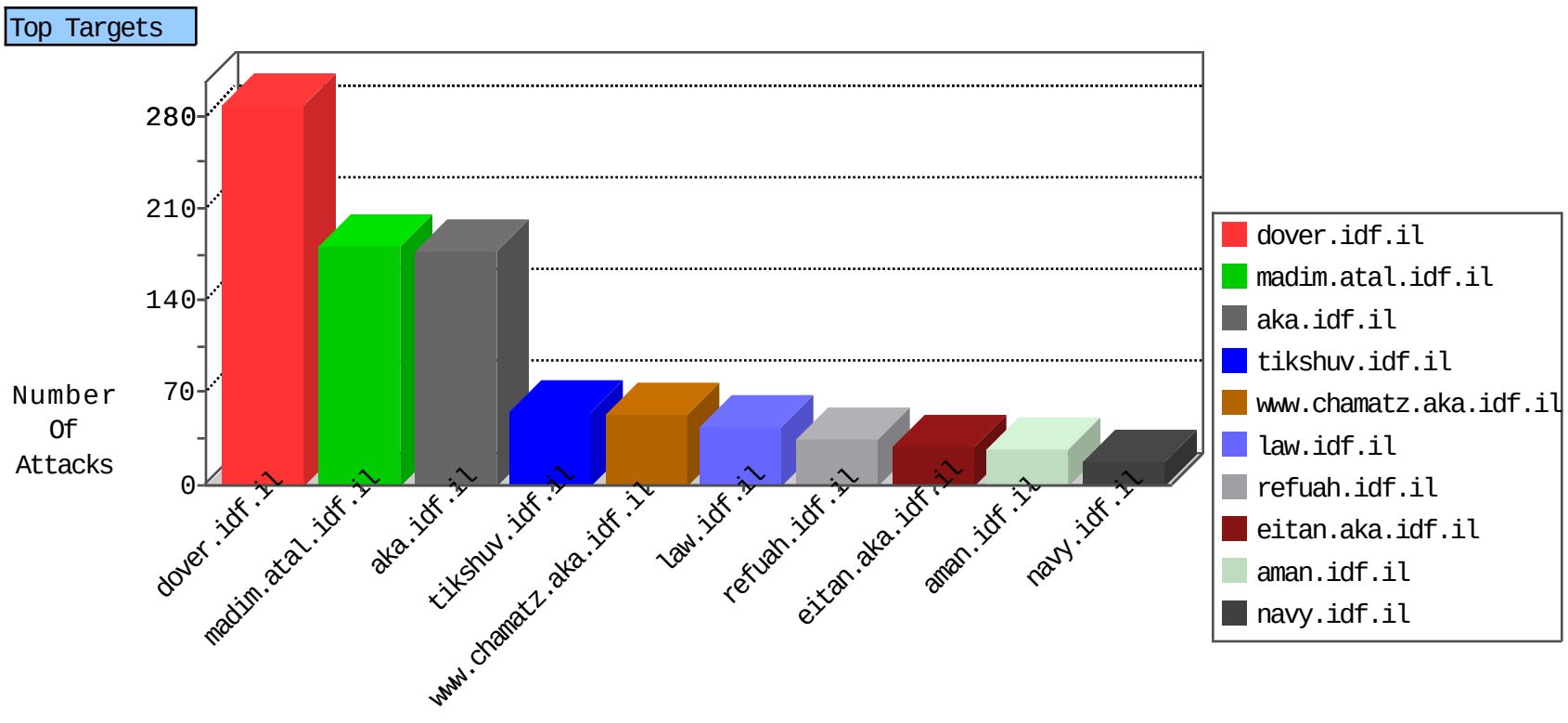
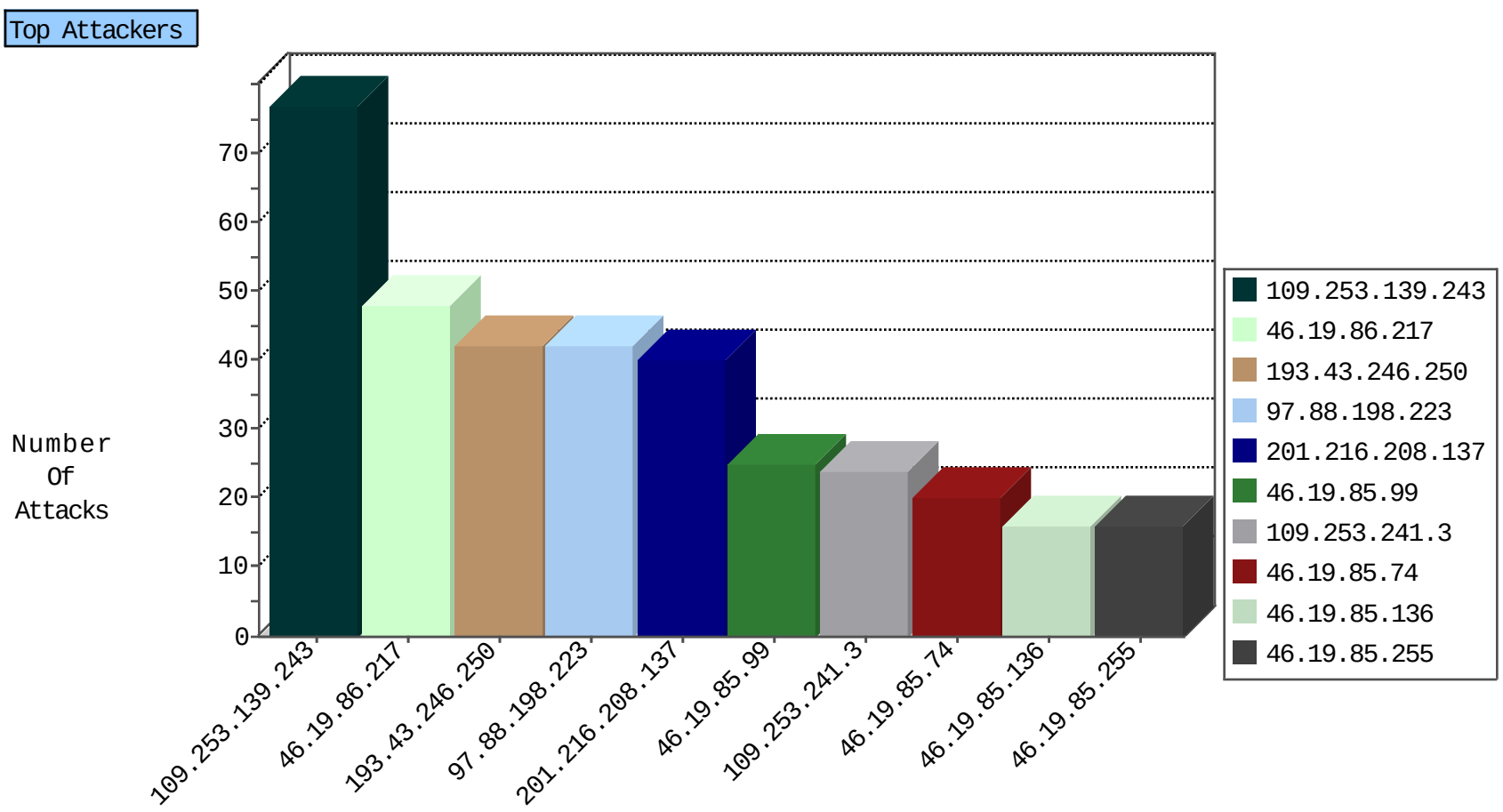
09-18-2016-08:04:09 to 09-18-2016-09:04:09

IDF Under Attack Daily Report



Top Target



Top Attackers

09-18-2016-08:04:09 to 09-18-2016-09:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	13
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	8
2.55.17.66	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	6
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
141.212.113.180	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	3
2.53.40.54	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
134.117.226.180	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
115.239.230.228	China	147.237.0.15	kosher-kravi.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
204.85.191.11	United States	147.237.72.166	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
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
160.80.221.39	Italy	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.139	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
46.19.86.189	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
51.255.218.57	France	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1

09-18-2016-08:04:09 to 09-18-2016-09:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
97.88.198.223	United States	147.237.77.226	www.chamatz.aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
201.216.208.137	Argentina	147.237.0.34	tikshuv.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	11
201.216.208.137	Argentina	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	7
71.171.93.66	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
97.88.198.223	United States	147.237.77.226	www.chamatz.aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
216.68.91.180	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
185.21.133.159	United Kingdom	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
184.168.193.34	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

09-18-2016-08:04:09 to 09-18-2016-09:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
97.88.198.223	147.237.77.226	United States	www.chamatz.aka.idf.il	SQL Injection - Select From	22
201.216.208.137	147.237.0.34	Argentina	tikshuv.idf.il	SQL Injection - Select From	22
216.68.91.180	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
71.171.93.66	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	3
184.168.193.34	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	2
115.239.230.228	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
84.111.190.4	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.228.136	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.63.41	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.136.144.104	147.237.77.233	Iran, Islamic Republic of	atal.idf.il	ET SCAN NMAP -sS window 1024	1
139.162.13.205	147.237.76.31	Singapore	nakchal.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
109.236.80.12	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential SSH Scan	1
93.172.148.107	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.178.120.96	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.72.135	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.106.108.116	147.237.77.216	Japan	dover.idf.il	Tehila - Perl LWP with fake user agent	1
212.235.43.127	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.114.177.190	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-18-2016-08:04:09 to 09-18-2016-09:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
62.0.217.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
80.178.198.75	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
62.0.200.169	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
184.168.193.34	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.86.206	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
194.90.25.122	Israel	147.237.76.201	e.atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
80.179.102.142	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
109.253.144.184	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
46.19.85.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
217.194.197.141	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.85.136	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.77	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.56	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.148.241	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.70	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.136	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.255	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.124	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.81	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.255	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.29.94.49	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.86.124	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.77	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.53.45.7	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.56	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.99	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	5
109.253.223.110	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.85.81	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
185.32.179.122	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.85.99	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.99	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.53.129.239	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.70	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.99	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
199.203.215.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.81	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
94.80.205.146	Italy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
82.208.160.57	Romania	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
80.191.127.224	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
82.80.28.195	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.31	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.229.24	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
109.253.159.201	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.210	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

09-18-2016-08:04:09 to 09-18-2016-09:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.139.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	76
46.19.86.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
109.253.241.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
185.32.179.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
147.236.238.20	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	5
84.108.232.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.108.232.224	Block	4
2.53.9.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.143.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
139.162.13.205	Singapore	147.237.76.31	nakchal.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
46.19.85.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.132.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.13.244.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.108.232.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1153-23238-he/dover.	Block	1
77.138.88.36	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
176.13.245.17	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
52.57.11.193	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
114.98.244.254	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/trackback/	Block	1
98.139.204.40	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
2.53.159.108	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
82.81.17.28	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
217.132.142.40	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
157.55.39.122	United States	147.237.72.166	aka.idf.il	Unknown Parameter 4f9c0c80 in www.aka.idf.il/main/home/default.aspx	None	1
66.249.79.139	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1375-he/refuah.aspx	Block	1
37.26.149.144	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.143.65	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
2.53.45.11	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.69.159.213	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.152.19	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar	Block	1
62.219.137.5	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.64.147.143	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
2.53.191.13	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
217.194.197.141	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1
157.55.39.203	United States	147.237.72.166	aka.idf.il	Unknown Parameter pageNum in www.aka.idf.il/patzar/klali/default.asp	None	1
68.180.228.238	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
46.19.85.20	Israel	147.237.76.42	refuah.idf.il	Suspicious Response Code	Block	1
109.253.157.70	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.46.188	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
89.237.96.140	France	147.237.77.216	dover.idf.il	Parameter Type Violation d in www.idf.il/scriptresource.axd	Block	1
80.246.139.201	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.115.26.56	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mainsachar	Block	1
66.249.75.137	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
2.55.141.118	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
217.194.197.141	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/robots.txt	Block	1
173.255.228.59	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/eitan/pratim/pirteyerua/	Block	1
77.126.69.184	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
109.253.223.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1

09-18-2016-08:04:09 to 09-18-2016-09:04:09