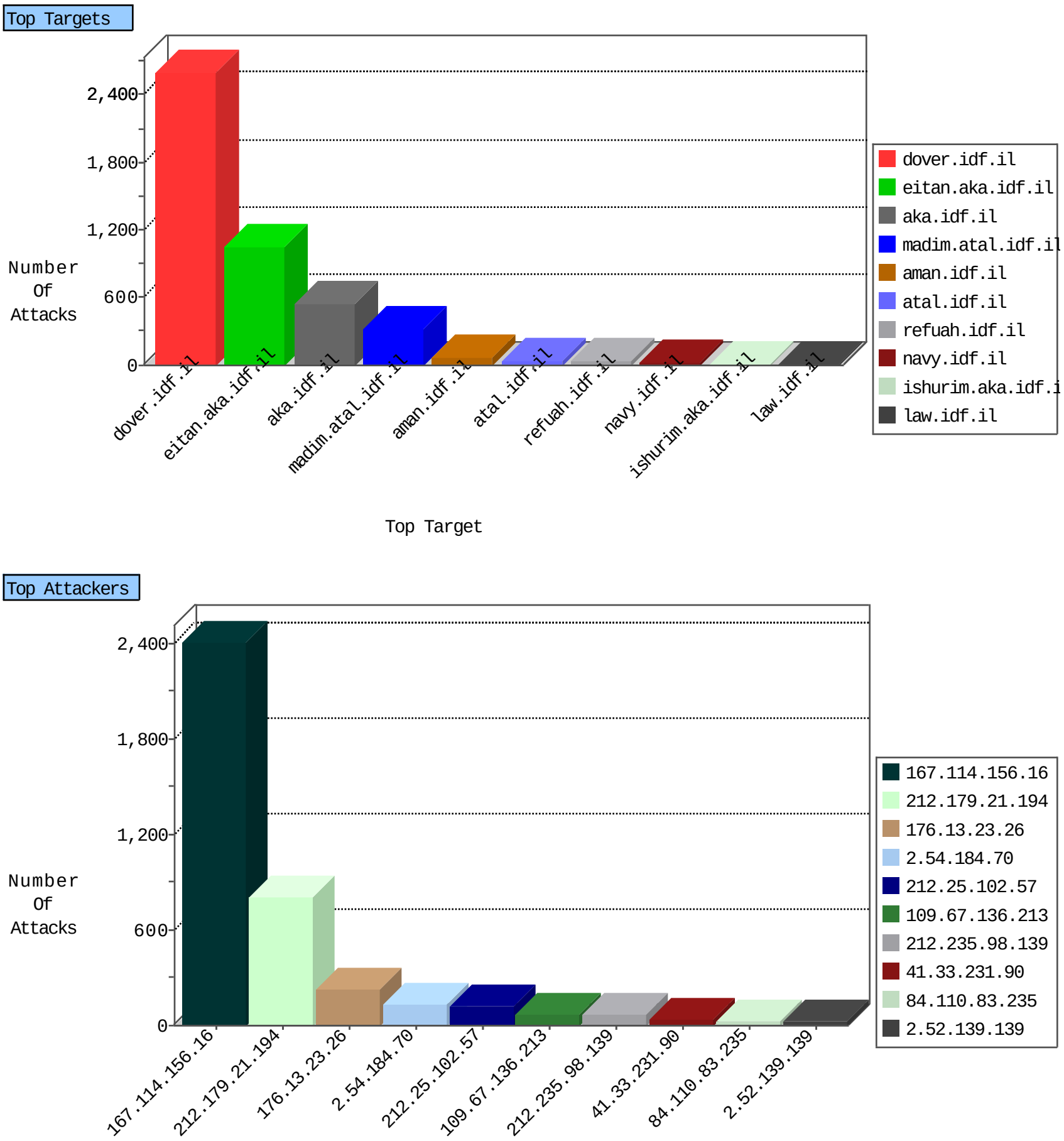
12-07-2015-14:04:01 to 12-07-2015-15:04:01

IDF Under Attack Daily Report



12-07-2015-14:04:01 to 12-07-2015-15:04:01

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	3328
109.67.49.70	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	9
79.178.115.148	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
66.249.65.40	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1
118.193.23.46	China	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
167.88.12.196	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	drop	1
71.6.167.142	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
167.88.7.229	United States	147.237.77.205	prisha.idf.il	block-sp-traf1	drop	1
167.88.7.239	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	drop	1
167.88.10.85	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	drop	1

12-07-2015-14:04:01 to 12-07-2015-15:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
116.123.160.95	Korea, Republic of	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

12-07-2015-14:04:01 to 12-07-2015-15:04:01

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
138.0.21.114	147.237.0.17		m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
120.26.137.112	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
85.65.120.95	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.166.134.245	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
159.122.238.155	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
120.26.137.112	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
96.94.72.226	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
82.166.206.253	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.198.164	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1

12-07-2015-14:04:01 to 12-07-2015-15:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.184.70	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	129
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	66
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
109.66.33.95	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	21
77.127.61.95	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
85.31.3.11	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.19.86.196	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
213.57.141.95	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
116.21.82.131	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
84.110.83.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	10
213.57.141.95	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	10
31.210.186.149	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
87.68.165.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.179.10.173	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	9
188.120.148.240	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.120.73.172	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
85.250.30.16	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	7
46.19.85.70	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.68.79.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.139.139	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
77.126.215.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.139.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.52.139.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.50.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.68.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.52.139.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.106.94.2		147.237.77.234	halag.idf.il	drop	SAM rule	drop	6
109.67.68.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.102.170.200	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
85.250.176.24	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.52.139.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
213.57.129.15	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.70	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
85.250.176.24	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.139.139	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.66.33.95	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.240	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
84.110.83.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.24.207.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.46.39.153	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.110.83.235	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
81.218.241.26	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
84.110.83.235	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
109.66.11.201	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
85.130.172.198	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	5
84.110.83.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5

12-07-2015-14:04:01 to 12-07-2015-15:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	735
212.25.102.57	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	120
176.13.23.26	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.23.26	Block	109
176.13.23.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
109.67.136.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
176.13.23.26	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 176.13.23.26	Block	15
77.126.220.155	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.126.220.155	Block	14
79.180.177.138	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	5
79.178.138.186	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	4
37.26.148.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
132.74.95.21	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/6/113476.pdf	Block	3
37.26.146.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.175.193.9	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	2
79.179.17.20	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
46.19.85.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.195	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.64.18	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
176.13.7.137	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
93.173.231.46	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 10.100.102.6/upnpcp/notify/event	Block	1
81.218.245.1	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
46.19.85.140	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
171.100.52.226	Thailand	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
200.10.236.95	Chile	147.237.77.74	law.idf.il	PHP Attempt	Block	1
2.52.136.174	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
107.178.195.171	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
176.12.149.188	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.251.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
62.219.162.144	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
37.142.215.232	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
149.78.106.143	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
79.180.177.138	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	1
79.176.130.109	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
192.114.2.36	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
176.13.16.248	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
94.159.144.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.81.80.242	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.43	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
171.100.52.226	Thailand	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
200.10.236.95	Chile	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
37.26.149.180	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
149.78.36.127	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.20.88	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.65.15.46	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.43	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18489-he/dover.aspx	Block	1
177.139.245.86	Brazil	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
66.87.114.252	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
176.13.3.39	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
85.250.176.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

12-07-2015-14:04:01 to 12-07-2015-15:04:01