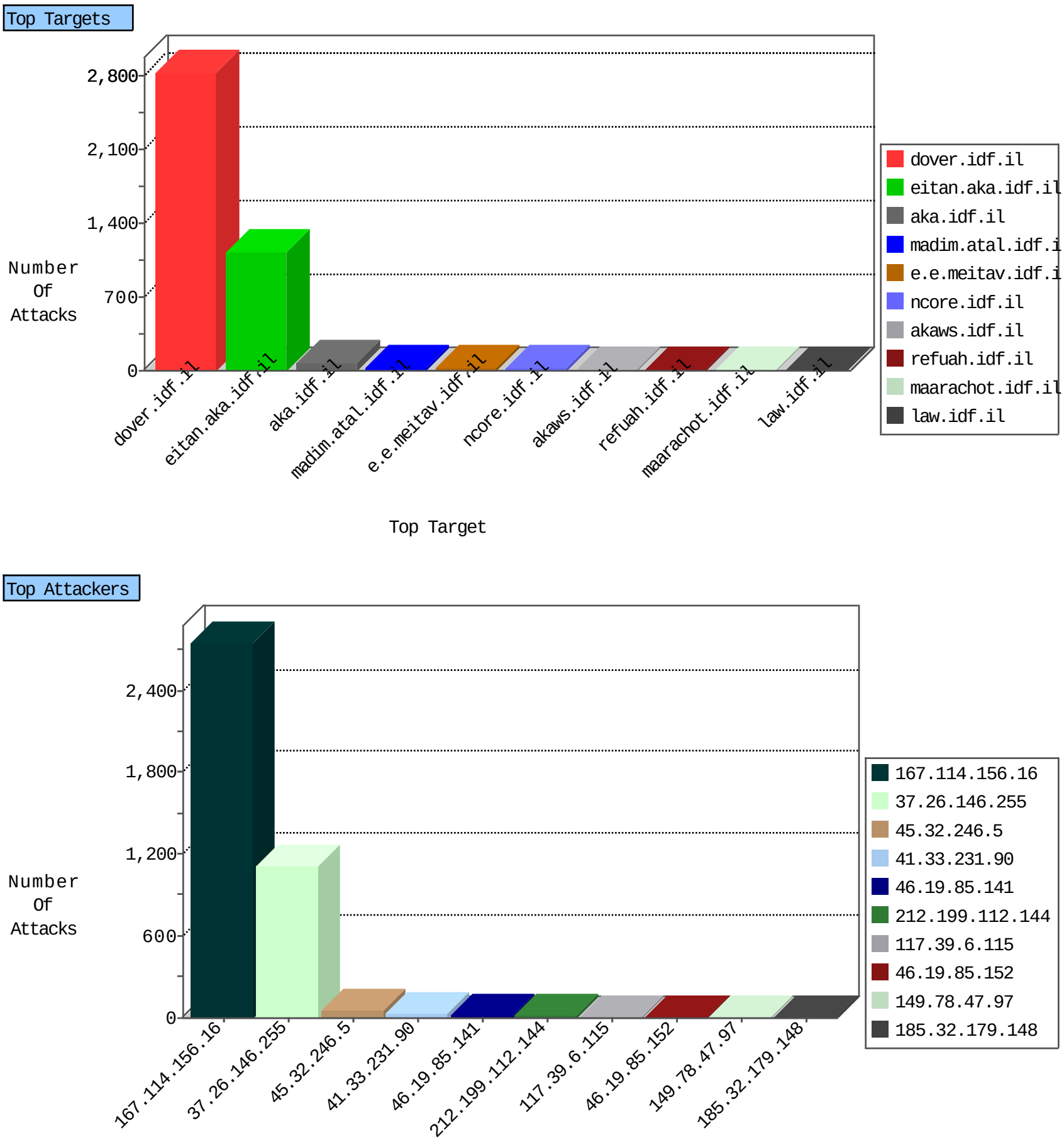
12-09-2015-06:04:01 to 12-09-2015-07:04:01

IDF Under Attack Daily Report



12-09-2015-06:04:01 to 12-09-2015-07:04:01

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	3440
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	156
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	143
66.249.64.50	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	72
45.32.246.5		147.237.76.177	ncore.idf.il	Invalid TCP Flags	drop	8
45.32.246.5		147.237.76.38	e.e.meitav.idf.i	Invalid TCP Flags	drop	8
45.32.246.5		147.237.0.35	akaws.idf.il	Invalid TCP Flags	drop	5
45.32.246.5		147.237.76.38	e.e.meitav.idf.i	Block_Udp_All_Nets	drop	2
45.32.246.5		147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	2
71.6.135.131	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
123.220.233.142	Japan	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.45	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
71.6.216.45	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1

12-09-2015-06:04:01 to 12-09-2015-07:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-09-2015-06:04:01 to 12-09-2015-07:04:01

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	4
66.249.64.50	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.112	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.29	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
117.39.6.115	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
45.32.246.5	147.237.0.35		akaws.idf.il	ET SCAN NMAP -f -sS	1
45.32.246.5	147.237.76.177		ncore.idf.il	ET SCAN NMAP -sS window 3072	1
117.39.6.115	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
45.32.246.5	147.237.76.177		ncore.idf.il	ET SCAN NMAP -sS window 1024	1
117.39.6.115	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
223.4.174.30	147.237.0.33	China	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
45.32.246.5	147.237.76.38		e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
117.39.6.115	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
45.32.246.5	147.237.76.38		e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
220.231.195.122	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
117.39.6.115	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
45.32.246.5	147.237.76.38		e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
117.39.6.115	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
45.32.246.5	147.237.0.35		akaws.idf.il	ET SCAN Potential SSH Scan	1
189.219.161.56	147.237.76.176	Mexico	test.ncore.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
89.163.140.142	147.237.72.217	Germany	e.idf.il	ET SCAN Potential SSH Scan	1
45.32.246.5	147.237.0.35		akaws.idf.il	ET SCAN NMAP -sS window 3072	1
177.230.255.100	147.237.0.34	Mexico	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
117.39.6.115	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
45.32.246.5	147.237.0.35		akaws.idf.il	ET SCAN NMAP -sS window 1024	1
45.32.246.5	147.237.76.177		ncore.idf.il	ET SCAN NMAP -sS window 4096	1
117.39.6.115	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
5.139.195.139	147.237.76.31	Russian Federation	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
45.32.246.5	147.237.76.177		ncore.idf.il	ET SCAN NMAP -sS window 2048	1
117.39.6.115	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
45.32.246.5	147.237.76.177		ncore.idf.il	ET SCAN NMAP -f -sS	1
117.39.6.115	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
220.231.195.122	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
45.32.246.5	147.237.76.38		e.e.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
117.39.6.115	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
45.32.246.5	147.237.76.38		e.e.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
220.231.195.122	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
117.39.6.115	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
45.32.246.5	147.237.76.38		e.e.meitav.idf.il	ET SCAN NMAP -f -sS	1
189.219.161.56	147.237.76.199	Mexico	e.nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
89.163.140.142	147.237.76.196	Germany	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
45.32.246.5	147.237.0.35		akaws.idf.il	ET SCAN NMAP -sS window 4096	1
177.236.1.49	147.237.0.34	Mexico	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
45.32.246.5	147.237.0.35		akaws.idf.il	ET SCAN NMAP -sS window 2048	1
128.204.196.48	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN NMAP -sS window 4096	1

12-09-2015-06:04:01 to 12-09-2015-07:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.146.255	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	915
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.85.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
149.78.47.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.148	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
45.32.246.5		147.237.0.35	akaws.idf.il	drop	SAM rule	drop	4
45.32.246.5		147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	4
45.32.246.5		147.237.76.177	ncore.idf.il	drop	SAM rule	drop	4
199.30.25.3	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
84.110.80.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
199.203.226.21	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.183.53.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.154.156	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.140.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.103	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.180.30.115	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
213.57.137.117	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
40.77.167.8	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
80.179.115.198	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
69.122.148.186	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.85.49	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
199.203.226.21	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
79.180.30.115	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
146.185.239.102	Russian Federation	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.111.73	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
196.210.55.60	South Africa	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.26	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
180.97.106.162	China	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
180.97.106.36	China	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
2.54.138.47	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.183	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.239	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.241	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
180.97.106.37	China	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
91.75.159.94	United Arab Emirates	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
198.20.87.98	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.46	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
180.97.106.162	China	147.237.77.61	e.cogat.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
180.97.106.36	China	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.121.184	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.111.73	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
184.105.247.243	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
180.97.106.37	China	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
198.20.87.98	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.56	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
180.97.106.162	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
46.19.85.251	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
180.97.106.36	China	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

12-09-2015-06:04:01 to 12-09-2015-07:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.255	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.146.255	Block	197
46.19.85.141	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	18
176.13.0.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.57.215.159	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.179.110.41	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg	Block	2
109.64.63.7	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	2
66.249.79.25	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
46.116.91.127	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
5.29.245.45	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.93.31.146		147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
104.131.98.186	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	1
154.5.161.167	Canada	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 154.5.161.167	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.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
66.249.78.96	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/m/templates/getfile/getfile.aspx	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
37.26.146.255	Israel	147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	Block	1
109.93.31.146		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
104.131.98.186	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /	Block	1
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.137	Block	1
84.109.12.200	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
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	1
109.160.241.31	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
104.131.98.186	United States	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on /	Block	1
70.24.51.115	Canada	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
176.13.1.62	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
66.249.64.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1613-15489-he/dover.aspx	Block	1
109.67.168.165	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
104.131.6.46	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on /	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1115-ar/dover.aspx	Block	1
207.46.13.38	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
141.212.121.176	United States	147.237.76.39	mobile.meitav.idf.il	Distributed Unauthorized URL Access on 147.237.76.39/	Block	1
70.24.51.115	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18538-en/kkkkkkk=620c1ab7kkkkkkk_620c1ab7	Block	1
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en	Block	1
109.67.168.165	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.maarachot.idf.il/xmlrpc.php	Block	1
104.131.8.205	United States	147.237.76.39	mobile.meitav.idf.il	Distributed Unauthorized URL Access on /	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
141.212.121.176	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
74.82.47.4	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9696-he/refuah.aspx	Block	1
192.118.10.10	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 192.118.10.10	Block	1

12-09-2015-06:04:01 to 12-09-2015-07:04:01