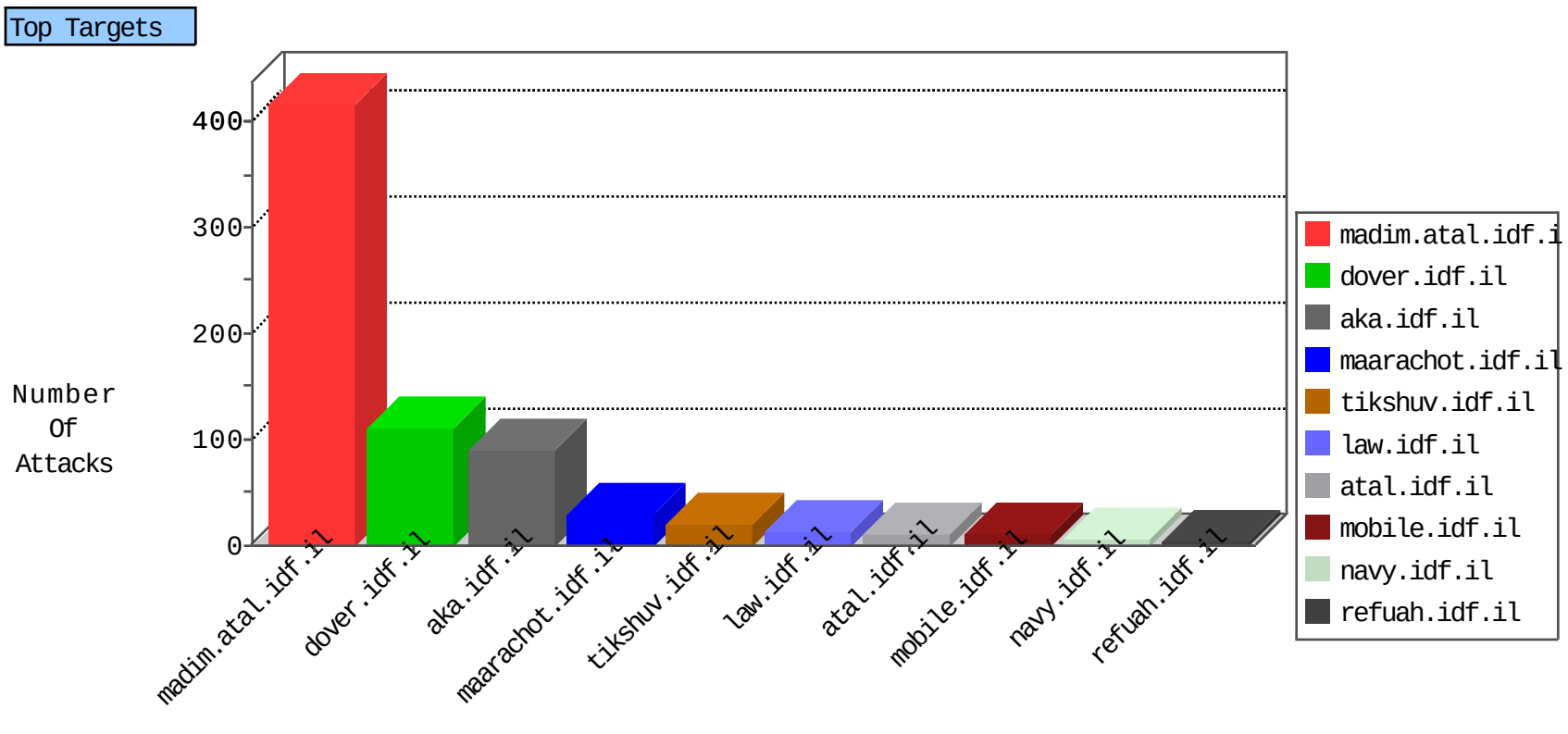
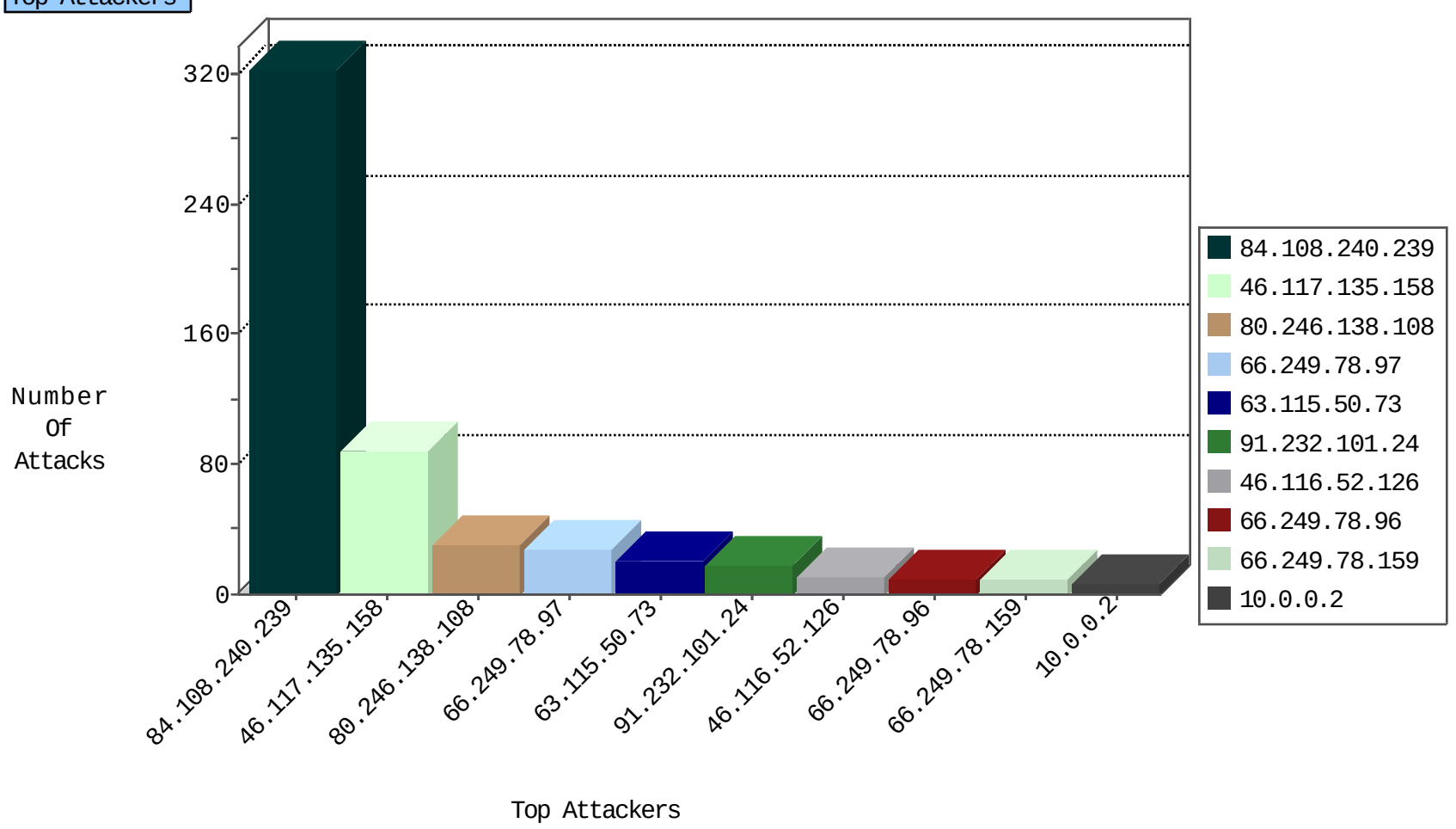
04-25-2015-22:03:06 to 04-25-2015-23:03:06

IDF Under Attack
04-25-2015-22:03:06

Top Targets



Top Attackers



04-25-2015-22:03:06 to 04-25-2015-23:03:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.97	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	4125
77.126.72.106	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1475
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	473
66.249.78.111	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	355
10.0.0.2		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	20
66.249.78.159	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
66.249.67.34	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	6
71.57.170.180	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
77.126.123.74	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
66.249.67.157	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
84.228.193.227	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

04-25-2015-22:03:06 to 04-25-2015-23:03:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.176.111.55	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.1	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
63.115.50.73	United States	147.237.0.34	tikshuv.idf.il	0932: HTTP: Shell Command Execution (bash)	Block	1
77.127.206.198	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
198.20.70.114	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1

04-25-2015-22:03:06 to 04-25-2015-23:03:06

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
80.246.138.108	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	30
63.115.50.73	United States	147.237.0.34	tikshuv.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
85.65.152.105	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
79.177.8.216	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
63.115.50.73	United States	147.237.0.19	madim.atal.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	2
63.115.50.73	United States	147.237.0.15	kosher-kravi.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	2
84.228.111.33	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.162.116.49	Sweden	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
157.7.84.80	Japan	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 2048	1
157.7.84.80	Japan	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -f -sS	1
104.192.0.20		147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
103.24.56.218	Indonesia	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
103.24.56.218	Indonesia	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.30	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.232.101.24	Lebanon	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
46.162.116.49	Sweden	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
88.249.106.23	Turkey	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
157.7.84.80	Japan	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
72.69.217.117	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
104.192.0.20		147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
103.24.56.218	Indonesia	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
63.115.50.73	United States	147.237.0.17	m.my-kosher-kravi.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	1
103.24.56.218	Indonesia	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
63.115.50.73	United States	147.237.0.17	m.my-kosher-kravi.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	1
103.24.56.218	Indonesia	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
98.143.148.107	United States	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.183.128.6	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.132.118	Russian Federation	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1

04-25-2015-22:03:06 to 04-25-2015-23:03:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
91.232.101.24	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
46.116.52.126	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
23.117.221.133	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
2.52.178.61	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
37.26.146.228	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
207.46.13.52	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
149.78.186.96	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
212.76.127.111	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.54.46.160	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
84.228.22.121	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
85.250.95.140	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
79.176.111.55	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	2
176.12.147.52	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
79.181.57.248	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
207.46.13.95	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
50.97.52.131	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.19.85.195	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
176.228.138.212	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	1
95.86.74.115	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
80.246.130.14	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.162.116.49	Sweden	147.237.76.201	e.atal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
169.229.3.94	United States	147.237.72.217	e.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
67.227.163.231	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.19.86.250	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
185.24.76.162	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
109.253.144.90	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
46.210.207.120	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
212.235.28.176	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
37.26.146.221	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
169.229.3.94	United States	147.237.77.212	e.dover.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
77.126.72.106	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.116.3.114	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
2.54.60.199	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.121.196	United States	147.237.72.217	e.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.210.207.120	Israel	147.237.77.226	www.chamatz.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
213.57.250.145	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1
176.12.146.41	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
93.173.22.1	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
2.54.60.199	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	1
141.212.121.197	United States	147.237.77.212	e.dover.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
85.250.102.190	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.19.85.1	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
93.173.22.1	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.120.107.188	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
5.29.86.162	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
87.68.214.121	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
84.108.240.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	323
46.117.135.158	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.117.135.158	Block	71
46.117.135.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
84.108.187.189	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	6
46.19.85.135	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	4
63.115.50.73	United States	147.237.0.34	tikshuv.idf.il	Multiple URL worm attacks from 63.115.50.73	Block	3
89.138.39.250	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
109.67.53.14	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	3
82.102.136.69	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
207.46.13.1	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/trajector/	Block	2
46.19.86.185	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
79.182.109.224	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
85.65.215.75	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
78.92.80.87	Hungary	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
2.52.7.226	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
192.81.210.204	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/894-he/tikshuv.aspx/shared/usercontrols/navmenu/undefined	Block	1
66.249.64.71	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1403-he/atal.aspx	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
94.102.53.195	Netherlands	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/includes/templates/error.tpl	Block	1
63.115.50.73	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/cgi-bin/php	Block	1
46.19.85.247	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-9367-he/dover.aspx	Block	1
164.138.121.56	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/0722-2.stm	Block	1
63.115.50.73	United States	147.237.0.34	tikshuv.idf.il	Malformed URL http/1.1	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.117.142.152	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.250.102.190	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
79.176.111.55	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
2.54.34.34	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.67.82	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/kl	Block	1
95.86.112.231	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
63.115.50.73	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Malformed URL from 63.115.50.73	Block	1
176.228.138.212	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Unknown Parameter KEY in www.aka.idf.il/ishurim/cityofficers/	None	1
46.120.72.140	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//https:/www.idf.il/	Block	1
79.176.155.112	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.45.202	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
212.92.142.183	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar++result:+×¤×ž× ×£×œ+×?×•+×?×?×™×″×•×?+/+×?×•+×£×″×?×›×ž×¡Ã¼+×ž×Ÿ× ×•×″×•×›×˜×¢Ã¼+ip	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/kamlar/	None	1
66.249.78.82	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
109.65.26.251	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
63.115.50.73	United States	147.237.0.19	madim.atal.idf.il	Malformed URL http/1.1	Block	1
176.228.138.212	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//1134-he/atal.aspx	Block	1
77.71.56.103	Bulgaria	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.57	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
93.172.136.204	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
46.121.15.10	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1