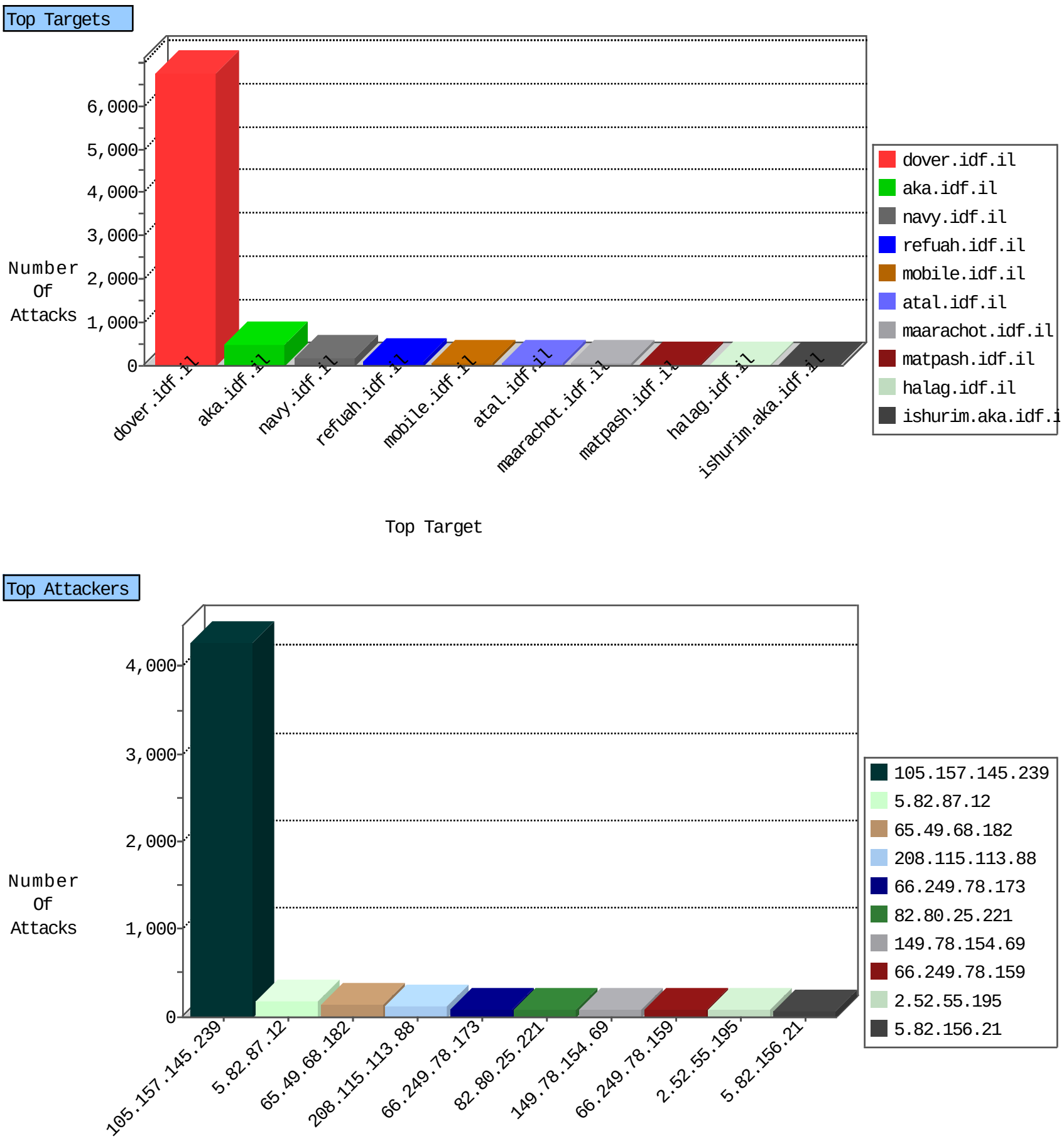
10-31-2015-12:04:09 to 10-31-2015-13:04:09

IDF Under Attack Daily Report



10-31-2015-12:04:09 to 10-31-2015-13:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	336
105.157.145.239	Morocco	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	273
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	169
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	77
217.66.254.148	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	41
87.68.35.15	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	34
109.67.185.219	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34
52.16.5.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	31
77.125.82.25	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
79.178.111.91	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
79.180.99.170	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	28
89.139.4.192	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
24.13.45.210	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	16
109.65.189.187	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
2.54.16.12	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
93.172.86.181	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
46.120.169.127	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
46.19.86.118	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
217.66.254.148	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.i	Block_Udp_All_Nets	drop	9
62.219.154.229	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
176.13.18.158	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
85.64.124.254	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
109.67.13.155	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
128.139.197.119	Israel	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	6
46.120.41.23	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
84.111.163.105	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
77.126.164.51	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.180.120.207	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
64.233.172.170	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
79.182.171.171	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
77.125.79.206	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
82.102.231.213	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
149.88.70.81	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
109.64.128.115	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.52.30.157	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.117.121.48	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
93.172.86.181	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
79.178.122.208	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.138.130	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
5.82.156.21	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.17.235	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
134.147.203.115	Germany	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	4
46.19.85.220	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.13.22.55	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.23.144	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.19.86.124	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
151.42.72.24	Italy	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
109.186.129.254	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3

10-31-2015-12:04:09 to 10-31-2015-13:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-31-2015-12:04:09 to 10-31-2015-13:04:09

Top Attackers In IDS

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

10-31-2015-12:04:09 to 10-31-2015-13:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
105.157.145.239	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3977
5.82.87.12	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	186
65.49.68.182	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	127
82.80.25.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	92
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	85
2.52.55.195	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	77
5.82.156.21	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
109.67.185.219	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
128.78.78.156	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
46.19.85.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
84.111.163.105	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
85.64.115.245	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
151.42.72.24	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
24.13.45.210	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	19
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
149.78.56.32	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
93.172.86.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
121.98.142.99	New Zealand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
78.95.86.191	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
85.64.120.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
100.100.23.4		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
217.66.254.148	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
66.249.84.167	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.66.7.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.84.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	12
151.80.31.112	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
198.58.103.92	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
100.100.57.151		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
79.183.2.178	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
84.18.64.180	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.65.189.187	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.65.202.175	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
5.102.254.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
207.46.13.130	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9

10-31-2015-12:04:09 to 10-31-2015-13:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
105.157.145.239	Morocco	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 105.157.145.239	Block	288
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	120
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	60
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	45
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	30
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	30
213.57.252.211	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main-sachar	Block	30
94.159.246.147	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	30
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	30
178.255.215.87	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.255.215.87	Block	15
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	15
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.6	Block	15
93.104.215.152	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	15
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20236-he/idfgdover.aspx	Block	15
213.57.251.96	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 213.57.251.96	Block	15
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
109.65.207.148	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	15
89.138.245.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	15
37.142.68.8	Israel	147.237.72.166	aka.idf.il	Unknown Parameter utm_source in www.aka.idf.il/main/home/default.aspx	None	15
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-17762-he/kkkkkkk=17a07365kkkkkkk_17a07365	Block	15
66.249.67.247	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/8/112198.pdf	Block	15
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/main/rabanut/general.aspx	Block	15
93.157.100.74	Poland	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	15
74.82.47.2	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	15
109.66.7.33	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
89.139.16.233	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	15
46.117.98.24	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId... in www.aka.idf.il/main/giyus/general.aspx	None	15
66.249.69.92	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-5512-he	Block	15
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1149-he/chinuch.aspx	Block	15
93.173.8.214	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
79.176.222.59	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	15
220.181.108.80	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/3/size338x0/1613.jpg	Block	15
141.212.121.192	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	15
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	15
89.139.171.165	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	15
52.7.48.171	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	15
68.64.169.226	United States	147.237.77.233	atal.idf.il	Unauthorized HTTP Method	Block	15
212.235.80.213	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/chinuch/general/default.asp	None	15
66.249.69.97	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1406-he/atal.aspx	Block	15
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
79.181.61.140	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	15
141.212.121.192	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	15
66.249.67.134	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/72019-he/maarachot.aspx	Block	15
89.238.188.119	United Kingdom	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	15
66.249.65.251	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/links.aspx	Block	15
68.64.169.226	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	15
66.249.78.59	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	15
213.57.251.96	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	15

10-31-2015-12:04:09 to 10-31-2015-13:04:09