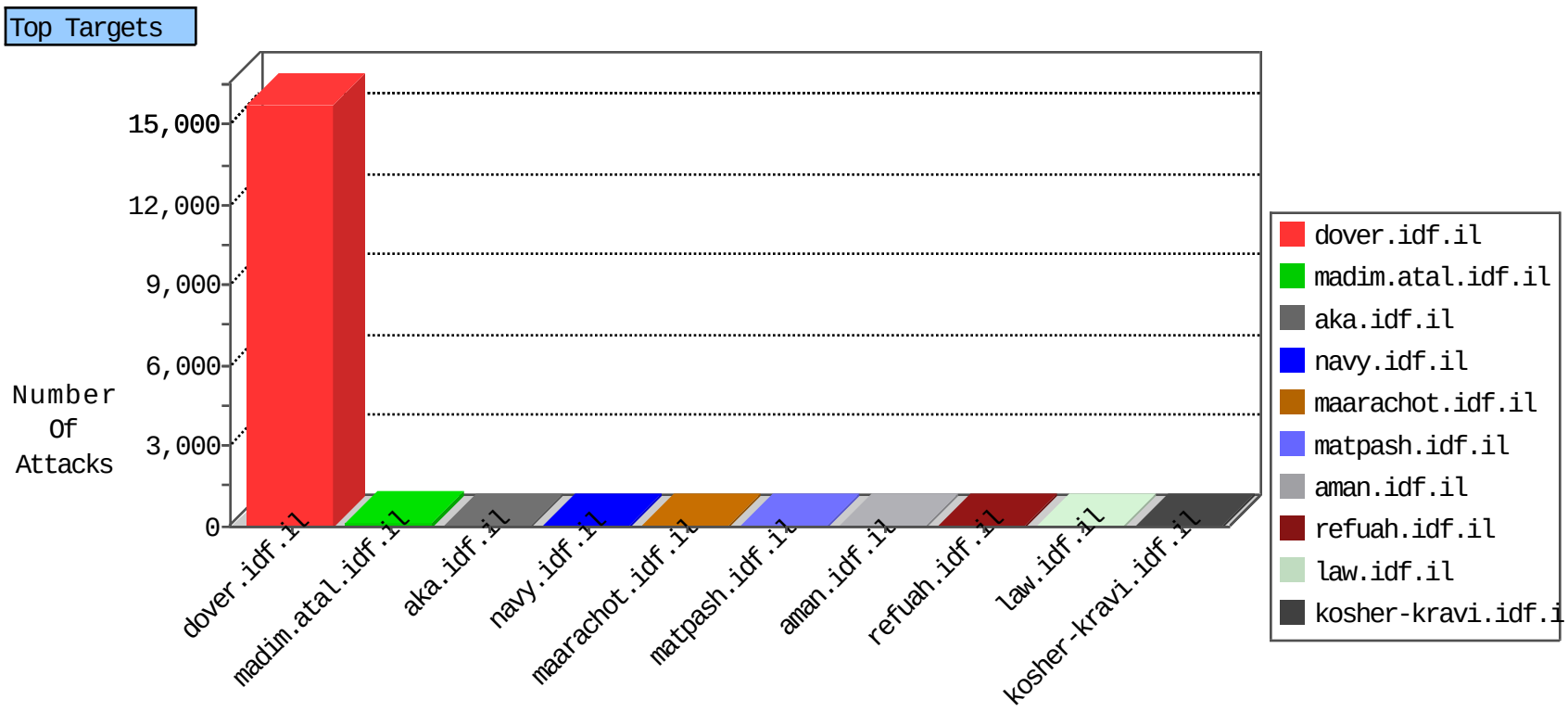
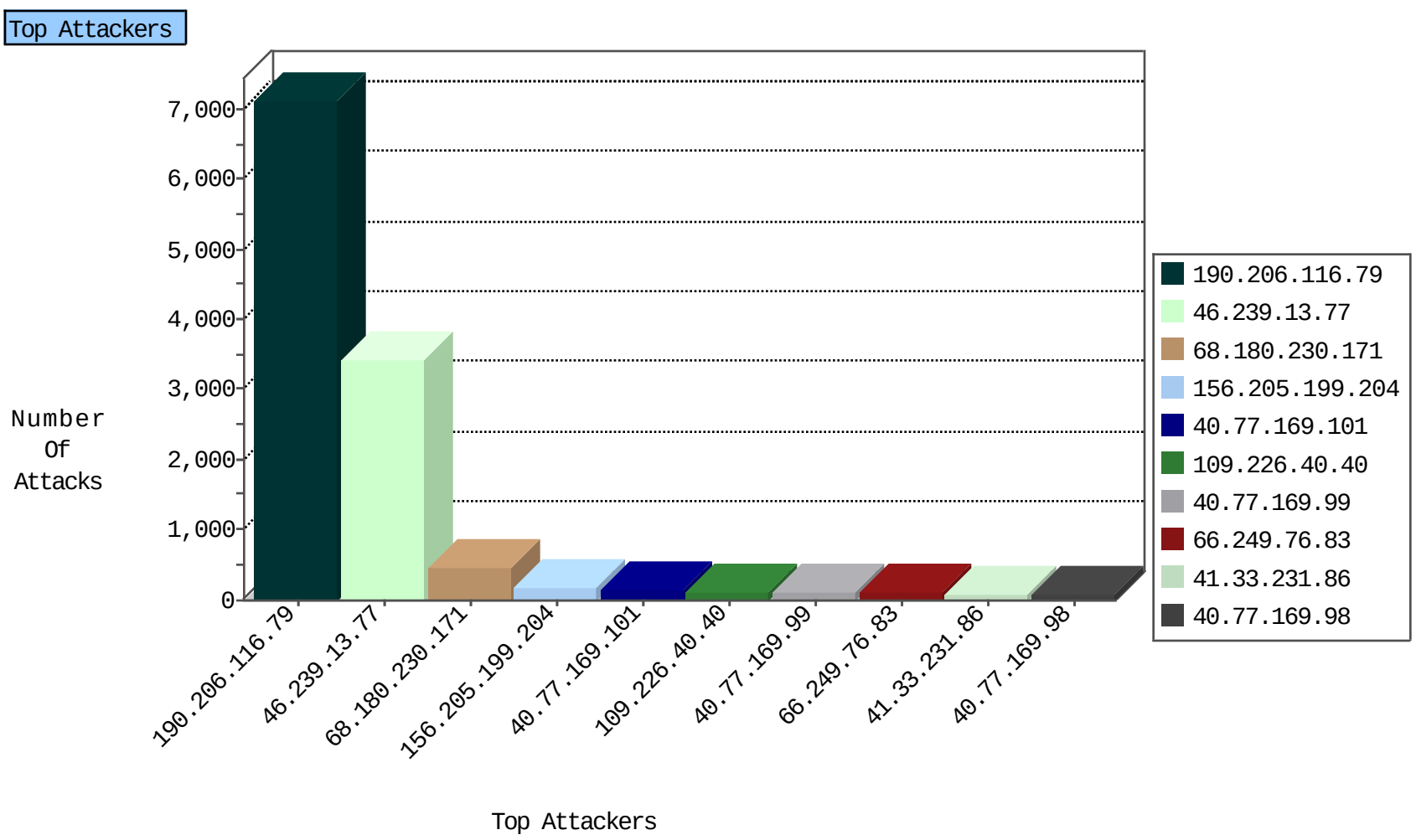
08-26-2016-19:04:04 to 08-26-2016-20:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-26-2016-19:04:04 to 08-26-2016-20:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	120427
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	31337
190.206.116.79	Venezuela	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	16956
190.206.116.79	Venezuela	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11518
68.180.230.171	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	294
104.152.52.64	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	224
68.180.230.171	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	180
156.205.199.204	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	103
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	102
66.249.76.83	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	97
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	92
40.77.169.99	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	65
156.205.199.204	Egypt	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	61
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	56
176.13.242.159	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	49
80.246.133.2	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	49
176.13.13.94	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	48
24.218.80.94	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	47
50.87.144.145	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	44
40.77.169.101	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	43
89.139.194.155	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	41
157.55.39.93	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	38
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	37
66.249.66.177	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	37
139.162.216.112	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	35
192.249.66.247	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	33
40.77.169.98	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	30
109.253.134.118	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	28
79.180.213.197	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	28
216.252.13.125	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	28
94.230.86.244	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	27
40.77.169.99	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	27
109.253.219.236	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	27
79.179.171.200	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	26
177.10.170.132	Brazil	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	26
84.108.66.251	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	24
80.246.133.134	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	23
84.108.28.19	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	23
46.19.85.227	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	22
80.246.133.2	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	20
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	19
40.77.169.103	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	19
109.66.124.155	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
109.253.210.223	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
104.152.52.64	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
37.26.148.213	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	17
40.77.169.97	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	17
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
37.142.238.202	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
66.249.92.114	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15

08-26-2016-19:04:04 to 08-26-2016-20:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
71.180.24.53	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	1

08-26-2016-19:04:04 to 08-26-2016-20:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	17
197.221.107.94	147.237.8.27	South Africa	e.madim.atal.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
163.172.169.150	147.237.76.177	United Kingdom	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
118.38.109.249	147.237.76.38	Korea, Republic of	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.224.160.106	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
46.227.67.172	147.237.76.34	Sweden	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
43.245.183.109	147.237.72.166	Indonesia	aka.idf.il	ET SCAN NMAP -sS window 3072	1
173.81.79.48	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.8.45	United Kingdom	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
97.105.173.114	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
46.227.67.172	147.237.76.202	Sweden	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
46.227.67.172	147.237.0.15	Sweden	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
46.120.122.219	147.237.76.86	Israel	navy.idf.il	Xenu Link Sleuth User Agent	1
43.245.183.109	147.237.72.166	Indonesia	aka.idf.il	ET SCAN NMAP -sS window 1024	1

08-26-2016-19:04:04 to 08-26-2016-20:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.239.13.77	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3202
46.239.13.77	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop		drop	237
190.206.116.79	Venezuela	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	165
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	70
40.77.169.98	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	52
40.77.169.97	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
40.77.169.102	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	33
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
79.176.135.200	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	27
40.77.169.100	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	19
46.19.85.48	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
40.77.169.100	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	5
40.77.169.101	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
79.177.83.20	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	4
40.77.169.101	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
40.77.169.102	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	3
40.77.169.103	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	3
89.237.114.167	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
40.77.169.100	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
70.214.105.80	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
94.43.218.249	Georgia	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	1
187.161.64.92	Mexico	147.237.0.200	m4u.idf.il	drop		drop	1
77.126.80.85	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
37.34.93.144	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.65.38.195	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
40.77.169.102	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
109.253.128.88	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
201.150.226.62	Mexico	147.237.0.33	idf.il	drop		drop	1
109.253.137.220	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
201.150.226.62	Mexico	147.237.0.35	akaws.idf.il	drop		drop	1
173.252.90.96	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
201.173.82.23	Mexico	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.219.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
109.253.135.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
78.250.247.215	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	7
109.64.137.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.64.170.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
77.126.5.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.116.91.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.138.124.191	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	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
201.150.226.62	Mexico	147.237.0.34	tikshuv.idf.il	Redundant HTTP Headers Content-Type	Block	1
40.77.169.99	United States	147.237.77.170	maarachot.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/main/smalim/showbig.aspx	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
157.55.39.35	United States	147.237.72.166	aka.idf.il	Unknown Parameter pagenum in aka.idf.il/chinuch/gallery/	None	1
66.249.69.67	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/3426.jpg	Block	1
201.173.47.198	Mexico	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
46.19.85.221	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.128.88	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.64.24	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size338x0/sip_storage	Block	1
166.137.97.58	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
89.248.167.131	Netherlands	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	1
66.249.69.72	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/2412.jpg	Block	1
201.173.91.4	Mexico	147.237.0.19	madim.atal.idf.il	Redundant HTTP Headers Content-Type	Block	1
77.138.33.231	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/booklets.aspx	Block	1
66.249.64.58	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1133-he/atal.aspx	Block	1
167.220.232.104	Japan	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
94.230.86.164	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
66.249.69.127	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
46.200.48.63	Ukraine	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
77.138.46.180	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
66.249.64.108	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/masaiyot29032011.aspx	Block	1
189.218.16.31	Mexico	147.237.0.15	kosher-kravi.idf.il	Redundant HTTP Headers Content-Type	Block	1
66.249.76.100	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
66.102.9.10	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/miluim/templates/inner.asp	Block	1