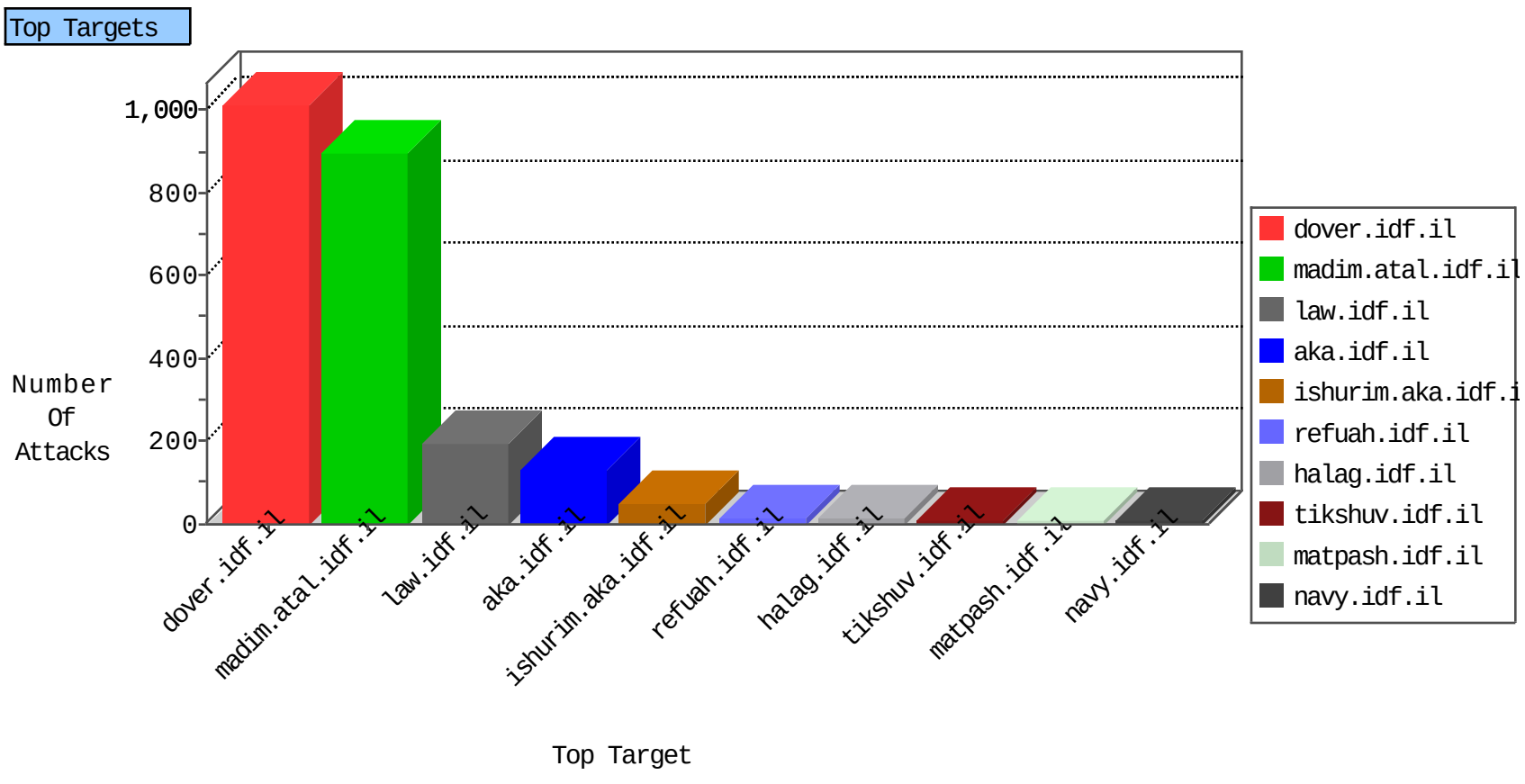
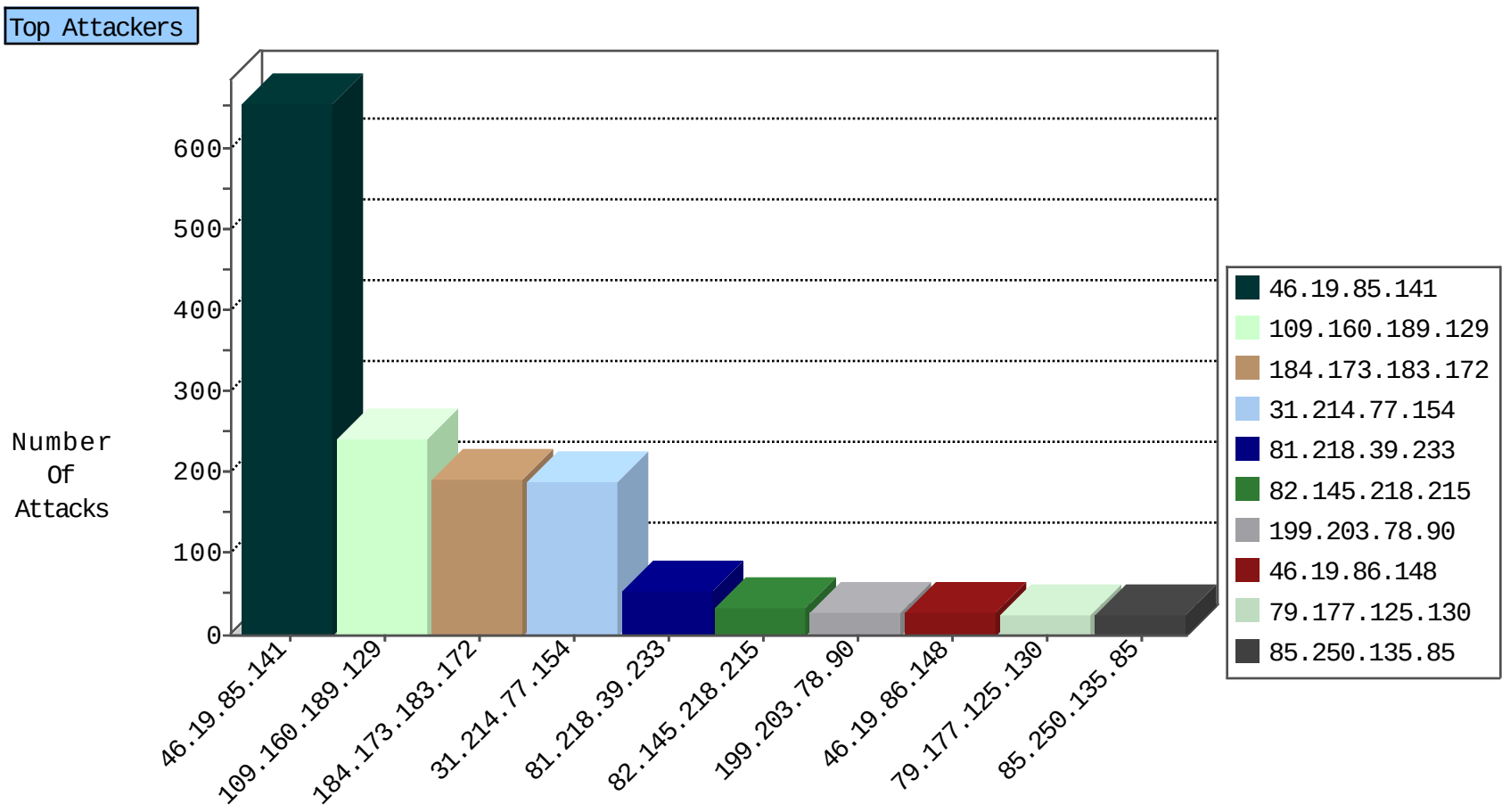
04-14-2015-20:03:07 to 04-14-2015-21:03:07

IDF Under Attack
04-14-2015-20:03:07

Top Targets



Top Attackers



04-14-2015-20:03:07 to 04-14-2015-21:03:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
212.179.21.195	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3341
66.249.78.173	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	739
199.203.78.90	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	335
80.246.138.206	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	108
124.232.142.220	China	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
85.130.174.226	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
14.198.223.26	Hong Kong	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

04-14-2015-20:03:07 to 04-14-2015-21:03:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	193
71.6.165.200	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	2
178.241.82.191	Turkey	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
79.177.185.212	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
46.116.107.159	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
84.209.116.95	Norway	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
109.64.162.209	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.167.142	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
109.201.152.245	Netherlands	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	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	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.27	e.madim.atal.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	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
37.142.159.40	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-14-2015-20:03:07 to 04-14-2015-21:03:07

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
46.117.192.21	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.182.36.106	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.178.141.133	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.65.12	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.66	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
210.200.0.78	Taiwan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
27.50.132.60	China	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 4096	1
203.209.80.11	Thailand	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
166.78.227.105	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
78.93.225.18	Saudi Arabia	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 2048	1
78.93.225.18	Saudi Arabia	147.237.76.86	navy.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.67	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.190.60	Japan	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
203.209.80.11	Thailand	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 4096	1
27.50.132.60	China	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	1
78.93.225.18	Saudi Arabia	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1

04-14-2015-20:03:07 to 04-14-2015-21:03:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
31.214.77.154	Kuwait	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	190
82.145.218.215	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
46.19.86.148	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
79.177.125.130	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
109.186.58.168	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
85.250.135.85	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
77.126.44.180	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
162.243.222.48	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
37.142.149.241	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
184.183.3.183	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
192.116.131.154	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
149.78.6.60	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
87.69.146.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
65.115.97.166	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
46.116.128.114	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
46.19.86.43	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
84.229.195.156	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
37.26.147.143	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
68.180.228.123	United States	147.237.76.42	refuah.idf.il	SAM rule	drop	drop	10
65.55.210.100	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
192.182.144.46	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
179.34.19.94		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
176.12.143.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
188.120.148.245	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
82.145.219.16	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
176.12.149.139	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
109.160.189.129	Israel	147.237.0.19	madim.atal.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
85.65.236.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
80.184.46.136	Kuwait	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
46.19.86.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
165.91.12.152	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
5.29.164.155	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
79.178.141.133	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
66.249.78.173	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
79.178.155.243	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.19.86.123	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
166.78.227.105	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
212.76.127.111	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
5.29.38.64	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.19.86.190	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
87.68.76.181	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
207.46.13.82	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
176.12.140.52	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
79.179.187.195	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
208.221.239.4	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
46.19.85.114	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
37.26.147.193	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
192.166.56.36	Germany	147.237.77.176	matpash.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
46.19.85.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	655
109.160.189.129	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.160.189.129	Block	231
81.218.39.233	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	54
87.69.161.127	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 87.69.161.127	Block	13
109.160.180.184	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.160.180.184	Block	3
87.69.161.127	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	3
188.120.132.137	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
109.160.180.184	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.228.47.145	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.229.34.156	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
176.12.136.178	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
198.199.121.221	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
81.218.44.9	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.180.179.144	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
66.249.65.152	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/m/	Block	1
46.19.85.97	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.133	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/registrationwizard/register.aspx	Block	1
79.180.180.180	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
188.143.232.72	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
109.253.130.156	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
66.249.78.173	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	1
87.69.161.127	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.65.22	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	1
207.46.13.31	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.31	Block	1
81.218.39.233	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/chinuch/gallery/showpicture.asp	None	1
77.127.150.159	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
166.78.227.105	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.65.153	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1247-he/atal.aspx	Block	1
213.57.213.60	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
79.181.59.205	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	1
188.165.15.78	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/french/info.stm	Block	1
125.94.92.46	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/window.location.href	Block	1
66.249.81.226	United States	147.237.76.31	nakchal.idf.il	URL is Above Root Directory nakhal.idf.il/../favicon.ico	Block	1
66.249.65.39	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/chinuch/miktzoa/default.asp	None	1
207.46.13.79	United States	147.237.72.166	aka.idf.il	Unknown Parameter cd5b9038 in www.aka.idf.il/main/home/default.aspx	None	1
77.127.238.163	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/general/&q=	Block	1
66.249.65.157	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1241-he/atal.aspx	Block	1
109.160.180.184	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyud	Block	1
85.64.159.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.85.162	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
79.181.180.250	Israel	147.237.72.166	aka.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
149.88.14.27	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	1
66.249.65.41	United States	147.237.72.166	aka.idf.il	Unknown Parameter itemid in www.aka.idf.il/kamlar/gallery/showpicture.asp	None	1
207.46.13.133	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.180.123.201	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1
178.255.87.242	United Kingdom	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Untraceable SSL Sessions from 178.255.87.242 (Unknown Server Certificate)	None	1
66.249.65.161	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1242-he/atal.aspx	Block	1
109.160.189.129	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1