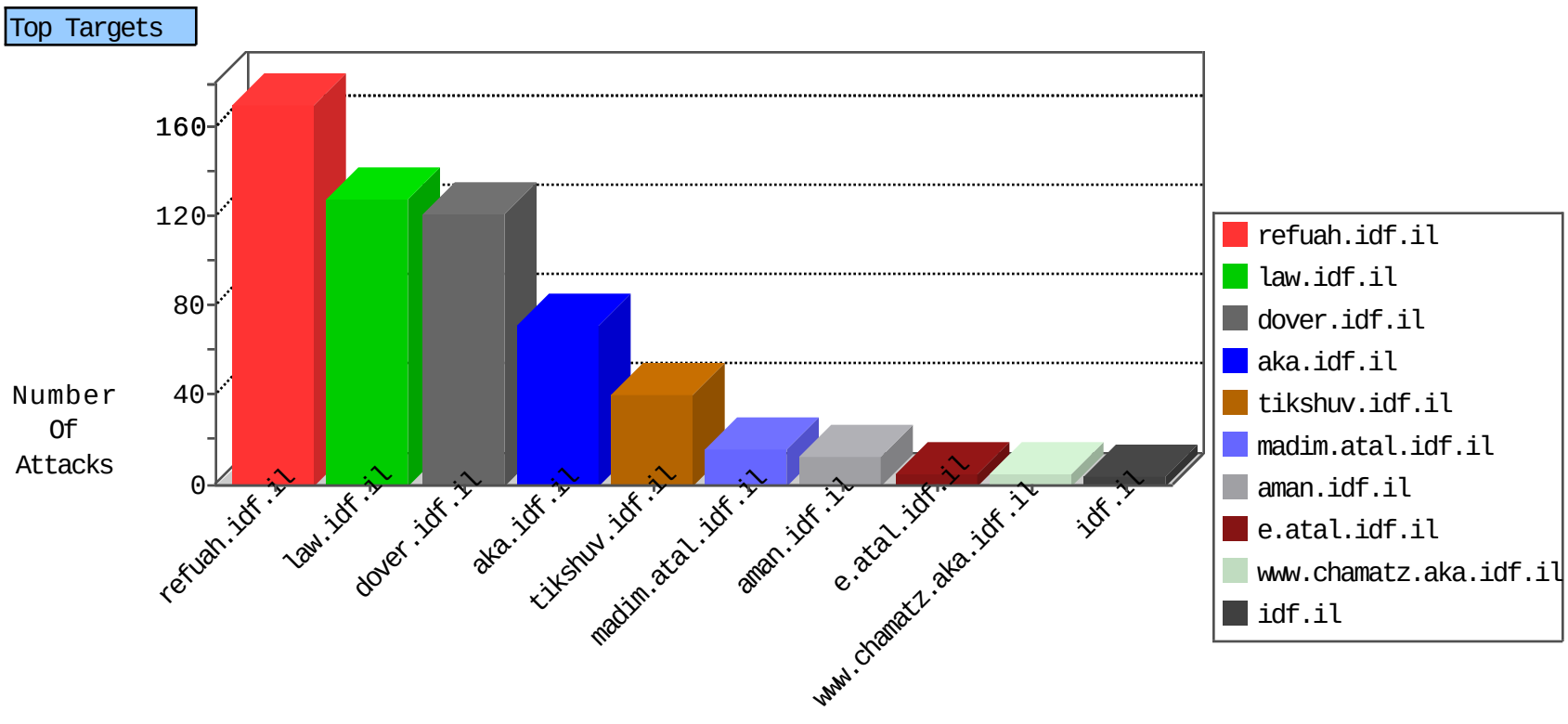
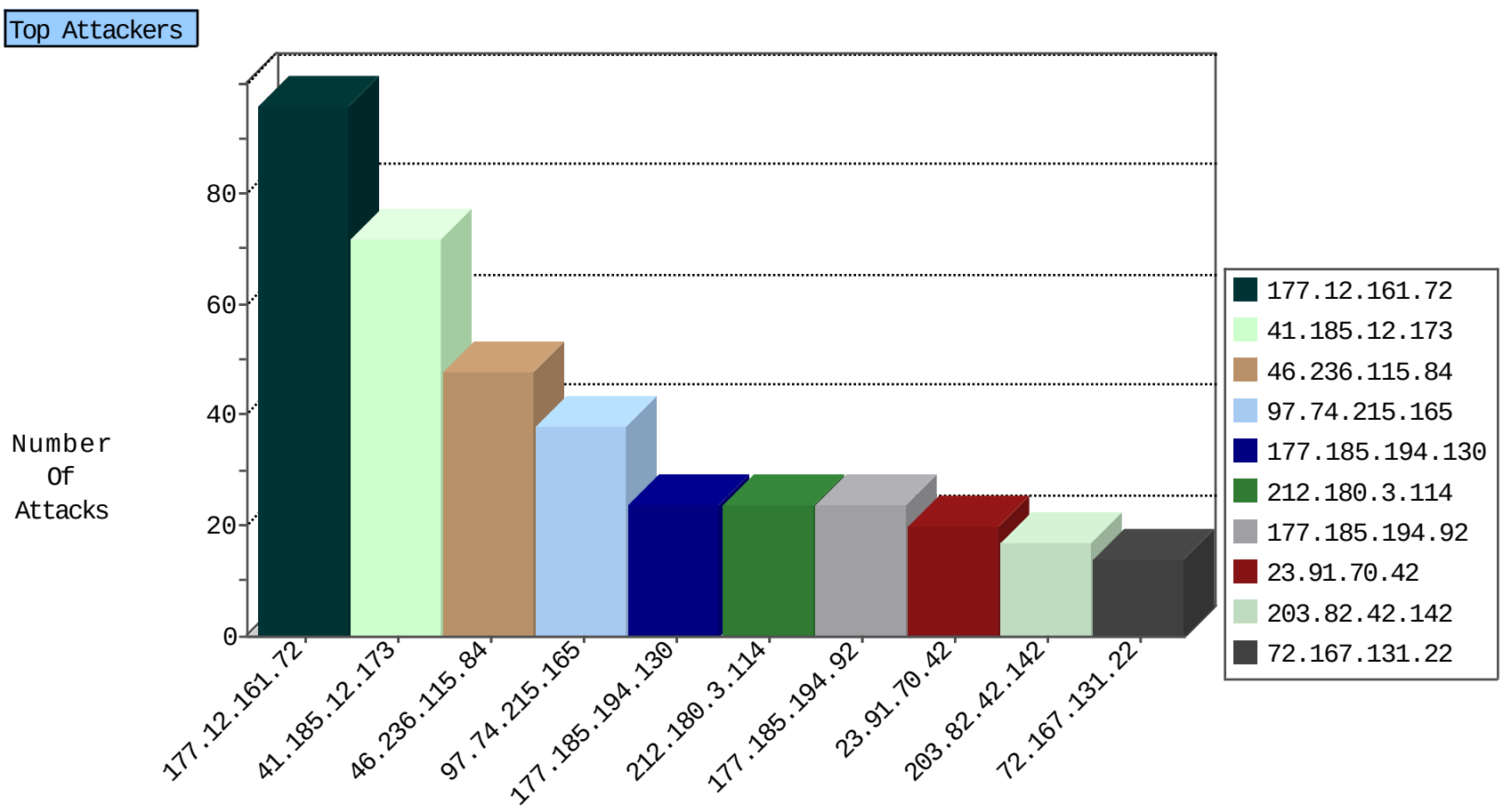
08-20-2016-19:04:00 to 08-20-2016-20:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-20-2016-19:04:00 to 08-20-2016-20:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.183.187	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
2.53.146.113	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
185.94.111.1	Russian Federation	147.237.76.196	e.sviva.idf.il	Black List	drop	1
93.158.200.86	Netherlands	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
104.148.55.162	United States	147.237.76.201	e.atal.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.44	e.refuah.idf.il	Black List	drop	1

08-20-2016-19:04:00 to 08-20-2016-20:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
97.74.215.165	United States	147.237.0.34	tikshuv.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
177.12.161.72	Brazil	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
97.74.215.165	United States	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
41.185.12.173	South Africa	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
177.12.161.72	Brazil	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
212.180.3.114	France	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
41.185.12.173	South Africa	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
69.7.43.246	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
212.247.61.153	Sweden	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
144.76.70.248	Germany	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
41.185.12.173	South Africa	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
177.185.194.92	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
46.236.115.84	Sweden	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
177.185.194.130	Brazil	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
72.167.131.22	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
23.91.70.42	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
177.12.161.72	Brazil	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
46.236.115.84	Sweden	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
69.30.198.186	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
66.240.192.138	United States	147.237.0.15	kosher-kravi.idf.il	2226: Backdoor: TCP Window Size 55808 Trojan	Block	1
162.210.196.129	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	1
184.168.193.34	United States	147.237.77.226	www.chamatz.aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

08-20-2016-19:04:00 to 08-20-2016-20:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
177.12.161.72	147.237.76.42	Brazil	refuah.idf.il	SQL Injection - Select From	72
41.185.12.173	147.237.76.42	South Africa	refuah.idf.il	SQL Injection - Select From	54
46.236.115.84	147.237.77.74	Sweden	law.idf.il	SQL Injection - Select From	36
97.74.215.165	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	20
212.180.3.114	147.237.72.166	France	aka.idf.il	SQL Injection - Select From	18
177.185.194.92	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	18
177.185.194.130	147.237.77.216	Brazil	dover.idf.il	SQL Injection - Select From	18
23.91.70.42	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	14
69.7.43.246	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
144.76.70.248	147.237.72.166	Germany	aka.idf.il	SQL Injection - Select From	8
212.247.61.153	147.237.72.166	Sweden	aka.idf.il	SQL Injection - Select From	8
72.167.131.22	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	4
184.168.193.34	147.237.77.226	United States	www.chamatz.aka.idf.il	SQL Injection - Select From	3
91.224.160.106	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
151.80.40.86	147.237.77.176	France	matpash.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
128.199.233.18	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
104.232.98.3	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
183.82.106.200	147.237.77.212	India	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
91.224.160.106	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	1
183.82.106.200	147.237.77.212	India	e.dover.idf.il	ET SCAN NMAP -f -sS	1
91.224.160.106	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
178.94.112.41	147.237.8.27	Ukraine	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
63.142.161.5	147.237.76.201	Canada	e.atal.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
109.67.213.226	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
183.82.106.200	147.237.77.212	India	e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
91.224.160.106	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential SSH Scan	1
179.182.250.107	147.237.8.28	Brazil	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
63.142.161.25	147.237.76.201	Canada	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
63.142.161.5	147.237.76.201	Canada	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1

08-20-2016-19:04:00 to 08-20-2016-20:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
203.82.42.142	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
41.238.110.25	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
87.117.203.20	United Kingdom	147.237.72.156	aman.idf.il	drop	SAM rule	drop	6
87.242.112.35	Russian Federation	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
5.172.255.77	Poland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
194.17.229.129	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.189.28.63	Germany	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
117.199.134.131	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
121.33.226.174	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
103.41.143.150	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
81.218.184.106	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	2
176.13.243.164	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
158.181.147.248	Kyrgyzstan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
85.130.231.105	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
31.13.113.67	Ireland	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	1
66.249.69.105	Israel	147.237.0.33	idf.il	drop		drop	1
175.177.80.88	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
31.13.113.93	Ireland	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	1
66.249.69.109	Israel	147.237.0.33	idf.il	drop		drop	1
176.13.6.199	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.52	United States	147.237.0.33	idf.il	drop		drop	1
66.249.93.107	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
176.13.15.61	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
141.212.122.53	United States	147.237.0.33	idf.il	drop		drop	1
109.253.199.225	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
63.142.161.5	Canada	147.237.76.201	e.atal.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	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
65.55.210.92	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
65.55.210.124	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
62.219.114.25	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
80.246.130.144	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.55.187.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.140.46	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
46.120.19.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
41.79.187.106	Tanzania, United Republic of	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.85.67	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.12.71	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.24.0	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.48.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.65.26.109	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
72.17.184.171	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
203.82.42.142	Philippines	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-15035-en/#21	Block	1
109.253.200.145	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
46.19.85.239	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
2.55.36.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
46.120.19.121	Israel	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Open Mode	None	1
176.13.22.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
45.33.27.141	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-15035-en/#17	Block	1
85.250.199.246	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl13 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
77.139.21.61	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash/sheelon.aspx	Block	1
204.79.180.88	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/default.aspx	Block	1
66.102.9.43	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
109.253.222.60	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
46.19.85.239	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
80.246.133.194	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/sites/skira/default.asp	None	1
46.229.164.102	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
185.120.126.5	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
87.69.110.85	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
77.139.138.198	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
207.46.13.25	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/sachar/klali.aspx	None	1
66.102.9.95	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
46.19.85.239	Israel	147.237.77.216	dover.idf.il	Malformed URL asp.net_sessionid=untjda45fpwsmu55yiaf3m25	Block	1
31.31.73.195	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-15035-en/#49	Block	1
66.249.76.120	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/ayosh15092010.aspx	Block	1
95.37.62.53	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.37.62.53	Block	1
78.46.116.99	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-15035-en/#30	Block	1
2.53.40.22	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
217.132.49.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/0/71700.pdf	Block	1
157.55.39.24	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/faq.aspx	None	1
46.19.85.239	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method .20.8afc=34d5e78d599ea6bd.1471558137.1.1471558137.1471558137.; in URL asp.net_sessionid=untjda45fpwsmu55yiaf3m25	Block	1
37.54.195.161	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
84.110.36.34	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1