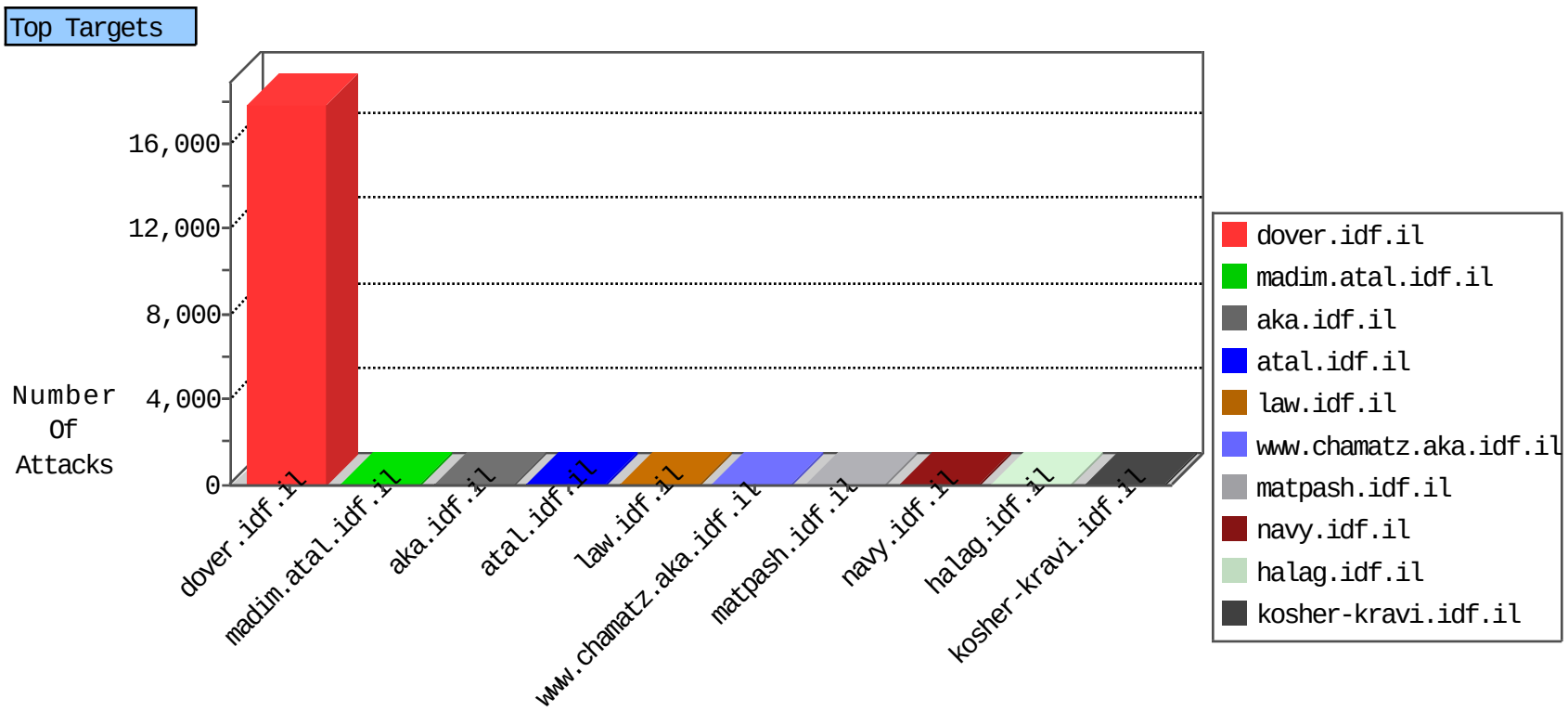
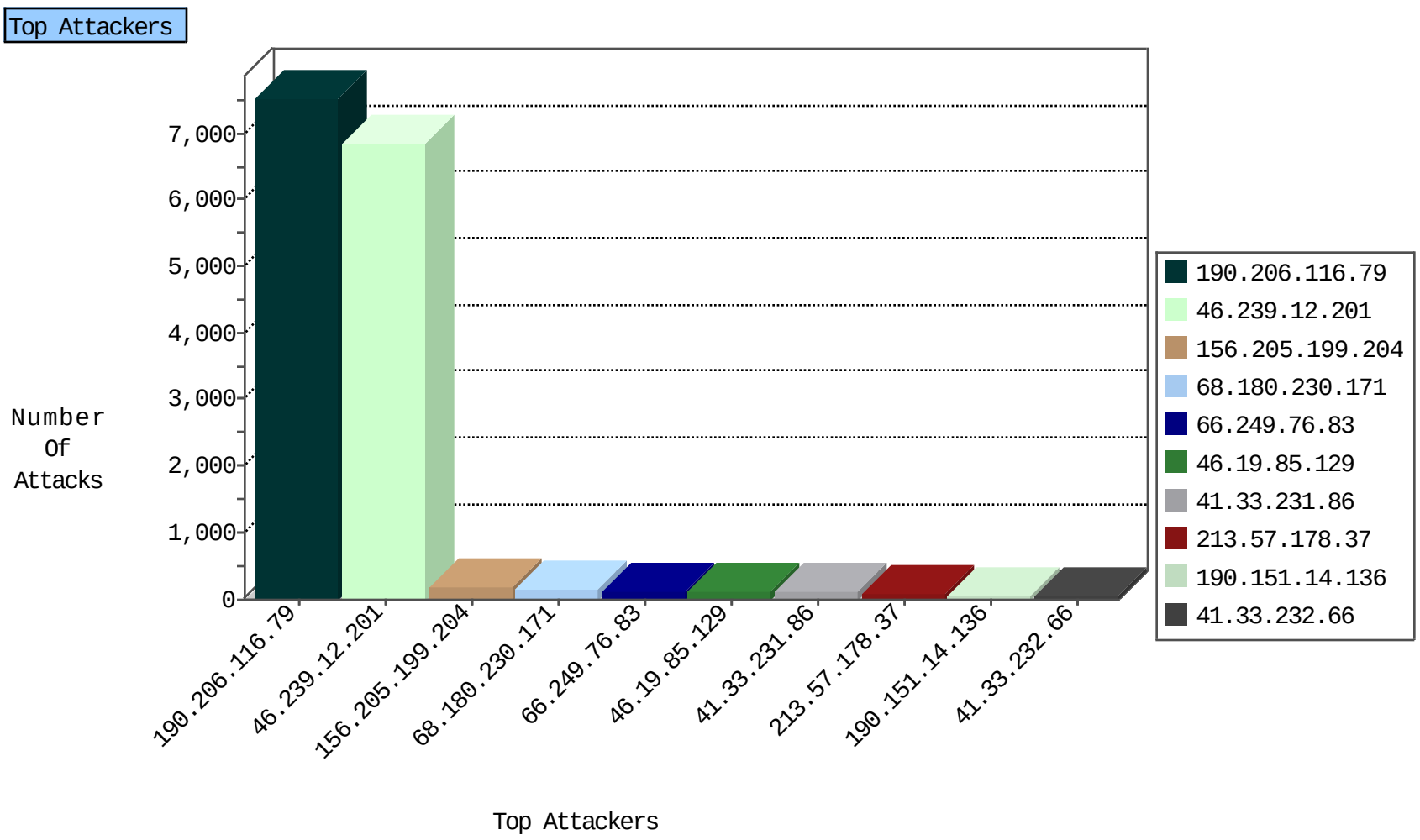
08-26-2016-08:04:02 to 08-26-2016-09:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-26-2016-08:04:02 to 08-26-2016-09:04:02

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	172571
190.206.116.79	Venezuela	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	67473
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	65543
190.206.116.79	Venezuela	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	34888
156.205.199.204	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	116
66.249.76.83	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	116
68.180.230.171	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	115
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	103
156.205.199.204	Egypt	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	72
213.57.178.37	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	62
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	55
194.90.99.129	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	47
109.253.204.213	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	44
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	43
50.87.144.145	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	43
176.13.240.18	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	43
68.180.230.171	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	41
139.162.216.112	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	40
157.55.39.181	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	35
190.151.14.136	Chile	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	35
5.22.132.77	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	30
190.151.14.136	Chile	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	29
79.177.96.250	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	27
157.55.39.93	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	27
176.13.14.75	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	24
176.13.246.39	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	24
176.13.14.75	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	24
176.13.246.39	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	24
62.90.202.90	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	23
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	22
66.249.66.177	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	21
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	21
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	20
176.13.246.39	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	20
157.55.39.194	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	19
46.116.27.167	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
79.177.197.11	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
192.249.66.247	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
108.171.131.178	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
176.13.3.107	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
217.132.154.89	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
66.249.92.114	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
80.246.133.221	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
157.55.39.93	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
80.246.133.78	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
109.253.211.26	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
5.22.131.113	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15
192.249.66.247	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	14
157.55.39.194	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	14
188.120.148.52	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	14
66.249.76.85	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	13
66.249.93.107	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	13

08-26-2016-08:04:02 to 08-26-2016-09:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.247.61.153	Sweden	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
185.96.92.54	United Kingdom	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5

08-26-2016-08:04:02 to 08-26-2016-09:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
185.96.92.54	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	18
212.247.61.153	147.237.77.233	Sweden	atal.idf.il	SQL Injection - Select From	8
91.201.236.50	147.237.76.38	Ukraine	e.e.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
220.249.194.151	147.237.76.31	China	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.64.103	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
189.251.12.57	147.237.76.86	Mexico	navy.idf.il	ET SCAN NMAP -sS window 2048	1
58.218.204.245	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
189.251.12.57	147.237.76.86	Mexico	navy.idf.il	ET SCAN NMAP -f -sS	1
58.218.204.245	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
183.82.106.200	147.237.77.205	India	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
183.82.106.200	147.237.77.205	India	prisha.idf.il	ET SCAN NMAP -f -sS	1
163.172.169.150	147.237.76.44	United Kingdom	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
123.206.85.139	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.76.38	Ukraine	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.245	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
189.251.12.57	147.237.76.86	Mexico	navy.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.245	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
186.117.17.198	147.237.76.31	Colombia	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.129.160.229	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
183.82.106.200	147.237.77.205	India	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
123.206.85.139	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1

08-26-2016-08:04:02 to 08-26-2016-09:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.239.12.201	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6649
46.239.12.201	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop		drop	200
40.77.169.102	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	38
40.77.169.99	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	22
167.220.232.104	Japan	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
182.75.146.54	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
40.77.169.100	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
40.77.169.99	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	9
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
185.130.6.49	Lithuania	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	6
207.54.144.207	United States	147.237.77.233	atal.idf.il	drop	SAM rule	drop	6
40.77.169.99	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	5
40.77.169.100	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
27.255.173.76	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.64.120.83	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
157.55.39.181	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
197.48.146.207	Egypt	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	1
74.82.47.24	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
77.42.252.196	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.242.30	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
46.120.129.196	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
37.187.157.108	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

08-26-2016-08:04:02 to 08-26-2016-09:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	114
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/apple-app-site-association	Block	1
157.55.39.179	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/piwik.php	Block	1
82.80.177.86	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.76.46	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/tizmoret/news/<a href=	Block	1
87.71.12.38	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 87.71.12.38 (Open Mode)	None	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.76.114	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/.well-known/apple-app-site-association	Block	1
207.46.13.24	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.76.47	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.47	Block	1
87.71.12.38	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.93.184	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
46.116.53.91	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl33 in aka.idf.il/main/sachar/payslips.aspx	None	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/div.item	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/homepage/homepage.aspx	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.93.186	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.64.103	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/8/113338.pdf	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.112	Block	1
157.55.39.35	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/ge...04	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
77.139.81.89	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
66.249.76.39	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding 82G0l3ebf[@G}u@oTlGh8I]nprO in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1

08-26-2016-08:04:02 to 08-26-2016-09:04:02