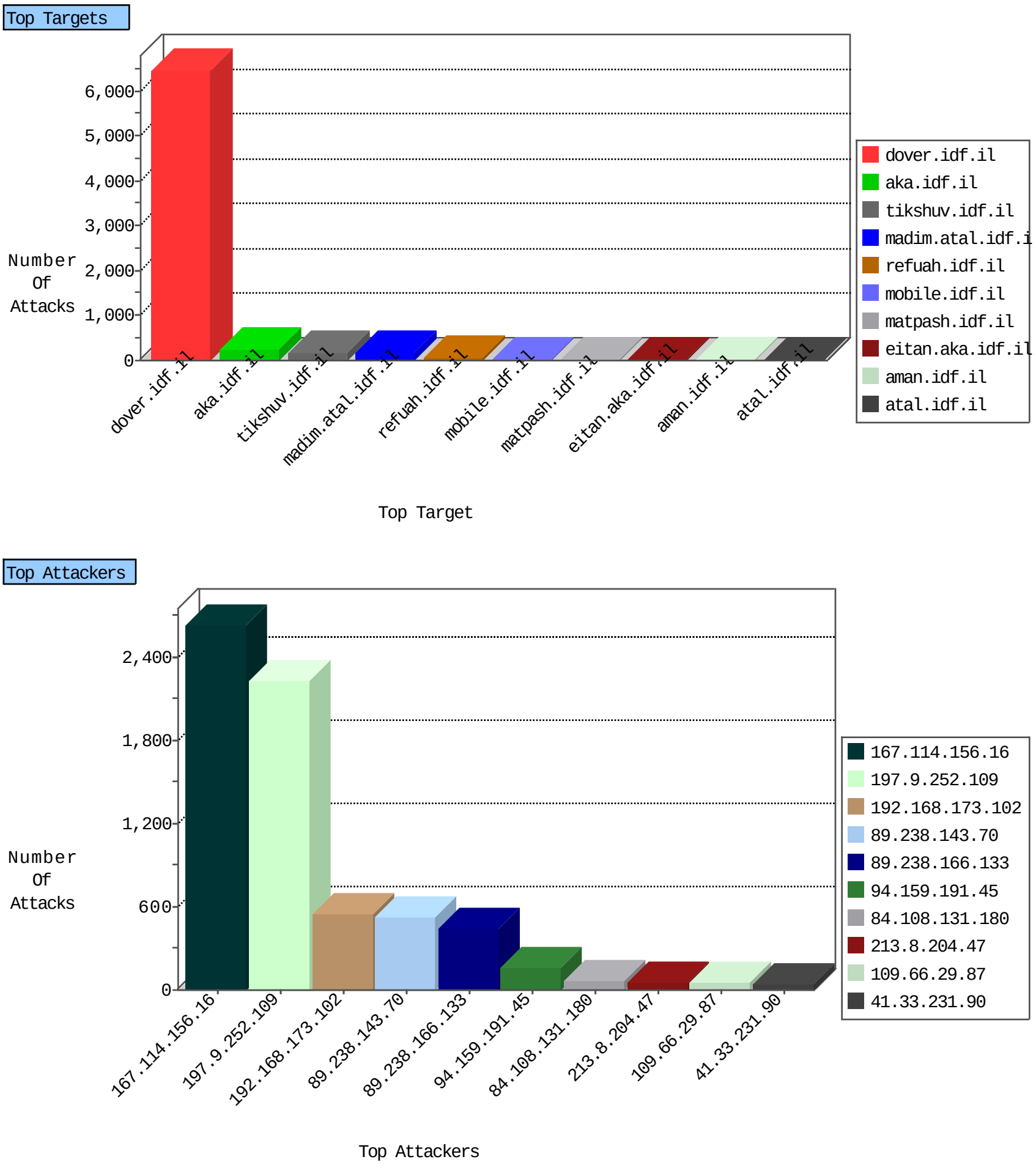
04-08-2016-00:04:05 to 04-08-2016-01:04:05

IDF Under Attack Daily Report



04-08-2016-00:04:05 to 04-08-2016-01:04:05

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	2623
89.238.143.70	United Kingdom	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	525
89.238.166.133	United Kingdom	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	431
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	9
197.9.252.109	Tunisia	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	8
120.132.50.135	China	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	4
197.9.252.109	Tunisia	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
107.150.32.62	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	2
192.3.220.210	United States	147.237.8.45	e.eitan.idf.il	Block_Ntp_All_Net	drop	2
197.9.252.109	Tunisia	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
107.150.32.61	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
69.197.185.19	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	2
107.150.32.61	United States	147.237.77.233	atal.idf.il	block-sp-traf1	forward	2
74.91.20.195	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	2
197.9.252.109	Tunisia	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
85.150.60.51	Netherlands	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
185.70.184.164	Netherlands	147.237.77.243	mobile.idf.il	L4 Source or Dest Port Zero	drop	1

04-08-2016-00:04:05 to 04-08-2016-01:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	10
213.8.204.32	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
87.69.19.30	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-08-2016-00:04:05 to 04-08-2016-01:04:05

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
66.249.69.34	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
208.100.26.228	147.237.0.15	United States	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
179.43.144.37	147.237.76.197	Switzerland	e.himush.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243	147.237.77.227		e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
221.226.31.210	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -f -sS	1
211.112.112.25	147.237.76.31	Korea, Republic of	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
197.9.252.109	147.237.77.216	Tunisia	dover.idf.il	portscan: TCP Distributed Portscan	1
179.43.144.37	147.237.77.179	Switzerland	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
132.74.95.21	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
221.226.31.210	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -sS window 2048	1
219.85.144.196	147.237.0.34	Taiwan	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

04-08-2016-00:04:05 to 04-08-2016-01:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.9.252.109	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1598
197.9.252.109	Tunisia	147.237.77.216	dover.idf.il	drop		drop	500
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	351
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	192
94.159.191.45	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	156
197.9.252.109	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	75
213.8.204.47	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	57
84.108.131.180	Israel	147.237.0.19	madim.atal.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	56
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
197.9.252.109	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
82.114.168.158	Yemen	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
154.73.28.50	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
141.0.14.73	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
197.9.252.109	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
197.9.252.109	Tunisia	147.237.77.216	dover.idf.il	Streaming Engine: TCP SYN Modified Retransmission	Data received before SYN was acknowledged. Stripping all packet data.	drop	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
54.241.198.78	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.54.131.40	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.149.239	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
94.159.191.45	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.95.49.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.65.114.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
17.142.156.109	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.64.60.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
164.138.23.232	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
207.46.13.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.116.70.148	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.42.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.16.121	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.183.194.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
164.138.23.232	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
31.210.187.12	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.67.169.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.16.121	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.178.14.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.242.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.53.11.49	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.253.218.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
193.37.128.187	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
157.55.39.161	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
54.206.118.10	Australia	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
46.19.86.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.198.93	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.54.171.30	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.105.40.89	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
84.95.49.218	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
134.35.95.33	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.66.29.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
2.53.8.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
84.108.131.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
149.202.239.135	France	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	6
109.64.195.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.138.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
83.6.102.16	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	3
46.19.86.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
167.114.156.198	Canada	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 167.114.156.198	Block	2
46.116.70.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.64.60.82	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
157.55.39.205	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	1
64.85.160.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/kesher	Block	1
109.253.218.44	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
17.142.156.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
89.139.163.102	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.69.10	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
213.8.204.32	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
149.202.239.135	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
79.181.4.21	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18063-he/dover.aspx	Block	1
31.172.191.135	Poland	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/forum	Block	1
120.132.50.135	China	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.elong.com/894-he/eitan.aspx	Block	1
107.150.32.61	United States	147.237.76.39	mobile.meitav.idf.il	Distributed Unauthorized URL Access on www.867bb.com/	Block	1
66.249.69.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
213.8.204.47	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 213.8.204.47	Block	1
157.55.39.194	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
109.65.138.43	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
167.114.156.198	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20187-he/dover.aspx)	Block	1
37.26.149.233	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
131.253.25.184	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
107.150.32.61	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on www.867bb.com/	Block	1
66.249.75.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/listpage/	Block	1
157.55.39.200	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
52.21.174.235	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/documents.asp	Block	1
197.9.252.109	Tunisia	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.66.23	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/m/	Block	1
41.108.245.233	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
141.0.14.73	Europe	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/5dc935ee3fe96098f0b7f87901e5bdf86b555295/	Block	1
107.150.32.62	United States	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.867bb.com/	Block	1
69.197.185.19	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.867bb.com/	Block	1
157.55.39.205	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.205	Block	1
54.88.169.180	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-12441-en/dover.aspx&quot	Block	1
109.186.184.42	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
2.54.131.40	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
87.70.20.12	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/163-7173-he/patzar.aspx+אימונ'+כושר+אישי'ים++"קופת num=100&as_qdr=all&complete=0&hl=en&ct=clnk&"חול'ים+	Block	1
207.46.13.71	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
46.19.85.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1