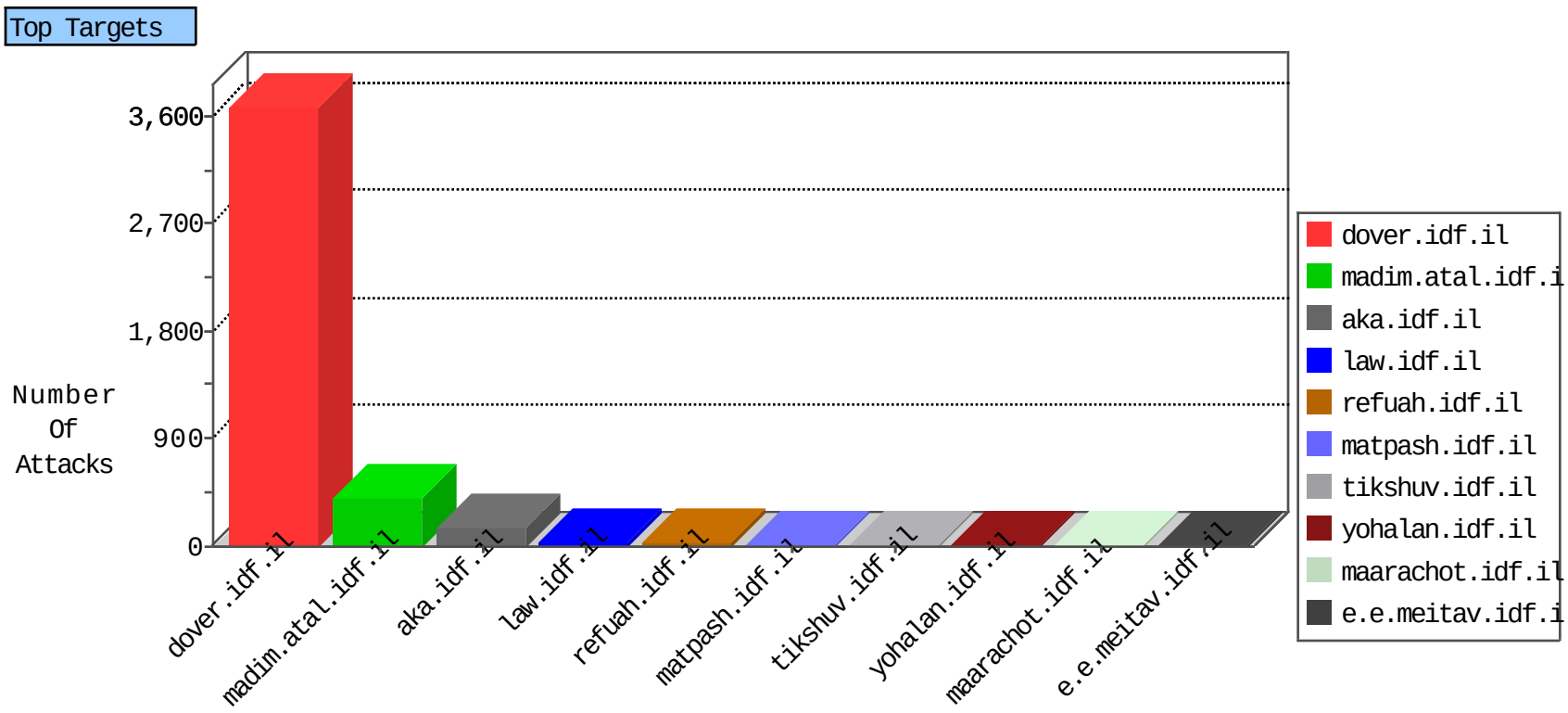
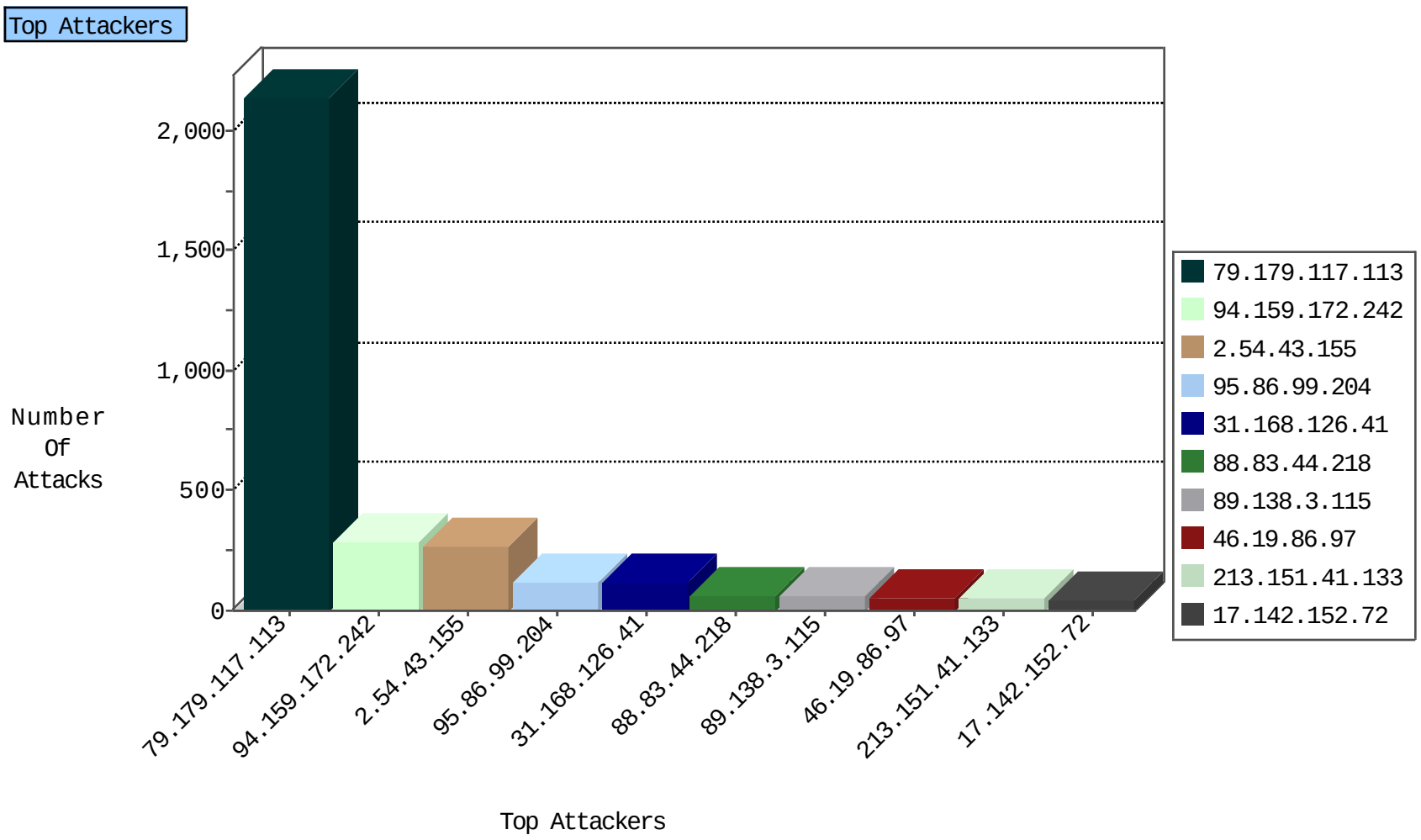
04-29-2015-00:03:04 to 04-29-2015-01:03:04

IDF Under Attack
04-29-2015-00:03:04

Top Targets



Top Attackers



04-29-2015-00:03:04 to 04-29-2015-01:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.67.92	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	811
82.145.216.4	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	6
93.173.140.229	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
46.19.86.97	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
84.94.33.204	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
182.35.244.63	China	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
70.199.101.209	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
183.48.216.188	China	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
114.188.86.143	Japan	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
46.19.86.188	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
219.78.5.208	Hong Kong	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
115.229.93.252	China	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

04-29-2015-00:03:04 to 04-29-2015-01:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
180.76.5.193	China	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	31
200.87.215.249	Bolivia	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
37.142.240.127	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
37.142.240.127	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
93.120.27.62	Romania	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
108.185.167.139	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
109.201.152.239	Netherlands	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.0.17	m.my-kosher-kravi.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
198.20.70.114	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1

04-29-2015-00:03:04 to 04-29-2015-01:03:04

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
104.148.38.35		147.237.77.216	dover.idf.il	SERVER-WEBAPP Mambo upload.php access	2
80.246.130.44	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.93.176	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
176.12.137.159	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.108.193.192	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.67.116	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.65	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
61.183.128.6	China	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
178.19.107.114	Poland	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
60.18.162.244	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
167.114.40.66	United States	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
5.196.147.122	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
139.194.160.216	Indonesia	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
222.69.94.13	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 3072	1
212.147.56.190	Switzerland	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
202.100.219.52	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
202.100.219.52	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.183.128.6	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
193.107.16.206	Russian Federation	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
60.18.162.244	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
60.18.162.244	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -f -sS	1
139.194.160.216	Indonesia	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
107.6.130.113	United States	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
222.186.59.91	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
212.147.56.190	Switzerland	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
74.113.47.90	United States	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
212.147.56.190	Switzerland	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -f -sS	1
202.100.219.52	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1

04-29-2015-00:03:04 to 04-29-2015-01:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
79.179.117.113	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2121
2.54.43.155	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	269
95.86.99.204	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	116
88.83.44.218	Sweden	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	63
89.138.3.115	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	58
213.151.41.133	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	48
17.142.152.72	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
89.139.51.131	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
46.19.86.97	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
178.8.56.200	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
17.142.152.110	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
17.142.152.89	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
17.142.152.111	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
109.253.156.195	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
88.254.69.226	Turkey	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
179.161.41.179	Brazil	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
190.194.172.85	Argentina	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
17.142.152.85	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
160.39.50.95	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
176.12.137.122	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
46.19.86.191	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
78.51.177.120	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
185.26.182.35	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
79.179.117.113	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	alert	12
109.253.132.116	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
176.12.144.27	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
69.150.27.15	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
46.19.85.231	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
91.228.167.130	Slovakia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
176.12.144.141	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
176.12.150.36	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
176.12.145.160	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
176.12.150.81	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
176.12.148.222	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
176.12.151.197	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
38.104.208.106	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
84.228.170.217	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
178.53.173.128	Kuwait	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
108.185.167.139	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
166.137.10.25	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
93.186.23.97	United Kingdom	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
94.197.120.235	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
46.19.85.28	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
24.114.64.61	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
46.19.85.242	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
17.142.152.86	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8

04-29-2015-00:03:04 to 04-29-2015-01:03:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
94.159.172.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	288
31.168.126.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	81
213.57.56.24	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	10
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	4
82.145.218.236	Europe	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
87.68.161.102	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
89.134.218.126	Hungary	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
157.55.39.44	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 157.55.39.44	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
157.55.39.10	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 157.55.39.10	Block	2
109.253.156.195	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.219	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 157.55.39.219	Block	2
157.55.39.44	United States	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il//usefulinformation/pages/reports.aspx	Block	2
79.183.133.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/igf	Block	1
157.55.39.220	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/arabic/pages/default.aspx	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	1
157.55.39.11	United States	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il//coordinationgaza/pages/default.aspx	Block	1
109.66.13.248	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
62.219.143.60	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/updateuserdetails.aspx	Block	1
184.168.27.42	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
84.111.122.188	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
176.12.144.27	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	1
212.97.132.195	Denmark	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on refua.atal.idf.il//wp/wp-admin/	Block	1
37.142.167.254	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//https:/www.idf.il/	Block	1
176.12.150.36	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
89.139.182.157	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.192.112.143	United Kingdom	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/declarationofemployment.aspx	None	1
162.254.149.38		147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/unitfs.asp	Block	1
157.55.39.11	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/general/	Block	1
109.66.32.121	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.78	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.78	Block	1
184.168.27.206	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on refua.atal.idf.il//wordpress/wp-admin/	Block	1
2.52.160.161	Israel	147.237.0.34	tikshuv.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 2.52.160.161	Block	1
176.12.144.141	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.250.127.83	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
157.55.39.134	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/pages/reports.aspx	Block	1
77.126.12.65	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
157.55.39.10	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/coordinationgaza/pages/default.aspx	Block	1
46.117.28.135	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
176.12.150.81	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
93.172.68.56	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
174.129.237.157	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
157.55.39.24	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.maarachot.idf.il/templates/general/general.aspx	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//938-he/refuah.aspx	Block	1
66.249.75.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
184.168.200.108	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on refua.atal.idf.il//test/wp-admin/	Block	1
14.29.209.255	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1

04-29-2015-00:03:04 to 04-29-2015-01:03:04