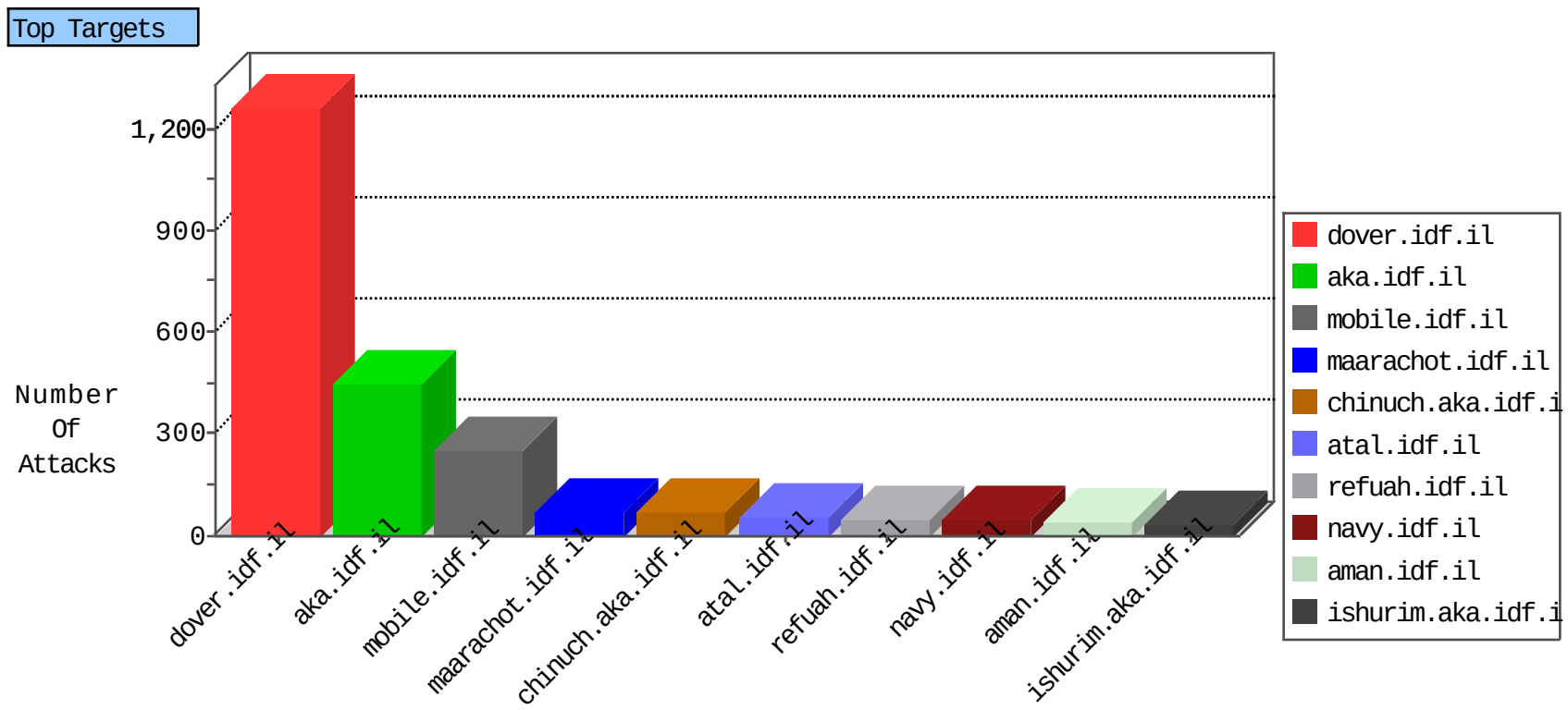
10-31-2015-10:04:01 to 10-31-2015-11:04:01

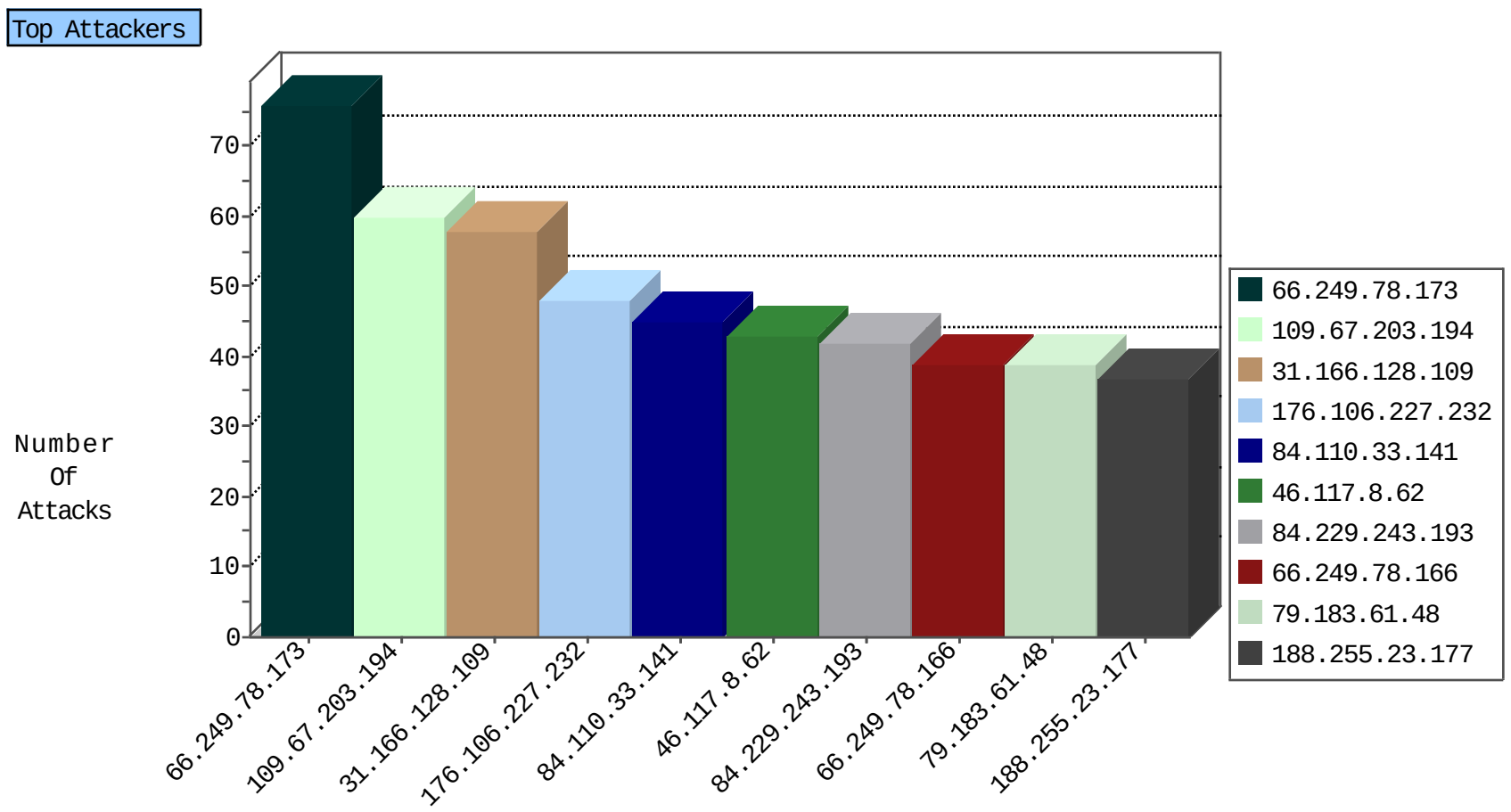
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-31-2015-10:04:01 to 10-31-2015-11:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.20	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1129
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	536
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	213
37.142.68.55	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	33
46.120.43.143	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
46.19.86.47	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
85.65.61.108	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	24
93.173.47.120	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
85.64.11.237	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
79.176.39.83	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
5.29.50.135	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
5.22.130.109	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
185.32.179.245	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
80.178.28.249	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
79.180.189.29	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
46.19.86.117	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
5.102.254.135	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.178.119.4	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
80.230.87.234	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
66.249.69.76	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5
89.138.204.42	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
80.246.136.56	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
109.67.61.238	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
46.117.8.62	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
77.127.174.148	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
85.65.47.30	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.85.143	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
79.177.135.185	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.60.104	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
78.229.100.85	France	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.13.17.54	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
37.142.68.112	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
82.176.14.143	Netherlands	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
37.26.149.129	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
2.54.11.213	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
149.78.88.18	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
89.139.165.32	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
79.179.12.251	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
84.108.194.28	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
185.120.126.43		147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
95.84.139.157	Russian Federation	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
89.138.236.109	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.77.44.199	Russian Federation	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
2.52.30.139	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
36.77.245.196	Indonesia	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	2
79.177.193.66	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
77.125.75.143	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

10-31-2015-10:04:01 to 10-31-2015-11:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.76.42	refuah.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

10-31-2015-10:04:01 to 10-31-2015-11:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	**Signature**	**Count**

10-31-2015-10:04:01 to 10-31-2015-11:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.106.227.232	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
31.166.128.109	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
188.255.23.177	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
2.54.158.121	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
37.142.68.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
66.249.81.218	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
5.29.50.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
31.166.128.109	Saudi Arabia	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
79.176.39.83	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
5.228.113.97	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
79.177.9.119	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
85.64.120.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
93.173.47.120	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
79.181.208.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
89.138.204.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
84.229.243.193	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.65.61.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
100.100.40.4		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
185.32.179.245	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.47	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.51	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
100.100.118.248		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
79.183.61.48	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.178.110.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.102.254.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.181	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.116.153.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.65.51.137	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.81.212	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.178.28.249	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.33	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.51.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.121.17.72	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
100.100.40.4		147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
46.117.8.62	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
100.100.44.31		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
31.168.245.206	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
95.26.143.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.110.33.141	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	45
37.142.220.250	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	30
109.65.51.137	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	30
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	30
109.67.203.194	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	30
66.249.78.52	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	30
46.117.8.62	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	30
109.67.203.194	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	30
31.168.245.206	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	30
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	30
79.183.61.48	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	30
37.142.68.96	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	30
84.229.243.193	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	30
40.77.167.44	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	24
212.116.169.152	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	15
68.180.230.167	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakhal.idf.il/1073-he/nakhal.aspx	Block	15
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	15
151.80.31.112	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
66.249.67.134	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/0/112760.pdf	Block	15
93.44.74.87	Italy	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1406-he/atal.aspx	Block	15
84.108.236.115	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	15
184.105.247.195	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/	Block	15
66.249.79.228	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8913-he/refuah.aspx	Block	15
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	15
66.249.67.27	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/2/112762.pdf	Block	15
85.64.118.128	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	15
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 104 cookies	Block	15
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_text.asp	Block	15
151.80.31.112	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/bagatz_sarbanim.stm_	Block	15
96.43.209.210	United States	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	15
66.249.67.143	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/1/109241.pdf	Block	15
84.109.184.98	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 84.109.184.98 (Open Mode)	None	15
184.105.247.196	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	15
66.249.79.235	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8910-he/refuah.aspx	Block	15
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	15
85.65.60.23	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	15
74.82.47.2	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	15
5.29.218.157	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1440-he/atal.aspx	Block	15
213.175.183.170	Lebanon	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.175.183.170	Block	15
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
176.13.0.46	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	15
96.43.209.210	United States	147.237.77.216	dover.idf.il	eMail Hoarding	Block	15
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	15
84.109.184.98	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	15
192.198.151.45	Europe	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/smalim/scriptresource.axd	None	15
66.249.79.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8974-he/refuah.aspx	Block	15
66.249.78.66	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	15
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/9/71549.pdf	Block	15
85.65.60.23	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	15
79.182.218.155	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Double URL Encoding	Block	15