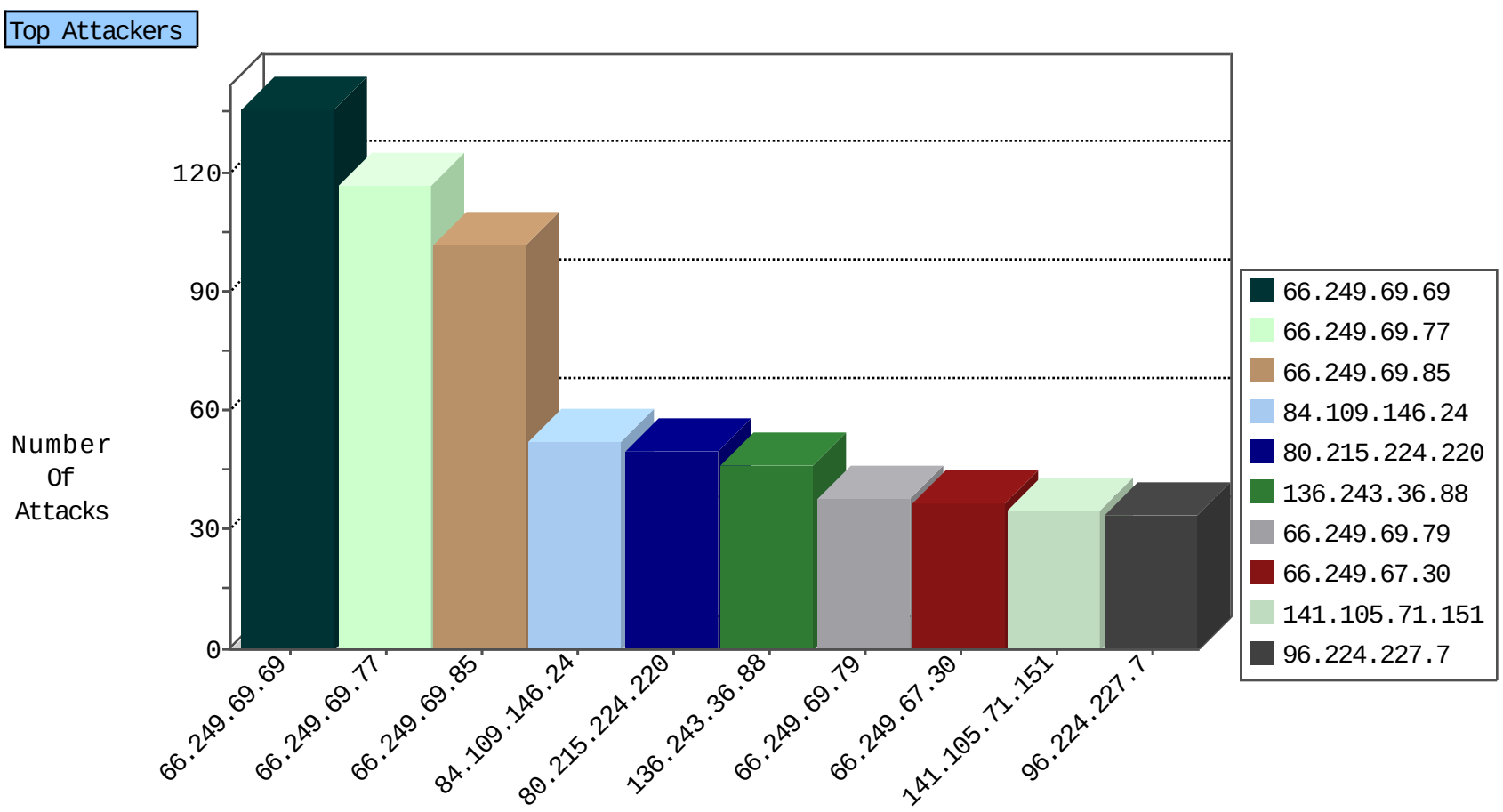
04-11-2015-05:03:07 to 04-11-2015-06:03:07

IDF Under Attack
04-11-2015-05:03:07

Top Targets



Top Attackers



04-11-2015-05:03:07 to 04-11-2015-06:03:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
89.138.244.152	Israel	147.237.0.15	kosher-kravi.idf.il	TCP Scan (vertical)	drop	315
66.249.69.69	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	135
66.249.69.77	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	114
66.249.69.85	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	102
66.249.69.79	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	38
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	37
192.116.159.183	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	32
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	26
66.249.78.166	United States	147.237.77.216	dover.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	25
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	25
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	22
66.249.69.97	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	21
66.249.69.95	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	20
66.249.69.87	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	18
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	18
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	16
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	16
66.249.69.50	United States	147.237.72.166	aka.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
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	14
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	13
66.249.64.132	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	12
66.249.69.93	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.69.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.67.100	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	11
66.249.69.109	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.69.101	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
66.249.69.55	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	10
66.249.69.42	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	10
66.249.78.167	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	10
66.249.67.34	United States	147.237.77.226	www.chamatz.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
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	9
66.249.69.120	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	8
66.249.69.5	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ip_Web_In	drop	8
66.249.64.146	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	8
66.249.78.86	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	7
66.249.67.50	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	7
66.249.67.92	United States	147.237.77.74	law.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	6
66.249.64.150	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
66.249.69.105	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	6
66.249.67.42	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	6
66.249.73.219	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	6
66.249.81.204	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	5
66.249.67.155	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	5
66.249.67.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	5
66.249.69.47	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	5

04-11-2015-05:03:07 to 04-11-2015-06:03:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	10
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	10
218.6.132.45	China	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	2
89.139.185.104	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
93.120.27.62	Romania	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1

04-11-2015-05:03:07 to 04-11-2015-06:03:07

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	24
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
89.138.244.152	Israel	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
221.235.188.212	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
60.18.162.244	China	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
221.235.188.212	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.6.132.45	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 2048	1
119.97.231.102	China	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 2048	1
61.160.224.128	China	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
60.18.162.244	China	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
221.235.188.212	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
218.6.132.45	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 3072	1
218.6.132.45	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -f -sS	1
121.240.226.74	India	147.237.77.176	matpash.idf.il	Tehila - Perl LWP with fake user agent	1
119.97.231.102	China	147.237.77.74	law.idf.il	ET SCAN NMAP -f -sS	1

04-11-2015-05:03:07 to 04-11-2015-06:03:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
84.109.146.24	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	52
80.215.224.220	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
136.243.36.88	Germany	147.237.77.176	matpash.idf.il	SAM rule	drop	drop	46
96.224.227.7	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
87.68.21.201	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
93.173.141.105	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
87.69.46.154	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
68.234.208.21	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
24.116.189.138	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
89.139.185.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
141.105.71.151	Russian Federation	147.237.77.216	dover.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	14
74.89.18.76	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
141.105.71.151	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
80.215.228.1	France	147.237.77.216	dover.idf.il		Bad TCP sequence	monitor	10
80.215.228.1	France	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	10
174.124.169.24	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
80.215.228.1	France	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	9
149.78.154.69	United States	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
204.237.22.235	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
109.67.27.63	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	6
109.253.147.85	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
98.190.57.75	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
46.19.85.138	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
207.46.13.82	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
65.55.210.87	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
68.172.52.70	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
93.83.226.216	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
190.1.8.171	Argentina	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.85.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
179.125.191.174	Brazil	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
115.25.81.69	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
84.228.144.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
157.55.39.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
157.55.39.114	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
84.108.45.246	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
141.105.71.151	Russian Federation	147.237.77.216	dover.idf.il	Unexpected post SYN packet - RST or SYN expected	drop	drop	2
80.215.224.220	France	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
159.224.160.225	Ukraine	147.237.72.166	aka.idf.il	SAM rule	drop	drop	2
207.46.13.82	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
190.144.125.235	Colombia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
37.218.136.126	Kyrgyzstan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
159.224.160.225	Ukraine	147.237.76.42	refuah.idf.il	SAM rule	drop	drop	2
141.105.71.151	Russian Federation	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	2

04-11-2015-05:03:07 to 04-11-2015-06:03:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
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
109.160.182.152	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 109.160.182.152	Block	2
157.55.39.172	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
217.69.133.223	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/doctor	Block	1
141.105.71.151	Russian Federation	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/homefront/faq/1.stm	Block	1
180.153.163.211	China	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files	Block	1
101.226.33.202	China	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf	Block	1
141.105.71.151	Russian Federation	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
14.222.61.155	China	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
180.153.214.188	China	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/2	Block	1
109.67.27.63	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
157.55.39.6	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0302-1.stm	Block	1
31.13.99.119	Ireland	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	1
188.165.15.75	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9043-he/refuah.aspx	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
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/idf_in_pictures/2003/august/21.stm	Block	1
192.111.146.34	United States	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
109.160.182.152	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/2/	Block	1

04-11-2015-05:03:07 to 04-11-2015-06:03:07