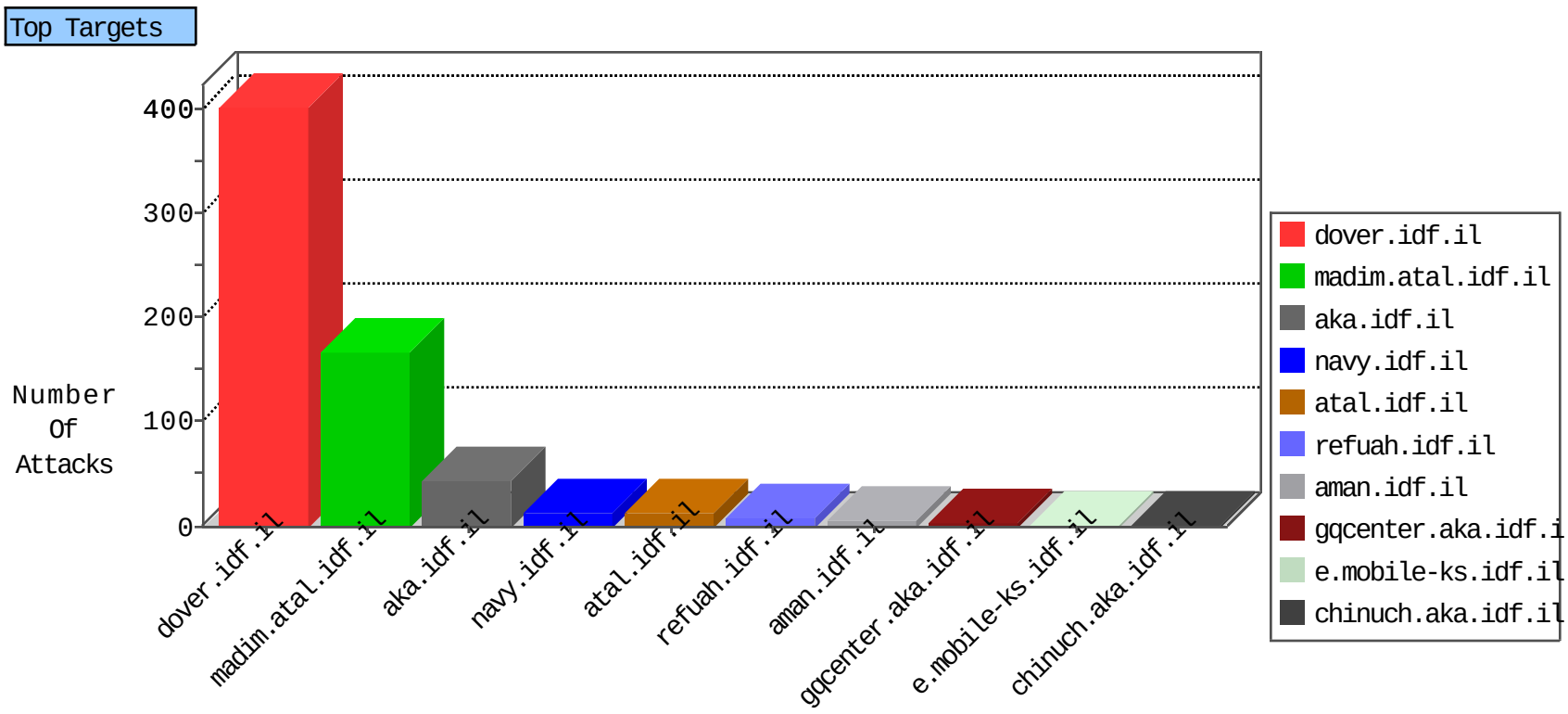
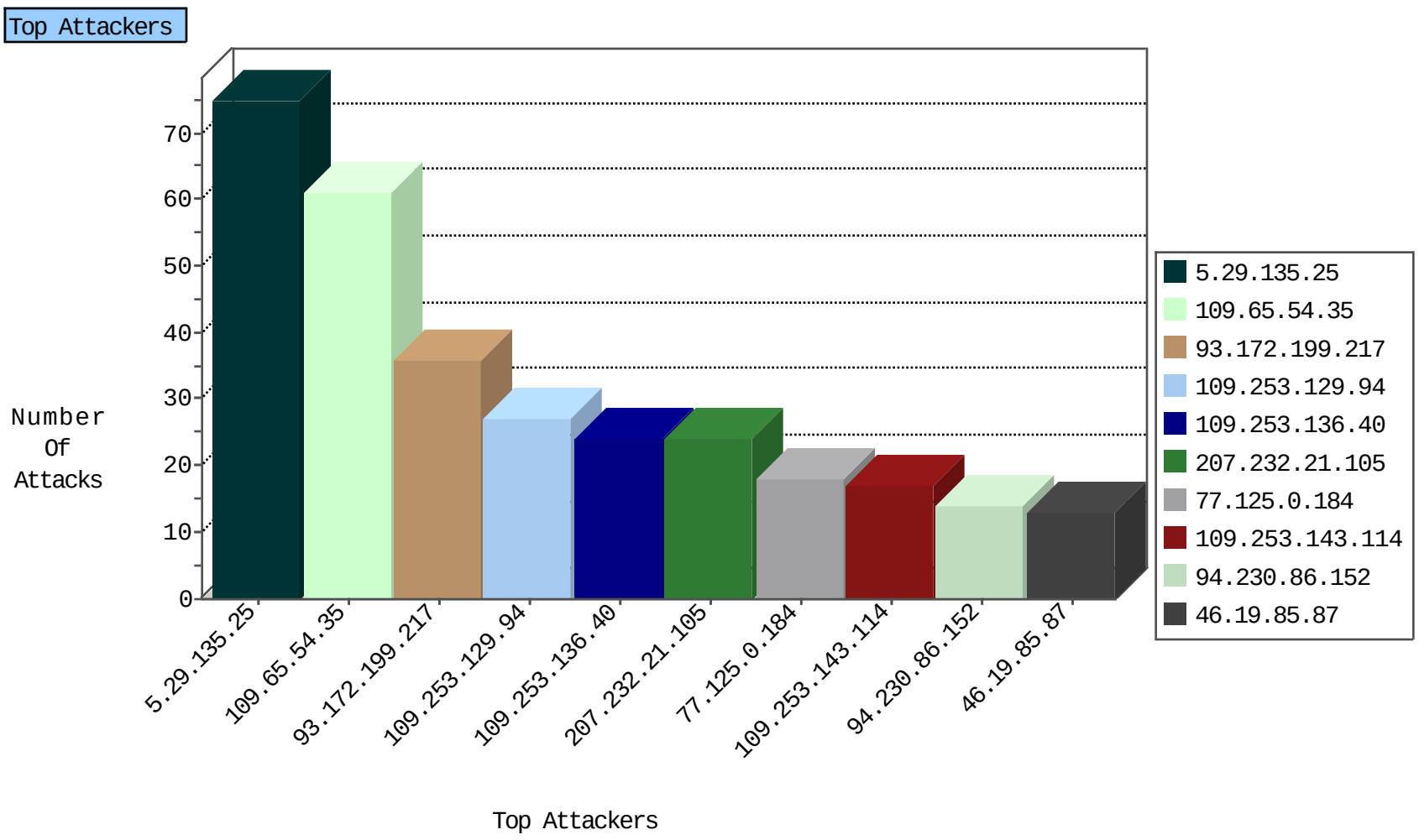
08-16-2016-21:04:00 to 08-16-2016-22:04:00

IDF Under Attack
Daily Report





08-16-2016-21:04:00 to 08-16-2016-22:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.78.2	Israel	147.237.76.86	navy.idf.il	Black List	drop	3
79.178.151.2	Israel	147.237.72.166	aka.idf.il	Black List	drop	2
93.158.200.93	Netherlands	147.237.76.30	himush.idf.il	Black List	drop	1
93.158.200.93	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
120.132.50.135	China	147.237.77.233	atal.idf.il	block-sp-traf1	forward	1

08-16-2016-21:04:00 to 08-16-2016-22:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

08-16-2016-21:04:00 to 08-16-2016-22:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
93.158.215.183	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
85.93.5.66	147.237.77.61	United Arab Emirates	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
84.21.228.166	147.237.76.38	Russian Federation	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
79.177.77.238	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	1
207.232.21.105	147.237.77.216	Israel	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
72.252.249.125	147.237.0.16	Jamaica	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
123.0.195.239	147.237.8.28	Taiwan	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
61.240.144.65	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
113.175.162.14	147.237.76.199	Vietnam	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.31.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.158.215.183	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
84.21.228.166	147.237.76.42	Russian Federation	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
84.21.228.166	147.237.76.34	Russian Federation	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
218.86.88.181	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
72.252.249.125	147.237.0.17	Jamaica	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
158.255.5.113	147.237.76.147	Russian Federation	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.78.197	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	1
122.72.53.188	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
46.172.71.251	147.237.77.234	Ukraine	halag.idf.il	ET SCAN NMAP -sS window 1024	1

08-16-2016-21:04:00 to 08-16-2016-22:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
93.172.199.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
109.253.129.94	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
109.253.136.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
207.232.21.105	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
77.125.0.184	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
109.253.143.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
94.230.86.152	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
93.172.194.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.19.85.87	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
85.64.27.237	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
93.173.170.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
109.253.139.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.53.7.66	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.121.118.215	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
87.68.15.234	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.55.129.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
31.210.188.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
77.124.55.70	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.253.215.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
74.208.218.66	United States	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
212.199.218.246	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	6
2.53.164.242	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.106.184.160	Germany	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
77.126.60.242	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.55.6.102	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.229.11.134	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
93.173.39.177	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.103	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
77.124.37.82	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.64.100.45	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
77.126.59.170	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.53.51.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.253.211.92	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.55.7.30	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
87.70.58.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.253.150.62	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.102.195.204	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
85.64.113.244	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.210.71	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
185.27.105.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
84.229.42.160	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.243.22	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
31.154.81.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
89.138.204.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.116.90.120	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.245.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.55.142.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.53.131.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
85.64.62.84	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

08-16-2016-21:04:00 to 08-16-2016-22:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.135.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	75
109.65.54.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
109.253.195.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
5.22.135.193	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.22.135.193	Block	6
80.246.139.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
77.124.9.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
5.29.60.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.116.110.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.146	Block	3
89.237.66.97	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus	Block	2
37.26.146.213	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
190.0.20.130	Colombia	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/general/	Block	2
2.53.12.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.138.78.67	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	2
89.237.66.97	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 89.237.66.97	Block	2
66.102.9.31	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.86.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.71.61.176	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 87.71.61.176	Block	2
66.102.9.42	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.86.62	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
84.111.168.123	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
185.3.144.19	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/nfpvp/llelh/templates/navmenu/navmenu.css.aspx	Block	1
77.139.88.37	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
109.253.243.22	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
64.62.219.59	United States	147.237.76.42	refuah.idf.il	Unauthorized Method POST for 147.237.76.42/894-he/refuah.aspx	Block	1
89.138.178.38	Israel	147.237.76.86	navy.idf.il	Abnormally Long Request method	Block	1
80.178.136.2	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
23.115.32.124	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/sitemap.aspx	Block	1
157.55.39.190	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/registrationwizard/register.aspx	Block	1
77.124.55.70	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mnrmb/templates/navmenu/navmenu.css.aspx	Block	1
96.232.86.148	United States	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
66.102.9.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
84.111.168.123	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	1
5.22.135.193	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ishurim.	Block	1
185.120.124.87	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catld in www.aka.idf.il/main/giyus/general.aspx	None	1
79.179.192.167	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Double URL Encoding - parameter: catId%5Cu003d58624 in www.aka.idf.il/main/giyus/general.aspx	Block	1
116.24.21.253	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 116.24.21.253	Block	1
89.138.178.38	Israel	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Method	Block	1
66.102.6.157	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
157.55.39.221	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
77.126.59.170	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/vmmrb/templates/navmenu/navmenu.css.aspx	Block	1
46.116.110.69	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
84.229.11.134	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dnwut/templates/navmenu/navmenu.css.aspx	Block	1
79.180.15.118	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
5.29.29.56	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
68.180.228.185	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1115-ar/dover.aspx	Block	1
116.24.21.253	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
89.138.178.38	Israel	147.237.76.86	navy.idf.il	NULL Character in Method	Block	1

08-16-2016-21:04:00 to 08-16-2016-22:04:00