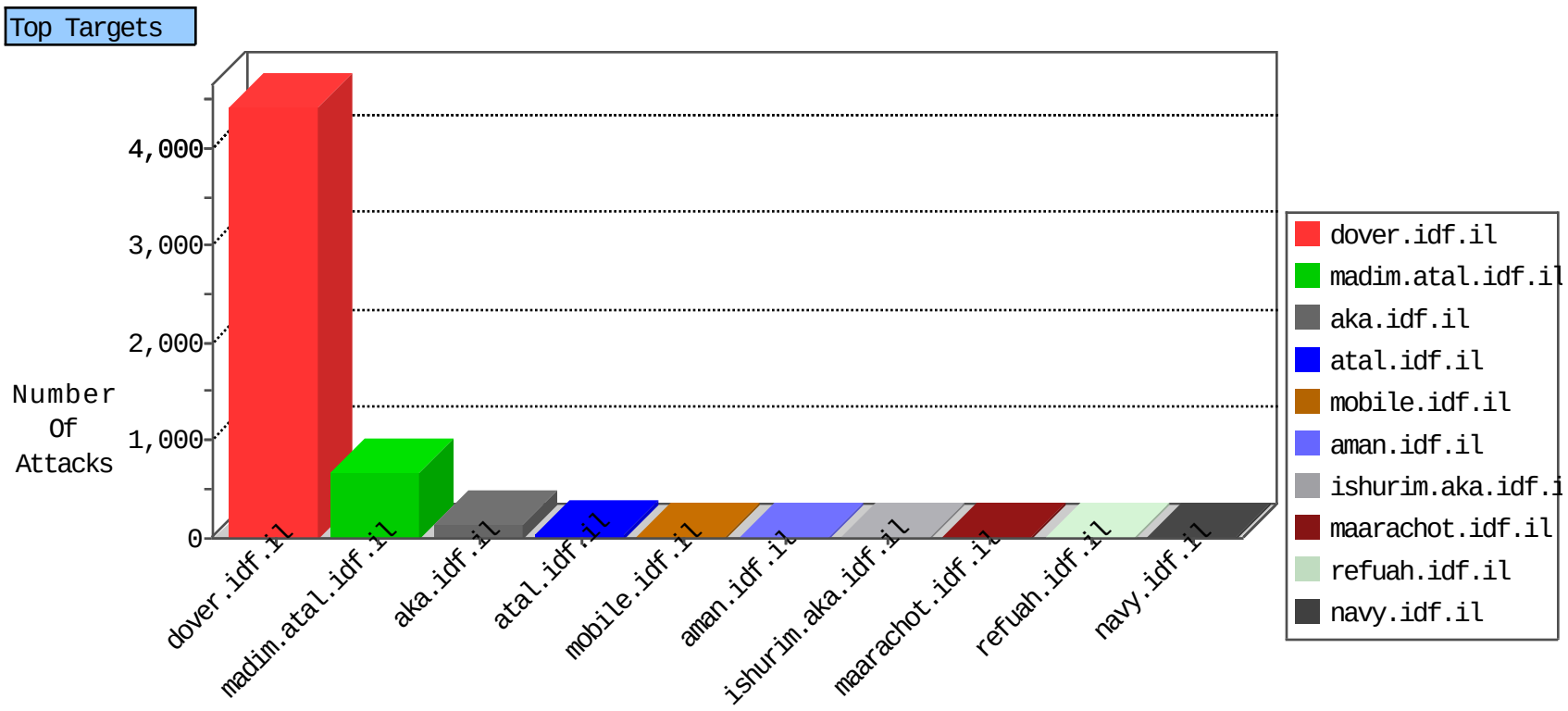
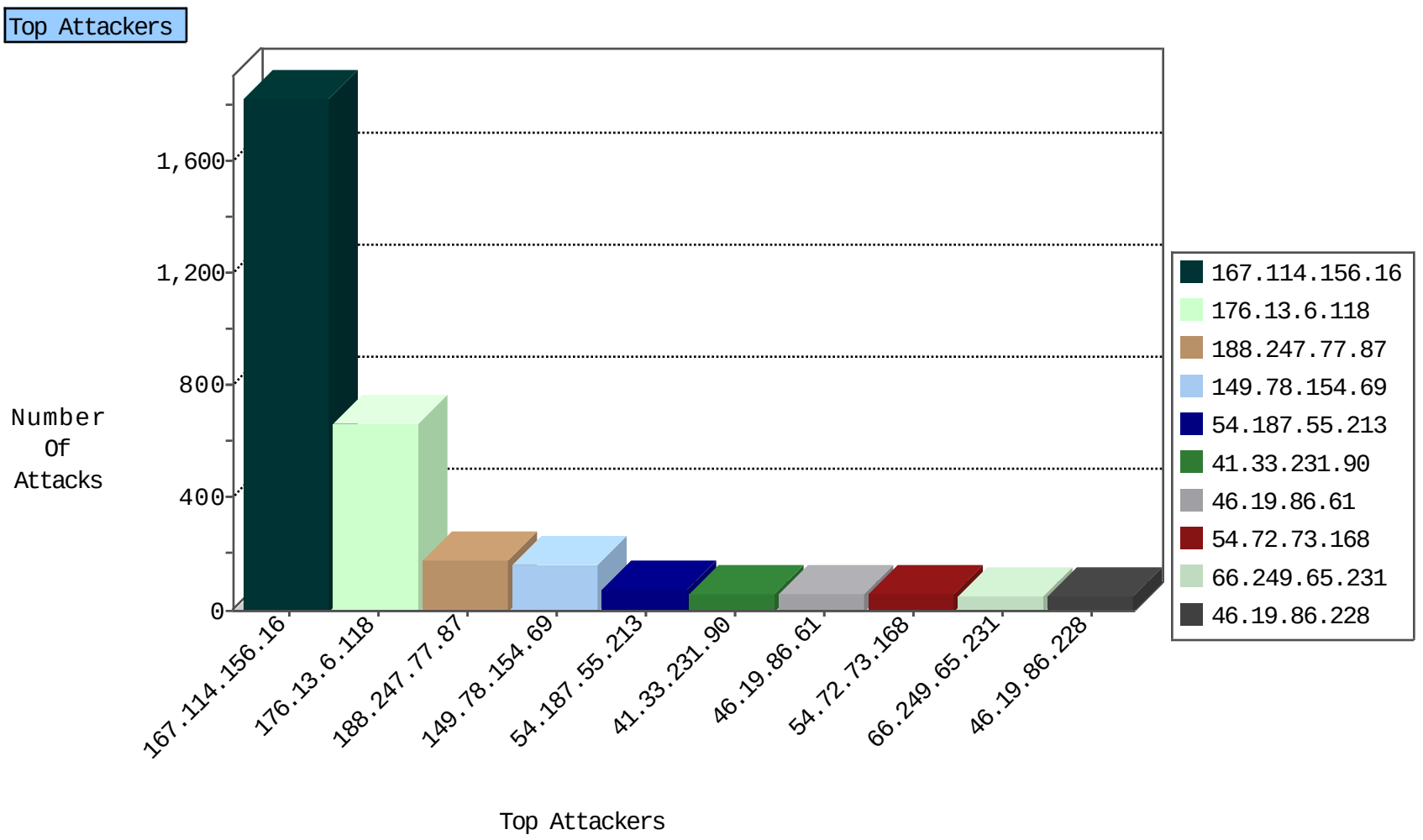
11-07-2015-15:04:01 to 11-07-2015-16:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-07-2015-15:04:01 to 11-07-2015-16:04:01

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	2883
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	339
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	81
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	60
213.57.144.71	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
46.120.228.218	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
156.184.123.122		147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
176.12.145.96	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
62.219.148.167	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
176.13.12.116	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
46.116.103.108	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
87.69.92.136	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
80.246.137.117	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
31.154.94.37	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.180.252.185	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
87.69.106.181	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
87.68.212.222	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
79.180.252.185	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.52.12.165	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
84.228.195.253	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.121.74.31	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
89.71.127.32	Poland	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
93.173.142.33	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
77.126.211.173	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
109.65.54.13	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
88.253.243.222	Turkey	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
146.185.57.7	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
77.126.72.51	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 unverified cookie	drop	2
84.111.48.73	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
40.77.167.9	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.86.144	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
176.12.151.150	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
85.64.157.155	Israel	147.237.72.166	aka.idf.il	Anomaly-TCP-shortheader	dest-reset	1
176.13.8.18	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
31.154.94.37	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
87.68.212.222	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
5.8.66.78	Russian Federation	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
85.64.157.155	Israel	147.237.72.166	aka.idf.il	Anomaly-TCP-SYN-FIN	dest-reset	1

11-07-2015-15:04:01 to 11-07-2015-16:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.230.25.249	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2

11-07-2015-15:04:01 to 11-07-2015-16:04:01

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	9
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
210.117.121.60	147.237.8.27	Korea, Republic of	e.madim.atal.idf.i	ET SCAN NMAP -sS window 3072	1
110.252.80.241	147.237.0.33	China	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
103.232.35.46	147.237.76.30	Hong Kong	himush.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.64.109	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
58.253.96.122	147.237.72.217	China	e.idf.il	ET SCAN NMAP -sS window 2048	1
46.151.52.8	147.237.77.212	Ukraine	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
202.79.243.160	147.237.77.216	Japan	dover.idf.il	Tehila - Perl LWP with fake user agent	1
176.13.12.101	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
103.232.35.46	147.237.76.30	Hong Kong	himush.idf.il	ET SCAN NMAP -sS window 4096	1
85.65.197.199	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
58.253.96.122	147.237.72.217	China	e.idf.il	ET SCAN NMAP -sS window 4096	1
58.253.96.122	147.237.72.217	China	e.idf.il	ET SCAN NMAP -f -sS	1
42.202.200.178	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

11-07-2015-15:04:01 to 11-07-2015-16:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
188.247.77.87	Jordan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	178
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	166
54.187.55.213	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	73
46.19.86.61	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	56
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	56
46.19.86.228	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	52
108.59.253.71	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
66.249.65.238	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38
66.249.65.231	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
5.246.161.206	Saudi Arabia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
46.120.106.45	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	35
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
212.179.90.106	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
79.181.118.103	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
87.69.80.220	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
79.179.191.191	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
109.64.227.152	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
80.246.133.206	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
31.154.94.11	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
64.229.49.203	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
66.102.8.238	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
79.180.129.34	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
77.126.220.88	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
176.13.9.246	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
23.27.245.15	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
82.80.25.221	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
157.55.39.89	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
1.39.63.152	India	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
87.69.189.34	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
66.249.65.224	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
79.178.55.202	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
80.246.130.57	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
80.246.130.198	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
100.100.91.13		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
88.253.243.222	Turkey	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
80.246.130.198	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
79.178.108.199	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
188.165.15.14	France	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
109.65.54.13	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
66.249.65.231	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
66.102.8.233	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.29.94.119	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.6.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	421
176.13.6.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	126
176.13.6.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	115
208.115.111.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	4
46.19.85.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.14.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.68.212.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
188.165.15.14	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
66.249.79.25	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
109.65.179.131	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	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
84.228.80.14	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
207.46.13.110	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
157.55.39.175	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-14322-he/dover.aspx×³Ö³Æ'Ö²Â¯Ö³â€šÖ²Â¿Ö³â€šÖ²Â½×³â‚ª×³Ã—×³Ö³Æ'Ö²Â¯Ö³â€šÖ²Â¿Ö³â€šÖ²Â½	Block	1
2.54.163.133	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1245-he/atal.aspx	Block	1
93.173.140.49	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
66.249.78.74	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/templatecontrols/news/www.google.com	Block	1
66.249.64.108	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
149.78.237.68	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/default.aspx	Block	1
85.65.176.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
37.46.39.222	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.64.42.109	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
199.187.122.91	United States	147.237.72.166	aka.idf.il	Unknown Parameter DocID in aka.idf.il/giyus/atuda/	None	1
149.88.150.212	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 149.88.150.212 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
85.250.146.250	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.104.168.50	United Kingdom	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
66.249.67.133	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
66.249.65.237	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-17805-he/dover.aspx	Block	1
199.203.186.162	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
151.80.31.136	Italy	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9841-he/refuah.aspx	Block	1
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/size100x0/3416.jpg	Block	1
109.163.234.5	Romania	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
79.180.228.150	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
207.46.13.72	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list20050529.htm	Block	1
157.55.39.34	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
2.54.161.5	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
87.68.212.222	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.69.41	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
176.13.11.78	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/size100x0/2617.jpg	Block	1
118.209.154.22	Australia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-14689-en/dover.aspx idf ground forces introduce new high-tech weapons	Block	1