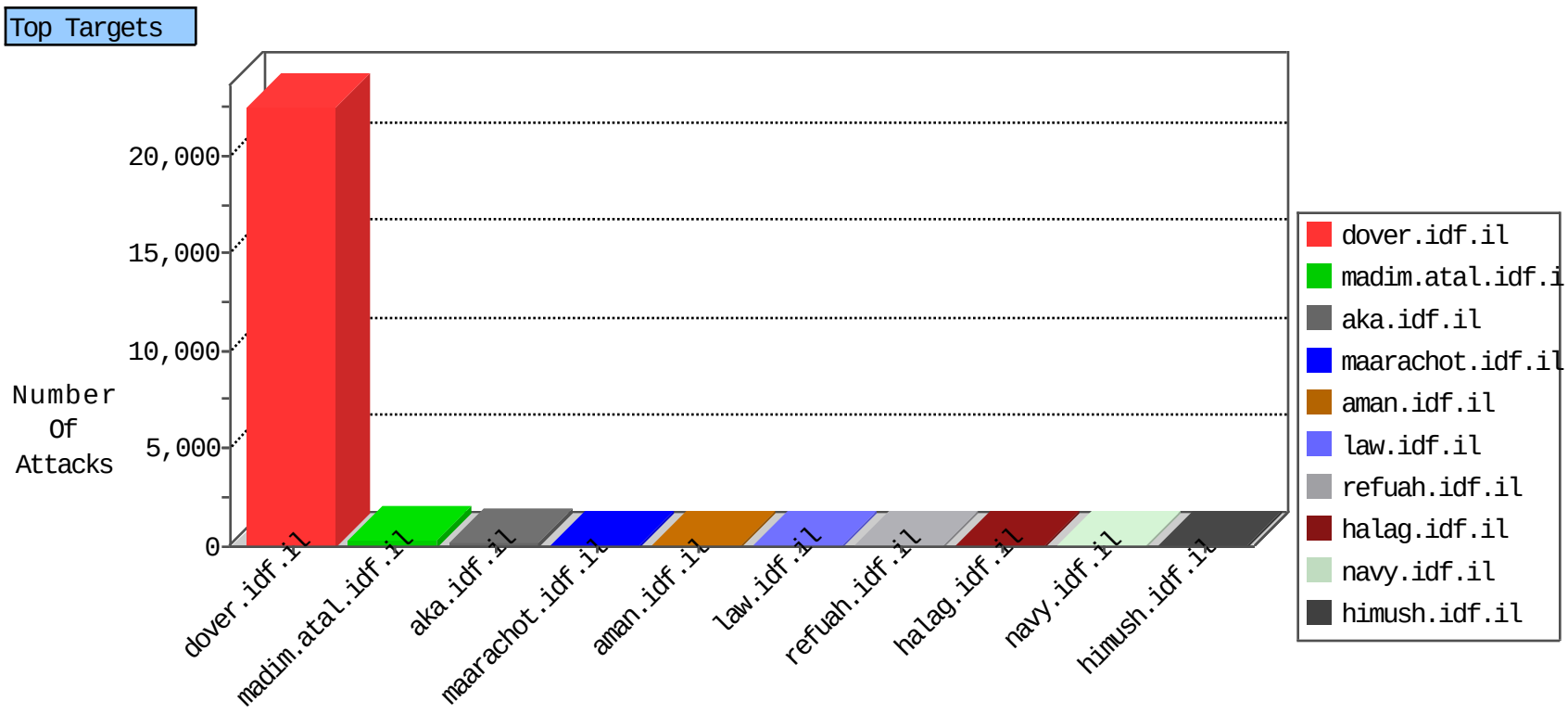
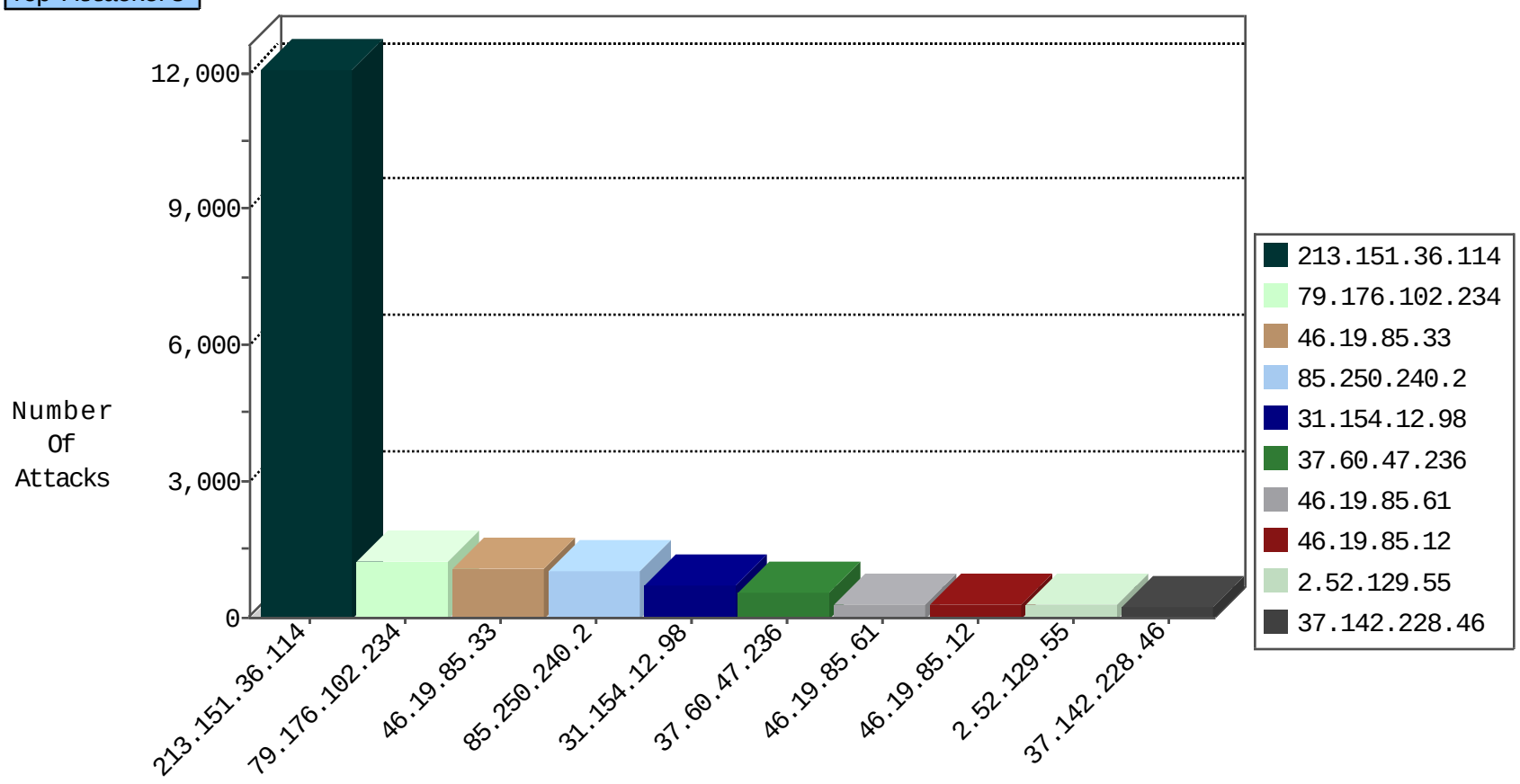
05-02-2015-22:03:02 to 05-02-2015-23:03:02

IDF Under Attack
05-02-2015-22:03:02

Top Targets



Top Attackers



05-02-2015-22:03:02 to 05-02-2015-23:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
85.64.224.118	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	154
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	142
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	19
79.177.33.174	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	9
79.179.136.162	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
176.12.147.69	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
10.0.0.11		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
109.66.160.211	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
84.229.39.139	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
176.12.141.123	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
149.78.150.238	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
84.95.205.8	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
85.250.102.190	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
149.78.139.14	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
94.159.210.33	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
10.0.0.12		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
5.22.130.161	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
84.229.175.55	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
36.38.112.9	Korea, Republic of	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
5.29.75.134	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
95.86.84.181	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
157.55.39.66	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
85.250.13.84	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
79.177.202.131	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

05-02-2015-22:03:02 to 05-02-2015-23:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
94.222.208.98	Germany	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
46.19.85.8	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
5.102.254.207	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
177.9.168.240	Brazil	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.167.142	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
109.64.32.66	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.165.200	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
5.29.158.175	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1

05-02-2015-22:03:02 to 05-02-2015-23:03:02

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
84.228.69.196	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.96	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
80.230.66.252	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.82	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.64	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
221.143.48.200	Korea, Republic of	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1
185.32.179.111	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	1
178.32.251.100	France	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
167.88.41.228		147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
66.249.75.13	United States	147.237.72.166	aka.idf.il	WEB-CGI redirect access	1
61.240.144.64	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
183.136.216.3	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
167.88.41.228		147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
87.69.199.64	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1

05-02-2015-22:03:02 to 05-02-2015-23:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
213.151.36.114	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12080
79.176.102.234	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1221
46.19.85.33	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1071
85.250.240.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1050
31.154.12.98	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	712
37.60.47.236	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	570
46.19.85.61	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	295
46.19.85.12	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	293
2.52.129.55	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	276
37.142.228.46	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	255
94.159.143.243	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	228
2.52.55.209	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	109
99.51.6.139	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	89
109.253.145.203	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	84
46.19.86.53	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	76
109.186.45.216	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	76
109.67.144.98	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	75
107.77.68.61	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	72
93.173.12.174	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	65
204.110.16.10	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	59
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	58
80.246.133.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	58
62.219.124.98	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
109.64.32.66	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	47
95.35.4.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
2.54.141.28	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
106.38.188.45	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	44
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
109.67.134.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
109.253.141.203	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
46.19.86.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
93.172.170.208	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
79.181.128.200	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
46.19.86.197	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
157.55.39.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
2.54.169.242	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
2.54.155.156	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
79.179.136.162	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
64.233.173.161	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
109.65.1.248	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
79.183.161.62	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
66.249.93.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
149.78.244.216	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
46.19.85.133	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
37.26.147.135	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	191
185.32.179.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	60
80.246.140.92	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	33
5.102.215.86	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	19
95.86.75.213	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	13
142.54.174.178	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 142.54.174.178	Block	11
79.178.6.185	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	11
84.228.155.114	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	8
85.250.73.63	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
37.142.228.46	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	6
95.86.75.213	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	6
66.249.75.5	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.75.5	Block	6
157.55.39.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
147.235.8.70	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	5
66.249.75.117	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.75.117	Block	5
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	5
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
157.55.39.61	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
2.54.154.181	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	3
79.177.29.187	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	3
109.65.163.153	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
207.46.13.101	United States	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
109.67.128.228	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	2
5.29.158.175	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
80.246.136.252	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
218.30.103.52	China	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	1
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/statistics/killed.stm	Block	1
46.116.143.36	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
180.76.5.22	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
79.181.135.130	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.111	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/163-5432-he/patzar.aspx	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Unknown Parameter d6369898 in www.aka.idf.il/main/home/default.aspx	None	1
66.249.75.5	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/asp/wars.asp	Block	1
46.229.164.113	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.229.164.113	Block	1
207.46.13.99	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/captcha.ashx	Block	1
66.249.81.225	Israel	147.237.76.31	nakchal.idf.il	URL is Above Root Directory www.nakhal.idf.il/../favicon.ico	Block	1
37.46.42.35	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
2.54.33.197	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//webresource.axd	Block	1
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	1
87.68.58.205	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.117.61.253	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
79.183.122.149	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.78.118	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/templates/getfile/getfile.aspx	Block	1
31.44.135.21	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
157.55.39.136	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
66.249.75.13	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.75.13	Block	1
109.66.101.221	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
84.108.38.28	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/soldiercontact.aspx	None	1

05-02-2015-22:03:02 to 05-02-2015-23:03:02