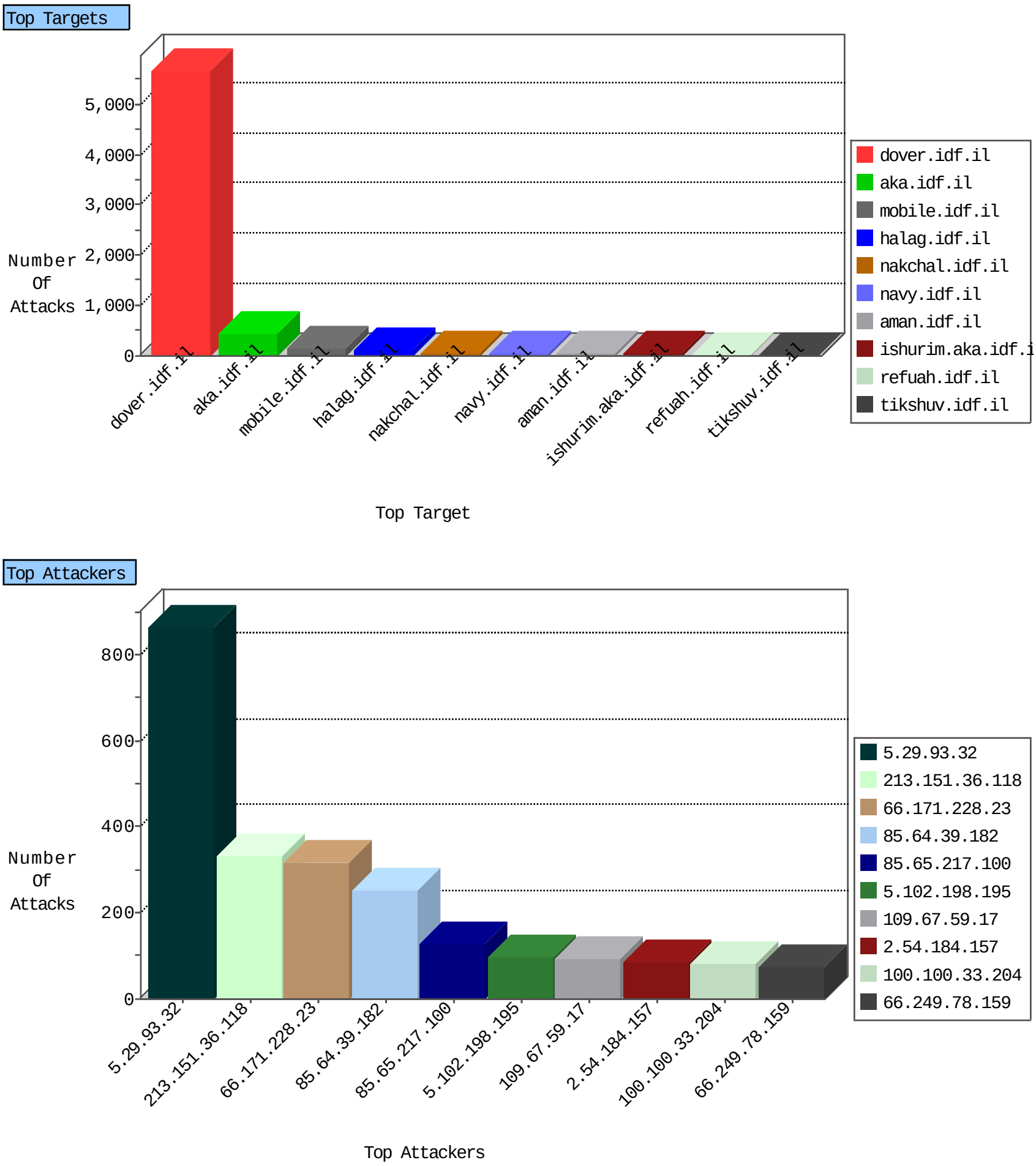
10-23-2015-14:04:04 to 10-23-2015-15:04:04

IDF Under Attack
Daily Report



10-23-2015-14:04:04 to 10-23-2015-15:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.11.184	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2674
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	295
46.19.86.186	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	60
2.54.184.157	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	47
93.172.0.25	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	42
2.54.184.157	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	34
84.108.10.160	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	34
89.139.48.155	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	23
46.19.85.153	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	22
5.102.198.195	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	19
46.19.85.174	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
46.121.74.77	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
46.120.18.15	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
79.182.121.186	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
185.32.179.197	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
79.179.51.101	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
85.65.217.100	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
205.185.134.27	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
94.197.120.180	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.178.155.7	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
212.76.99.38	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
41.237.175.17	Egypt	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
85.65.14.106	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
5.29.177.240	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
79.177.151.97	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.237.20.79	Italy	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
5.22.129.73	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.85.9	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
79.180.152.229	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
62.90.131.54	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.48.185.130	United Arab Emirates	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
204.42.253.2	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	3
94.159.152.35	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
79.179.215.51	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.3.70	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
85.64.179.223	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
94.159.181.201	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
204.42.253.2	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	3
222.186.61.7	China	147.237.76.201	e.atal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
79.180.63.247	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
149.88.181.214	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
109.64.134.134	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
85.65.217.100	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
94.159.181.201	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
37.142.135.13	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
79.180.21.140	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
79.178.155.7	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
176.13.5.175	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.85.174	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.19.85.153	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2

10-23-2015-14:04:04 to 10-23-2015-15:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-23-2015-14:04:04 to 10-23-2015-15:04:04

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	6
66.249.67.200	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
37.143.82.50	147.237.8.24	Netherlands	e.lifestyle.idf	ET SCAN NMAP -sS window 1024	1
212.71.252.159	147.237.0.33	United Kingdom	idf.il	ET SCAN Potential SSH Scan	1
176.12.139.187	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
110.53.152.5	147.237.76.34	China	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
45.63.55.158	147.237.76.177		ncore.idf.il	ET SCAN NMAP -sS window 1024	1
43.229.53.89	147.237.0.35	Japan	akaws.idf.il	ET SCAN Potential SSH Scan	1
37.143.82.50	147.237.8.24	Netherlands	e.lifestyle.idf	ET SCAN NMAP -sS window 4096	1
37.26.147.134	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
139.162.195.220	147.237.76.198	Netherlands	e.yohalan.idf.i	ET SCAN Potential SSH Scan	1
45.33.7.101	147.237.77.121		e.navy.idf.il	ET SCAN Potential SSH Scan	1

10-23-2015-14:04:04 to 10-23-2015-15:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.29.93.32	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	866
213.151.36.118	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	333
66.171.228.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	316
85.64.39.182	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	253
85.65.217.100	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	118
5.102.198.195	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	77
93.168.0.210	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
176.13.15.252	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
77.127.6.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
149.78.102.137	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
85.64.241.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
149.88.242.190	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
93.172.0.25	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
37.24.151.1	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
37.26.146.191	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
100.100.102.20		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	36
93.172.9.170	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
85.27.200.33	Denmark	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
77.126.196.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
82.205.119.171	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
2.54.184.157	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
100.100.33.204		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	32
213.151.37.70	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
89.16.142.24	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
46.19.85.174	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
213.57.239.152	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
149.88.181.214	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
66.249.93.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
2.54.2.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
100.100.33.204		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
37.142.64.81	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
37.142.182.108	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	25
5.28.134.131	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
66.249.93.196	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
100.100.72.222		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	23
100.100.33.204		147.237.0.34	tikshuv.idf.i	drop	First packet isn't SYN	drop	22
46.19.85.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22

10-23-2015-14:04:04 to 10-23-2015-15:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.59.17	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.67.59.17	Block	64
68.180.230.167	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakhal.idf.il/1073-he/nakhal.aspx	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
5.102.207.184	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 5.102.207.184	Block	42
37.26.146.182	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	28
212.179.231.74	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	28
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
109.67.59.17	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	28
82.241.241.24	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gyus	Block	28
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
184.105.139.68	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/	Block	14
66.249.67.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	14
5.29.177.240	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	14
109.65.66.64	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
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	14
157.55.39.255	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
37.26.146.149	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	14
84.228.248.191	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	14
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/1065-he/dover.aspx	Block	14
197.210.217.66	Nigeria	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
109.65.110.26	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
176.12.145.56	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
85.64.80.50	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mfa/terrorism+obstacle+to	Block	14
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx	Block	14
5.102.207.184	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/4/2094.jpg	Block	14
109.66.105.219	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
79.182.98.104	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	14
176.13.5.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
37.46.39.46	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	14
2.52.160.227	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	14
87.68.154.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	14
216.218.206.67	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	14
31.44.139.55	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	14
79.183.212.61	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_pictures.asp	Block	14
176.106.227.184	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	14
66.249.67.200	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
2.54.142.13	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	14
94.159.171.66	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	14
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unknown Parameter siteid in www.aka.idf.il/sites/home/default.asp	None	14
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	14
31.168.173.2	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14

10-23-2015-14:04:04 to 10-23-2015-15:04:04