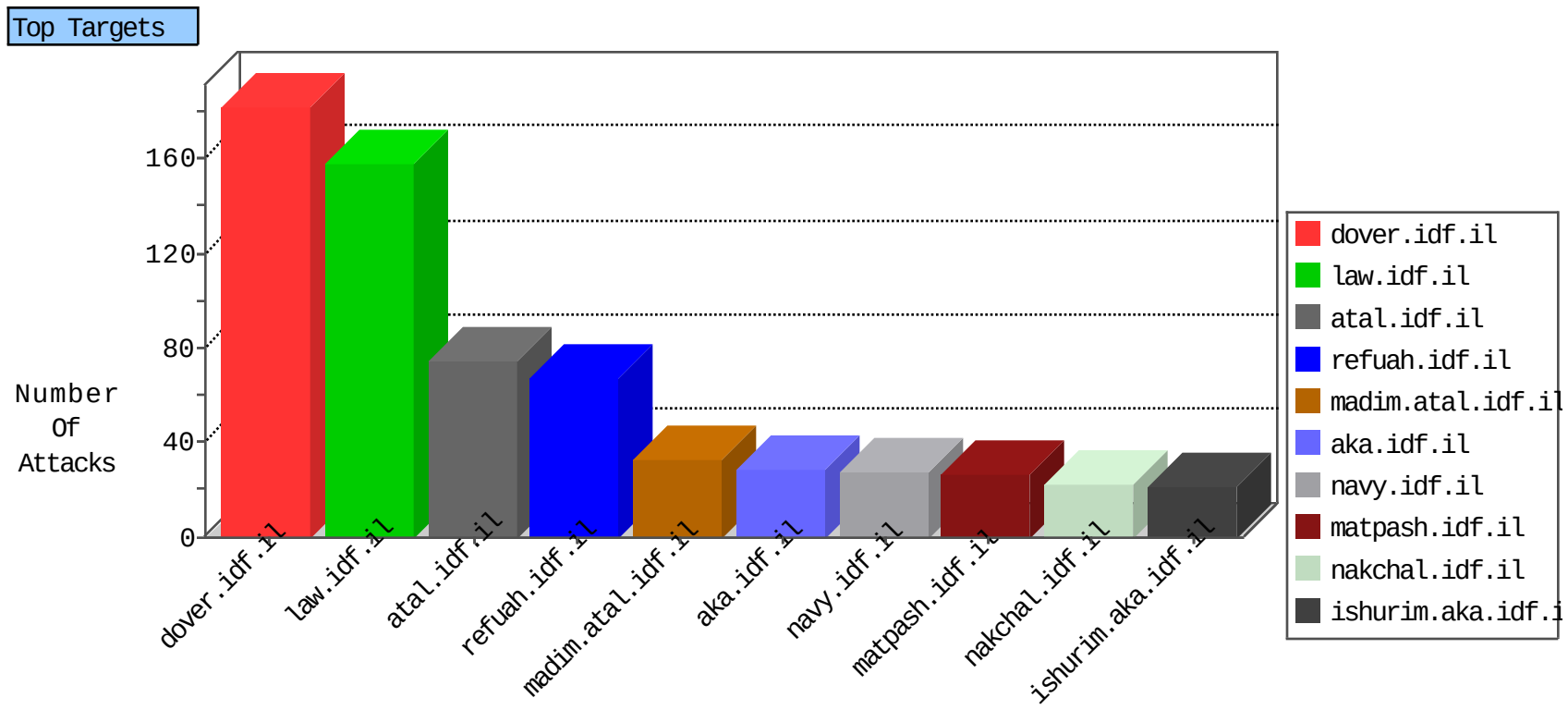
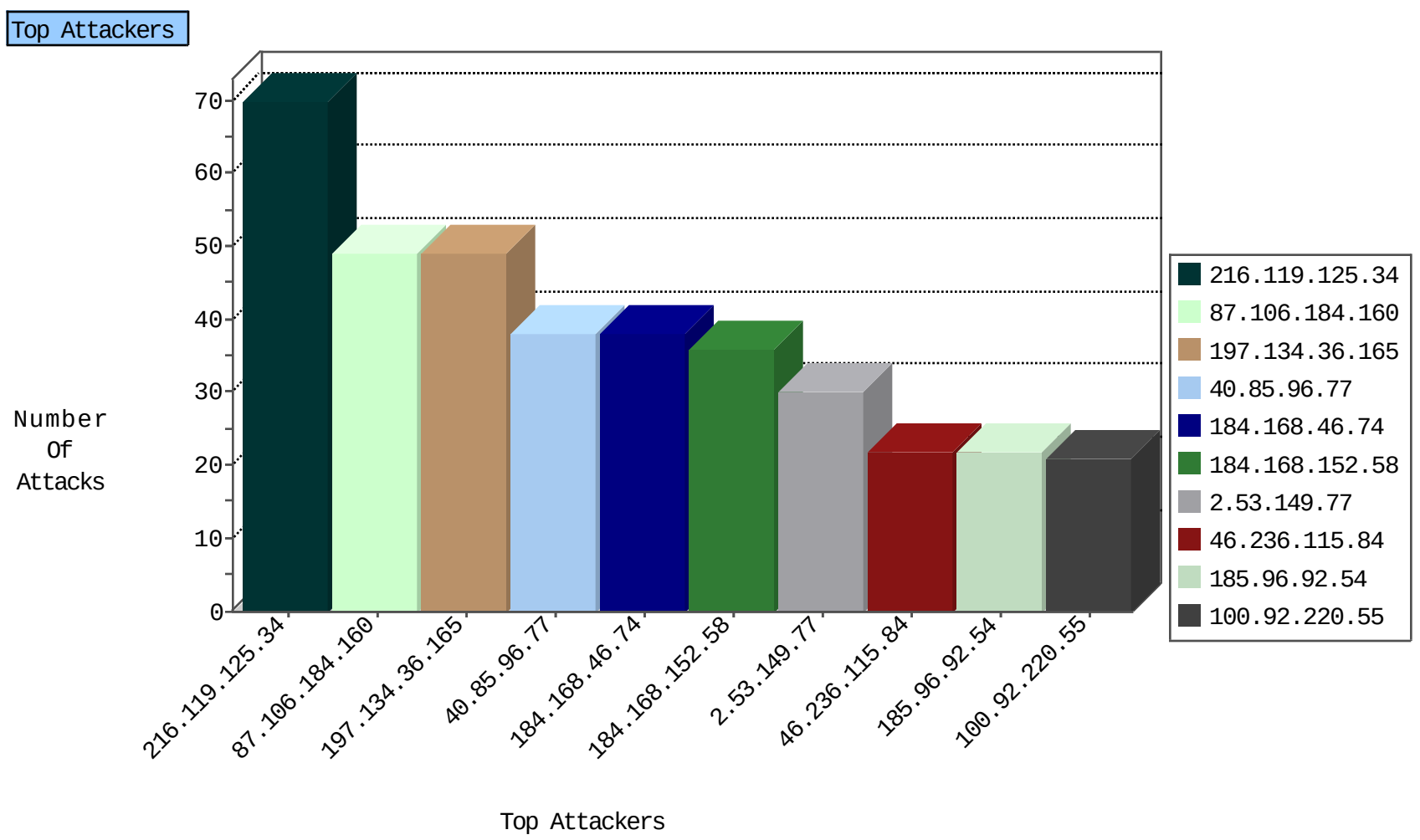
08-21-2016-01:06:40 to 08-21-2016-02:06:40

IDF Under Attack
Daily Report

Top Targets



Top Attackers



08-21-2016-01:06:40 to 08-21-2016-02:06:40

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.181.126	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
183.60.48.25	China	147.237.76.34	yohalan.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
93.174.93.156	Netherlands	147.237.76.34	yohalan.idf.il	Black List	drop	1

08-21-2016-01:06:40 to 08-21-2016-02:06:40

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.106.184.160	Germany	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
184.168.46.74	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
216.119.125.34	United States	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	11
216.119.125.34	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	7
87.106.184.160	Germany	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
40.85.96.77	Ireland	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.27.33	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
62.149.132.252	Italy	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
40.85.96.77	Ireland	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
184.168.46.74	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
128.187.112.5	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
46.236.115.84	Sweden	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
208.52.175.27	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.63.196.229	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.192.31	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
83.168.250.50	Sweden	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
40.85.96.77	Ireland	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
213.203.204.143	Germany	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
177.185.194.45	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.77.136.81	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
137.117.80.178	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
185.96.92.54	United Kingdom	147.237.76.31	nakchal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
185.96.92.54	United Kingdom	147.237.76.31	nakchal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2
69.197.163.195	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2
81.88.48.113	Italy	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
184.168.192.134	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

08-21-2016-01:06:40 to 08-21-2016-02:06:40

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
216.119.125.34	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	52
87.106.184.160	147.237.76.42	Germany	refuah.idf.il	SQL Injection - Select From	31
184.168.46.74	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	20
40.85.96.77	147.237.77.216	Ireland	dover.idf.il	SQL Injection - Select From	20
185.96.92.54	147.237.76.31	United Kingdom	nakchal.idf.il	SQL Injection - Select From	16
46.236.115.84	147.237.77.233	Sweden	atal.idf.il	SQL Injection - Select From	16
213.203.204.143	147.237.77.233	Germany	atal.idf.il	SQL Injection - Select From	8
50.63.196.229	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
208.52.175.27	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
128.187.112.5	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
184.168.192.31	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	8
62.149.132.252	147.237.77.74	Italy	law.idf.il	SQL Injection - Select From	8
50.77.136.81	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
137.117.80.178	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	7
83.168.250.50	147.237.77.74	Sweden	law.idf.il	SQL Injection - Select From	7
177.185.194.45	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	7
184.168.27.33	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	3
184.168.192.134	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	3
173.208.249.36	147.237.8.27	United States	e.madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
46.172.71.251	147.237.77.235	Ukraine	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.225.138	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
123.206.73.185	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
104.232.98.3	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.77.216	China	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
50.198.251.213	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
173.208.249.36	147.237.8.27	United States	e.madim.atal.idf.i	ET SCAN NMAP -sS window 2048	1
46.172.71.251	147.237.77.243	Ukraine	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
173.208.249.36	147.237.8.27	United States	e.madim.atal.idf.i	ET SCAN NMAP -f -sS	1
161.18.107.181	147.237.0.34	Colombia	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.232.98.3	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 3072	1
183.60.48.25	147.237.76.86	China	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
177.37.175.79	147.237.8.28	Brazil	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

08-21-2016-01:06:40 to 08-21-2016-02:06:40

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.134.36.165	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
184.168.152.58	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	24
100.92.220.55		147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	21
87.242.112.35	Russian Federation	147.237.77.233	atal.idf.il	drop	SAM rule	drop	18
195.154.235.88	France	147.237.76.86	navy.idf.il	drop	SAM rule	drop	18
158.85.253.245	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	18
184.168.152.58	United States	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	6
184.168.152.58	United States	147.237.77.233	atal.idf.il	drop	SAM rule	drop	6
184.168.27.81	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
46.19.85.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
199.58.86.209	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
77.126.31.56	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	1
176.13.235.165	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.244.20	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.247.247	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
168.1.128.51	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

08-21-2016-01:06:40 to 08-21-2016-02:06:40

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.149.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
212.76.111.33	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	5
77.139.134.183	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/faq.aspx	Block	3
109.67.183.144	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
77.138.190.216	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/drushim	Block	2
157.55.39.83	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	2
2.53.38.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
178.168.49.26	Moldova, Republic of	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/booklets.aspx	Block	2
24.101.39.187	United States	147.237.76.86	navy.idf.il	NULL Character in Header Name at Âˆ•f¬ðª[[#2]]•[[#4]][»€â½%$[[#11]]l[[#20]][[#0]]¢0=Þ£[[#12]][[#16]][8ëÄØ\ú	Block	1
85.65.145.131	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
68.180.228.185	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/mainfs.asp	Block	1
66.102.9.105	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
24.101.39.187	United States	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Header Name Âˆ•f¬ðª[[#2]]•[[#4]][»€â½%$[[#11]]l[[#20]][[#0]]¢0=Þ£[[#12]][[#16]][8ëÄØ\ú	Block	1
180.76.15.151	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8935-he/refuah.aspx	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/robots.txt	Block	1
66.249.73.146	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20346-he/idfgdover.aspx	Block	1
24.101.39.187	United States	147.237.76.86	navy.idf.il	NULL Character in Method ,[[#0]][[#0]][[#0]][[#22]]¡	Block	1
66.249.64.59	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/robots.txt	Block	1
24.101.39.187	United States	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Header Value	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
24.101.39.187	United States	147.237.76.86	navy.idf.il	Unauthorized Method POST for 147.237.76.86/	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
66.249.64.108	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/23122010masaiyot.aspx	Block	1
24.101.39.187	United States	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Method ,[[#0]][[#0]][[#0]][[#22]]¡	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
66.249.79.154	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
24.101.39.187	United States	147.237.76.86	navy.idf.il	Unknown HTTP Request Method ,[[#0]][[#0]][[#0]][[#22]]¡ in URL	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
66.249.65.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.177	Block	1
24.101.39.187	United States	147.237.76.86	navy.idf.il	Malformed URL	Block	1
84.109.241.2	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
68.180.228.99	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	1
46.19.86.187	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1
66.249.66.188	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1

08-21-2016-01:06:40 to 08-21-2016-02:06:40