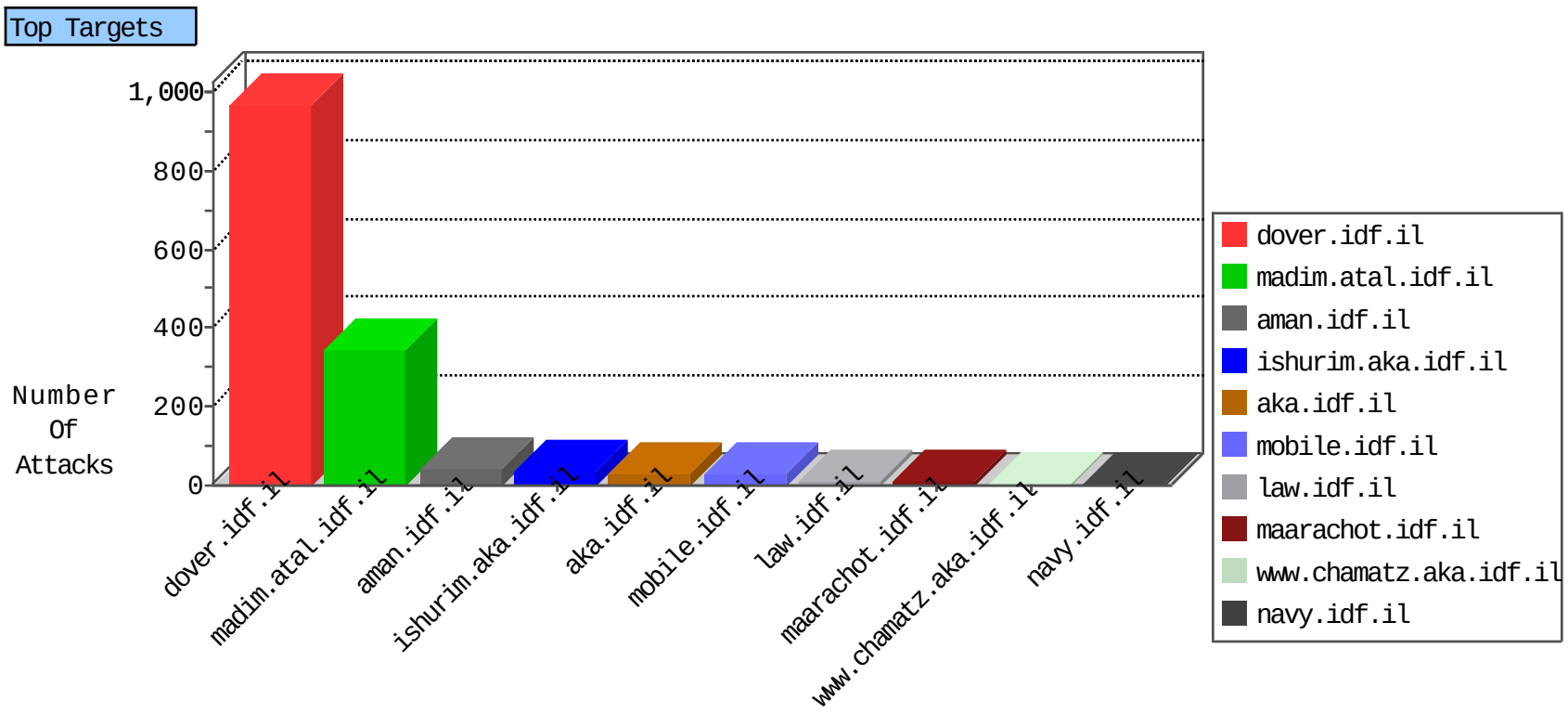
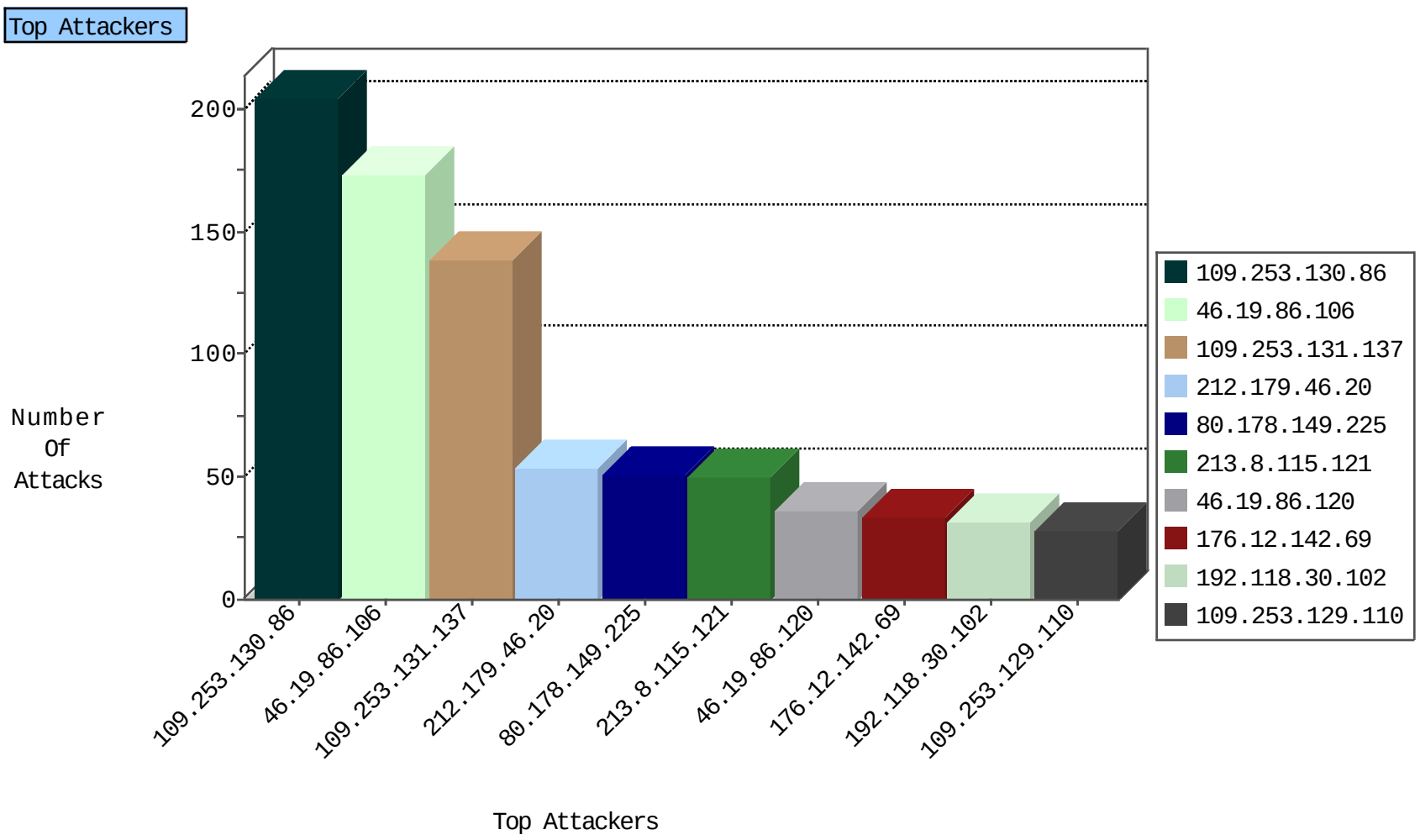
04-24-2015-11:03:01 to 04-24-2015-12:03:01

IDF Under Attack
04-24-2015-11:03:01

Top Targets



Top Attackers



04-24-2015-11:03:01 to 04-24-2015-12:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	347
213.57.208.95	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	179
84.228.120.13	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	161
79.176.213.191	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	104
109.253.138.219	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	81
93.172.27.159	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
89.139.165.164	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
103.224.105.10	India	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
188.120.148.200	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
10.0.0.15		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
212.76.109.212	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
109.64.19.67	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
66.249.79.75	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
122.226.102.84	China	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
141.138.156.16	France	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
84.228.215.130	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
23.95.82.226	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
193.5.216.100	Switzerland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
79.179.200.184	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.19.85.151	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
80.246.133.1	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
188.138.9.50	Germany	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1

04-24-2015-11:03:01 to 04-24-2015-12:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	5
85.65.48.101	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
213.57.112.207	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
31.7.57.198	Switzerland	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
220.181.125.15	China	147.237.77.233	atal.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
2.54.157.90	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
79.178.106.174	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
31.7.57.198	Switzerland	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.170	maarachot.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
31.7.57.198	Switzerland	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.31	nakchal.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
31.7.57.198	Switzerland	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.74	law.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

04-24-2015-11:03:01 to 04-24-2015-12:03:01

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
66.249.65.30	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.73.203	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.134	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
61.240.144.65	China	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
61.183.128.6	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
61.183.128.6	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.132.118	Russian Federation	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
61.183.128.6	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1

04-24-2015-11:03:01 to 04-24-2015-12:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.19.86.106	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	174
212.179.46.20	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	54
80.178.149.225	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
213.8.115.121	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
46.19.86.120	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
176.12.142.69	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
109.253.129.110	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
37.131.65.128	Bahrain	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
109.253.137.6	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
77.125.79.28	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
81.218.251.252	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
82.102.169.113	Israel	147.237.77.243	mobile.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
77.125.252.43	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
85.65.247.51	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
109.253.129.245	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
109.253.133.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
212.179.86.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
176.12.145.217	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
62.204.9.126	Finland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
176.12.139.46	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
46.19.86.38	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
168.63.137.102	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
176.12.150.245	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
79.176.173.208	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
103.224.105.10	India	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
185.4.253.19	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
176.12.140.204	Israel	147.237.77.243	mobile.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.121.82.80	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
79.177.118.98	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
66.249.93.160	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
109.253.147.99	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.86.79	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
93.172.164.112	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
79.182.27.168	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
212.76.127.111	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
80.179.114.27	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.85.241	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
79.179.54.138	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
87.69.224.29	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
192.116.175.162	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.85.4	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
37.142.211.179	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
85.72.135.153	Greece	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
31.13.97.113	Ireland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
50.185.70.101	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
109.160.171.112	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
85.250.1.212	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
46.116.209.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
46.19.85.241	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
87.69.172.83	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.253.130.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	205
109.253.131.137	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.131.137	Block	138
66.249.79.66	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.66	Block	4
46.19.86.130	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
66.6.46.224	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.6.46.224	Block	2
2.54.166.145	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
66.249.79.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.74	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
84.228.196.197	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm	Block	1
2.52.23.212	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//894-he/refuah.aspx	Block	1
213.57.112.207	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/8/	Block	1
157.55.39.166	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
66.249.65.15	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
109.160.247.161	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
77.127.230.208	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.65.182	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
188.165.15.13	France	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
141.212.122.82	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/	Block	1
84.229.180.207	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
217.132.93.218	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
66.249.79.74	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
176.12.137.249	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.65.22	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
46.19.86.140	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
79.176.173.208	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
66.249.73.136	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
203.133.170.167	Korea, Republic of	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.6.46.224	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1514-en/dover.aspx#.vtn7rb3f2bo.tumblr	Block	1
146.185.56.110	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
87.68.252.186	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//https:/www.aman.idf.il/	Block	1
5.29.45.198	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arafat/english/kkkkkkk=652ce764kkkkkkk_652ce764	Block	1
66.249.65.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
46.117.27.31	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_SERVER_HELLO)	None	1
109.253.131.137	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
81.218.251.252	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.73.150	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/m/	Block	1
207.241.237.220	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
149.78.214.102	United States	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/giyus/terms.aspx	None	1
66.249.65.10	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.65.10	Block	1
87.68.252.186	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
31.210.187.154	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
184.105.139.68	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
66.249.65.153	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
46.120.22.21	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il./	Block	1
84.94.62.72	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.58	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
213.57.112.207	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 213.57.112.207	Block	1
157.55.39.127	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/1.he/infocenteritem/	Block	1
66.249.65.10	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/contactus/contactus.aspx	Block	1