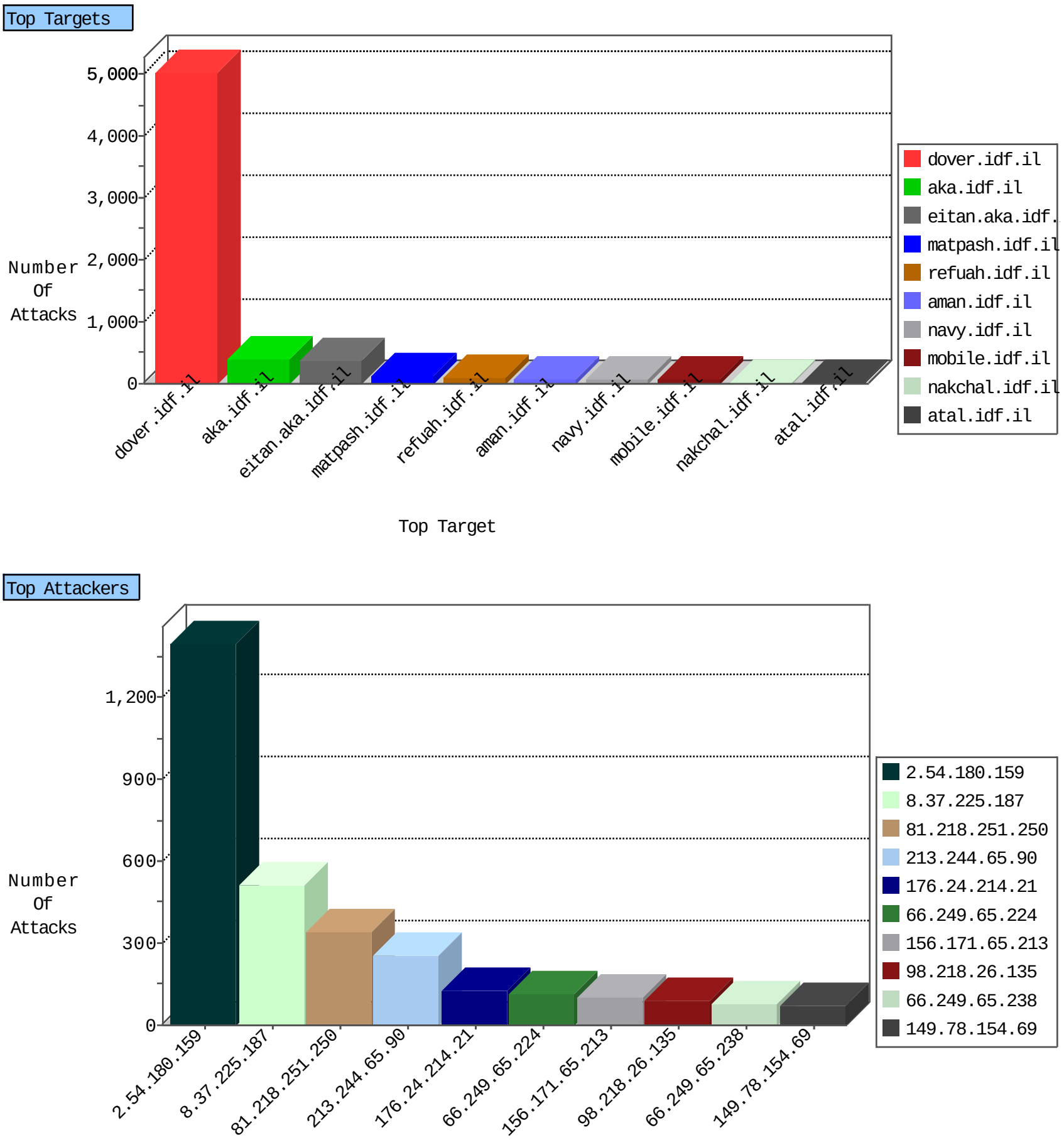
10-24-2015-11:04:07 to 10-24-2015-12:04:07

IDF Under Attack
Daily Report



10-24-2015-11:04:07 to 10-24-2015-12:04:07

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	304
213.57.53.96	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	39
109.64.13.205	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	36
149.78.188.220	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	32
84.108.249.220	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	29
85.65.60.37	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
85.65.59.94	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	17
185.32.179.219	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	16
79.183.110.168	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
82.80.196.44	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
77.125.157.16	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
93.172.156.204	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
46.120.129.152	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
82.213.16.130	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
176.12.140.175	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
89.139.174.135	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.182.148.4	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
109.65.206.169	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
62.90.152.241	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
207.244.75.50	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
79.183.99.106	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
92.232.83.105	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.86.167	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
2.52.63.64	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
37.46.39.210	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
2.54.150.226	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
79.176.81.142	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.19.86.167	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.0.116.44	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
134.147.203.115	Germany	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	2
37.26.146.200	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.106.226.137	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
93.172.156.204	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
93.172.156.204	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
185.120.126.49		147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.86.167	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
93.173.226.93	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
84.110.32.166	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
79.182.39.109	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
87.69.73.242	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
84.111.216.58	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
109.64.13.205	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
223.100.67.157	China	147.237.76.197	e.himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
5.28.153.226	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
79.180.22.243	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
176.13.11.152	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1

10-24-2015-11:04:07 to 10-24-2015-12:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.135.44.164	Oman	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
79.176.168.201	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4

10-24-2015-11:04:07 to 10-24-2015-12:04:07

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	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
169.45.161.174	147.237.72.166	Netherlands	aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
125.65.165.215	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.138	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
201.158.203.53	147.237.0.19	Mexico	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
169.45.161.174	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
125.65.165.215	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
125.65.165.215	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
54.224.149.230	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1

10-24-2015-11:04:07 to 10-24-2015-12:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.180.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1401
8.37.225.187	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	507
213.244.65.90	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	253
176.24.214.21	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	129
156.171.65.213		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	104
98.218.26.135	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	91
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	73
62.145.207.44	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
82.145.223.56	Europe	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	54
5.29.157.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
37.142.224.233	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	51
17.142.145.3	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
37.8.36.65	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
66.249.65.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
17.142.152.86	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
17.142.152.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
188.29.164.165	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
176.12.140.175	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
85.65.215.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
17.142.152.81	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
100.100.124.223		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	25
103.7.250.251	Bangladesh	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
151.80.31.115	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
84.108.249.220	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
17.142.152.68	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
85.65.60.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
17.142.152.94	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
84.228.91.177	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
84.229.32.25	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
17.142.156.109	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
176.12.147.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
85.65.172.214	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
100.100.33.204		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	19
37.26.149.219	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	18
2.52.166.133	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
93.172.156.204	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
85.65.59.94	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
157.55.39.255	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
46.116.169.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17

10-24-2015-11:04:07 to 10-24-2015-12:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.251.250	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 81.218.251.250	Block	322
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	56
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	42
84.94.22.26	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	28
74.208.16.178	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	14
151.80.31.115	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
85.65.11.142	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
79.177.59.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
186.202.153.171	Brazil	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	14
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.238	Block	14
92.37.214.162	Russian Federation	147.237.77.216	dover.idf.il	Unknown HTTP Request Method COOK in URL www.idf.il/1283-19218-en/dover.aspx	Block	14
46.121.102.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
82.118.24.206	Sweden	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	14
77.125.85.206	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	14
176.13.5.80	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mivtza	Block	14
85.65.186.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gyus	Block	14
79.181.112.133	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
188.143.232.41	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation fromDate in www.cogat.idf.il/901-en/cogat.aspx	Block	14
66.249.73.197	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	14
50.116.30.23	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	14
96.233.128.50	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	14
84.94.22.26	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 84.94.22.26	Block	14
77.126.165.16	Israel	147.237.76.31	nakchal.idf.il	Parameter Type Violation search in nakhal.idf.il/1119-he/nakhal.aspx	Block	14
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	14
182.118.60.176	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/webresource.axd?d	Block	14
87.69.241.92	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 87.69.241.92 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	14
2.52.63.64	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	14
79.183.67.107	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1440-he/atal.aspx	Block	14
207.46.13.144	United States	147.237.77.216	dover.idf.il	Parameter Type Violation a in www.idf.il/	Block	14
54.179.134.216	Singapore	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /	Block	14
109.186.184.54	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	14
79.176.7.84	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	14
183.79.223.2	Japan	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.231	Block	14
87.69.241.92	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	14
31.168.147.148	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/tfasim.aspx	None	14
81.218.251.250	Israel	147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	Block	14
74.82.47.3	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	14
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
149.88.103.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
84.110.35.79	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
79.176.7.84	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
185.13.194.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
89.71.246.224	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/dover.aspx/	Block	14
46.19.85.180	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	14

10-24-2015-11:04:07 to 10-24-2015-12:04:07