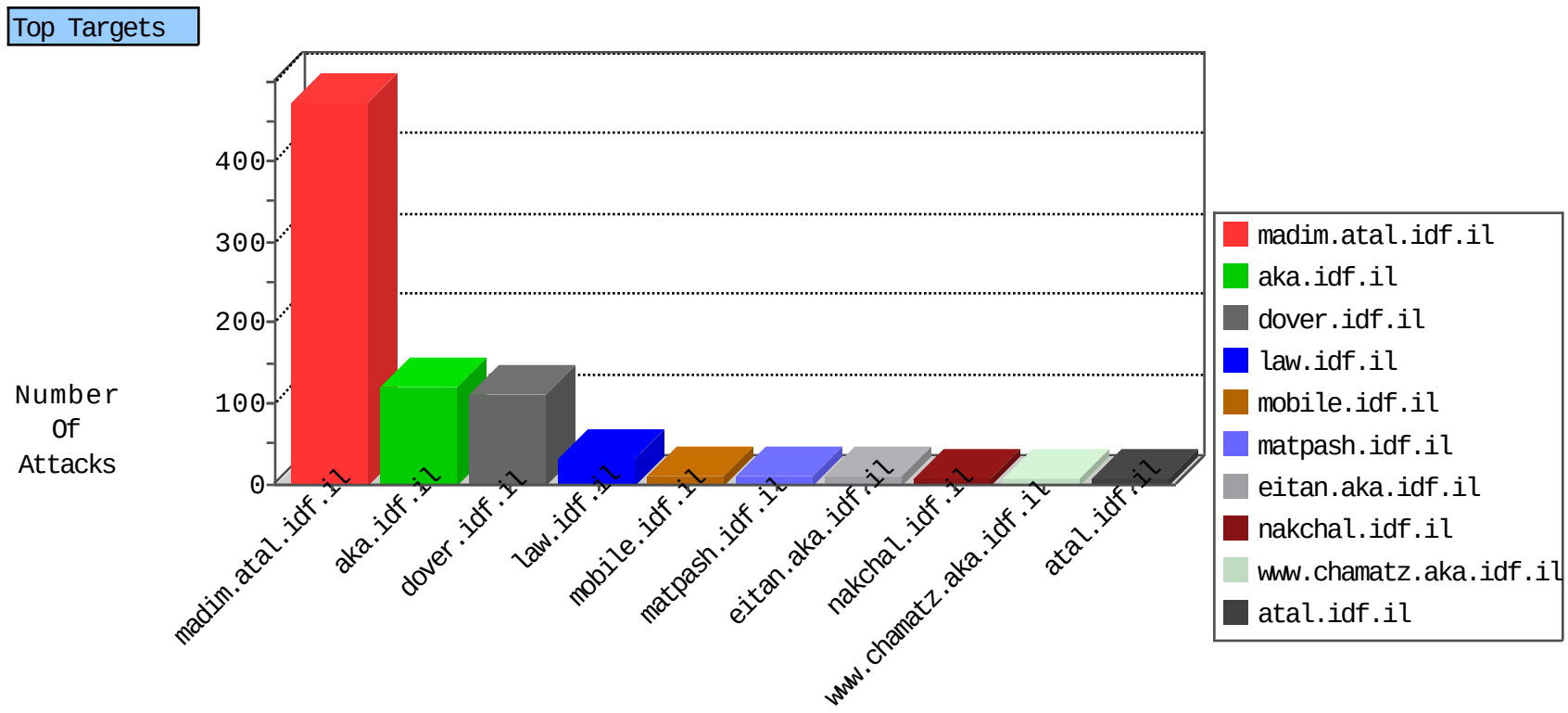
08-29-2016-10:04:02 to 08-29-2016-11:04:02

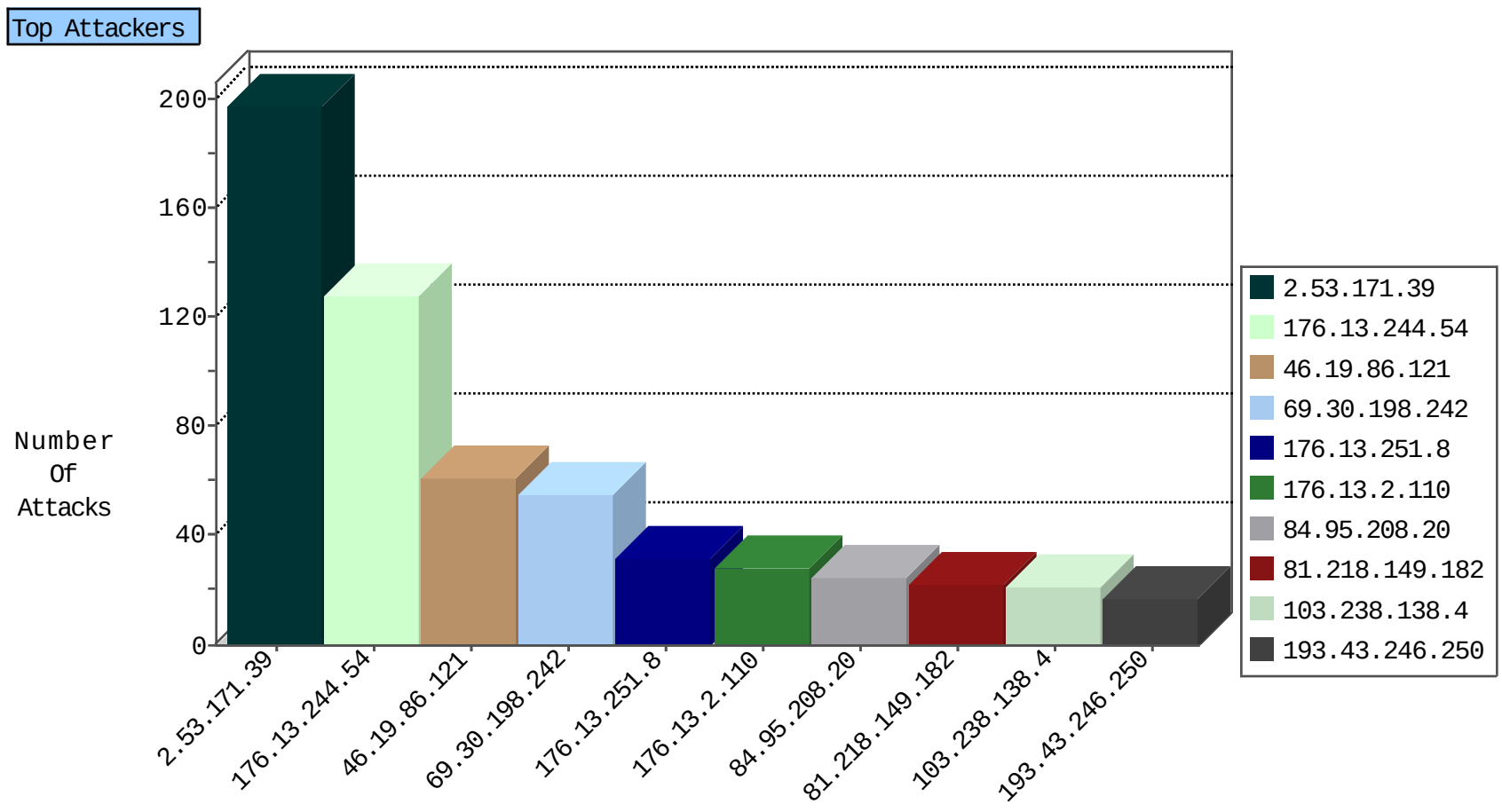
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

08-29-2016-10:04:02 to 08-29-2016-11:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.248.163.3	Netherlands	147.237.76.30	himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
178.239.62.141	Netherlands	147.237.76.86	navy.idf.il	Black List	drop	1
173.231.189.39	United States	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
31.168.121.73	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
173.231.189.39	United States	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
46.239.13.233	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	1
176.13.244.54	Israel	147.237.0.19	madim.atal.idf.il	DOSS-SSL-ClearText	drop	1

08-29-2016-10:04:02 to 08-29-2016-11:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.198.242	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	33
69.30.198.242	United States	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	11
69.30.198.242	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	7
103.238.138.4	Indonesia	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
69.30.198.242	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.30.198.242	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	1
69.30.198.242	United States	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	1

08-29-2016-10:04:02 to 08-29-2016-11:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
103.238.138.4	147.237.77.74	Indonesia	law.idf.il	SQL Injection - Select From	15
31.168.121.73	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
109.67.218.12	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
62.219.114.144	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
77.125.17.90	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.3.147.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
50.116.123.135	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.2.110	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.46.41.57	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.194.8	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.165.49	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.174.93.187	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
213.8.204.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.194.184	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.143.136.88	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.179.125.116	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
203.192.13.164	147.237.77.216	China	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.148.163	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.116.127.117	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.226.95	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.11	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
158.116.225.93	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.148	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.145.68	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.174.187	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.8.241.234	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.71.3.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.233.71	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.49.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.88.198.94	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.172.132	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.201.225.149	147.237.76.196	Ukraine	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1

08-29-2016-10:04:02 to 08-29-2016-11:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
81.218.149.182	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
46.19.85.199	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	7
176.67.62.200	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
185.99.33.8	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.146.127	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
109.64.143.15	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
82.205.127.192	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
141.95.0.58	United Kingdom	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
184.168.46.19	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
95.35.16.12	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.64.143.15	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
176.13.231.215	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
176.13.9.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
192.169.7.223	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	2
176.13.225.190	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.95.0.58	United Kingdom	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	2
62.0.200.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.95.0.58	United Kingdom	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
176.13.249.238	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.248	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	2
31.168.221.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
106.38.241.105	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
46.28.53.150	United Kingdom	147.237.0.200	m4u.idf.il	drop		drop	1
169.229.3.91	United States	147.237.0.33	idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.77.212	e.dover.idf.il	drop	First packet isn't SYN	drop	1
59.94.156.211	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.225.190	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.8.28	e.mobile-ks.idf.il	drop	First packet isn't SYN	drop	1
109.253.146.146	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.72.217	e.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	1
193.169.70.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
1.241.109.76	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.34	yohalan.idf.il	drop	First packet isn't SYN	drop	1
109.253.193.219	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
106.38.241.105	China	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
176.13.2.110	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	1
109.67.100.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	1
31.154.33.190	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
109.253.210.127	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
106.38.241.105	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
141.212.121.179	United States	147.237.0.35	akaws.idf.il	drop		drop	1
109.67.100.78	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.179	e.mazi.idf.il	drop	First packet isn't SYN	drop	1

08-29-2016-10:04:02 to 08-29-2016-11:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.171.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	198
176.13.244.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	126
46.19.86.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
176.13.251.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
176.13.2.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
109.253.128.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
77.138.66.34	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.138.66.34	Block	7
217.41.241.4	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/brothers/skira/default.asp	Block	6
212.199.224.24	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.199.224.24	Block	5
81.218.131.152	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 81.218.131.152	Block	5
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
77.139.26.89	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	5
194.90.99.193	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.90.99.193	Block	4
81.218.70.243	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 81.218.70.243	Block	4
2.55.153.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.138.210.55	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar	Block	3
176.13.15.29	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
2.53.35.242	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.53.46.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.5	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
46.19.85.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
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	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
109.253.134.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	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
77.139.33.40	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.33.40	Block	2
85.250.11.165	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
61.216.2.13	Taiwan	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
192.114.3.241	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/8/	Block	1
66.249.79.169	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
168.235.205.150	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/exampcert/	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
199.203.226.21	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1250-he/atal.aspx	Block	1
180.76.15.5	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/scroller/jquery.jcarousel.css	Block	1
77.139.33.40	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/	Block	1
109.186.93.136	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
66.102.9.10	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/drushim/	Block	1
212.199.224.24	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/5/	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
194.90.34.226	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
81.218.131.152	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
2.53.5.109	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.64	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_moreinfo.asp	Block	1
185.32.179.201	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1

08-29-2016-10:04:02 to 08-29-2016-11:04:02