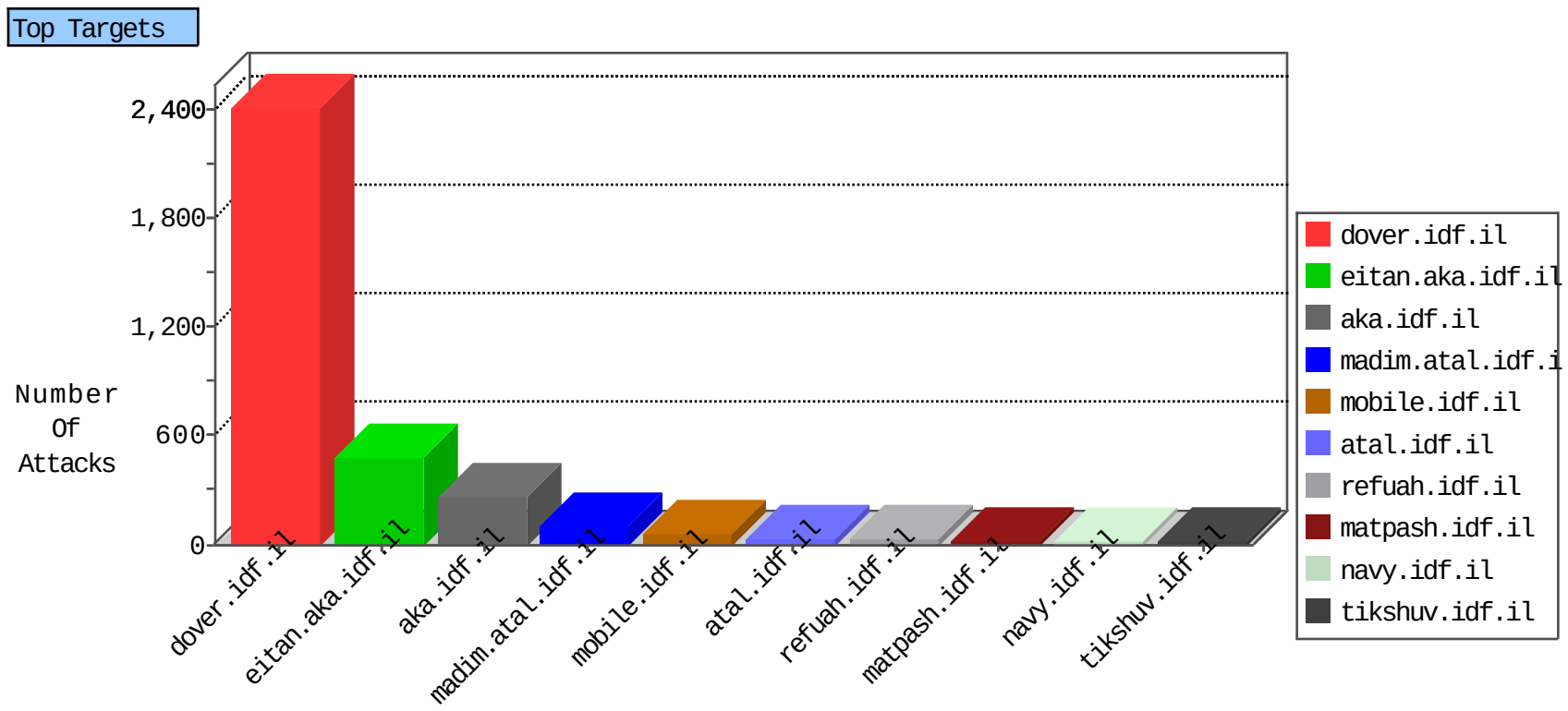
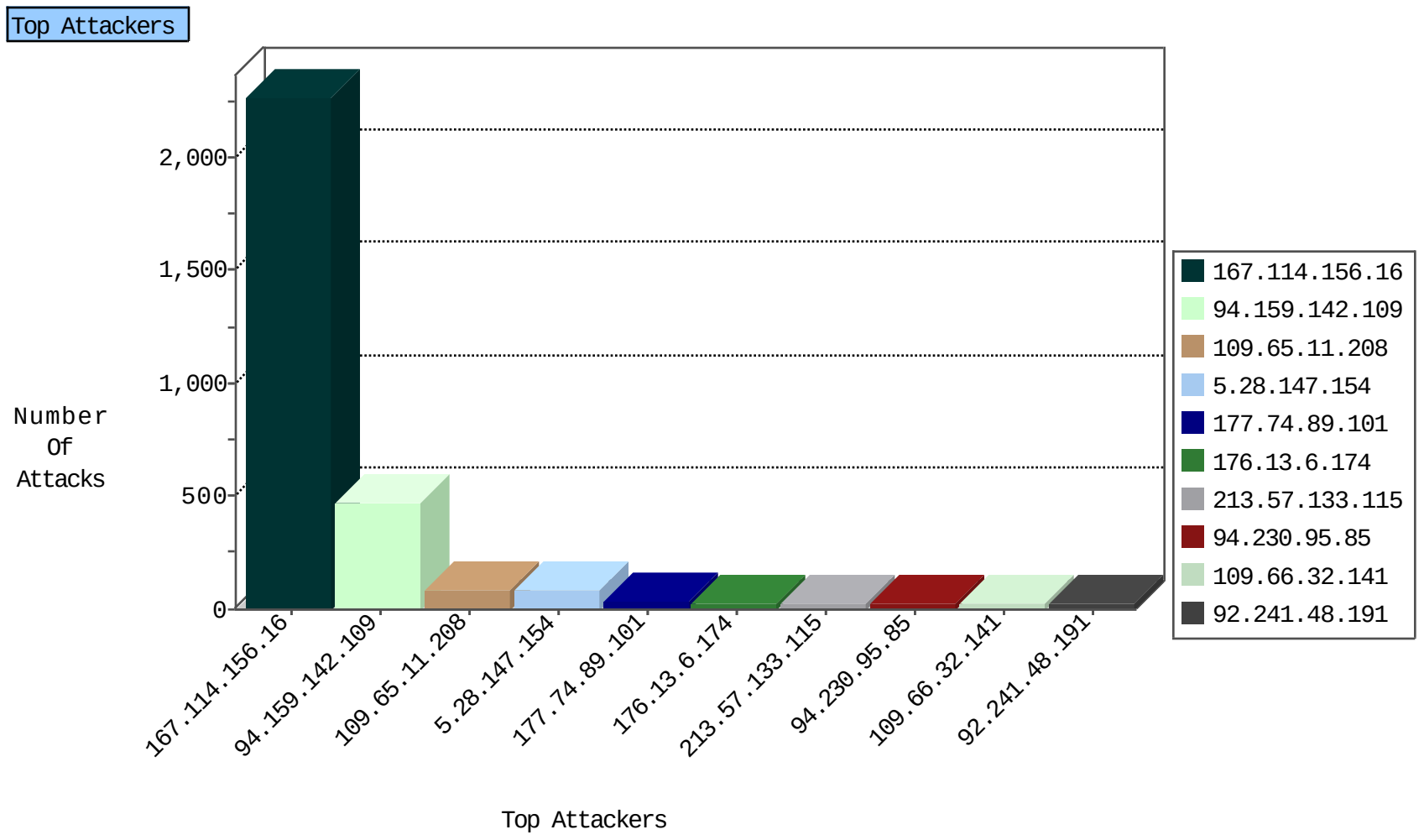
12-09-2015-22:04:05 to 12-09-2015-23:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-09-2015-22:04:05 to 12-09-2015-23:04:05

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	DOS-Tool-SwitchbladG	dest-reset	3341
66.249.78.15	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	188
179.215.212.60	Brazil	147.237.77.176	matpash.idf.il	Frk_Under_Attack_Con_Tcp	drop	2

12-09-2015-22:04:05 to 12-09-2015-23:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.12.70.34	United States	147.237.77.176	matpash.idf.il	21609: HTTP: pChart Directory Traversal Vulnerability	Block	1
69.30.218.234	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
62.210.85.77	France	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1

12-09-2015-22:04:05 to 12-09-2015-23:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.75.106	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
177.74.89.101	147.237.8.45	Brazil	e.eitan.idf.il	ET SCAN Potential SSH Scan	2
177.74.89.101	147.237.76.201	Brazil	e.atal.idf.il	ET SCAN Potential SSH Scan	2
177.74.89.101	147.237.0.17	Brazil	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
177.74.89.101	147.237.76.30	Brazil	himush.idf.il	ET SCAN Potential SSH Scan	2
66.249.81.215	147.237.77.216	Russian Federation	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.50	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
177.74.89.101	147.237.76.31	Brazil	nakchal.idf.il	ET SCAN Potential SSH Scan	1
78.193.2.8	147.237.76.199	France	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
187.160.131.35	147.237.77.235	Mexico	sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
177.74.89.101	147.237.72.166	Brazil	aka.idf.il	ET SCAN Potential SSH Scan	1
177.74.89.101	147.237.77.234	Brazil	halag.idf.il	ET SCAN Potential SSH Scan	1
60.250.134.220	147.237.76.30	Taiwan	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
177.74.89.101	147.237.77.121	Brazil	e.navy.idf.il	ET SCAN Potential SSH Scan	1
177.74.89.101	147.237.8.24	Brazil	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
177.74.89.101	147.237.0.34	Brazil	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
177.74.89.101	147.237.76.198	Brazil	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
177.74.89.101	147.237.76.196	Brazil	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
177.74.89.101	147.237.0.15	Brazil	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
177.74.89.101	147.237.76.147	Brazil	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
210.6.140.252	147.237.76.30	Hong Kong	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.128.144.131	147.237.77.226	Canada	www.chamatz.aka.idf.il	ET SCAN NMAP -f -sS	1
177.74.89.101	147.237.76.34	Brazil	yohalan.idf.il	ET SCAN Potential SSH Scan	1
78.193.2.8	147.237.76.200	France	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
187.252.224.95	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
177.74.89.101	147.237.77.243	Brazil	mobile.idf.il	ET SCAN Potential SSH Scan	1
177.74.89.101	147.237.72.156	Brazil	aman.idf.il	ET SCAN Potential SSH Scan	1
177.74.89.101	147.237.77.233	Brazil	atal.idf.il	ET SCAN Potential SSH Scan	1
177.74.89.101	147.237.8.28	Brazil	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
177.74.89.101	147.237.77.74	Brazil	law.idf.il	ET SCAN Potential SSH Scan	1
177.74.89.101	147.237.0.35	Brazil	akaws.idf.il	ET SCAN Potential SSH Scan	1
177.74.89.101	147.237.76.199	Brazil	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
177.74.89.101	147.237.0.19	Brazil	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
177.74.89.101	147.237.76.197	Brazil	e.himush.idf.il	ET SCAN Potential SSH Scan	1
177.74.89.101	147.237.0.16	Brazil	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
177.74.89.101	147.237.76.148	Brazil	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.77.226	Canada	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1
177.74.89.101	147.237.76.39	Brazil	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
94.243.223.7	147.237.8.45	Russian Federation	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1

12-09-2015-22:04:05 to 12-09-2015-23:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
94.159.142.109	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	438
5.28.147.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	40
5.28.147.154	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	40
94.230.95.85	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
176.13.6.174	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
66.249.74.6	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
92.241.48.191	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	13
213.57.133.115	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
46.117.215.250	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
213.57.133.115	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
87.69.166.14	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
46.19.86.92	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.66.154.124	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.8.204.39	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.12.147.52	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.26.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.180.154.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.8.204.39	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.228.188.205	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
65.60.190.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.3.146.174	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.109.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.62.137	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.32.141	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.121	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.66.32.141	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.57.133.115	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
199.30.25.242	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
92.241.48.191	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
109.66.32.141	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
213.57.131.54	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.176.26.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.64.196.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.89.228	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
185.3.146.90	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.65.62.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.69.166.14	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.85.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.117.215.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
109.66.32.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.1.104	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
87.69.166.14	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.66.32.141	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
37.26.148.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.166.91.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.12	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.178.239.22	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.89.228	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3

12-09-2015-22:04:05 to 12-09-2015-23:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.11.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	87
94.159.142.109	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 94.159.142.109	Block	36
176.13.6.174	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
84.94.175.153	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/mas.aspx	Block	5
176.13.10.151	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.62.142	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/images/shared/err_page.png	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
46.116.189.243	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	2
46.19.86.92	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
176.12.147.52	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
176.12.148.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
87.69.166.14	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
46.116.67.198	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.1.104	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.201.154.138	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.180.154.44	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
52.35.187.114	United States	147.237.0.34	tikshuv.idf.il	Multiple NULL Character in Method from 52.35.187.114	Block	1
195.154.146.225	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
92.97.40.136	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
84.109.144.143	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.51	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
173.252.90.120	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.176.26.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.225.246	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.86.120.162	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.86.120.162	Block	1
66.249.64.23	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
213.8.204.39	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
87.106.22.163	Germany	147.237.77.176	matpash.idf.il	Admin Blocking	Block	1
5.29.46.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
109.201.154.228	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
81.24.209.144	Ukraine	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/iturim/resources/images/body/images/main.jpg	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.64.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20145-he/dover.aspx	Block	1
52.35.187.114	United States	147.237.0.34	tikshuv.idf.il	NULL Character in Method	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
93.173.240.51	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
85.64.231.141	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	1
176.12.143.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.107.80	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.66.154.124	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
95.86.120.162	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1153-he/dover.aspx&sa=u&ved=0ahukewivn4auz8_jahwict4khaasahcqfggimaa&usg=afqjcnhnqiwitkiydw0x3dfj1oixh14v-q	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.190	Block	1
87.106.22.163	Germany	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/admin	Block	1
46.120.216.233	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
41.44.223.30	Egypt	147.237.77.74	law.idf.il	PHP Attempt	Block	1
149.78.80.3	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8900-he/refuah.aspx	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1

12-09-2015-22:04:05 to 12-09-2015-23:04:05