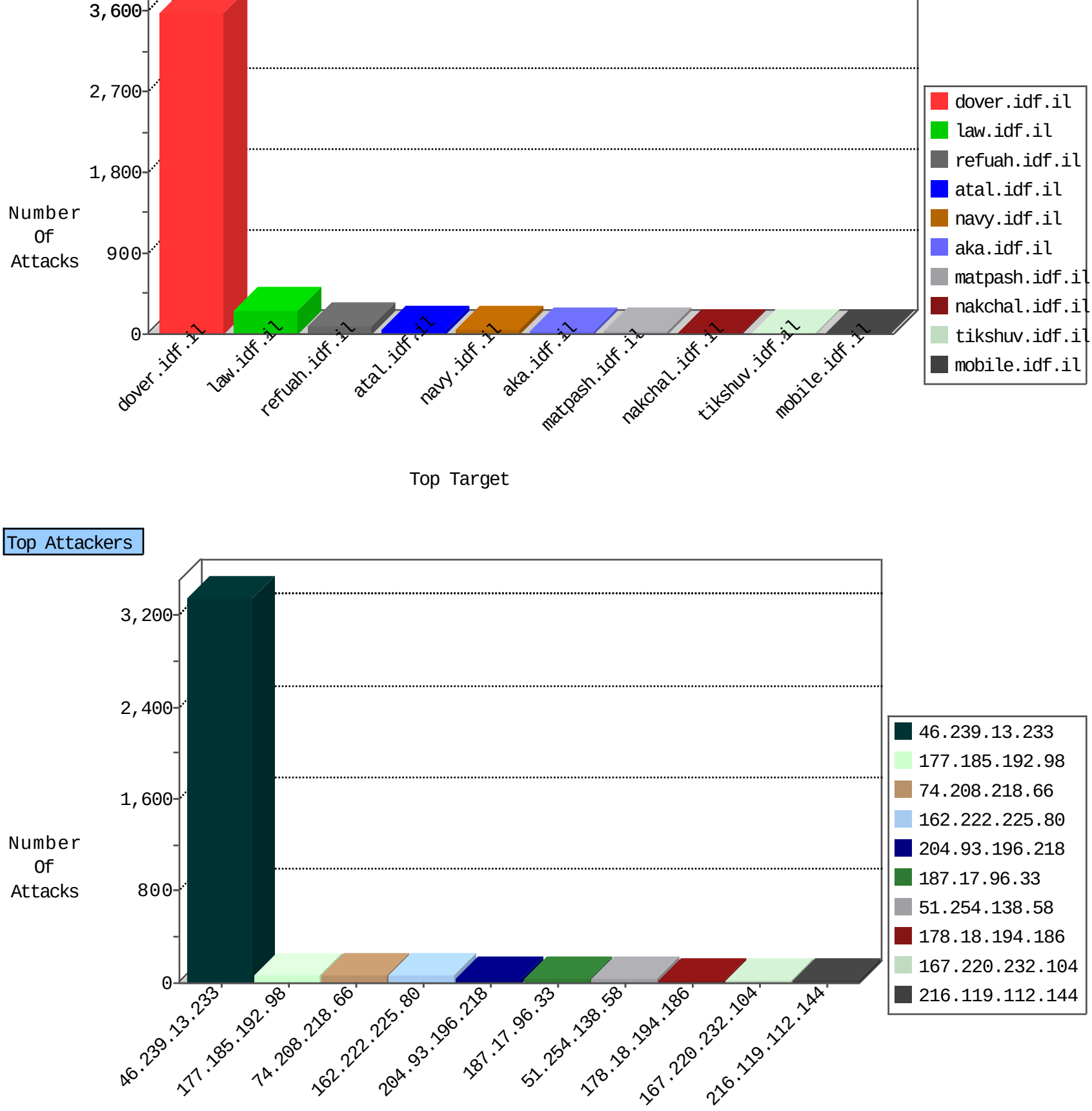
08-29-2016-01:07:52 to 08-29-2016-02:07:52

IDF Under Attack Daily Report



08-29-2016-01:07:52 to 08-29-2016-02:07:52

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	9
82.80.78.2	Israel	147.237.72.166	aka.idf.il	Black List	drop	3
46.239.13.233	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	2
173.231.189.39	United States	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.34	yohalan.idf.il	Black List	drop	1
52.204.200.107	United States	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
82.80.78.2	Israel	147.237.77.176	matpash.idf.il	Black List	drop	1
199.30.24.164	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
66.240.236.119	United States	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
173.231.189.39	United States	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1

08-29-2016-01:07:52 to 08-29-2016-02:07:52

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.254.138.58	France	147.237.77.216	dover.idf.il	25004: HTTP: WordPress Pingback Redirect Request	Block	32
178.18.194.186	Turkey	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
74.208.218.66	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
162.222.225.80	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
204.93.196.218	United States	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	11
177.185.192.98	Brazil	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	11
37.59.96.212	France	147.237.77.216	dover.idf.il	25004: HTTP: WordPress Pingback Redirect Request	Block	10
167.114.5.68	Canada	147.237.77.216	dover.idf.il	25004: HTTP: WordPress Pingback Redirect Request	Block	9
37.187.110.12	France	147.237.77.216	dover.idf.il	25004: HTTP: WordPress Pingback Redirect Request	Block	9
51.254.138.219	France	147.237.77.216	dover.idf.il	25004: HTTP: WordPress Pingback Redirect Request	Block	9
204.93.196.218	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	7
177.185.192.98	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	7
23.91.70.45	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
62.149.132.179	Italy	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
213.65.31.82	Sweden	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
108.175.157.102	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
74.208.218.66	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
216.119.112.144	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
187.17.96.33	Brazil	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
202.124.109.87	New Zealand	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
173.198.251.2	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
187.17.96.33	Brazil	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
74.208.230.195	United States	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.63.197.9	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
187.17.96.33	Brazil	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
162.222.225.80	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
46.105.73.239	France	147.237.77.216	dover.idf.il	25004: HTTP: WordPress Pingback Redirect Request	Block	3
164.132.56.109	Italy	147.237.77.216	dover.idf.il	25004: HTTP: WordPress Pingback Redirect Request	Block	2
92.222.3.117	France	147.237.77.216	dover.idf.il	25004: HTTP: WordPress Pingback Redirect Request	Block	2
192.169.164.219	United States	147.237.77.216	dover.idf.il	25004: HTTP: WordPress Pingback Redirect Request	Block	2
192.169.172.171	United States	147.237.77.216	dover.idf.il	25004: HTTP: WordPress Pingback Redirect Request	Block	2
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
50.63.197.204	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
167.114.44.14	Canada	147.237.77.216	dover.idf.il	25004: HTTP: WordPress Pingback Redirect Request	Block	1
216.249.102.195	United States	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	1
51.254.141.152	France	147.237.77.216	dover.idf.il	25004: HTTP: WordPress Pingback Redirect Request	Block	1

08-29-2016-01:07:52 to 08-29-2016-02:07:52

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
177.185.192.98	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	54
74.208.218.66	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	53
162.222.225.80	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	46
204.93.196.218	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	20
187.17.96.33	147.237.77.216	Brazil	dover.idf.il	SQL Injection - Select From	20
216.119.112.144	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	18
178.18.194.186	147.237.77.74	Turkey	law.idf.il	SQL Injection - Select From	16
213.65.31.82	147.237.77.74	Sweden	law.idf.il	SQL Injection - Select From	8
62.149.132.179	147.237.77.74	Italy	law.idf.il	SQL Injection - Select From	8
50.63.197.9	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
202.124.109.87	147.237.76.42	New Zealand	refuah.idf.il	SQL Injection - Select From	8
23.91.70.45	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
173.198.251.2	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
74.208.230.195	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	6
108.175.157.102	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	5
109.67.212.171	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	4
50.63.197.204	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	3
118.69.62.83	147.237.76.86	Vietnam	navy.idf.il	ET SCAN NMAP -sS window 1024	1
216.249.102.195	147.237.76.86	United States	navy.idf.il	SQL Injection - Select From	1
163.172.169.150	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.50.45	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
211.23.156.152	147.237.77.61	Taiwan	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN NMAP -sS window 1024	1

08-29-2016-01:07:52 to 08-29-2016-02:07:52

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.239.13.233	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3158
46.239.13.233	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop		drop	200
207.178.197.44	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	24
167.220.232.104	Japan	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
95.211.70.193	Netherlands	147.237.76.86	navy.idf.il	drop	SAM rule	drop	18
216.249.107.200	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	18
212.147.60.96	Switzerland	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	18
167.114.44.14	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
177.12.172.43	Brazil	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
96.251.45.13	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
84.245.33.104	Netherlands	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
97.88.198.223	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
91.219.122.2	Poland	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
184.168.46.19	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
93.186.250.66	Italy	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
188.165.250.173	France	147.237.77.233	atal.idf.il	drop	SAM rule	drop	6
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.169.7.223	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	3
212.143.142.56	Israel	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	2
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.120.122.219	Israel	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.76.198	e.yohalan.idf.il	drop	SAM rule	drop	1
106.38.241.105	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
46.120.122.219	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
212.143.165.117	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.76.199	e.nakchal.idf.il	drop	SAM rule	drop	1
125.77.28.26	China	147.237.0.33	idf.il	drop		drop	1
193.90.12.88	Norway	147.237.0.35	akaws.idf.il	drop		drop	1
183.129.160.229	China	147.237.76.30	himush.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.76.202	e.halag.idf.il	drop	SAM rule	drop	1
198.100.148.112	Canada	147.237.0.35	akaws.idf.il	drop		drop	1
183.129.160.229	China	147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	1
106.38.241.105	China	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.76.196	e.sviva.idf.il	drop	SAM rule	drop	1
106.38.241.105	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
64.113.32.29	United States	147.237.0.35	akaws.idf.il	drop		drop	1
216.249.102.195	United States	147.237.76.86	navy.idf.il	drop	Virtual defragmentation error: Timeout	drop	1

08-29-2016-01:07:52 to 08-29-2016-02:07:52

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.179.133.153	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
207.46.13.109	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
46.121.63.204	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/5/	Block	3
2.53.60.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
167.220.232.104	Japan	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in URL from 167.220.232.104	Block	2
46.120.18.45	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
77.122.109.234	Ukraine	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
139.162.161.192	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to /	Block	1
46.121.63.204	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.121.63.204	Block	1
188.163.107.178	Ukraine	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/blog/	Block	1
2.55.144.200	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
157.55.39.252	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/drushim/info.aspx	None	1
192.169.7.223	United States	147.237.76.42	refuah.idf.il	Unauthorized Method HEAD for 147.237.76.42/	Block	1
82.80.30.245	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Open Mode	None	1
5.29.238.254	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
167.220.232.104	Japan	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL /1283-17306-en/dover.aspx#011200	Block	1
66.249.69.237	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/edim/yoman/enlarge.asp	Block	1
207.46.13.64	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mp/	Block	1
91.210.145.125	Ukraine	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/blog/	Block	1
46.19.86.125	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 46.19.86.125	Block	1
68.180.229.39	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1111-he/nakhal.aspx	Block	1
92.202.23.1	Germany	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
176.13.244.44	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1

08-29-2016-01:07:52 to 08-29-2016-02:07:52