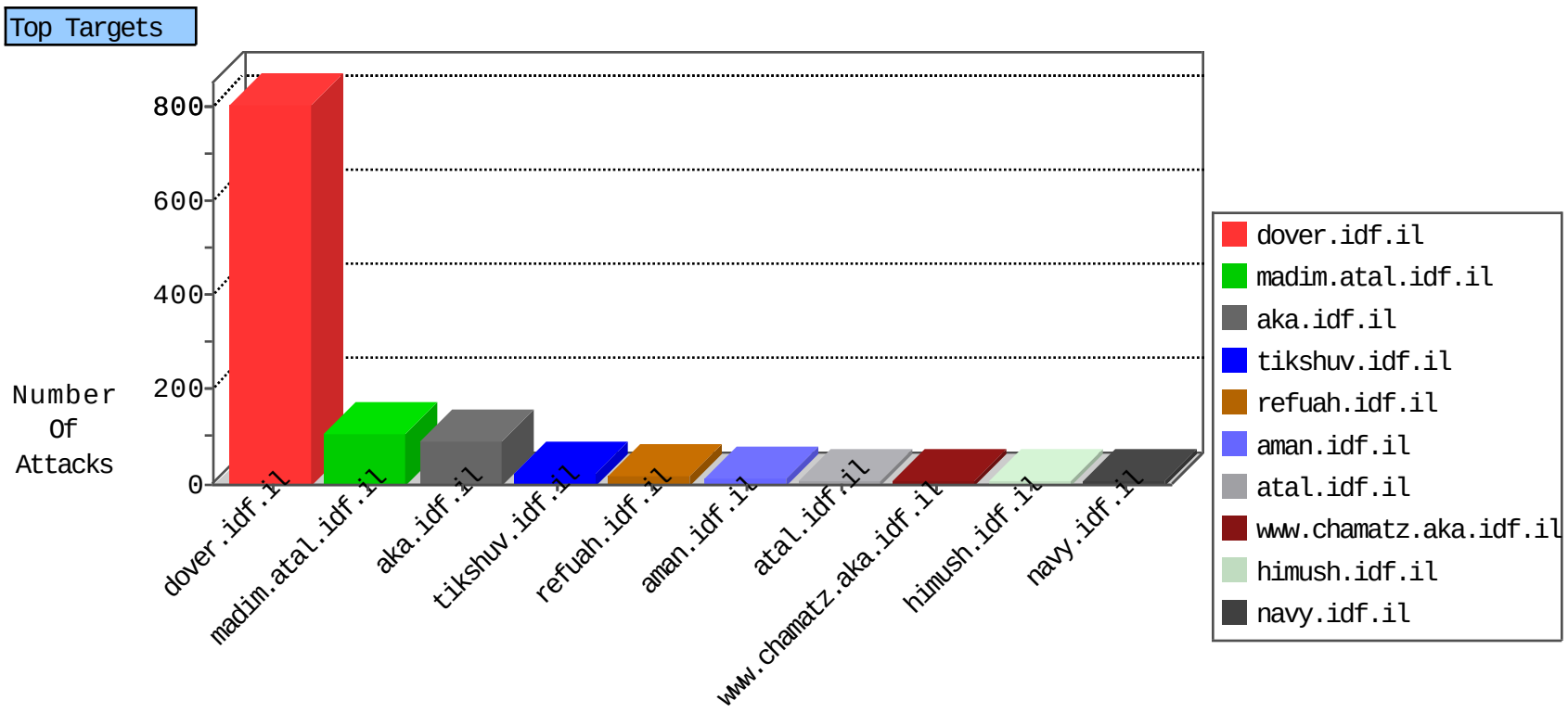
04-14-2015-23:03:08 to 04-15-2015-00:03:08

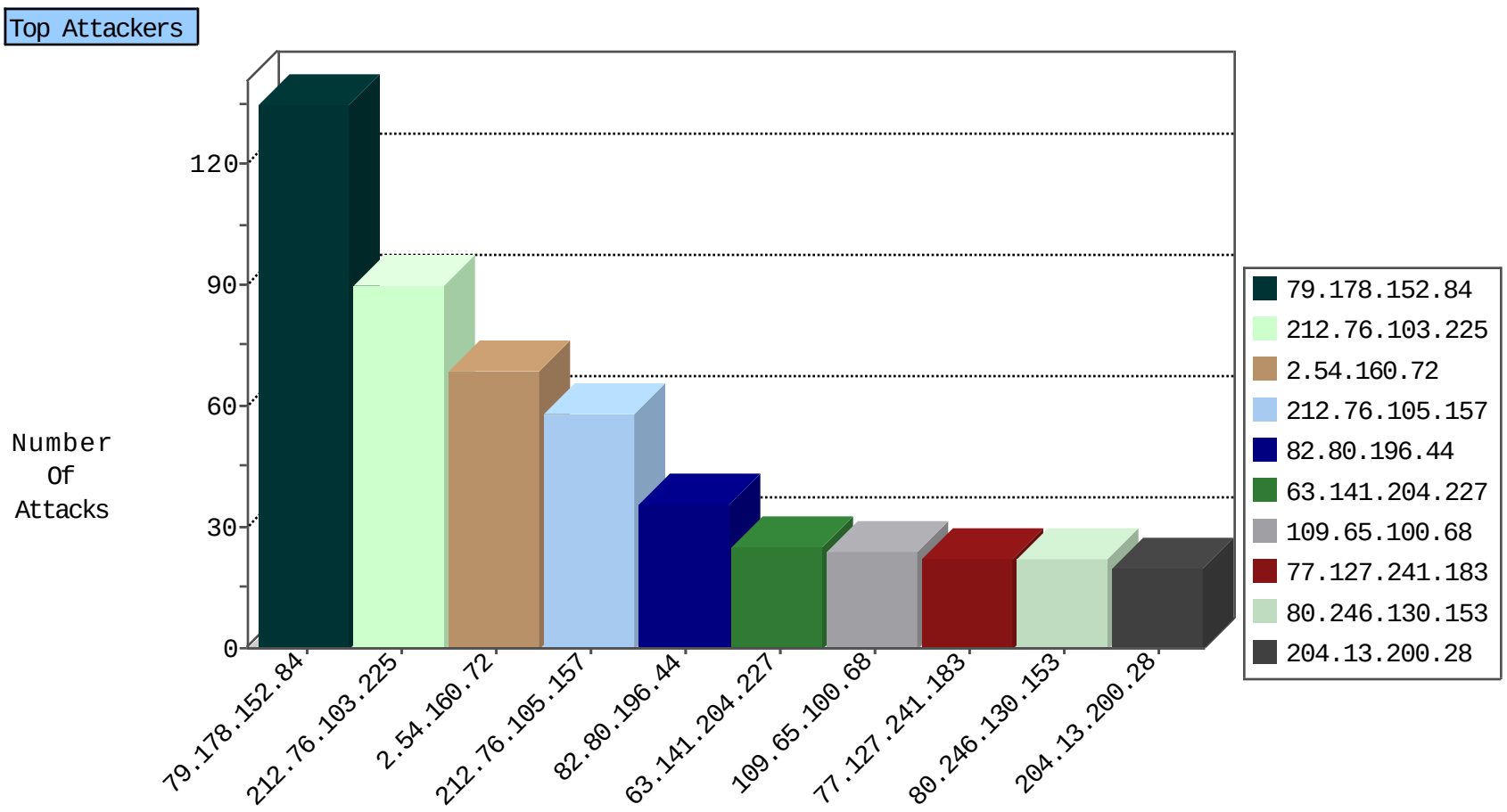
IDF Under Attack
04-14-2015-23:03:08

Top Targets



Top Target

Top Attackers



Top Attackers

04-14-2015-23:03:08 to 04-15-2015-00:03:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.85	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	493
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	206
87.68.79.191	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	108
61.160.215.104	China	147.237.0.34	tikshuv.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
109.67.130.6	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2
61.160.215.104	China	147.237.76.34	yohalan.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
71.6.135.131	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
58.177.161.82	Hong Kong	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

04-14-2015-23:03:08 to 04-15-2015-00:03:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	14
77.127.241.183	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
180.76.5.193	China	147.237.77.226	www.chamatz.aka.idf.il	DVRep_P-N_40-59	Permit	5
5.29.109.192	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.165.200	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.241	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
184.96.119.189	United States	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
184.96.119.189	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
109.64.7.176	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
192.116.131.219	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1

04-14-2015-23:03:08 to 04-15-2015-00:03:08

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	5
66.249.64.150	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
77.126.174.46	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.76	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
94.100.31.179	Netherlands	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
117.135.163.104	China	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
104.197.13.221		147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
94.100.31.179	Netherlands	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
94.100.31.179	Netherlands	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
94.100.31.179	Netherlands	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
94.100.31.179	Netherlands	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
122.228.207.76	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
104.197.13.221		147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1
104.197.13.221		147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -f -sS	1
193.189.116.220	Poland	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
94.100.31.179	Netherlands	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
94.100.31.179	Netherlands	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1

04-14-2015-23:03:08 to 04-15-2015-00:03:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
79.178.152.84	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	135
212.76.103.225	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	90
212.76.105.157	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	58
109.65.100.68	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
80.246.130.153	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
46.19.86.44	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
66.249.81.212	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
63.141.204.227	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	14
109.64.7.176	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
89.138.1.184	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
63.141.204.227	United States	147.237.0.34	tikshuv.idf.i	First packet isn't SYN	drop	drop	11
46.19.86.28	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
41.210.176.138	Uganda	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
66.249.81.218	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
2.54.29.212	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
2.52.162.74	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
79.179.17.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
77.127.226.200	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
2.54.165.114	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
77.127.241.183	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	7
77.127.241.183	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	7
46.19.86.96	Israel	147.237.0.34	tikshuv.idf.i	Invalid ACK number	Bad TCP sequence	monitor	7
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
85.65.244.190	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
66.249.64.142	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
89.139.168.29	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.19.85.88	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
176.12.145.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
66.249.81.215	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
85.250.20.121	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
66.249.78.173	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
38.140.38.26	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
184.96.119.189	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
157.55.39.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
207.46.13.89	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
109.65.197.74	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
202.228.139.164	Japan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.229.141.98	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
109.253.138.115	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
212.76.127.212	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
85.64.126.184	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
95.86.69.199	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
68.180.228.123	United States	147.237.76.42	refuah.idf.il	SAM rule	drop	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
79.176.159.68	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.160.72	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.160.72	Block	68
82.80.196.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	36
79.183.13.127	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	9
77.125.90.26	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
2.54.8.211	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	2
46.117.63.114	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
198.20.69.74	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	2
202.83.19.7	India	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 202.83.19.7	Block	2
149.88.67.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
64.41.200.104	United States	147.237.72.167	ishurim.aka.idf.il	Multiple Untraceable SSL Sessions from 64.41.200.104 (Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE))	None	2
92.253.38.45	Jordan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/qr/	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
64.41.200.104	United States	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 64.41.200.104 (Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE))	None	2
23.229.5.100	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
64.41.200.104	United States	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE)	None	1
85.250.218.69	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
66.249.65.147	United States	147.237.76.30	himush.idf.il	Unknown Parameter lang in www.chimush.atal.idf.il/994-he/himush.aspx	None	1
184.96.119.189	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	1
109.160.180.184	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
64.41.200.104	United States	147.237.77.243	mobile.idf.il	Multiple Untraceable SSL Sessions from 64.41.200.104 (Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE))	None	1
80.246.130.89	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/giyus	Block	1
207.46.13.133	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim1/	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/0112-1.stm	Block	1
66.249.65.43	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.65.43	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/home/def...78&catid=38978	Block	1
64.41.200.104	United States	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE)	None	1
86.108.79.202	Jordan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/qar/	Block	1
77.127.241.183	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
2.54.160.72	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
66.249.67.111	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/yohalan/main/main.asp	Block	1
138.134.102.16	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.65.18	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
46.120.239.229	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
213.151.45.52	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/kapatz/citizencontact.aspx	None	1
69.30.240.46	United States	147.237.77.226	www.chamatz.aka.idf.il	Illegal HTTP Version	Block	1
66.249.65.43	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/asp/wars.asp	Block	1
157.55.39.121	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
64.41.200.104	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE)	None	1
92.253.38.45	Jordan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//qar/	Block	1
77.127.241.183	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.67.119	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/yohalan/forums/asp/showforum.asp	Block	1
66.249.65.22	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
64.41.200.104	United States	147.237.0.16	my-kosher-kravi.idf.il	Multiple Untraceable SSL Sessions from 64.41.200.104 (Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE))	None	1
84.228.111.51	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
69.91.194.108	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.65.147	United States	147.237.76.30	himush.idf.il	Unknown Parameter &SortDir in www.chimush.atal.idf.il/938-he/himush.aspx	None	1
178.202.188.185	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/idf_in_pictures/2003/november/06.stm	Block	1
79.178.21.83	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
23.229.5.100	United States	147.237.72.166	aka.idf.il	Admin Blocking	Block	1
202.83.19.7	India	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1