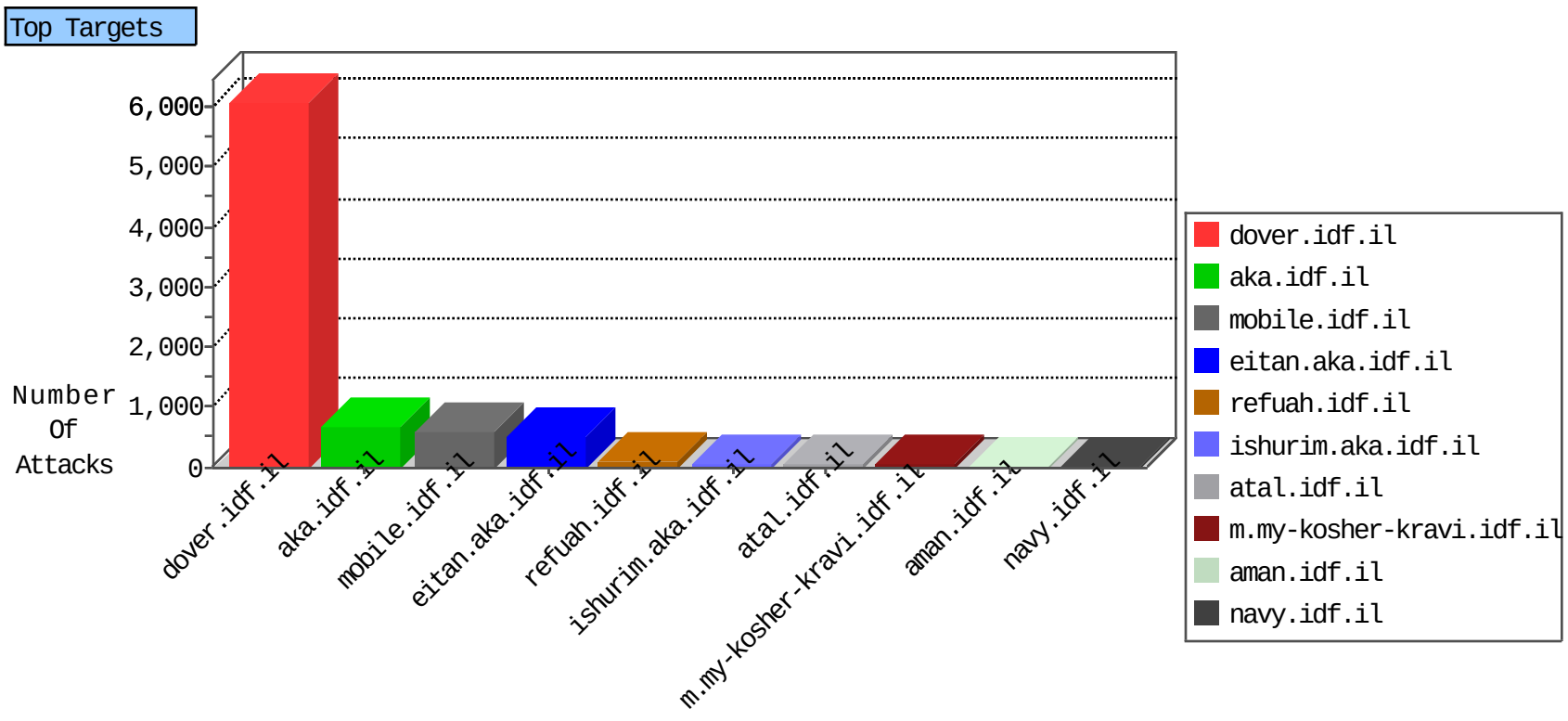
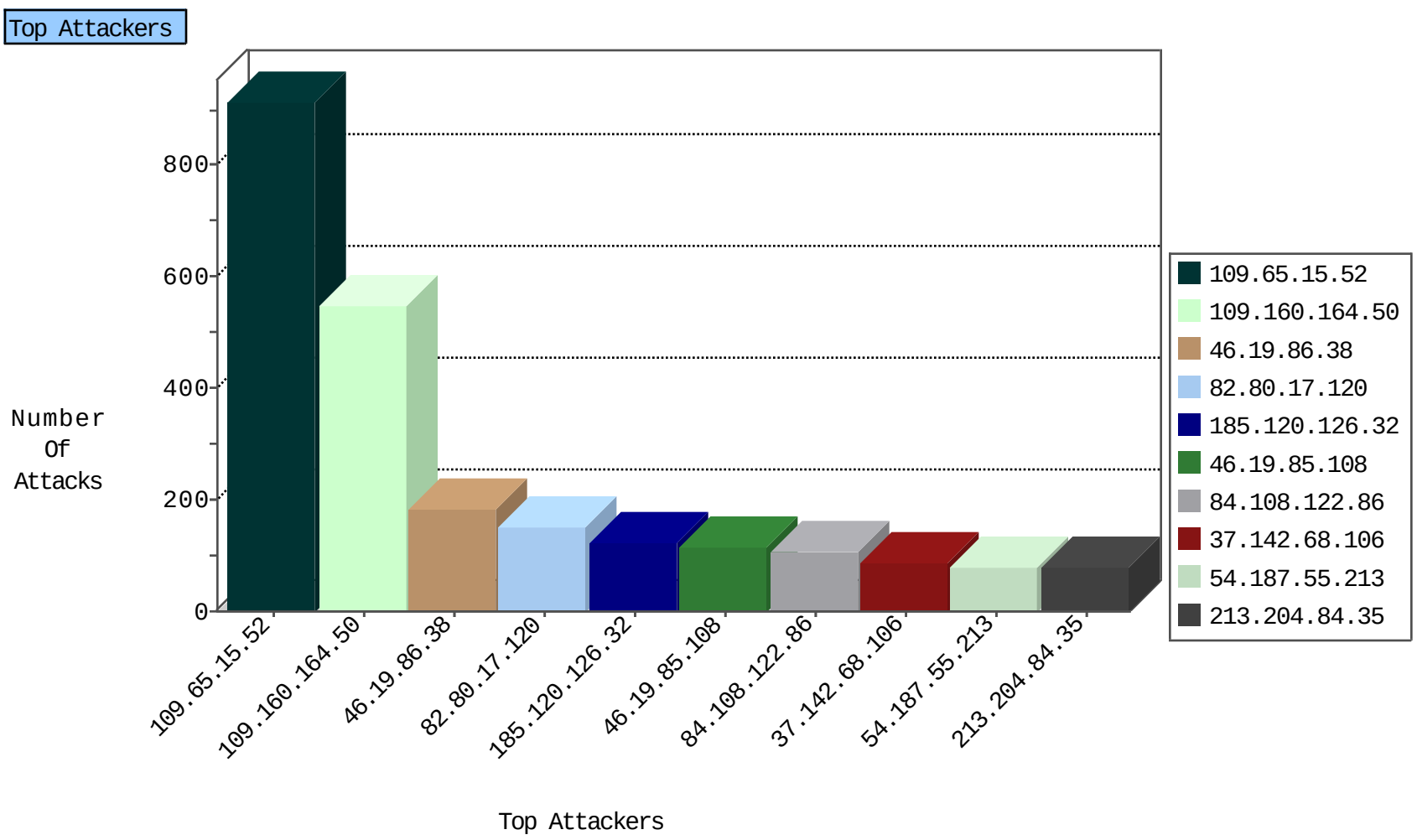
10-31-2015-19:04:07 to 10-31-2015-20:04:07

IDF Under Attack Daily Report





10-31-2015-19:04:07 to 10-31-2015-20:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	617
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	54
37.142.68.106	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	46
2.54.150.87	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	40
109.66.57.84	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	34
31.44.135.206	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	31
213.55.176.187	Switzerland	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
213.57.250.168	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	29
2.54.175.122	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
89.138.214.54	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
84.111.14.41	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
37.26.148.216	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
37.142.68.106	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
77.125.247.14	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
95.86.94.228	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	17
46.19.85.180	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	16
37.26.149.223	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	14
46.19.86.38	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	13
79.181.139.15	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
46.116.241.127	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
149.78.35.97	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
109.186.160.79	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
37.142.68.99	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
79.182.20.207	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
46.19.86.38	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
62.219.155.244	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
46.19.86.38	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
62.219.155.244	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
80.246.136.219	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
89.138.241.196	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
5.29.178.252	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
79.176.29.228	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
87.69.245.63	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
37.142.211.10	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
37.26.148.190	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
194.90.37.100	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
89.139.171.27	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
46.19.86.212	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
109.65.12.42	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.182.218.155	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
84.229.155.144	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
64.233.172.178	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.182.111.49	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
77.126.218.173	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
37.142.182.30	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.86.225	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
85.65.138.187	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.52.189.67	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.106.227.160	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.179.212.126	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
87.69.230.10	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
89.139.0.102	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4

10-31-2015-19:04:07 to 10-31-2015-20:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.204.84.35	Lebanon	147.237.77.216	dover.idf.il	12371: TCP: Hulk DDoS Tool	Block	6

10-31-2015-19:04:07 to 10-31-2015-20:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	7
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3

10-31-2015-19:04:07 to 10-31-2015-20:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.65.15.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	915
46.19.86.38	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	168
82.80.17.120	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	149
185.120.126.32		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	122
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	80
146.50.79.106	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
213.204.84.35	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	73
37.26.148.216	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
5.29.224.141	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
46.19.86.206	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
84.228.210.132	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
79.181.221.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
5.102.254.117	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
5.29.119.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
46.120.74.245	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
77.42.217.92	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
100.100.50.139		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	43
2.54.150.87	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
46.19.85.109	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
2.102.94.235	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
66.249.81.212	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
109.186.20.201	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
2.54.191.169	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
188.161.10.185	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
100.100.95.220		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	27
84.228.177.246	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
79.183.61.177	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
64.233.172.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
66.102.9.81	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
99.100.202.76	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
149.78.112.202	Israel	147.237.76.31	nakchal.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
66.249.81.218	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
79.176.182.13	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
64.233.172.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
213.139.53.18	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
98.211.110.170	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
100.100.63.242		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	22
192.118.11.120	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
64.233.172.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.160.164.50	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 109.160.164.50	Block	495
84.108.122.86	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	90
46.19.85.108	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	90
176.13.13.134	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	60
176.13.0.60	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	45
87.68.156.244	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	45
46.19.86.187	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	30
37.142.68.106	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	30
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
77.126.218.173	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	30
157.55.39.106	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/brothers/skira/default.asp	None	15
79.176.165.115	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	15
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/kapatz/citizencontact.aspx	Block	15
109.65.111.71	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	15
46.19.86.172	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
218.200.139.242	China	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/miluim/about.aspx	Block	15
79.179.145.252	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
31.13.109.121	Ireland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	15
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-19043-en/dover.aspx>,	Block	15
109.160.164.50	Israel	147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	Block	15
87.69.160.97	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/mas.aspx	Block	15
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8860-he/refuah.aspx	Block	15
46.19.85.62	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	15
199.16.156.124	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/1/size220x0/17451.jpg	Block	15
80.178.192.6	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
157.55.39.171	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	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
66.249.69.81	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1242-he/atal.aspx	Block	15
109.65.155.15	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	15
218.200.139.242	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	15
85.65.0.239	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	15
79.181.25.83	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	15
37.8.79.225	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	15
185.13.195.37	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	15
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
89.139.190.233	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	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
46.19.85.62	Israel	147.237.77.216	dover.idf.il	Malformed URL fffffff=0b91110bfffffff_0b91110b	Block	15
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/5/size220x0/17455.jpg	Block	15
80.246.133.227	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
2.52.157.11	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	15
79.177.167.76	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https:/www.aman.idf.il/	Block	15
66.249.69.89	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	15
109.160.149.222	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	15
85.250.154.247	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	15
46.117.213.53	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	15
79.181.142.235	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
185.35.62.11	Switzerland	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	15
109.160.164.50	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	15
93.173.163.4	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15