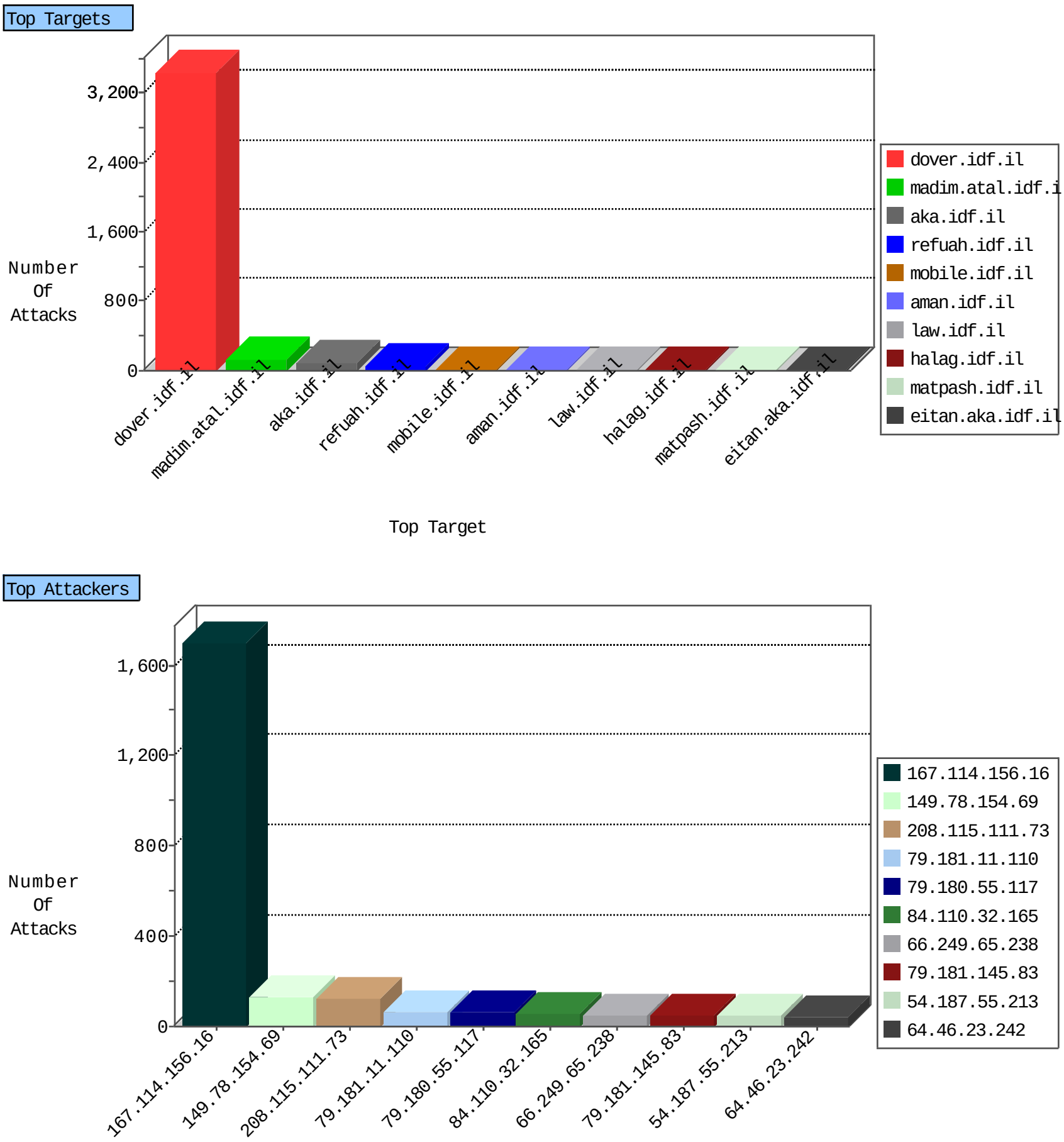
11-07-2015-10:04:05 to 11-07-2015-11:04:05

IDF Under Attack Daily Report



11-07-2015-10:04:05 to 11-07-2015-11:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3074
197.242.164.62	Mozambique	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
46.116.78.6	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
37.77.49.14	Iraq	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
197.249.4.37	Mozambique	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
109.186.160.72	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
123.151.149.222	China	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
41.67.119.176	Egypt	147.237.72.156	aman.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
5.8.66.78	Russian Federation	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
79.179.171.89	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
82.221.105.7	Iceland	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
185.3.144.100	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

11-07-2015-10:04:05 to 11-07-2015-11:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-07-2015-10:04:05 to 11-07-2015-11:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
193.105.134.220	147.237.8.24	Sweden	e.lifestyle.idf	ET SCAN NMAP -sS window 1024	1
80.82.64.109	147.237.77.234	Netherlands	halag.idf.il	ET SCAN Potential SSH Scan	1
197.245.150.111	147.237.76.31	South Africa	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
193.107.17.72	147.237.0.35	Seychelles	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.174.106	147.237.72.217	Netherlands	e.idf.il	ET SCAN Potential SSH Scan	1

11-07-2015-10:04:05 to 11-07-2015-11:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	131
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	118
79.180.55.117	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
84.110.32.165	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
79.181.11.110	Israel	147.237.76.42	refuah.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	50
79.181.145.83	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
64.46.23.242	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
31.154.94.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
213.57.153.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
66.249.65.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
85.250.84.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
185.3.144.89	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
46.19.85.24	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
84.228.202.252	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
141.0.9.76	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
46.19.85.110	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
37.26.146.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
37.26.147.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
37.77.49.14	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
77.125.10.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
2.54.2.124	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
208.69.40.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
188.165.15.14	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
207.46.13.172	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
197.242.164.62	Mozambique	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.181.11.110	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
207.46.13.11	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
79.181.5.146	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
40.77.167.39	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
40.77.167.66	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
82.80.25.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.65.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.182.33.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
157.55.39.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
185.3.144.100	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8

11-07-2015-10:04:05 to 11-07-2015-11:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.183.128.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
79.176.107.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	25
185.32.179.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
176.12.136.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
79.176.107.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
80.246.139.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
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	4
46.120.48.61	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.120.48.61	Block	3
185.32.179.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.176.146.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.108.153.86	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/ajax/updatestatus.php	Block	2
46.120.48.61	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
79.178.178.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
46.120.155.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.108.153.86	Israel	147.237.72.156	aman.idf.il	PHP Attempt	Block	2
207.46.13.172	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.64.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/2952.pdf	Block	1
109.186.119.227	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/login.aspx	None	1
79.181.11.110	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
45.55.176.38		147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
63.141.241.254	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cloud.ph/	Block	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
208.115.111.73	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
133.130.98.204	Japan	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1250-he/atal.aspx	Block	1
66.249.64.108	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
79.182.146.186	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en	Block	1
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_moreinfo.asp	Block	1
64.19.78.242	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
84.201.138.16	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
208.115.111.73	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/templatecontrols/news/×œ×›×ª×‘×″ ×″×žœ ×?×″	Block	1
159.255.163.132	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
66.249.64.113	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/7/757.pdf	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
84.228.220.104	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
67.212.175.138	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/eitan/pratim/pirteykatava/	Block	1
217.69.136.209	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/homefront/	Block	1
66.249.64.118	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/4/314.pdf	Block	1
46.120.48.61	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	1
77.237.146.28	Czech Republic	147.237.77.235	sviva.idf.il	Unauthorized URL Access to /	Block	1
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
188.138.17.205	France	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to 147.237.76.147/	Block	1
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2958.pdf	Block	1
104.131.87.17	United States	147.237.76.200	eitan.aka.idf.il	Unknown Parameter &l in www.eitan.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	1

11-07-2015-10:04:05 to 11-07-2015-11:04:05