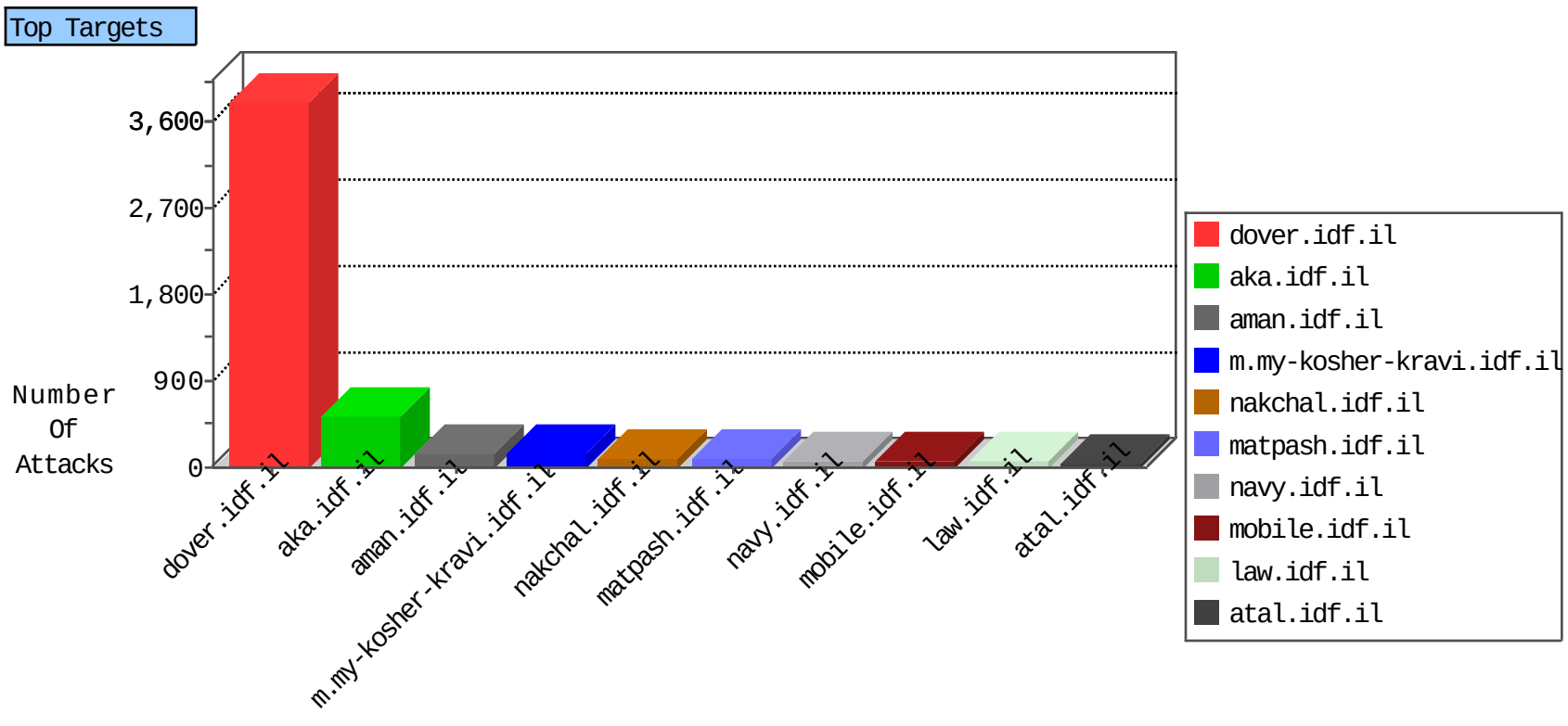
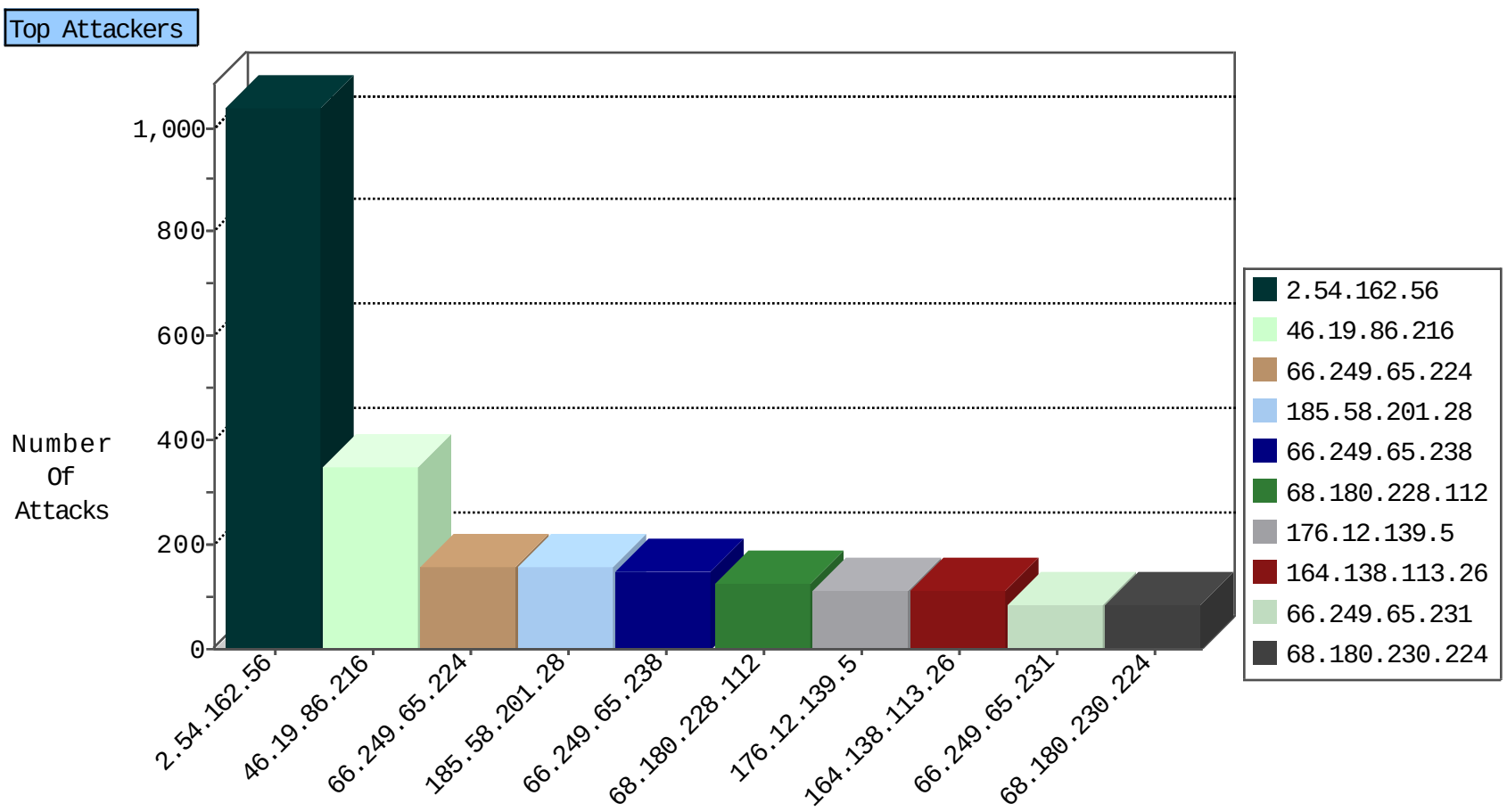
10-24-2015-13:04:04 to 10-24-2015-14:04:04

IDF Under Attack Daily Report



Top Target



Top Attackers

10-24-2015-13:04:04 to 10-24-2015-14:04:04

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	139
46.19.86.216	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	61
46.19.86.216	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	36
46.19.86.216	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	23
79.180.128.8	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	23
37.26.149.148	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
46.116.203.113	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15
84.109.76.14	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
109.66.66.97	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
81.218.132.244	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
84.108.116.236	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
5.29.37.132	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	7
46.19.85.153	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
109.64.125.254	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
109.65.9.35	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
37.26.149.148	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
79.178.126.204	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.183.129	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
10.0.0.7		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
46.19.85.90	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
109.66.112.118	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
79.176.203.57	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
46.19.86.25	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
5.29.151.170	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
87.69.121.14	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
77.125.105.239	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
84.109.10.54	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
109.67.183.28	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
101.186.66.48	Australia	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
212.117.140.158	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
103.252.202.59	Singapore	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
10.0.0.7		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
176.57.141.208	Germany	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
79.181.142.15	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
89.248.172.98	Netherlands	147.237.76.176	test.ncore.idf.i	Block_Udp_All_Nets	drop	1
185.21.122.119	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
79.181.142.15	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
84.108.116.236	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
109.65.199.162	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
87.69.153.226	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
81.130.214.82	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
172.19.5.245		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
89.139.179.195	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
79.176.131.58	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1

10-24-2015-13:04:04 to 10-24-2015-14:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.132.77.12	Azerbaijan	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3

10-24-2015-13:04:04 to 10-24-2015-14:04:04

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
223.16.227.101	147.237.8.24	Hong Kong	e.lifestyle.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
175.143.156.208	147.237.76.31	Malaysia	nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
175.143.156.208	147.237.76.31	Malaysia	nakchal.idf.il	ET SCAN NMAP -f -sS	1
94.102.48.194	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.0.16		my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
46.151.55.40	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
175.143.156.208	147.237.76.31	Malaysia	nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
111.93.198.54	147.237.0.33	India	idf.il	ET SCAN NMAP -sS window 4096	1
93.174.93.138	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
46.151.55.40	147.237.77.226	Ukraine	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1

10-24-2015-13:04:04 to 10-24-2015-14:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.162.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1023
46.19.86.216	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	293
185.58.201.28	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	145
93.173.252.13	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
119.224.29.36	New Zealand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
5.29.180.34	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
100.100.33.204		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	44
212.117.140.158	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	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	34
37.26.146.203	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
81.218.152.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
109.66.199.48	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	27
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
88.251.159.144	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
84.109.76.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
89.138.95.54	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
46.19.85.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
66.249.65.224	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
176.16.57.58	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
54.245.64.111	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	19
100.100.60.199		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
52.16.5.197	United States	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
2.54.183.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
80.246.130.13	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
38.111.147.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
109.186.44.182	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
37.142.122.201	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
79.179.200.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
94.230.86.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
84.229.248.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
37.142.215.22	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
2.54.139.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
37.26.148.142	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
66.249.65.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
151.80.31.115	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
101.186.66.48	Australia	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
103.252.202.59	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.121.208.64	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.116.169.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
66.249.65.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10

10-24-2015-13:04:04 to 10-24-2015-14:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.139.5	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation __EVENTVALIDATION in m.my-kosher-kravi.idf.il/templates/training/training.aspx	Block	84
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	84
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.238	Block	84
164.138.113.26	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	56
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	Multiple Unauthorized URL Access from 66.249.65.224	Block	56
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	42
164.138.113.26	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/4/	Block	42
46.116.137.111	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	42
151.80.31.115	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.231	Block	28
93.172.14.49	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	28
176.13.9.37	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	28
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	28
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/</font	Block	28
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	14
2.54.33.164	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
79.183.17.153	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
66.249.93.154	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyu	Block	14
176.12.139.5	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.12.139.5	None	14
62.219.137.5	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	14
137.116.71.170	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	14
85.64.150.93	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	14
46.121.78.93	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.121.78.93	Block	14
213.57.34.37	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/talpiotquestionnaire.aspx	None	14
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	14
164.138.113.26	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 164.138.113.26	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
58.8.151.174	Thailand	147.237.77.74	law.idf.il	E-mail collector robots 14	Block	14
2.88.28.220	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	14
81.130.214.82	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	14
141.212.122.160	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	14
66.249.64.249	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	14
85.65.3.177	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	14
46.121.78.93	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	14
58.8.151.174	Thailand	147.237.77.74	law.idf.il	eMail Hoarding	Block	14
84.94.48.157	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	14
31.154.91.156	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	14
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	14
149.78.0.157	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
85.65.172.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
46.121.78.93	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	14
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	14
58.8.151.174	Thailand	147.237.77.176	matpash.idf.il	E-mail collector robots 14	Block	14
112.233.57.57	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	14
84.109.97.90	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	14
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1395-en/dover.aspx	Block	14
185.120.126.48		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
149.78.0.157	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	14

10-24-2015-13:04:04 to 10-24-2015-14:04:04