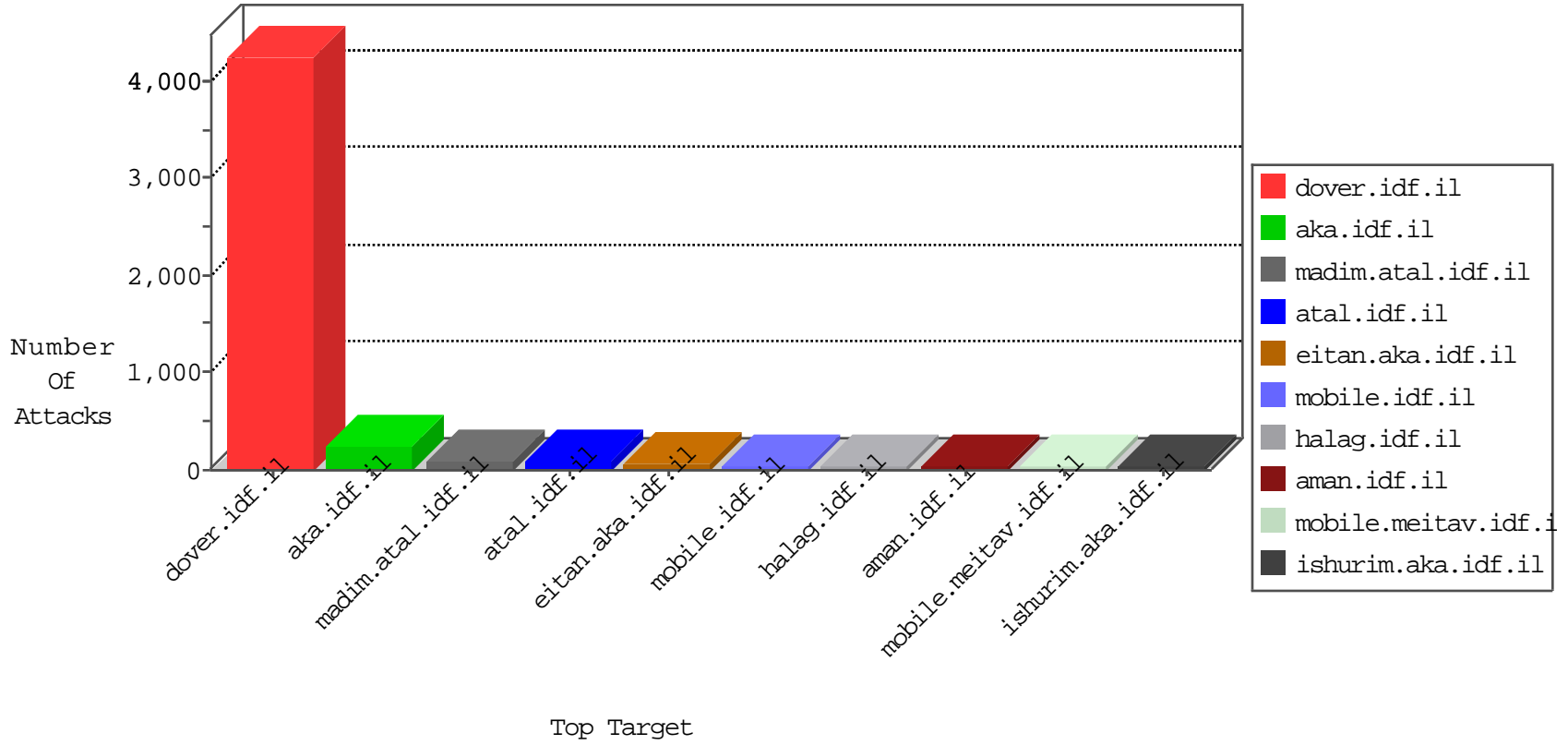


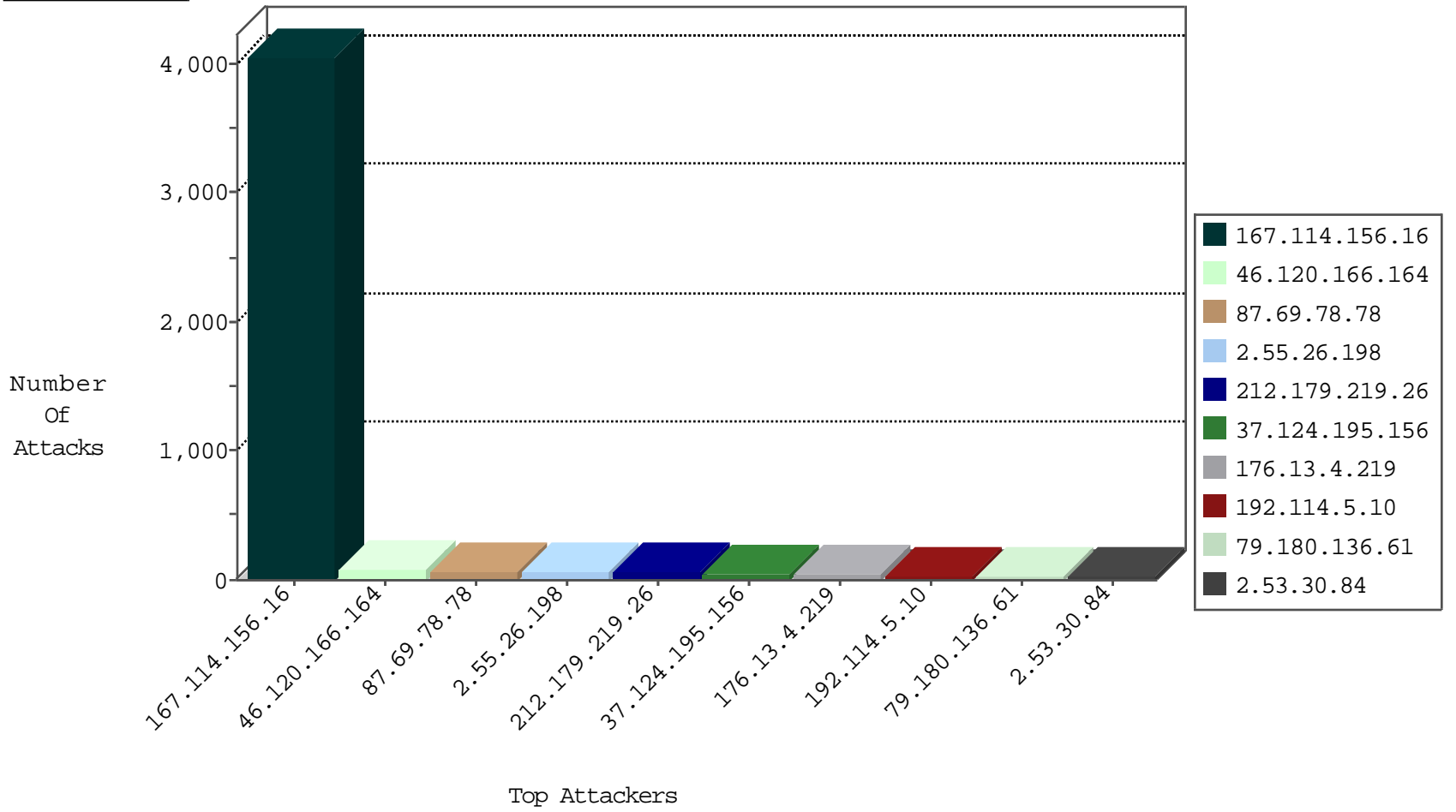
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4059
69.30.226.101	United States	147.237.77.233	atal.idf.il	block-sp-trafl	forward	2
204.12.196.235	United States	147.237.77.19	law-forum.idf.il	block-sp-trafl	forward	2
69.30.198.146	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-trafl	forward	2
204.12.196.236	United States	147.237.76.42	refuah.idf.il	block-sp-trafl	forward	2
69.30.202.226	United States	147.237.77.74	law.idf.il	block-sp-trafl	forward	2
173.208.197.253	United States	147.237.76.42	refuah.idf.il	block-sp-trafl	forward	2
180.97.106.161	China	147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.116	Netherlands	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	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
46.120.166.164	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	76
37.124.195.156	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
87.69.78.78	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
176.13.4.219	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
2.53.30.84	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
212.179.219.26	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
79.180.136.61	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
176.13.17.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.144.62.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.179.219.26	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
79.182.147.73	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
41.239.11.239	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
176.13.12.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
82.80.181.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.179.141.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.179.219.26	Israel	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	9
79.180.136.61	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
87.69.153.226	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
80.246.136.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
37.46.39.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.176.31.125	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.22.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.114.23.211	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.147.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.219.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
93.172.160.120	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
2.55.38.218	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.130.203	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.182.34.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.120.166.164	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
93.173.231.81	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.182.147.73	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
79.178.141.206	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
176.13.4.219	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
93.172.160.120	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
66.249.93.148	Europe	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5
80.246.136.178	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
116.66.197.134	Nepal	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.179.219.26	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
79.177.186.186	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
212.179.219.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
80.246.136.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
79.177.186.186	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
212.179.219.26	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
80.246.136.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.142.64.6	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
157.55.2.172	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
80.246.130.203	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.26.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
192.114.5.10	Israel	147.237.76.39	mobile.meitav.idf.il	Distributed Suspicious Response Code	Block	30
87.69.78.78	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 87.69.78.78	Block	19
84.95.198.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
117.25.155.110	China	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 117.25.155.110	Block	9
176.13.12.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
109.253.202.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
79.181.98.82	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	4
79.181.98.82	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/4/	Block	3
198.245.51.13	Canada	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
93.173.135.244	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	3
198.245.51.13	Canada	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	3
2.55.38.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.225.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	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
217.195.174.105	Czech Republic	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g5lei5nuhg	Block	2
2.55.3.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.148.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.102.7.226	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
89.138.40.42	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 89.138.40.42	Block	2
207.46.13.178	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/894-he/nakhal.aspx)	Block	1
66.249.66.177	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/resources/scripts/mootools.ext.js	Block	1
185.3.147.245	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz/res#012ources/images/innerpage/goback.gif	Block	1
39.41.55.136	Pakistan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
66.249.66.99	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_	Block	1
2.55.38.218	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
89.138.40.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19748-he/idfgdover.aspx	Block	1
185.3.147.245	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 185.3.147.245	Block	1
117.25.155.110	China	147.237.76.86	navy.idf.il	Admin Blocking	Block	1
46.120.166.164	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
87.69.78.78	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/opmissingperson/mobile	Block	1
2.53.36.216	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/general/mobile	Block	1
204.12.196.235	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to www.369bs.com/	Block	1
79.179.164.43	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1
66.249.66.103	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
5.148.27.54	United Kingdom	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
93.172.160.120	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
84.228.0.52	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct137 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
188.10.117.186	Italy	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
69.30.198.146	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to www.app-softwares.com/	Block	1
117.25.155.110	China	147.237.76.86	navy.idf.il	Multiple Admin Blocking from 117.25.155.110	Block	1
46.121.159.172	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	1
87.69.78.78	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/homepage/mobile	Block	1
204.12.196.237	United States	147.237.72.167	ishurim.aka.idf.il	Distributed Unauthorized URL Access on www.369bs.com/	Block	1
79.181.98.82	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 79.181.98.82	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/size100x0/2808.jpg	Block	1
176.67.114.223	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
87.69.78.78	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 87.69.78.78	Block	1