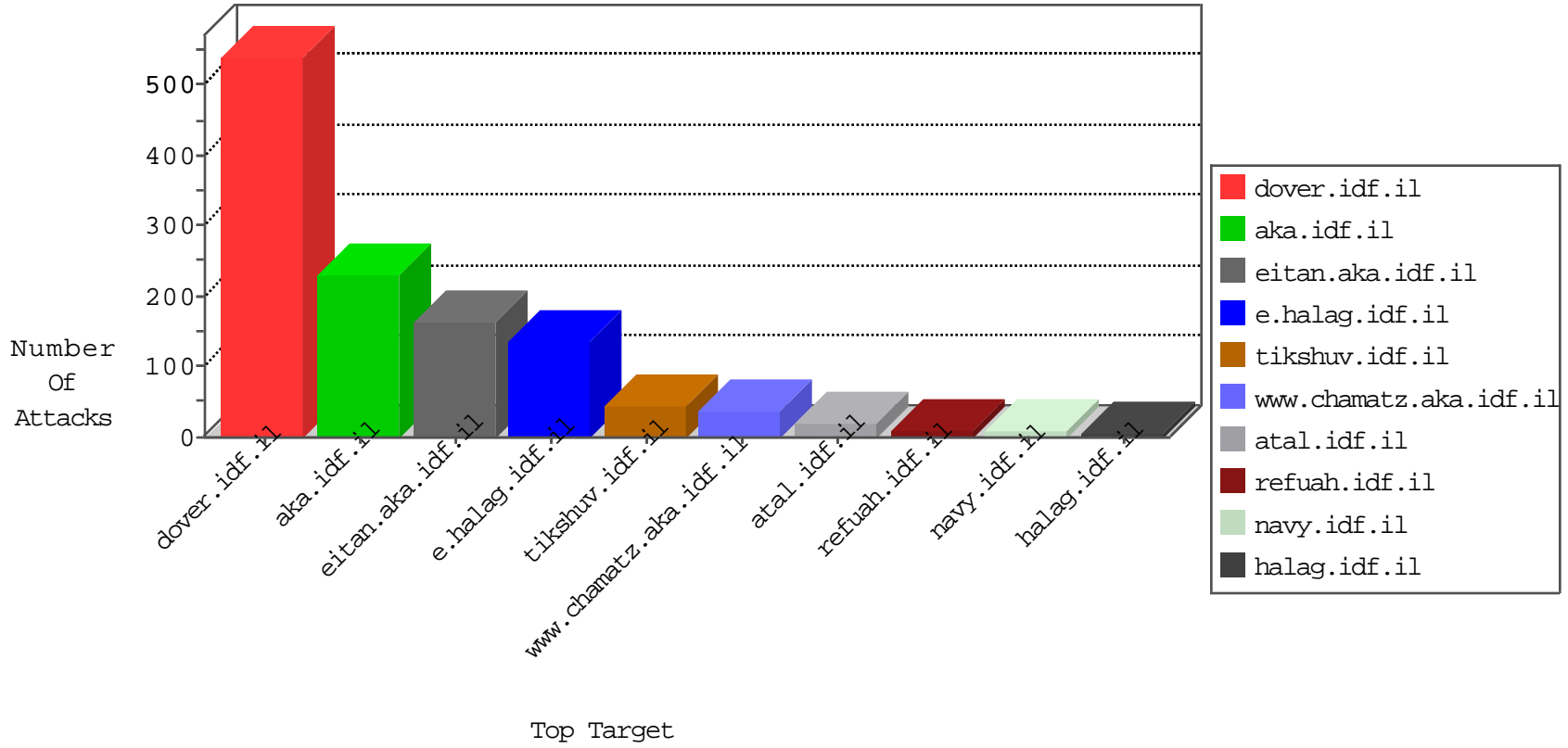


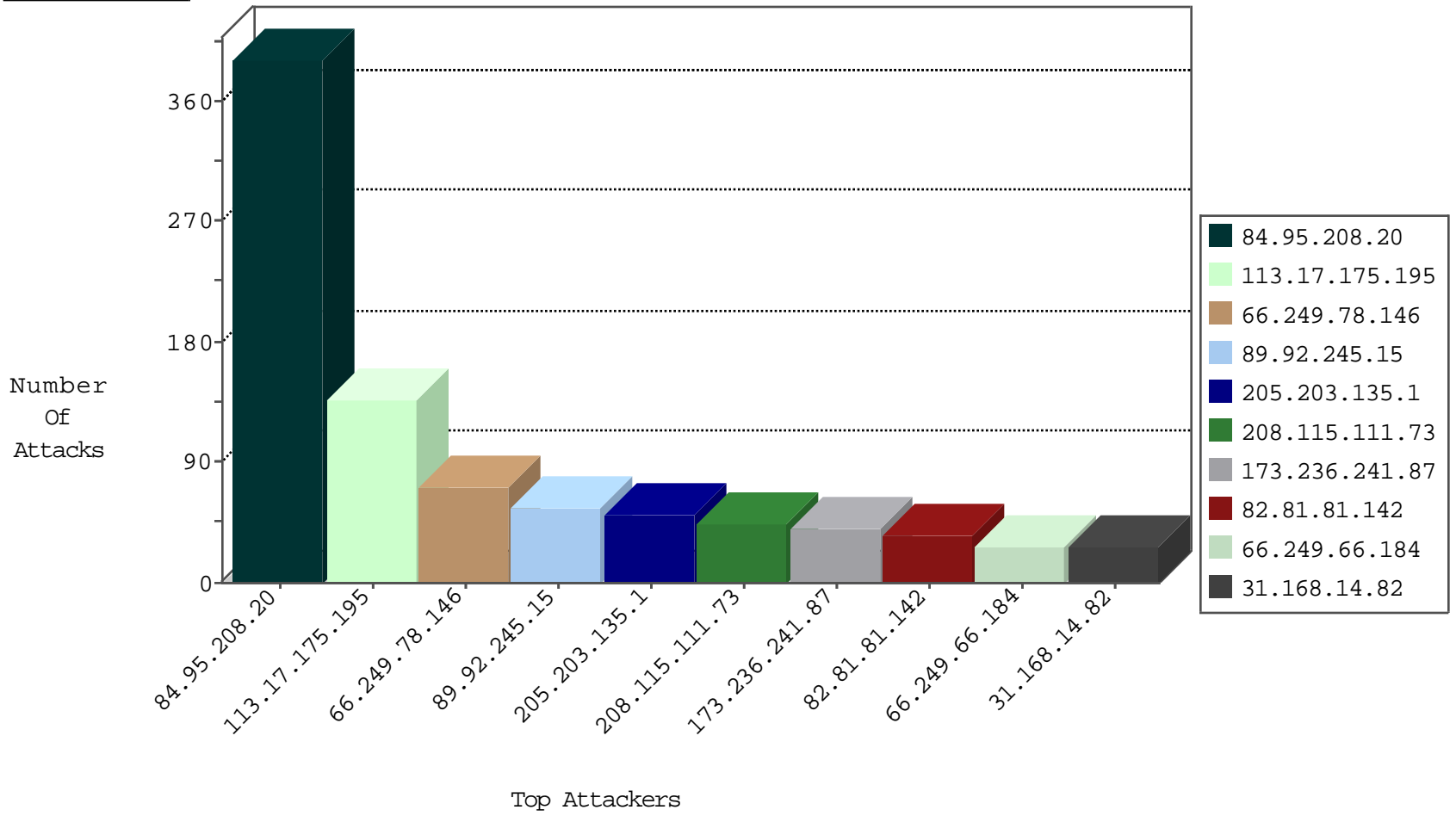
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
113.17.175.195	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	136
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
81.218.65.210	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
173.208.197.254	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
69.30.198.146	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
69.30.198.148	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
123.151.42.61	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1
74.91.18.45	United States	147.237.77.19	law-forum.idf.il	block-sp-traf1	drop	1
107.150.32.58	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	drop	1
125.202.88.129	Japan	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
74.91.20.196	United States	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1
185.103.252.98	Russian Federation	147.237.76.148	ggcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
107.150.32.59	United States	147.237.77.233	atal.idf.il	block-sp-traf1	drop	1
69.30.198.149	United States	147.237.77.234	halag.idf.il	block-sp-traf1	drop	1
173.208.197.252	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

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

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
89.92.245.15	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
173.236.241.87	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
82.81.81.142	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
31.168.14.82	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
82.165.137.121	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
95.91.210.156	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
82.81.81.138	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
50.116.30.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
93.158.152.201	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.173	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.46.41.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
82.81.55.167	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
174.69.169.216	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
157.55.39.26	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
40.77.167.59	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.78.223	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.82.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.9.122.203	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.184	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.100.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.64.167	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.195.110	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.93.249	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.64.170	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.64.172	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.199	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
8.37.70.243	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.64.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

04-25-2016-02:04:03 to 04-25-2016-03:04:03

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
82.81.81.146	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	122
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	72
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	25
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	12
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	10
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	8
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	7
149.202.239.134	France	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	6
149.202.239.135	France	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1283-en/dover.aspx parameter PageNum	Block	6
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	5
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	3
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
40.77.167.59	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
207.46.13.173	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.95.208.20	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
54.210.18.124	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
207.46.13.63	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.66.184	Block	1
141.212.122.129	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to /x	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/div.item	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
164.132.161.91	Italy	147.237.72.166	aka.idf.il	Unauthorized Method GET for www.aka.idf.il/iturim/asp/searchresults.asp	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/tmuna/	Block	1
117.78.13.18	China	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/robots.txt	Block	1
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/894-en	Block	1
52.29.5.56	Germany	147.237.77.74	law.idf.il	Suspicious Response Code	Block	1
173.208.197.254	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.xy966.com/	Block	1
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	1
66.249.64.191	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/m/templates/getfile/getfile.aspx	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/daily	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/piwik.php	Block	1
149.202.239.134	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
52.29.5.56	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
141.212.122.129	United States	147.237.76.30	himush.idf.il	Unauthorized URL Access to /x	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
54.210.18.124	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/2/	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	1
141.212.122.129	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /x	Block	1