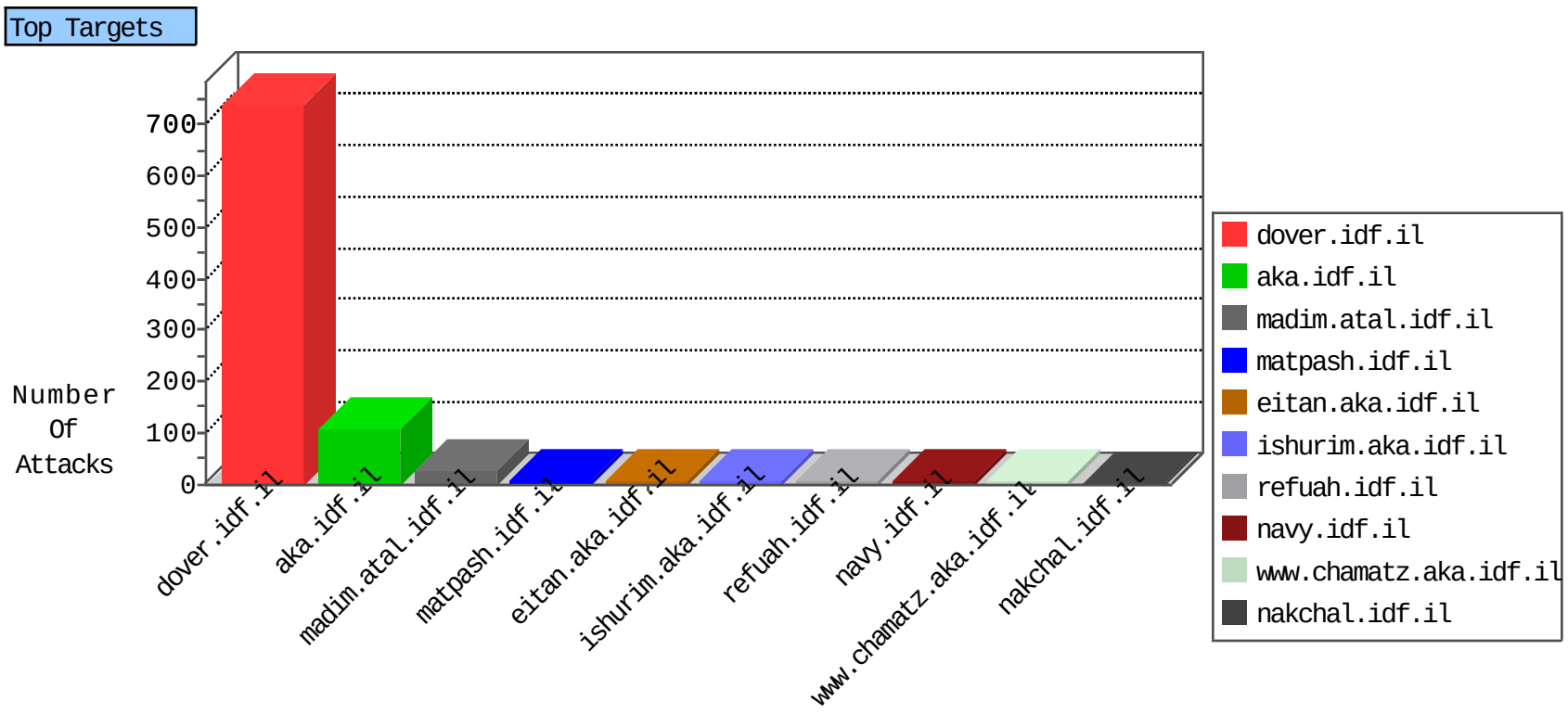
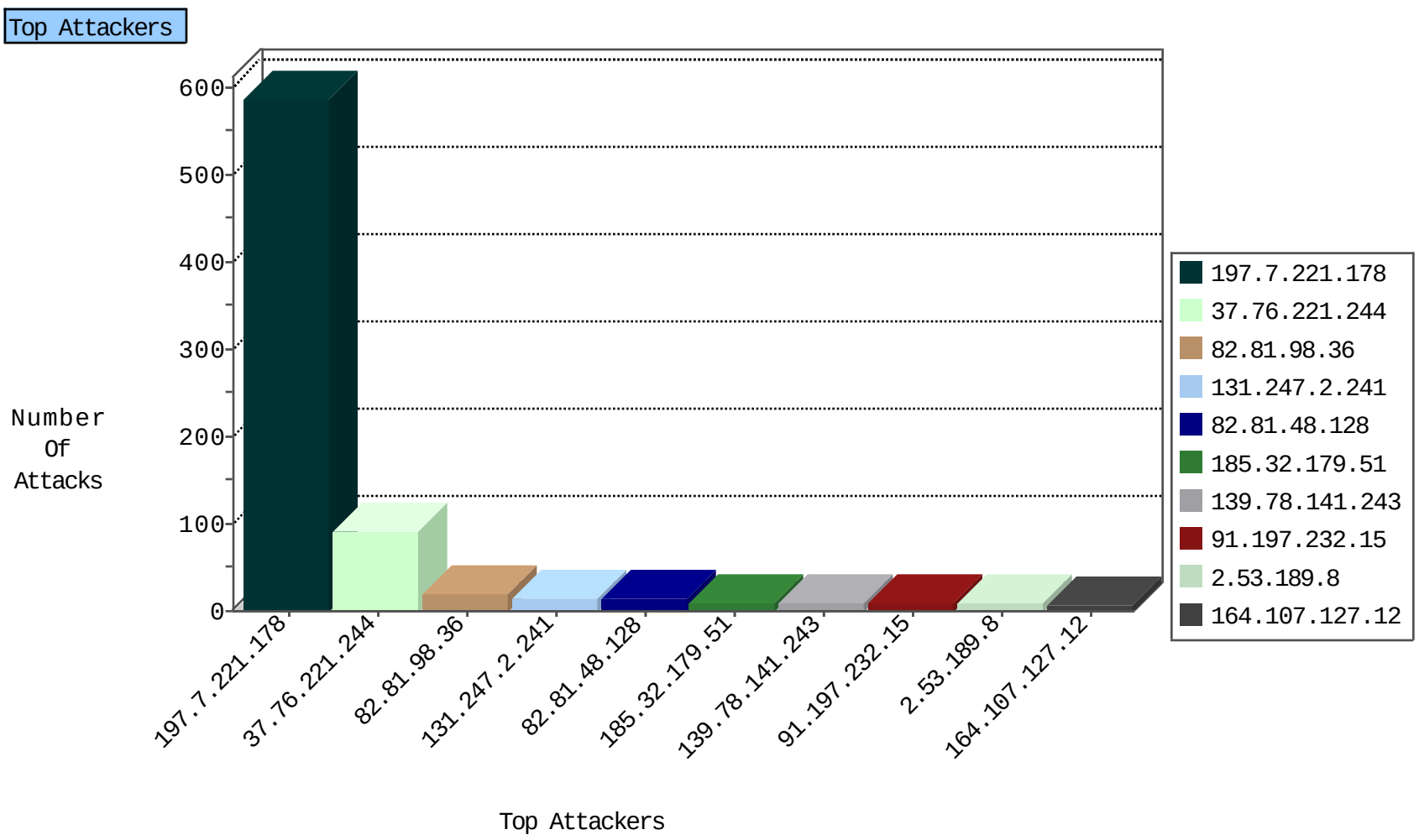
09-18-2016-01:06:12 to 09-18-2016-02:06:12

IDF Under Attack
Daily Report





09-18-2016-01:06:12 to 09-18-2016-02:06:12

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	522
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	15
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	10
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	7
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	7
109.67.136.175	Israel	147.237.77.216	dover.idf.il	Black List	drop	6
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	6
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
160.80.221.37	Italy	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	2
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
143.225.229.236	Italy	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
131.179.150.72	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
60.169.75.94	China	147.237.76.34	yohalan.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
192.33.90.68	Switzerland	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
128.42.142.45	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.2	New Zealand	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
60.169.75.94	China	147.237.76.34	yohalan.idf.il	JLM_Purple_Con_Limit_Http	drop	1

09-18-2016-01:06:12 to 09-18-2016-02:06:12

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
71.6.165.200	United States	147.237.72.167	ishurim.aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

09-18-2016-01:06:12 to 09-18-2016-02:06:12

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
116.71.128.85	147.237.0.17	Pakistan	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
112.53.68.214	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.197.232.15	147.237.77.233	Russian Federation	atal.idf.il	ET SCAN Potential SSH Scan	1
91.197.232.15	147.237.76.197	Russian Federation	e.himush.idf.il	ET SCAN Potential SSH Scan	1
91.197.232.15	147.237.76.34	Russian Federation	yohalan.idf.il	ET SCAN Potential SSH Scan	1
171.250.48.230	147.237.76.199	Vietnam	e.nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.197.232.15	147.237.8.46	Russian Federation	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
128.127.0.45	147.237.76.197	Italy	e.himush.idf.il	ET SCAN NMAP -sS window 3072	1
91.197.232.15	147.237.8.14	Russian Federation	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
125.94.166.74	147.237.77.205	China	prisha.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
41.230.31.128	147.237.77.74	Tunisia	law.idf.il	ET SCAN NMAP -sS window 3072	1
116.71.128.85	147.237.0.35	Pakistan	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
113.229.106.33	147.237.77.235	China	sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
103.250.226.246	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
91.197.232.15	147.237.77.205	Russian Federation	prisha.idf.il	ET SCAN Potential SSH Scan	1
91.197.232.15	147.237.76.44	Russian Federation	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
202.155.58.28	147.237.0.200	Indonesia	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
91.197.232.15	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN Potential SSH Scan	1
157.122.97.182	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
91.197.232.15	147.237.8.27	Russian Federation	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
128.127.0.45	147.237.76.197	Italy	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
91.197.232.15	147.237.0.16	Russian Federation	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
116.100.67.131	147.237.76.198	Vietnam	e.yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

09-18-2016-01:06:12 to 09-18-2016-02:06:12

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.76.221.244	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	89
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
82.81.98.36	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
82.81.48.128	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
2.53.189.8	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
95.141.29.37	Netherlands	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
176.13.237.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
109.253.212.42	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
37.46.39.20	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
141.0.12.250	Norway	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.46.38.75	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.100	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.76.221.244	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.199	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
185.32.179.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.53.138.50	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.199	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.32.179.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
185.32.179.51	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.146.147	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	2
141.226.161.184	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.156	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
87.68.245.12	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
147.235.8.86	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.19.86.50	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
185.32.179.51	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
147.235.8.86	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
2.53.189.8	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
141.212.122.26	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.67.30.30	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
71.6.165.200	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.85.5	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
130.75.152.106	Germany	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
218.156.17.203	Korea, Republic of	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
84.108.192.255	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
46.19.86.100	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.27	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
213.57.169.246	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
80.179.143.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
193.188.136.20	Lebanon	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid sequence number	alert	1
46.19.85.73	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
5.102.242.53	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
218.156.17.203	Korea, Republic of	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
84.109.108.130	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
185.32.179.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
109.253.157.214	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-18-2016-01:06:12 to 09-18-2016-02:06:12

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.81.98.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
93.172.221.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.6.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.138.216.183	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	2
45.79.142.205	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/eitan/pratim/pirteyerua/	Block	1
157.55.39.7	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
77.138.6.197	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/smalim/smalim.aspx	Block	1
87.69.103.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.50	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.123	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	1
77.138.6.197	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/faq.aspx	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
77.138.118.217	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunderugtafkidim.aspx	Block	1
5.29.20.50	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
94.199.151.22	United Kingdom	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
66.249.93.211	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/favicon.ico	Block	1
40.84.224.137	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
132.69.245.66	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
66.249.93.213	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/894-he/dover.aspx	Block	1

09-18-2016-01:06:12 to 09-18-2016-02:06:12