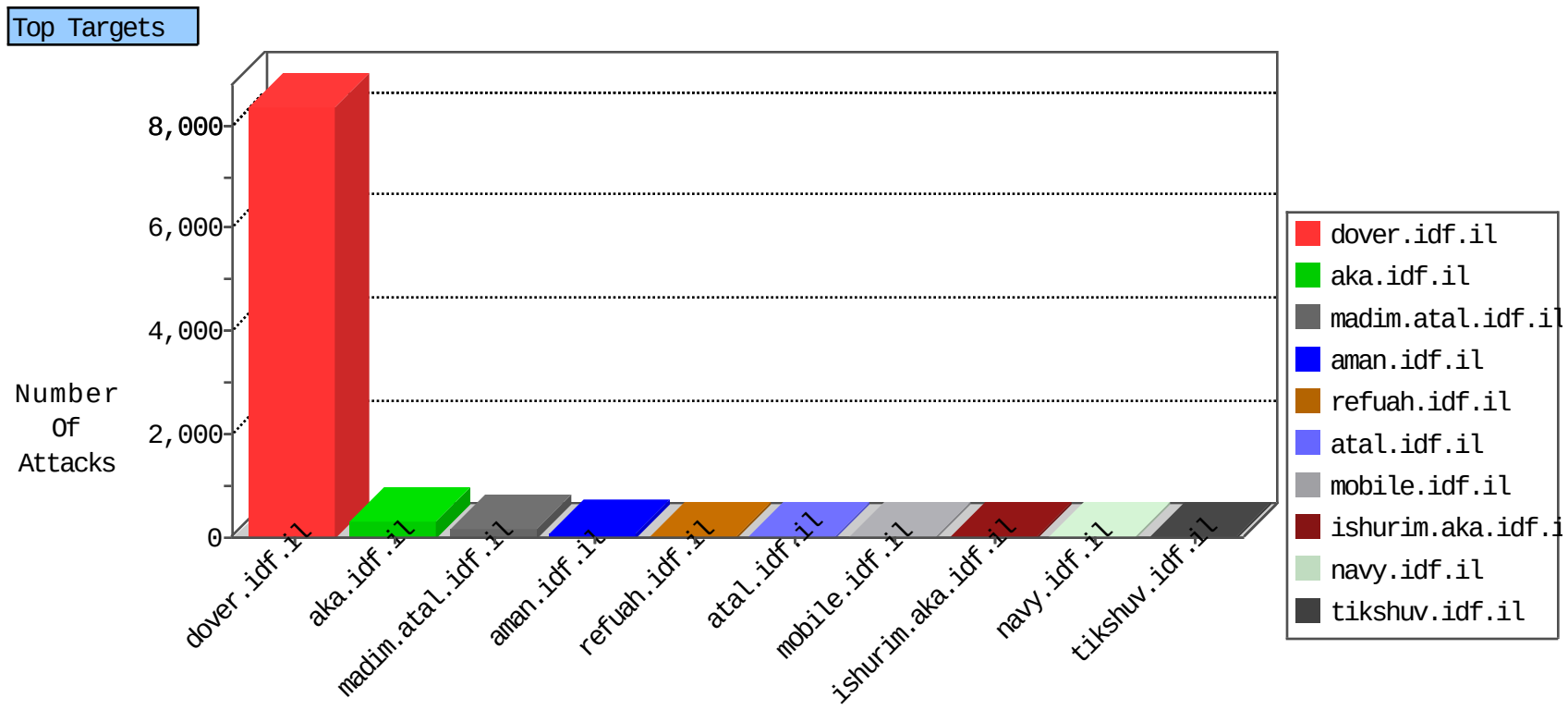
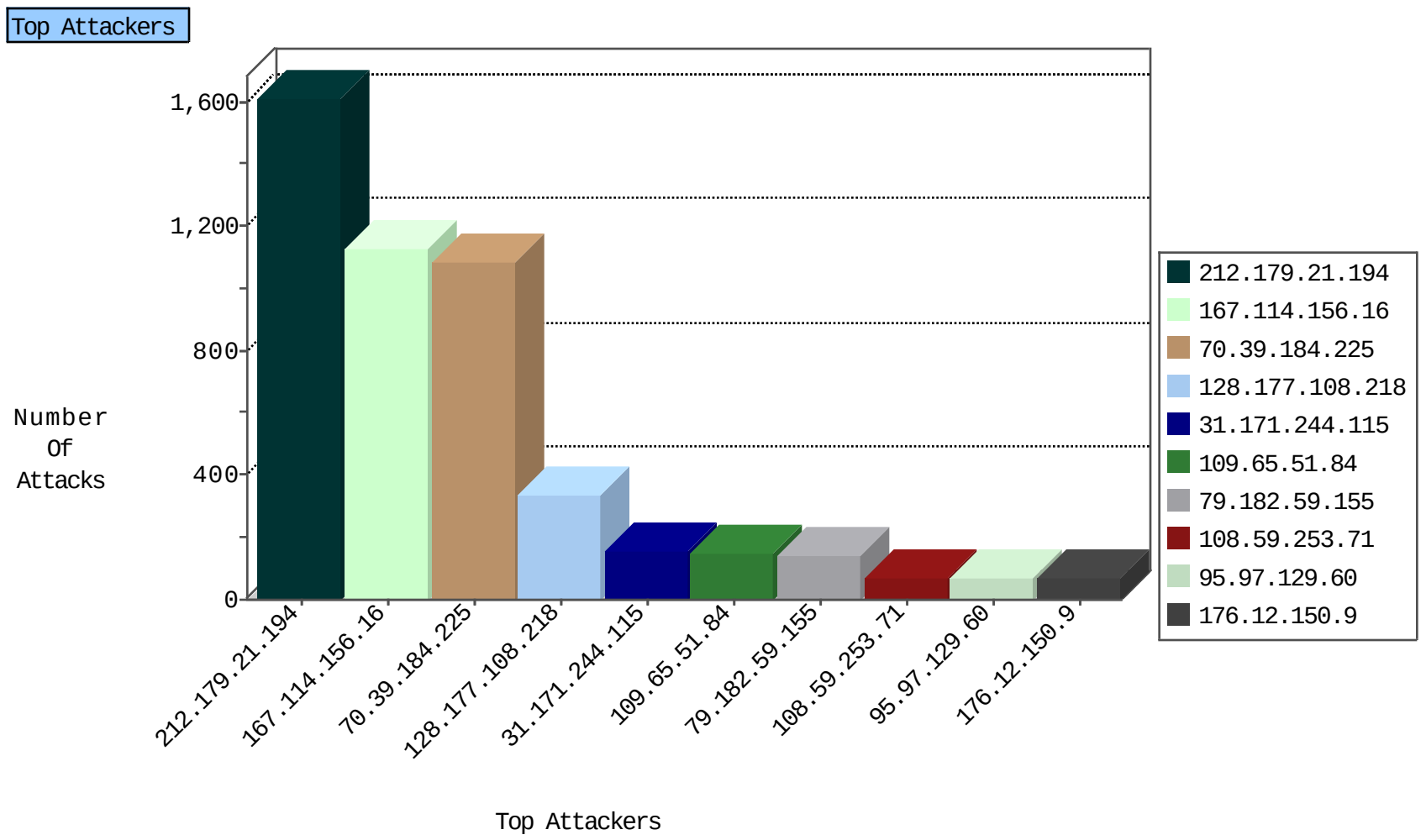
11-05-2015-15:04:00 to 11-05-2015-16:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-05-2015-15:04:00 to 11-05-2015-16:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1721
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	587
66.249.65.231	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	388
185.32.179.157	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	44
79.182.67.83	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	39
212.117.143.250	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	33
93.173.191.167	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
84.110.54.200	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
84.228.87.148	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
37.26.147.221	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	26
2.52.32.225	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
95.97.129.60	Netherlands	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
80.246.136.102	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
46.19.85.85	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	16
176.13.1.253	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	16
2.52.131.12	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	16
132.73.203.152	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
62.219.147.101	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	14
213.57.44.152	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	14
80.246.139.205	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	14
82.80.196.44	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
185.32.179.42	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
192.114.87.2	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
213.57.184.196	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
77.126.61.124	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
80.246.136.153	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
85.159.214.126	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
176.12.141.60	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
109.66.38.50	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
79.183.23.128	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
62.219.139.130	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
2.54.46.38	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
77.127.205.101	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
85.64.249.42	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
83.130.109.201	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
188.138.172.127	Moldova, Republic of	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
185.32.179.155	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
83.149.99.157	Netherlands	147.237.0.35	akaws.idf.il	Invalid TCP Flags	drop	5
199.203.176.50	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.86.107	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
93.172.1.157	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
83.149.99.157	Netherlands	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	5
46.19.85.120	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
93.173.15.13	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
185.32.179.110	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
83.149.99.157	Netherlands	147.237.0.16	my-kosher-kravi.idf.il	Invalid TCP Flags	drop	5
46.120.170.120	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
85.64.178.249	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
79.179.111.189	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4

11-05-2015-15:04:00 to 11-05-2015-16:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-05-2015-15:04:00 to 11-05-2015-16:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	**Signature**	**Count**

11-05-2015-15:04:00 to 11-05-2015-16:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1603
70.39.184.225	Satellite Provider	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1080
128.177.108.218	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	332
31.171.244.115	Switzerland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	157
109.65.51.84	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	146
79.182.59.155	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	140
108.59.253.71	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	70
199.203.176.50	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	63
82.102.239.214	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	57
95.97.129.60	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	54
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	47
37.24.144.214	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
78.95.36.229	Romania	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	43
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
63.168.168.5	Yemen	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
105.197.232.178	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
196.221.194.134	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
94.76.44.252	Bahrain	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
77.127.161.80	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
2.54.18.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
216.177.129.184	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
185.27.105.182	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	32
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	32
77.126.61.124	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
93.172.145.122	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
79.182.168.108	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29
85.64.178.249	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29
212.179.90.106	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
192.116.98.164	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
84.110.54.200	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
5.22.134.160	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
51.39.129.190	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
2.54.34.38	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
79.180.20.13	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
89.138.241.246	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
38.74.18.44	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
212.106.84.110	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
38.111.147.88	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
100.100.10.51		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	24
46.19.86.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
86.104.161.74	Romania	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
105.157.167.196	Morocco	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
46.19.86.86	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
207.46.13.29	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
109.66.62.244	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.150.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
176.13.18.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
2.52.137.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
5.42.198.91	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	5
84.108.61.37	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.108.61.37	Block	5
185.120.126.26		147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	5
185.120.126.26		147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/pages/fan_status.php	Block	5
84.108.61.37	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	3
46.19.86.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.137.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.116.167.185	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
84.109.90.213	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
85.64.202.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
176.13.17.234	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
149.78.57.247	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy.	Block	2
46.19.86.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.180.124.106	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in tikshuv.idf.il/site/story.aspx	Block	1
2.54.59.131	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
178.255.87.242	United Kingdom	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/robots.txt	Block	1
149.78.57.247	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/ufi/reaction/	Block	1
66.249.65.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20028-he/dover.aspx	Block	1
85.65.84.109	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.139.52.44	Jordan	147.237.77.216	dover.idf.il	Unknown HTTP Request Method p://www.idf.il/Style/Shared/nav.css in URL	Block	1
5.28.166.126	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
188.165.15.14	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/funeral.stm)	Block	1
79.182.225.205	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1
66.249.79.107	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/forums.aspx	Block	1
66.33.212.126	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
93.173.15.13	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 93.173.15.13	Block	1
8.29.198.38	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/feed/	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/links.aspx	Block	1
78.47.8.52	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
2.54.59.131	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
185.46.121.194	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/print_text.asp	Block	1
87.68.55.224	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ufi/reaction/	Block	1
217.69.133.221	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il/main/	Block	1
5.28.180.185	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
207.46.13.29	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1116-he/Ã¬Â¦Ã¬â€?	Block	1
66.249.79.109	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.65.80	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
93.173.15.13	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/sip_storage/files/	Block	1
84.108.61.37	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	1
37.26.149.177	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.179.21.194	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
79.177.194.57	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyu/	Block	1
5.28.134.45	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl75 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
162.243.210.82	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1

11-05-2015-15:04:00 to 11-05-2015-16:04:00