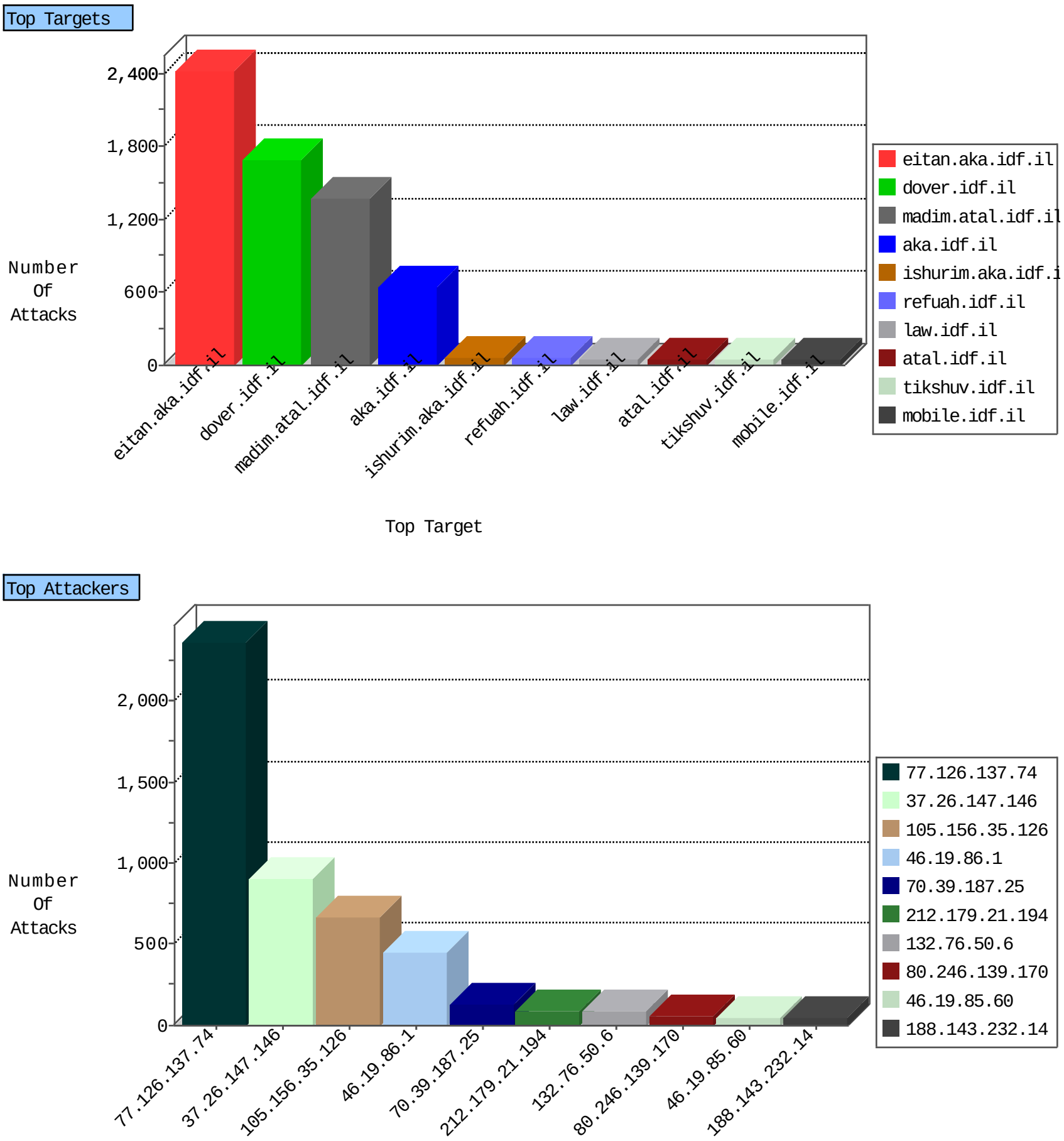
10-25-2015-15:04:09 to 10-25-2015-16:04:09

IDF Under Attack Daily Report



10-25-2015-15:04:09 to 10-25-2015-16:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.53	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	469
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	240
192.198.151.43	Europe	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	185
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	132
80.246.139.170	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	101
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	78
5.28.170.44	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
192.116.127.113	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
5.28.139.186	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	29
132.76.50.6	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	29
46.19.85.60	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	29
109.64.99.220	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	25
129.15.64.252	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	22
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	22
46.19.86.118	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	18
85.64.69.242	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	17
79.178.192.180	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
5.29.55.226	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	16
199.203.215.1	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
79.176.108.139	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
79.178.12.174	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
132.64.171.234	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
37.26.149.217	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
185.32.179.3	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
2.54.154.212	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
176.12.137.127	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
80.74.101.7	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
176.13.23.125	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
5.29.55.226	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
132.66.40.116	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
37.142.68.0	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
87.68.248.153	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
212.143.110.33	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
84.108.236.55	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
194.90.209.199	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
95.86.98.24	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.120.58.60	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
221.121.150.221	Australia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
85.250.137.96	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
109.65.105.29	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
132.70.66.9	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
87.69.17.251	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
37.26.149.224	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
176.12.149.48	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
194.114.146.227	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.23.125	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	3
77.125.93.8	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
93.184.3.154	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
176.13.12.154	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3

10-25-2015-15:04:09 to 10-25-2015-16:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.17.163	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
79.181.196.232	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

10-25-2015-15:04:09 to 10-25-2015-16:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.93.196	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
37.142.64.59	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
189.28.15.187	147.237.76.38	Brazil	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
149.78.80.3	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.66.2.188	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.63.56	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
87.69.207.137	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.43.246	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.179.98.174	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.117.162.127	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.114.91.232	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.184.5	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
132.76.50.6	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.63.56	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.172.133.48	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.65.161.3	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.166.184.140	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

10-25-2015-15:04:09 to 10-25-2015-16:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
105.156.35.126	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	670
70.39.187.25	Satellite Provider	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	131
46.19.85.60	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
2.54.144.234	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
2.54.32.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.12	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
100.100.44.182		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
80.74.101.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
207.232.12.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
2.52.176.224	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
79.182.228.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.92	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
100.100.49.47		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
129.15.64.252	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
85.64.69.242	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
100.100.63.132		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
192.114.105.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
84.108.236.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.182.38.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
82.216.201.63	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.179.133.9	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.26.149.141	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
185.32.179.3	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
176.106.226.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.52.46.27	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.26.147.240	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
134.245.122.86	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.244	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
1.39.14.8	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.179.61.34	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
77.127.247.146	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
172.56.37.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.189	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.13.15.34	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
95.86.119.200	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
79.179.141.100	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.149.142	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	4
93.184.3.154	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.143	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.83.161	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.179.227.81	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
85.250.209.157	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

10-25-2015-15:04:09 to 10-25-2015-16:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.126.137.74	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2366
37.26.147.146	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 37.26.147.146	Block	908
46.19.86.1	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	434
132.76.50.6	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	70
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/894-en/eitan.aspx	Block	53
77.127.134.60	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	42
31.168.83.82	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	28
146.185.234.48	Russian Federation	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 146.185.234.48	Block	28
188.143.232.14	Russian Federation	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 188.143.232.14	Block	28
46.19.86.53	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	28
31.154.148.122	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/tizmoret/faq/default.asp	None	28
109.67.35.45	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/resources/controls/captcha.ashx	Block	28
31.168.66.62	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash	Block	28
2.54.187.78	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	28
192.116.94.214	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	14
66.249.64.244	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	14
79.183.17.58	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	14
2.52.176.224	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
212.179.15.202	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/	Block	14
176.12.146.10	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	14
46.19.86.1	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtMobile in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	14
109.65.63.191	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
5.29.94.94	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	14
66.249.93.158	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyu	Block	14
66.249.64.253	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1302	Block	14
193.203.48.27	Ukraine	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to 147.237.0.19/	Block	14
84.109.229.76	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
2.54.40.104	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cp in www.aka.idf.il/main/giyus/userdetails/updateuserdetails.aspx	None	14
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training	Block	14
5.29.94.94	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/xmlrpc.php	Block	14
109.65.107.15	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	14
66.249.65.181	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	14
194.90.192.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	14
37.26.149.251	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
146.185.234.48	Russian Federation	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/templates/news/news.in.aspx/templates/sendtofriend/sendtofriend.aspx	Block	14
85.64.32.163	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
212.235.124.168	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	14
66.249.67.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	14
188.143.232.14	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/656-en/	Block	14
46.19.86.152	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
66.249.65.188	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	14
203.133.170.9	Korea, Republic of	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
149.78.108.217	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	14
46.19.85.244	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	14
85.65.107.48	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	14
2.54.177.72	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
213.57.245.11	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
66.249.67.89	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-16021-he/dover.aspx	Block	14

10-25-2015-15:04:09 to 10-25-2015-16:04:09