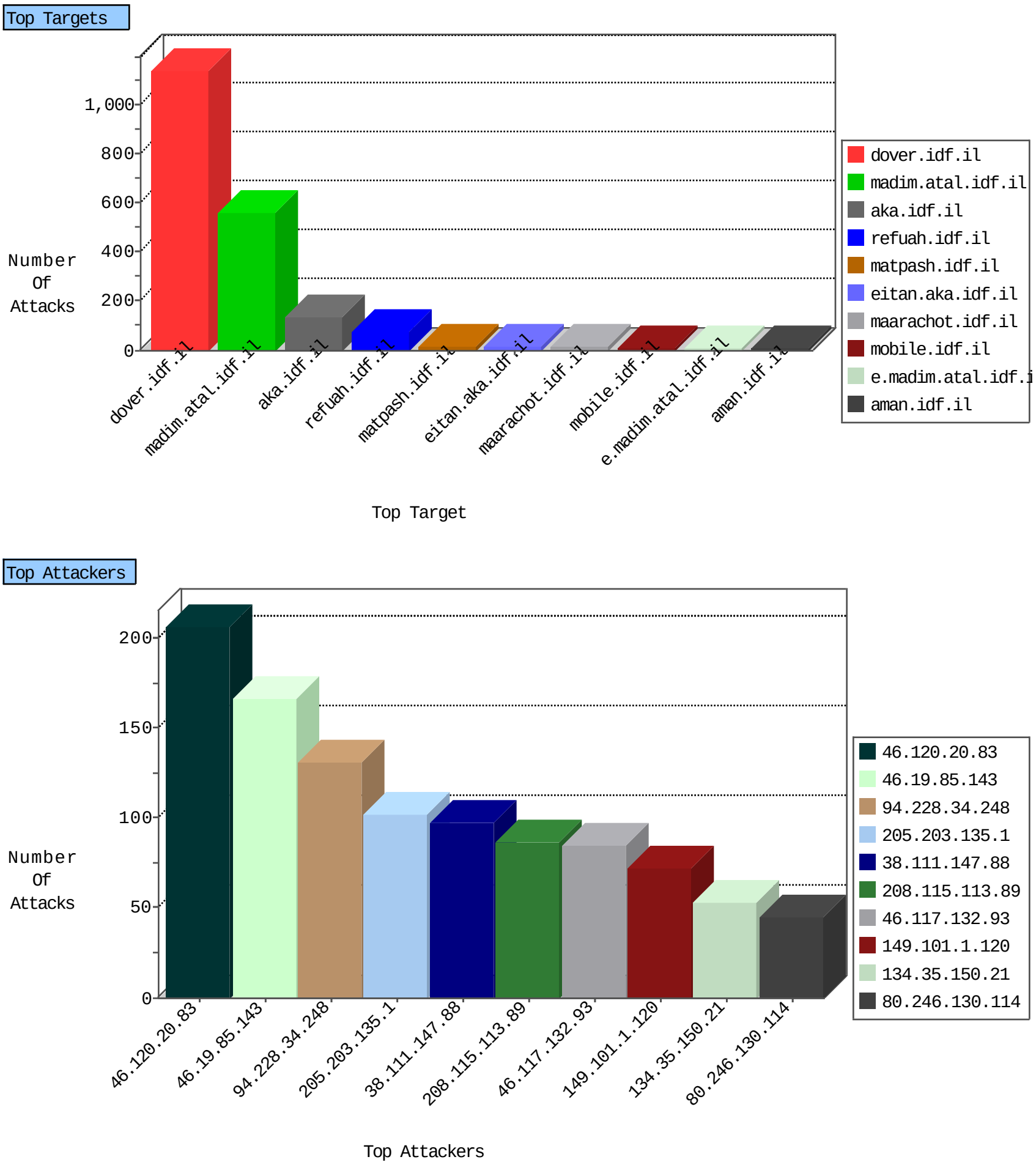
05-04-2016-23:04:04 to 05-05-2016-00:04:04

IDF Under Attack Daily Report



05-04-2016-23:04:04 to 05-05-2016-00:04:04

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	HTTP-POST-Segmented-DoS	dest-reset	531
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	530
66.249.73.192	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	322
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
222.221.132.193	China	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
71.6.165.200	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
118.19.92.65	Japan	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
151.80.110.211	France	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
185.103.252.24	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

05-04-2016-23:04:04 to 05-05-2016-00:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-04-2016-23:04:04 to 05-05-2016-00:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
85.65.194.134	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
66.249.64.186	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.69.104	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
174.37.194.144	147.237.8.27	United States	e.madim.atal.idf.i	ET SCAN NMAP -sS window 3072	1
174.37.194.144	147.237.8.27	United States	e.madim.atal.idf.i	ET SCAN NMAP -f -sS	1
40.76.80.20	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 4096	1
125.27.35.80	147.237.76.30	Thailand	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
40.76.60.52	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 4096	1
120.199.111.137	147.237.0.33	China	idf.il	ET SCAN NMAP -f -sS	1
112.169.84.95	147.237.76.200	Korea, Republic of	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
112.169.84.95	147.237.76.44	Korea, Republic of	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
112.169.84.95	147.237.76.31	Korea, Republic of	nakchal.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
112.169.84.95	147.237.0.34	Korea, Republic of	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1
174.37.194.144	147.237.8.27	United States	e.madim.atal.idf.i	ET SCAN NMAP -sS window 2048	1
66.240.213.93	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.140.23	147.237.8.27	United Kingdom	e.madim.atal.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
40.76.80.20	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
120.199.111.137	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 2048	1
40.76.60.52	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 3072	1
113.240.250.154	147.237.0.15	China	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
112.169.84.95	147.237.76.86	Korea, Republic of	navy.idf.il	ET SCAN Potential SSH Scan	1
112.169.84.95	147.237.76.38	Korea, Republic of	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
112.169.84.95	147.237.76.30	Korea, Republic of	himush.idf.il	ET SCAN Potential SSH Scan	1

05-04-2016-23:04:04 to 05-05-2016-00:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
94.228.34.248	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	131
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
38.111.147.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	98
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	87
149.101.1.120	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
80.246.130.114	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	44
37.26.146.213	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
134.35.150.21	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
173.240.18.221	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
185.99.45.49	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
66.249.73.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.50	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
198.58.102.95	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.50	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
73.52.143.72	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
198.58.96.215	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
198.58.103.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.177.153.250	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.20	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
79.177.153.250	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
50.205.33.70	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
185.89.217.233	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
157.55.39.134	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
85.130.132.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.50	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
66.249.73.137	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.26.146.195	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.20	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.50	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
87.71.111.62	Israel	147.237.0.19	madim.atal.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
185.99.45.49	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
107.72.162.63	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.53.33.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
128.242.249.12	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.216	Israel	147.237.0.19	madim.atal.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.93.184	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.120.20.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	205
46.19.85.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	167
46.117.132.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	85
2.53.19.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
46.19.85.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
87.71.111.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
46.19.85.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
84.228.252.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
132.64.31.133	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/article/mobile	Block	4
95.86.98.188	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	4
46.19.85.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.89.217.229	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.11.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.19.145	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtMobile in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	2
79.177.199.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.69.149.137	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 87.69.149.137	Block	2
185.89.217.233	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
68.180.231.43	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
213.8.204.72	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
87.71.111.62	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	1
73.198.47.13	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
188.0.236.221	Moldova, Republic of	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/hnap1/	Block	1
66.249.78.18	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	1
54.183.183.53	United States	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
109.253.133.97	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	1
66.249.66.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2348.jpg	Block	1
185.89.217.228	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
88.198.44.46	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
46.19.86.245	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	1
2.53.135.220	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
188.0.236.221	Moldova, Republic of	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/2370.jpg	Block	1
54.183.183.53	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	1
66.249.73.137	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1361-he/dover.aspx	Block	1
93.172.167.202	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 93.172.167.202	Block	1
5.153.234.154	Sweden	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
80.246.130.114	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
195.154.199.235	France	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/giyus/booklets.aspx	None	1
54.201.150.44	United States	147.237.76.147	chinuch.aka.idf.il	PHP Attempt	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Multiple Untraceable SSL Sessions from 169.229.3.91 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
87.69.149.137	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/8/	Block	1
70.88.119.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.78.4	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1396-he/atal.aspx	Block	1
46.118.156.202	Ukraine	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1133-he/dover.aspx	Block	1
5.153.234.154	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
84.228.175.166	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1