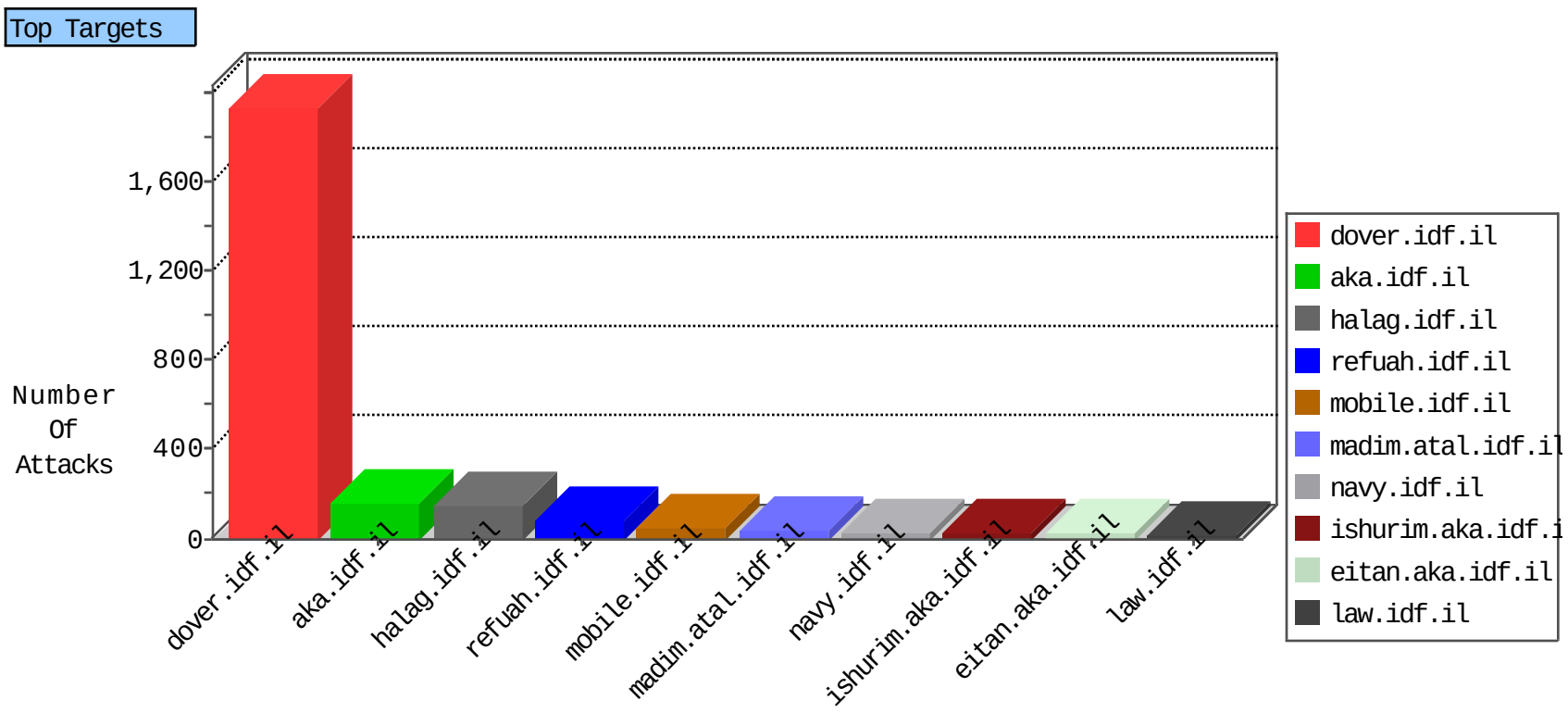
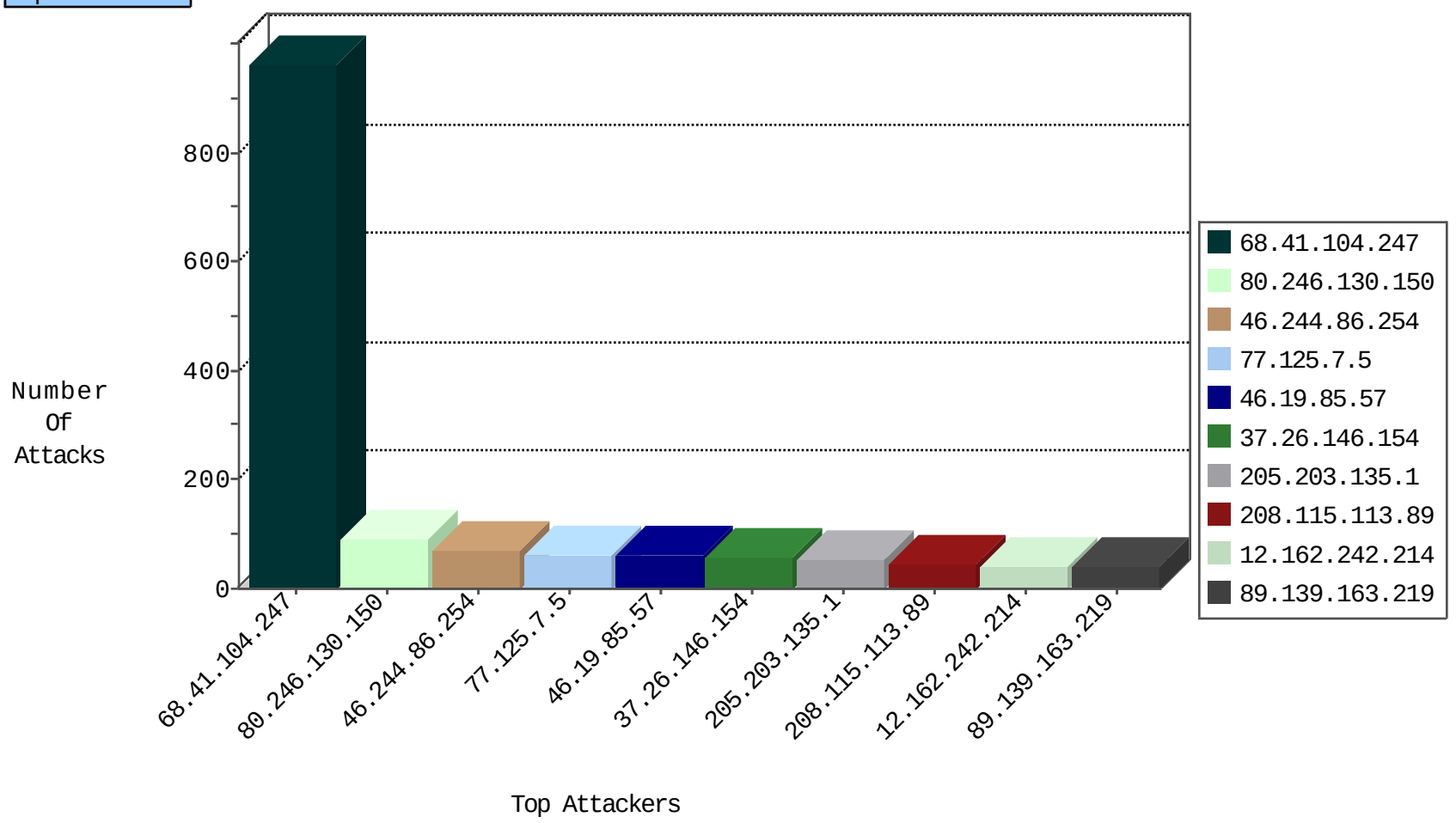
05-03-2016-23:04:01 to 05-04-2016-00:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



05-03-2016-23:04:01 to 05-04-2016-00:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.79.89	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3409
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	28
66.249.65.121	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	5
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
71.6.216.51	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
218.57.11.7	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
123.56.204.153	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
69.197.185.18	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	drop	1
185.94.111.1	Russian Federation	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
71.6.216.56	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
69.197.185.21	United States	147.237.72.156	aman.idf.il	block-sp-traf1	drop	1
185.94.111.1	Russian Federation	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.116	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	1
69.197.185.21	United States	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1
185.94.111.1	Russian Federation	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
107.150.32.59	United States	147.237.77.19	law-forum.idf.il	block-sp-traf1	drop	1

05-03-2016-23:04:01 to 05-04-2016-00:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-03-2016-23:04:01 to 05-04-2016-00:04:01

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
174.37.194.144	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
220.188.80.214	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	2
66.102.6.131	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
220.188.80.214	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
220.188.80.214	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
220.188.80.214	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	2
220.188.80.214	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	2
220.188.80.214	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
80.82.64.146	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
220.188.80.214	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
220.188.80.214	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
220.188.80.214	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
220.188.80.214	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
203.86.29.220	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
220.188.80.214	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	147.237.77.216	United States	dover.idf.il	ET DROP Dshield Block Listed Source	1
220.188.80.214	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1
220.188.80.214	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.64.146	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.57.11.7	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
220.188.80.214	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
203.86.29.220	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1
203.86.29.220	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -f -sS	1

05-03-2016-23:04:01 to 05-04-2016-00:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
68.41.104.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	916
80.246.130.150	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	88
46.244.86.254	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
77.125.7.5	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	61
37.26.146.154	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
12.162.242.214	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
89.139.163.219	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	39
199.58.86.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
37.26.146.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
66.249.65.65	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
64.233.172.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
46.19.85.57	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
5.22.131.20	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
79.176.127.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	18
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
46.19.85.57	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	17
64.233.172.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
66.249.65.21	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	17
2.248.19.136	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
46.19.86.189	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.57	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
198.58.103.160	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.180.116.100	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
45.59.183.96	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.57	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
82.166.165.147	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	9
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.115	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
66.249.79.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
84.108.145.24	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.102.8.243	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.79.107	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
198.58.103.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.79.107	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.53.180.224	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.20.61	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.141.231	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.79.107	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.79.107	Israel	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	6
188.120.148.158	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.122	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.165.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
46.19.86.189	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.86.189	Block	6
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
85.64.112.89	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	4
66.102.8.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.220.145.244	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.86.189	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	2
2.53.19.152	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 2.53.19.152	Block	2
46.19.86.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.143.159.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/5/size100x0/3365.jpg	Block	1
176.13.20.61	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
85.64.112.89	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/3/	Block	1
46.19.85.127	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.127	Block	1
66.249.79.114	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
66.249.65.217	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/7/67537.pdf	Block	1
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.255.253.15	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/favicon.ico	Block	1
77.125.7.5	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout.css	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/expand.js	Block	1
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
208.109.252.167	United States	147.237.0.34	tikshuv.idf.il	Admin Blocking	Block	1
85.65.83.146	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/newsarchive.aspx	Block	1
46.19.85.252	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.65.224	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
46.19.86.231	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	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
5.255.253.75	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
79.182.124.136	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1810-he/	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery.plugins/jquery.charts.js	Block	1
208.109.252.167	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/admin/	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
89.139.163.219	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
2.53.19.152	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/newsflash/mobile	Block	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
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/datepicker.css	Block	1
157.55.39.91	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1392-en/cogat.asp	Block	1
80.246.130.150	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
46.19.85.127	Israel	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 46.19.85.127	Block	1
66.249.79.44	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
66.220.145.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
98.100.198.111	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.19.86.189	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	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
66.249.66.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
46.117.107.241	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
173.252.88.91	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1810-he/	Block	1
46.19.85.127	Israel	147.237.77.216	dover.idf.il	Multiple Malformed URL from 46.19.85.127	Block	1
66.249.79.107	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.107	Block	1