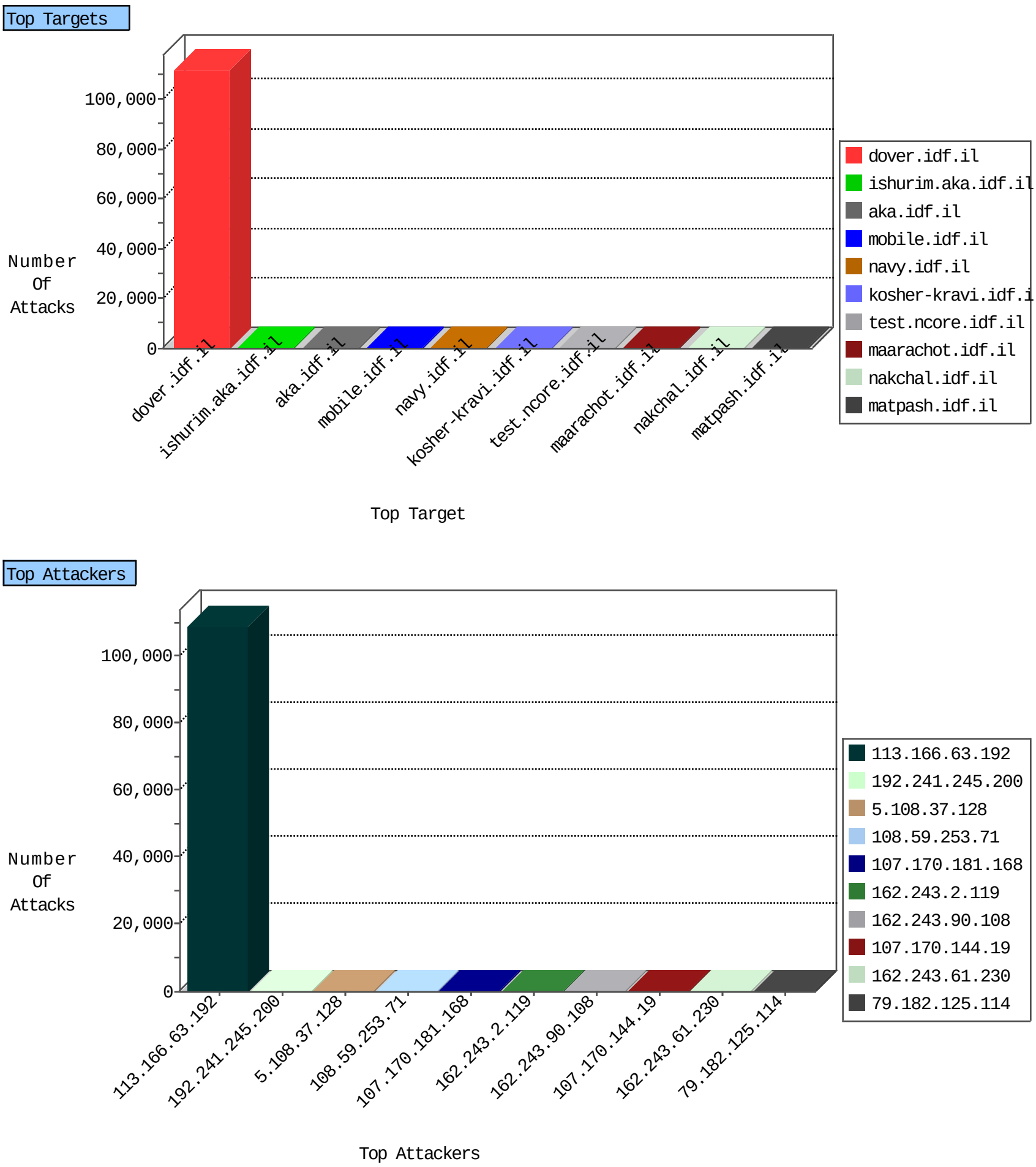
04-21-2015-01:03:01 to 04-21-2015-02:03:01

IDF Under Attack
04-21-2015-01:03:01



04-21-2015-01:03:01 to 04-21-2015-02:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
212.150.244.228	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	695
220.181.108.172	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	236
66.249.67.39	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	38
142.105.60.180	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	27
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	13
94.159.212.206	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
176.12.138.97	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
212.150.244.228	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
70.199.102.168	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
71.6.216.35	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.59	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1

04-21-2015-01:03:01 to 04-21-2015-02:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
71.6.167.142	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	2
71.6.165.200	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	2
198.20.70.114	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.50	e.tikshuv.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	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
84.111.63.141	Israel	147.237.72.166	aka.idf.il	C1000098: Block - dns poisoning	Block	1
66.240.192.138	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1

04-21-2015-01:03:01 to 04-21-2015-02:03:01

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
84.111.63.141	Israel	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
66.249.78.190	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.31	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
128.30.52.70	United States	147.237.76.86	navy.idf.il	Tehila - Perl LWP with fake user agent	2
114.112.90.54	China	147.237.76.176	test.ncore.idf.i	ET SCAN NMAP -sS window 1024	1
111.203.22.56	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.67	China	147.237.76.38	e.e.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
176.31.175.247	Spain	147.237.72.14	dover.idf.il(old	ET SCAN Potential SSH Scan	1
114.112.90.54	China	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
111.203.22.56	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
208.184.217.221	United States	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1
192.161.63.36	United States	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1

04-21-2015-01:03:01 to 04-21-2015-02:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
113.166.63.192	Vietnam	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	108973
192.241.245.200	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	239
5.108.37.128	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	188
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	168
107.170.181.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	142
162.243.2.119	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	135
162.243.90.108	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	122
107.170.144.19	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	112
162.243.61.230	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	95
79.182.125.114	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	86
46.19.86.204	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	64
85.65.70.228	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	57
89.139.183.165	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	53
140.139.231.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
85.72.40.4	Greece	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
67.238.21.22	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
73.39.233.212	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
41.189.161.60	Ghana	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
76.119.134.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
178.92.52.119	Ukraine	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
72.69.78.228	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
77.126.68.71	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
91.225.122.62	Ukraine	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
31.116.149.50	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
88.198.157.214	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
207.46.13.52	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
176.37.21.112	Ukraine	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
2.25.42.158	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
142.105.60.180	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
207.46.13.1	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
207.46.13.35	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
109.66.106.90	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
46.116.211.238	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
176.12.144.16	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
77.75.79.11	Czech Republic	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
157.55.39.31	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
97.74.24.189	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
75.141.237.64	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
109.65.5.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
109.253.134.75	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
2.52.154.172	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
69.242.232.57	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
137.151.174.128	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9

04-21-2015-01:03:01 to 04-21-2015-02:03:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.176.99.126	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.176.99.126	Block	3
79.176.99.126	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	2
176.12.141.0	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
176.12.143.195	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
37.142.234.205	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	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
176.12.139.238	Israel	147.237.72.166	aka.idf.il	Double URL Encoding - parameter: search in www.aka.idf.il/main/giyus/pniothandler1.asmx/search	Block	1
212.76.108.210	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 212.76.108.210	Block	1
157.55.39.3	United States	147.237.72.166	aka.idf.il	Unknown Parameter 4f9c0c80 in www.aka.idf.il/main/home/default.aspx	None	1
66.249.73.211	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
85.65.111.199	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
31.13.99.114	Ireland	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.74	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/032204-5.stm	Block	1
87.68.50.44	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
176.12.150.87	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
109.253.136.78	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$LoginControl$captcha$captchaText in www.aka.idf.il/main/giyus/login.aspx	None	1
66.249.64.61	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/templates/templatecontrols/links/undefined	Block	1
157.55.39.208	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
197.124.120.92	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
109.253.149.104	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.67.40	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/m/	Block	1

04-21-2015-01:03:01 to 04-21-2015-02:03:01