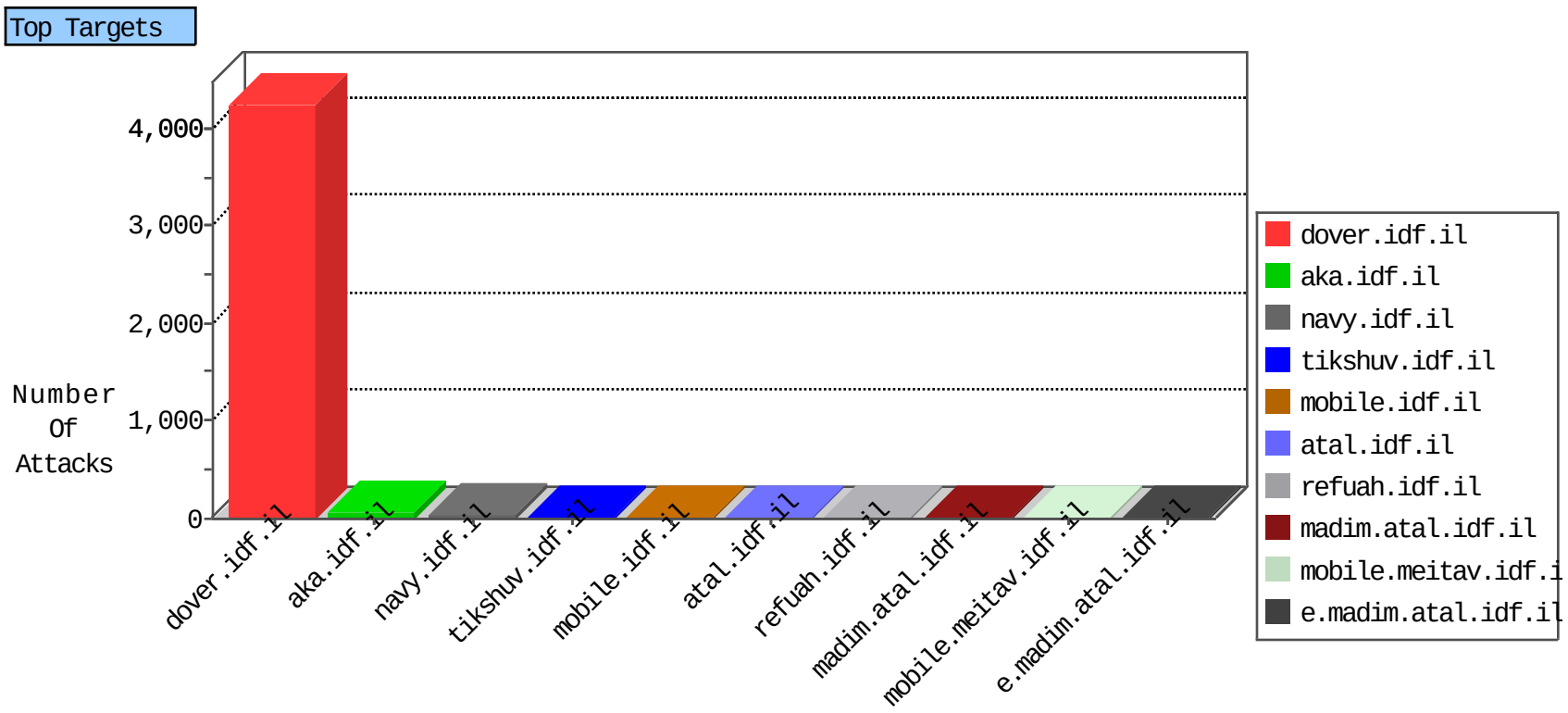
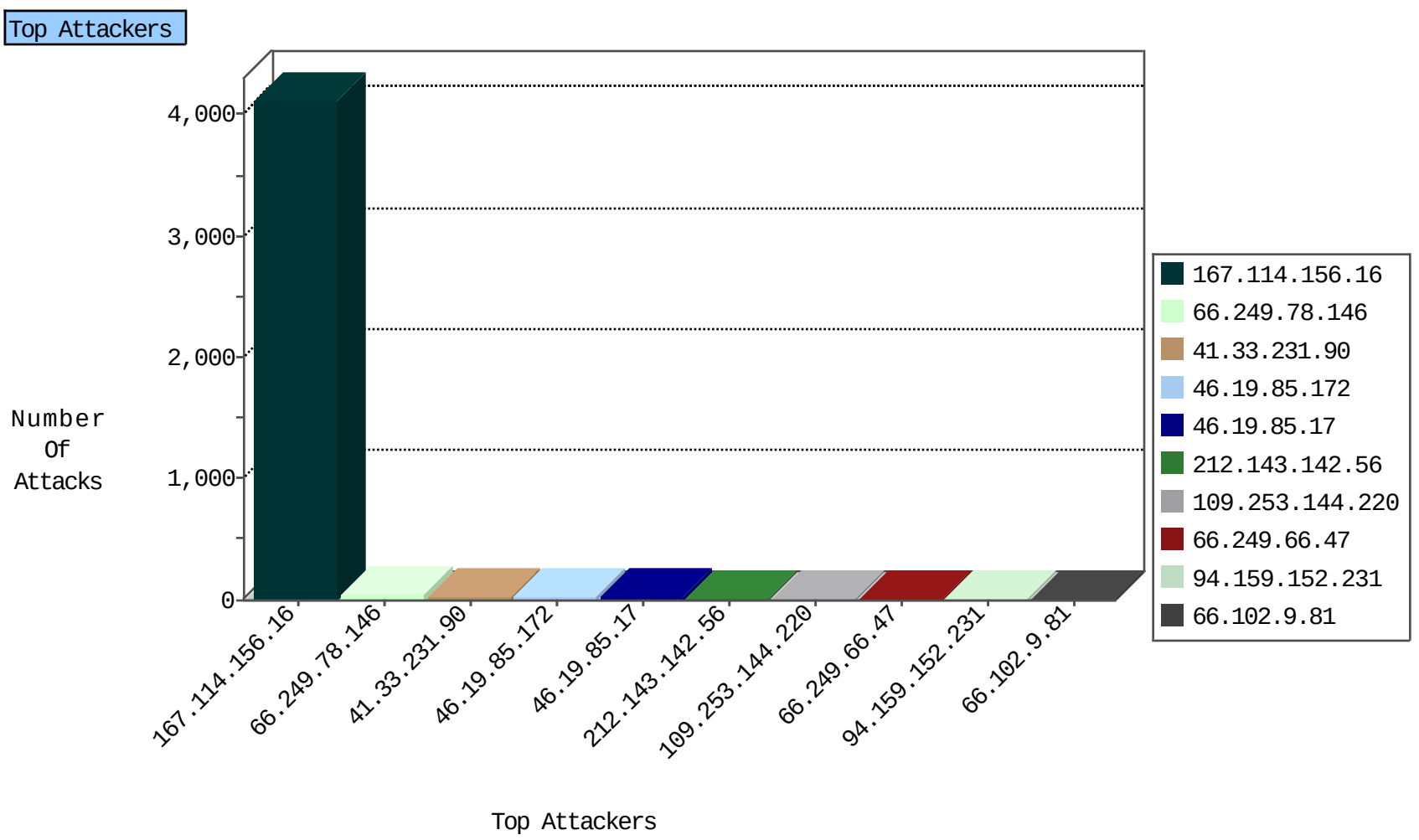
04-14-2016-07:04:09 to 04-14-2016-08:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-14-2016-07:04:09 to 04-14-2016-08:04:09

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	4112
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
82.81.90.118	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
184.105.139.88	United States	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	1
162.216.114.158	United States	147.237.77.235	sviva.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.112	United States	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
103.1.92.135	Nepal	147.237.0.35	akaws.idf.il	L4 Source or Dest Port Zero	drop	1
184.105.139.68	United States	147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
162.216.114.158	United States	147.237.77.234	halag.idf.il	Block_Udp_All_Nets	drop	1

04-14-2016-07:04:09 to 04-14-2016-08:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.159.152.231	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
185.106.92.47	Russian Federation	147.237.76.39	mobile.meitav.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	4
109.253.146.200	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
40.77.167.92	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
79.177.13.231	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
185.106.92.47	Russian Federation	147.237.76.39	mobile.meitav.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
66.249.66.158	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

04-14-2016-07:04:09 to 04-14-2016-08:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	37
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
185.106.92.47	147.237.76.39	Russian Federation	mobile.meitav.idf.il	ET WEB_SERVER Muieblackcat scanner	1
109.87.13.248	147.237.76.39	Ukraine	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
46.4.79.76	147.237.72.14	Germany	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
109.87.13.248	147.237.76.42	Ukraine	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
107.158.255.194	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1

04-14-2016-07:04:09 to 04-14-2016-08:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
66.249.66.47	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.17	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.172	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.17	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.172	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.144.220	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.102.9.81	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.17	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.17	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.179.21.194	Israel	147.237.8.27	e.madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
64.233.172.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.172	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.86.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.154.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.179.22.235	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.16.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.134.81	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.102.9.91	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	3
37.26.147.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.235.98.139	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
109.253.144.220	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.66.141	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
80.178.9.129	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
212.235.98.139	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
2.53.167.91	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
2.53.9.24	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
64.233.172.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.144.220	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
141.212.122.205	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
84.191.4.97	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.39.222.159	Netherlands	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.27	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
64.233.172.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.139.112	United States	147.237.0.35	akaws.idf.il	drop		drop	1
37.26.148.210	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
82.80.159.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.106	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.53.62.12	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
198.20.69.98	United States	147.237.76.199	e.nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.206	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
103.237.74.34	Hong Kong	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
5.39.222.159	Netherlands	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.210	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.26.149.166	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

04-14-2016-07:04:09 to 04-14-2016-08:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.183.16	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	4
109.253.209.206	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	3
80.179.22.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
62.90.11.134	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/templatecontrols/generic/	Block	3
176.13.19.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 68.180.230.45	Block	1
5.39.222.159	Netherlands	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
178.238.37.158	Czech Republic	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
83.27.132.105	Poland	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.64.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
203.127.58.236	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
119.73.253.6	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.75.79.101	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/33/	Block	1
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/eitan/mesiratmeida/	Block	1
50.62.161.206	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
184.168.152.148	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on refua.atal.idf.il/test/wp-admin/	Block	1
83.27.132.105	Poland	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/wp-login.php	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
203.127.96.245	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.65	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/elram	Block	1
79.178.23.62	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
219.74.166.247	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
58.64.181.66	Hong Kong	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
185.77.91.113	Turkey	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/index.php	Block	1
84.191.4.97	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/an	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/1/3251.pdf	Block	1
203.127.96.253	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.234	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/templates/inner.asp	Block	1
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	1
109.65.230.223	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
207.46.13.192	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
5.39.222.159	Netherlands	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
81.31.35.48	Czech Republic	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on refua.atal.idf.il/wp-admin/	Block	1
62.90.131.122	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
198.71.230.19	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1

04-14-2016-07:04:09 to 04-14-2016-08:04:09