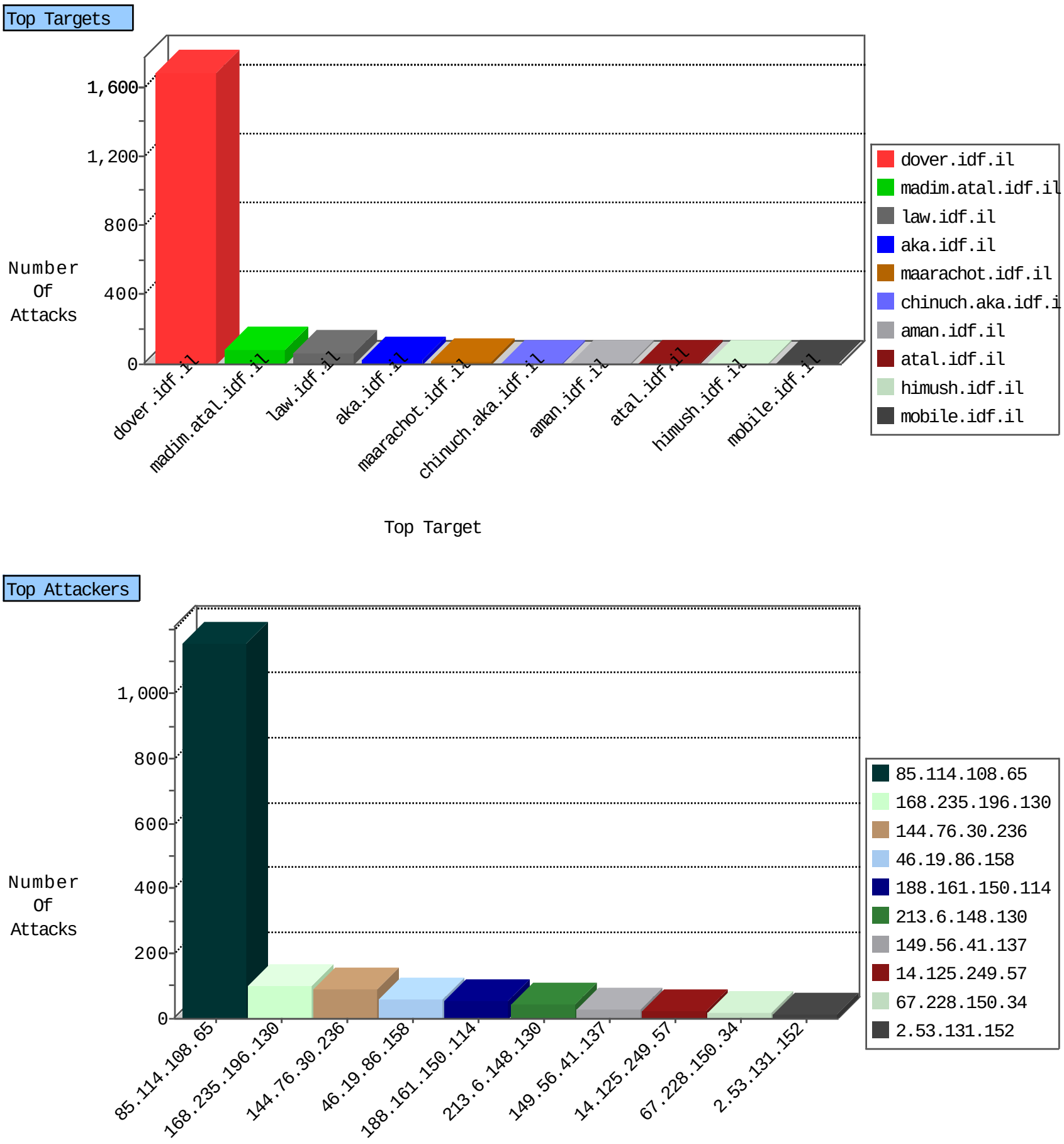
08-23-2016-08:04:07 to 08-23-2016-09:04:07

IDF Under Attack Daily Report



08-23-2016-08:04:07 to 08-23-2016-09:04:07

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	HTTP Page Flood Attack	drop	6854
85.114.108.65	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	1125
168.235.196.130	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	45
2.53.42.129	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
185.24.207.97	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
77.138.147.13	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
222.124.182.106	Indonesia	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
149.56.41.137	United States	147.237.77.74	law.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	6
212.76.127.10	Israel	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	5
45.35.64.142	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
192.249.66.247	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	5
168.235.196.130	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
222.223.56.37	China	147.237.0.15	kosher-kravi.idf.il	Invalid TCP Flags	drop	2
222.223.56.37	China	147.237.0.16	my-kosher-kravi.idf.il	Invalid TCP Flags	drop	2
222.223.56.37	China	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	2
73.70.2.209	United States	147.237.76.30	himush.idf.il	Black List	drop	2
222.223.56.37	China	147.237.0.19	madim.atal.idf.il	Invalid TCP Flags	drop	2
222.223.56.37	China	147.237.0.33	idf.il	Invalid TCP Flags	drop	1
209.126.136.2	United States	147.237.76.177	ncore.idf.il	Black List	drop	1
137.74.157.88	Hong Kong	147.237.76.176	test.ncore.idf.il	Black List	drop	1
222.223.56.37	China	147.237.0.35	akaws.idf.il	Invalid TCP Flags	drop	1
185.94.111.1	Russian Federation	147.237.76.177	ncore.idf.il	Black List	drop	1
86.59.4.133	Austria	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	1

08-23-2016-08:04:07 to 08-23-2016-09:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
144.76.30.236	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	70
144.76.30.236	Germany	147.237.76.147	chinuch.aka.idf.il	C1000074: HTTP: majestic bot	Permit	8
67.228.150.34	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
138.201.127.112	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	4
144.76.30.236	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
144.76.30.236	Germany	147.237.77.233	atal.idf.il	C1000074: HTTP: majestic bot	Permit	2
144.76.29.162	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
51.255.65.75	France	147.237.76.42	refuah.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
123.126.68.125	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

08-23-2016-08:04:07 to 08-23-2016-09:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
67.228.150.34	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	14
84.109.180.213	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	7
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	2
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	2
84.109.180.213	147.237.77.74	Israel	law.idf.il	Xenu Link Sleuth User Agent	2
190.196.178.78	147.237.77.234	Chile	halag.idf.il	ET SCAN NMAP -sS window 3072	1
195.88.208.193	147.237.76.31	Russian Federation	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
190.196.178.78	147.237.77.234	Chile	halag.idf.il	ET SCAN NMAP -sS window 4096	1
62.219.21.30	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.98.120	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.6.148.130	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	Tehila - Perl LWP with fake user agent	1
190.252.180.154	147.237.0.35	Colombia	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

08-23-2016-08:04:07 to 08-23-2016-09:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
85.114.108.65	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	304
168.235.196.130	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	92
149.56.41.137	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	22
188.161.150.114	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
213.6.148.130	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
144.76.30.236	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
82.166.40.154	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
188.161.105.210	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
62.0.207.1	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
184.66.227.135	Canada	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
166.137.8.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
222.124.182.106	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
194.165.146.148	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.66.227.135	Canada	147.237.72.166	aka.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
176.13.241.77	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1

08-23-2016-08:04:07 to 08-23-2016-09:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.114.108.65	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 85.114.108.65	Block	207
46.19.86.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	57
188.161.150.114	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.161.150.114	Block	33
213.6.148.130	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.6.148.130	Block	29
14.125.249.57	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 14.125.249.57	Block	16
2.53.131.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
14.125.249.57	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	6
80.246.136.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
66.249.79.37	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.37	Block	6
188.161.150.114	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
109.67.226.249	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	4
62.0.116.102	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	3
194.90.105.112	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	2
10.161.40.23		147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	2
79.177.54.132	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
85.114.108.65	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.67.226.249	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/9/	Block	2
176.13.21.31	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	2
82.81.69.86	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
213.6.148.130	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/app_files/	Block	1
68.180.230.171	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	1
109.67.226.249	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/421-he/patzar.aspx	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/giyus/general.aspx	Block	1
208.115.111.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
46.19.85.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
84.111.94.176	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
68.180.231.45	United States	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.tech.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
194.90.105.112	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/sip_storage/files/4/	Block	1
62.0.116.102	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1384-he/dover.aspx	Block	1
77.139.91.187	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
66.249.64.61	Israel	147.237.0.19	madim.atal.idf.i	Distributed Unauthorized URL Access on madim.atal.idf.il/robots.txt	Block	1
199.30.25.32	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
14.125.249.57	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/default.aspx	Block	1
68.180.230.107	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/reserve/	Block	1
212.179.231.195	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
192.243.55.136	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/templatecontrols/news/sip_storage/files/6/1446.pdf/	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/rabanut/general.aspx	Block	1
77.139.181.192	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/sachar	Block	1
66.249.76.30	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/apple-app-site-association	Block	1
199.30.25.48	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
82.81.69.86	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
68.180.230.171	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-ar/dover.aspx	Block	1
194.90.105.112	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 194.90.105.112	Block	1
50.205.250.182	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	1
85.114.108.65	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/uniscan661/	Block	1
77.139.216.183	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/information.aspx	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
207.46.13.187	United States	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/robots.txt	Block	1

08-23-2016-08:04:07 to 08-23-2016-09:04:07