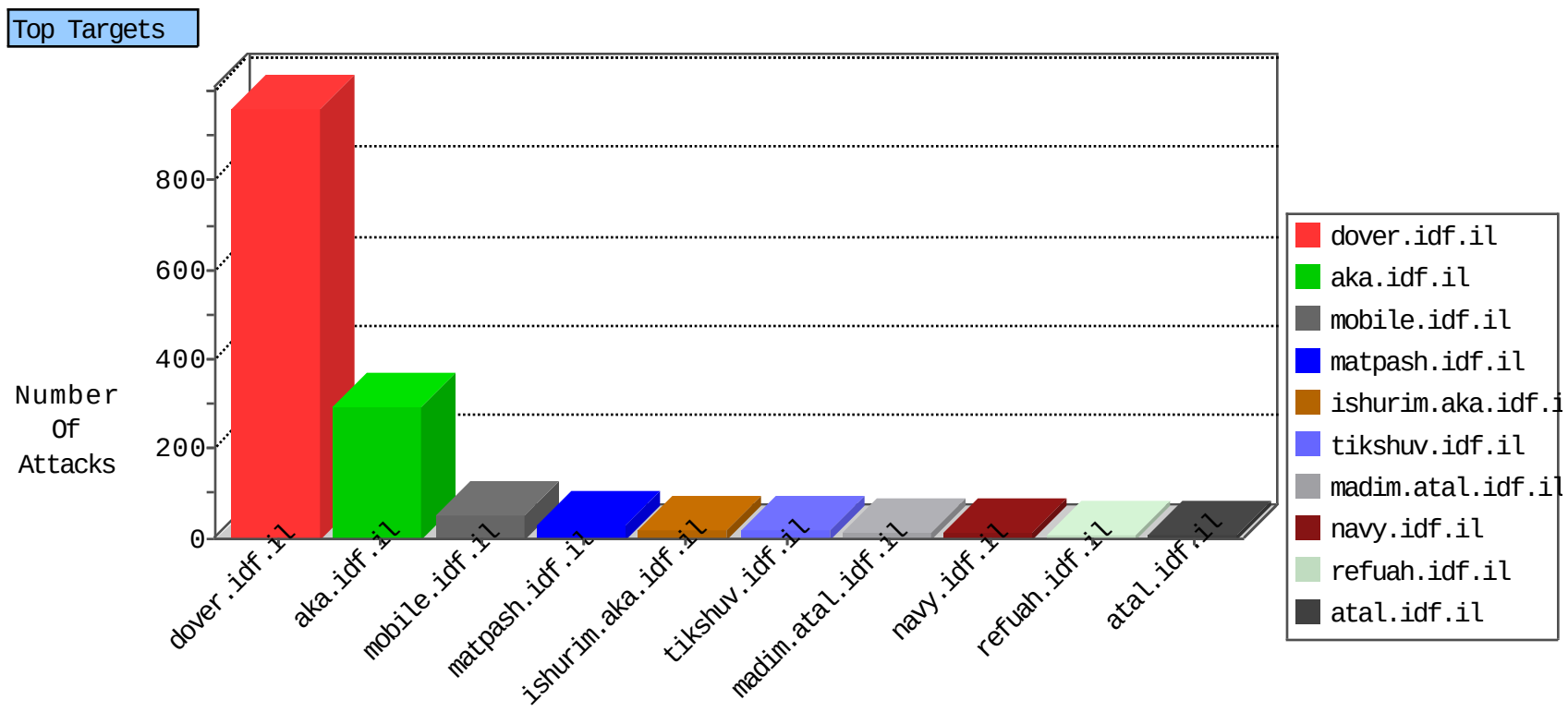
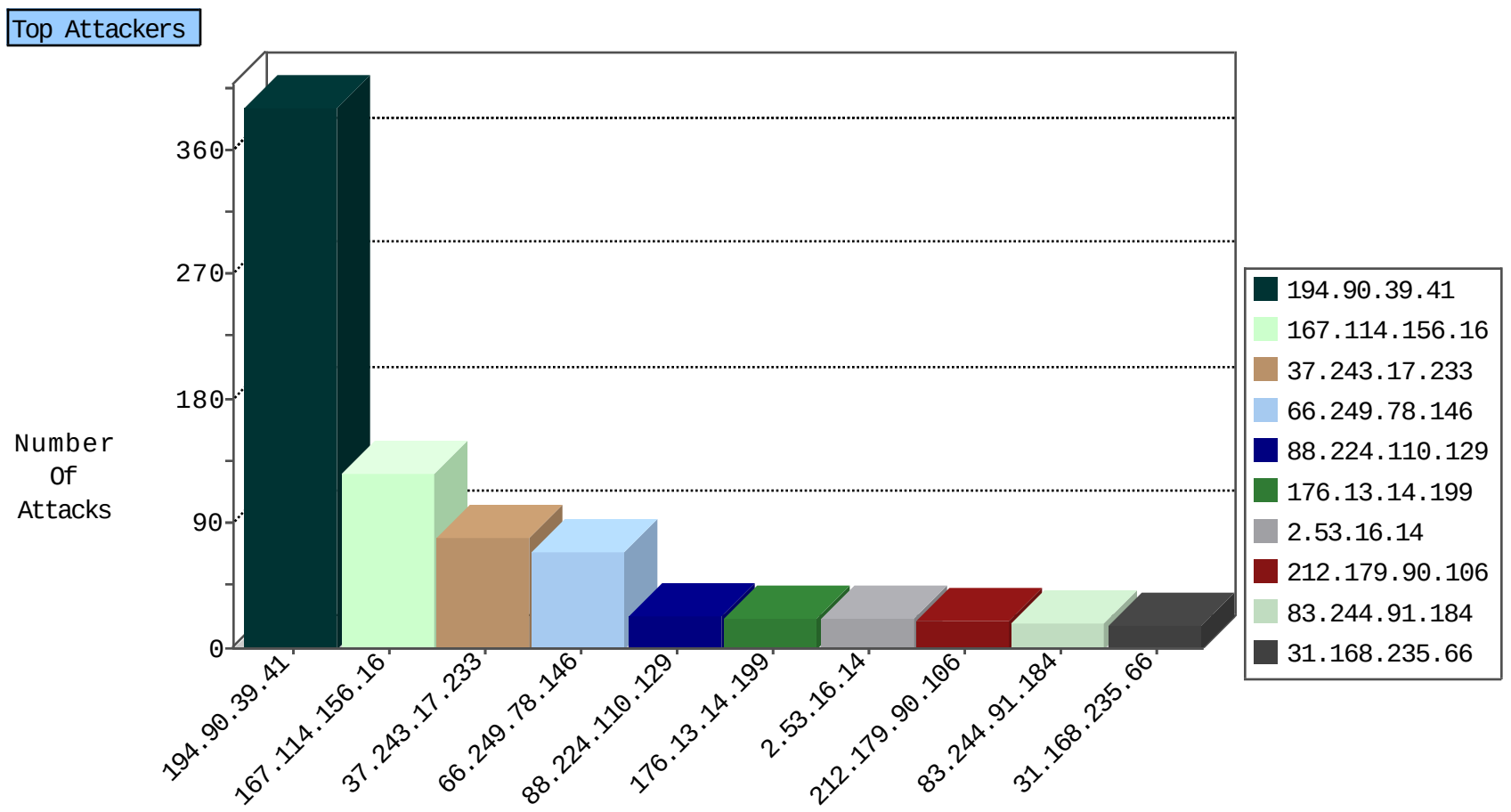
04-26-2016-15:04:05 to 04-26-2016-16:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-26-2016-15:04:05 to 04-26-2016-16:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	4509
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	4251
176.77.16.186	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3250
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	7
192.118.64.213	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
80.179.209.34	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2
71.6.135.131	United States	147.237.76.38	e.e.meitav.idf.i	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
211.111.21.34	Korea, Republic of	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

04-26-2016-15:04:05 to 04-26-2016-16:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-26-2016-15:04:05 to 04-26-2016-16:04:05

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	4
117.20.41.62	147.237.76.34	Singapore	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.77.179	Ukraine	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
88.224.110.129	147.237.77.176	Turkey	matpash.idf.il	SERVER-WEBAPP admin.php access	1
80.82.78.38	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
117.20.41.62	147.237.76.197	Singapore	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.77.179	Ukraine	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
88.249.106.23	147.237.76.44	Turkey	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
202.29.86.129	147.237.8.28	Thailand	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.20.173	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-26-2016-15:04:05 to 04-26-2016-16:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.90.39.41	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	391
37.243.17.233	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	80
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	68
2.53.16.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
176.13.14.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
31.168.235.66	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
94.159.153.77	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
83.244.91.184	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.15.255	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
31.154.251.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
144.76.93.46	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.95	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.232	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
69.175.127.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
37.26.149.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
88.224.110.129	Turkey	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
107.170.186.68	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	7
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
94.159.181.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.64.248.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.71.37.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.19	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.16.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.101.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.126.69.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
83.244.91.184	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
66.249.93.247	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
132.64.30.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.242.21	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
204.237.2.151	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.102.242.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.116.24.12	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
157.55.39.154	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
185.4.255.170	Lebanon	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	5
73.34.149.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.39.74	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.46	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.147.218	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
82.205.16.88	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

04-26-2016-15:04:05 to 04-26-2016-16:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.142.68.61	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.142.68.61	Block	10
2.53.155.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
88.224.110.129	Turkey	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 88.224.110.129	Block	6
87.68.22.67	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 87.68.22.67	Block	5
88.224.110.129	Turkey	147.237.77.176	matpash.idf.il	PHP Attempt	Block	4
88.224.110.129	Turkey	147.237.77.176	matpash.idf.il	Multiple Admin Blocking from 88.224.110.129	Block	4
213.8.71.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.8.71.26	Block	3
5.29.107.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.177	Israel	147.237.76.86	navy.idf.il	Distributed Abnormally Long Request	Block	2
46.19.85.177	Israel	147.237.76.86	navy.idf.il	Distributed Malformed URL	Block	2
46.19.85.177	Israel	147.237.76.86	navy.idf.il	Distributed Unknown HTTP Request Method	Block	2
78.40.183.202	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
54.237.118.69	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
185.4.255.170	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
141.212.122.161	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	1
80.246.136.19	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
213.254.241.7	France	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$btnSearch in www.aka.idf.il/main/sachar/default.aspx	None	1
66.249.79.87	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx	Block	1
46.120.96.28	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
175.44.15.154	China	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/miluim/about.aspx	Block	1
79.176.100.111	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
66.102.8.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
194.90.128.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.90.128.185	Block	1
149.50.12.164	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/general/mobile	Block	1
46.19.85.177	Israel	147.237.76.86	navy.idf.il	Distributed Illegal HTTP Version	Block	1
84.111.42.164	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
54.149.253.151	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
175.44.15.154	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 175.44.15.154	Block	1
37.142.68.61	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/contactus/mobile	Block	1
79.176.100.111	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
212.47.238.193	France	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
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2367.jpg	Block	1
149.50.89.238	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/9/113579.pdf)	Block	1
2.53.182.87	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
54.194.11.113	Ireland	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
175.44.15.154	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.142.68.61	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/homepage/mobile	Block	1
79.176.100.111	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/3141.jpg	Block	1
157.55.39.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.55.155.152	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
88.224.110.129	Turkey	147.237.77.176	matpash.idf.il	Admin Blocking	Block	1
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
54.206.115.22	Australia	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
184.105.247.195	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
141.212.122.161	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
40.77.167.53	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/גיליונות	Block	1

04-26-2016-15:04:05 to 04-26-2016-16:04:05