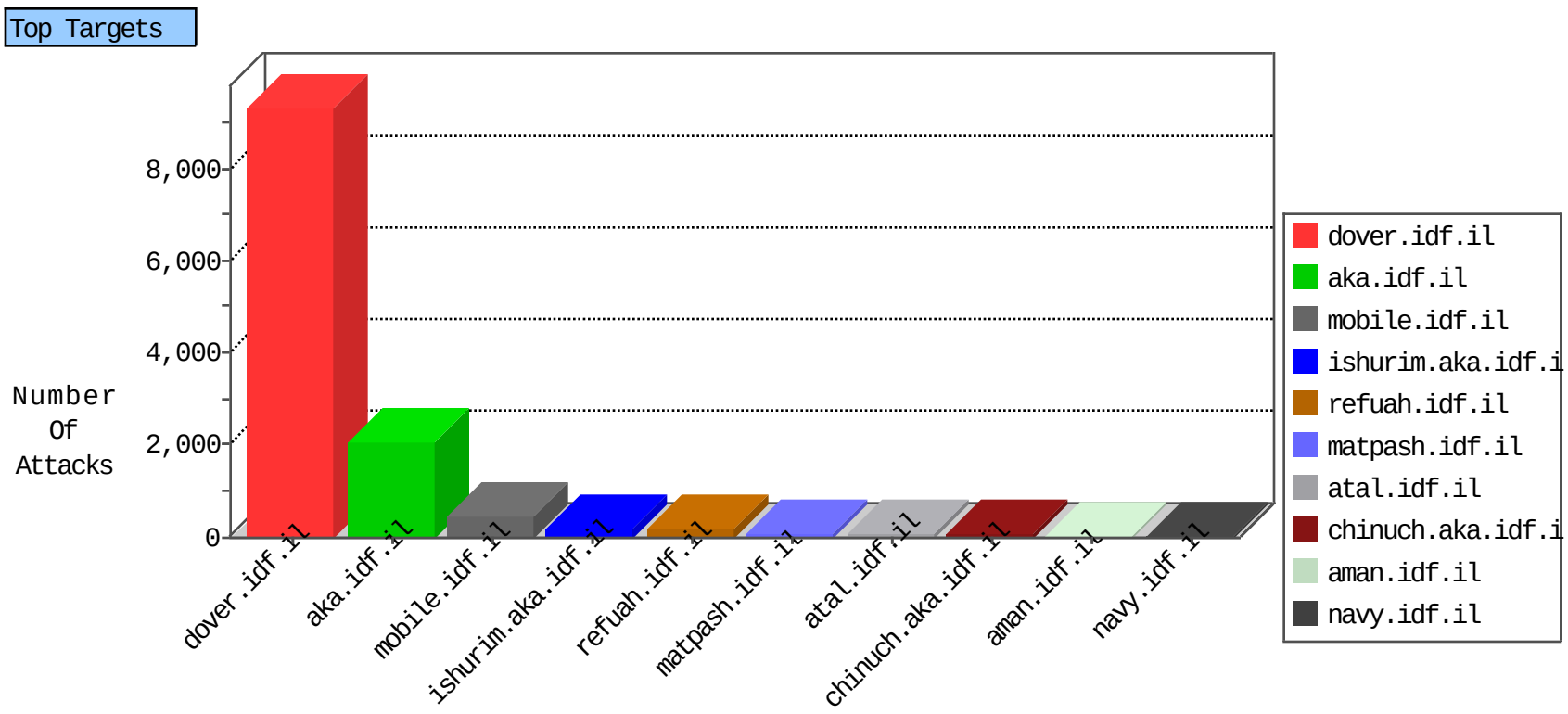
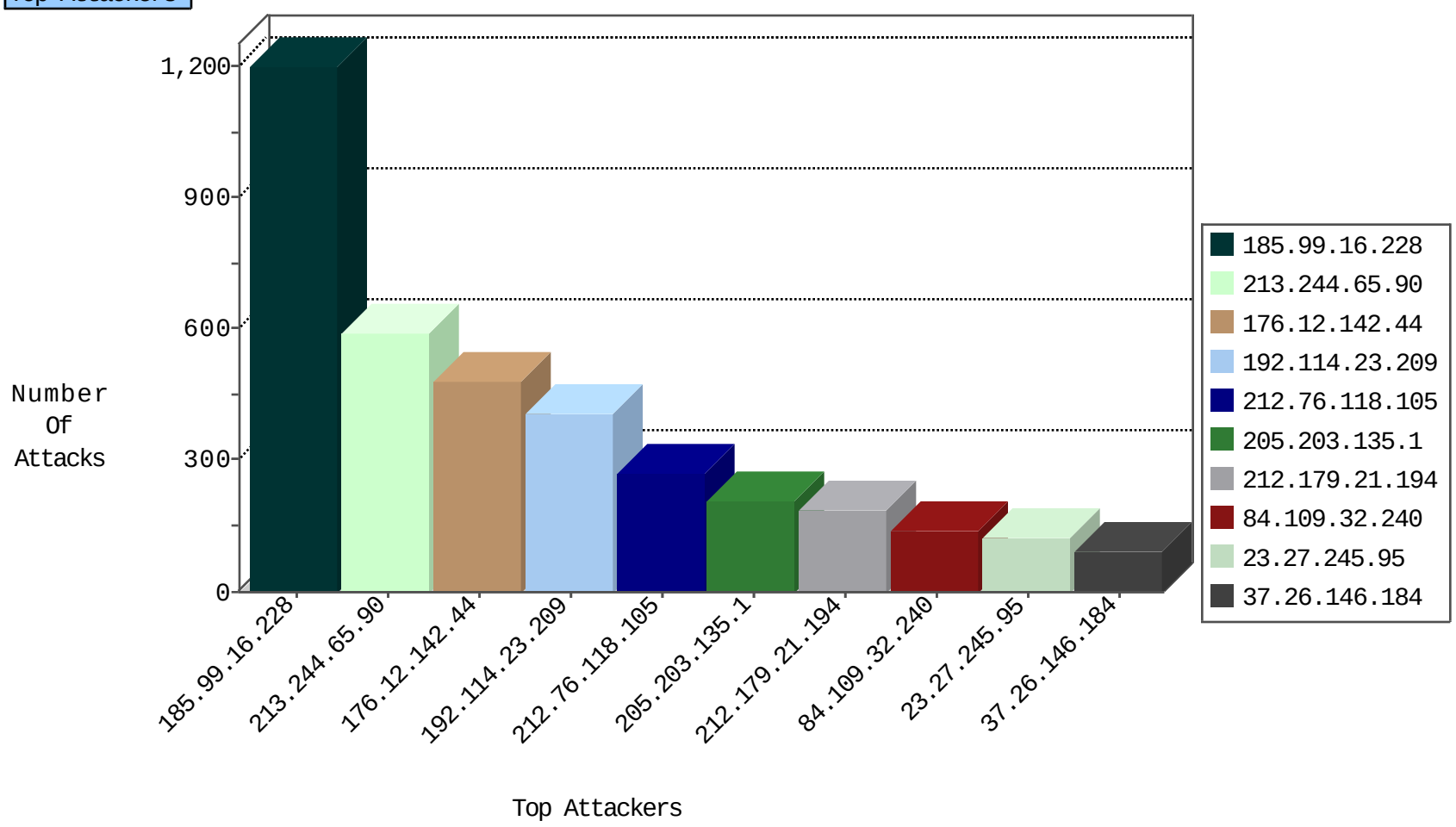
11-01-2015-10:04:09 to 11-01-2015-11:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-01-2015-10:04:09 to 11-01-2015-11:04:09

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.i	SYN Flood full table	drop	910
213.244.65.90	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	474
185.32.179.88	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	467
2.54.158.240	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	222
85.65.197.159	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	36
212.76.113.234	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	36
83.244.55.42	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	SYN Flood full table	drop	30
62.19.27.59	Italy	147.237.77.216	dover.idf.i	SYN Flood full table	drop	21
46.121.247.68	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	21
84.228.232.50	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	19
2.54.152.165	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	16
109.65.28.1	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	16
109.65.20.155	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	15
31.168.13.78	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	15
2.54.182.236	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	15
37.26.147.151	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	15
2.54.151.38	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	12
212.143.3.44	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	12
2.54.129.9	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	11
192.114.23.209	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	11
91.231.192.149	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	11
77.126.235.143	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	10
213.8.118.14	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	10
212.150.214.130	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	10
46.121.79.190	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	10
2.54.31.189	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	10
149.78.37.178	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	10
37.26.147.238	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	9
37.26.147.138	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	9
185.33.114.11	Lebanon	147.237.77.216	dover.idf.i	SYN Flood full table	drop	8
37.26.147.151	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	8
176.13.10.233	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	8
46.120.230.223	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	7
93.173.239.37	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	7
84.94.73.234	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	7
2.54.41.16	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	7
109.67.196.25	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	6
212.235.98.139	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	6
2.54.152.165	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	6
70.208.67.13	United States	147.237.77.216	dover.idf.i	SYN Flood full table	drop	6
37.26.148.136	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	6
176.13.4.97	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	6
176.106.226.7	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	6
199.203.196.185	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	6
0.0.0.0		147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	6
192.114.23.209	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	6
2.52.24.85	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	6
79.183.196.213	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	5
176.106.226.97	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	5
46.19.85.229	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	5

11-01-2015-10:04:09 to 11-01-2015-11:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.143.54.217	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
91.231.192.149	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4

11-01-2015-10:04:09 to 11-01-2015-11:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.52.190.229	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	17
192.198.151.36	147.237.72.167	Europe	ishurim.aka.idf.i	ET SCAN NMAP -sA (2)	2
82.166.3.82	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.179.58	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.179.11.34	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.178.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.127.206.56	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.114.146.227	147.237.72.167	Israel	ishurim.aka.idf.i	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
176.13.8.78	147.237.77.216	Israel	dover.idf.il	INDICATOR-SCAN myscan	1
176.12.145.102	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.160.236.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.250.119.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.136.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.13.22	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.147.86.8	147.237.77.170	United Kingdom	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.178.170.54	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.203.215.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.19.27.59	147.237.77.216	Italy	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.8.78	147.237.77.216	Israel	dover.idf.il	GPL SCAN myscan	1
149.78.237.201	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.68.151.230	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

11-01-2015-10:04:09 to 11-01-2015-11:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.99.16.228		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1203
213.244.65.90	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	588
192.114.23.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	395
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	209
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	177
23.27.245.95	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	123
82.166.3.82	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	87
84.94.32.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	81
176.13.11.245	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	76
100.100.59.35		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	72
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
77.127.14.93	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
79.179.141.146	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
2.54.152.165	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
46.19.86.110	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
2.54.187.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
199.203.53.3	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
2.52.3.105	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
46.19.85.206	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	48
66.249.81.218	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
46.19.86.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
62.219.230.90	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
212.143.57.184	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
46.19.85.194	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	42
91.231.192.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
79.178.141.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
173.56.28.176	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
83.244.55.42	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
37.76.198.126	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	41
176.13.19.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
68.196.94.231	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
37.26.146.177	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
5.102.254.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
54.244.22.103	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	38
62.0.102.6	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
79.176.28.95	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
37.26.146.158	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
212.25.102.57	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
37.26.146.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
5.29.205.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
178.135.109.9	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
2.54.41.16	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
79.178.126.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30

11-01-2015-10:04:09 to 11-01-2015-11:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.142.44	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 176.12.142.44	Block	465
212.76.118.105	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.76.118.105	Block	255
84.109.32.240	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 84.109.32.240	Block	120
37.26.146.184	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	90
176.13.5.153	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	60
46.19.85.218	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	59
46.121.79.190	Israel	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/1518-he/refuah.aspx parameter ctl00$ContentPlaceHolder1$txtContent	Block	45
176.13.5.86	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	45
40.77.167.90	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	30
2.54.160.108	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	30
62.90.184.141	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/sachar	Block	30
80.246.136.144	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	30
217.132.50.2	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	30
79.178.126.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	30
70.39.157.196	United States	147.237.76.200	eitan.aka.idf.il	Unknown Parameter &y in www.eitan.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	30
109.67.21.56	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	30
46.19.85.25	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	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
2.54.187.39	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	25
62.219.175.10	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	15
84.228.168.212	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl67 in www.aka.idf.il/main/sachar/payslips.aspx	None	15
80.74.105.107	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
46.19.85.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/kio	Block	15
192.115.180.11	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	15
176.12.150.251	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	15
68.64.169.226	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	15
151.80.31.112	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catI.. in www.aka.idf.il/main/giyus/general.aspx	None	15
212.143.3.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/updateuserdetails.aspx	Block	15
84.94.182.42	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	15
46.19.85.67	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	15
180.76.15.152	China	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	15
74.82.47.3	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	15
66.249.75.62	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/421-he/patzar.aspx	Block	15
176.12.142.10	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
85.250.124.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	15
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.13	Block	15
80.246.136.41	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	15
194.114.146.227	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	15
40.77.167.91	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	15
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/sites/home/default.asp	None	15
2.54.161.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	15
157.55.39.39	United States	147.237.72.166	aka.idf.il	Unauthorized Method GET for www.aka.idf.il/kamlar/contact/default.asp	Block	15
66.249.67.138	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	15
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 106 cookies	Block	15
84.108.4.145	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	15
46.19.85.67	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	15
185.120.126.2		147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
79.177.19.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	15
66.249.78.47	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/templates/imagevideogallerylobby/imagevideogallerylobby.aspx	Block	15

11-01-2015-10:04:09 to 11-01-2015-11:04:09