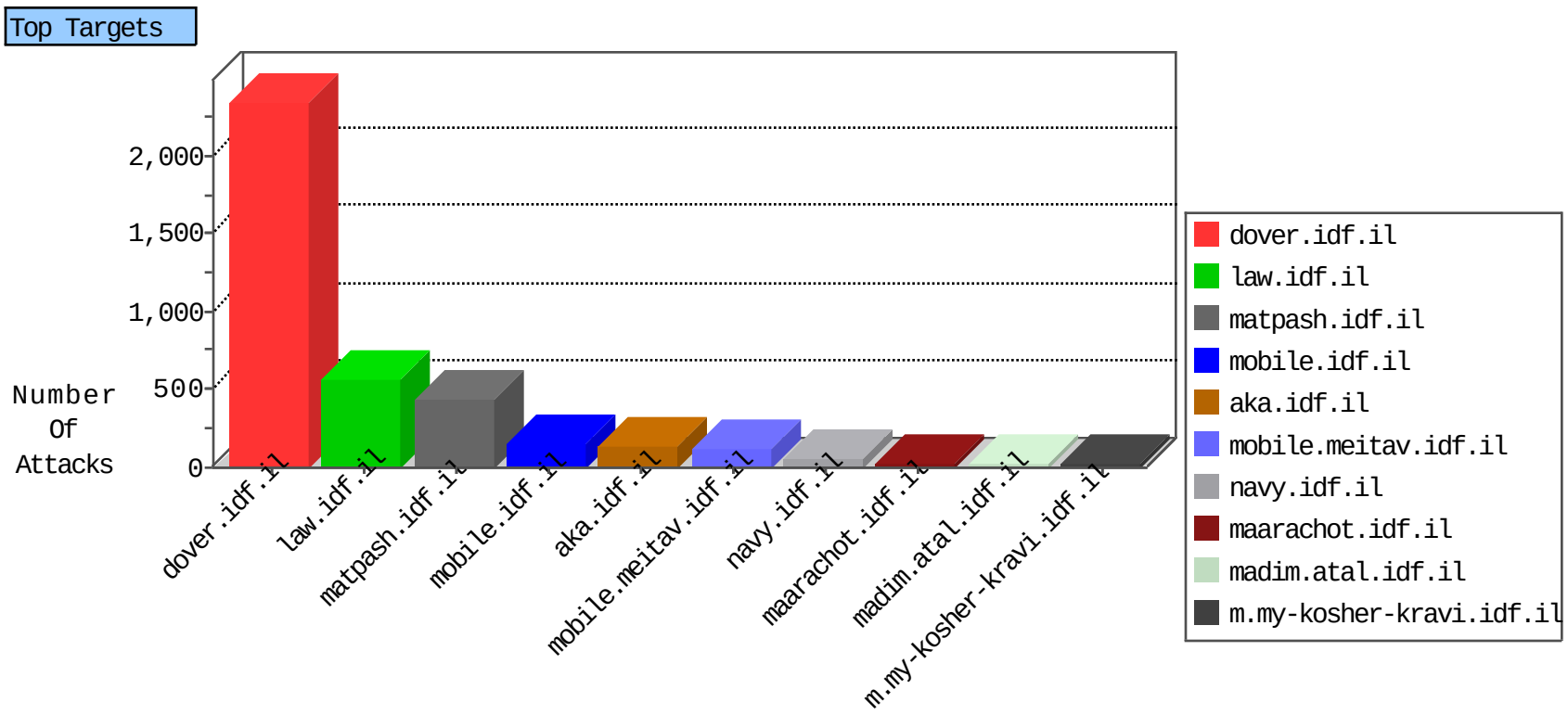
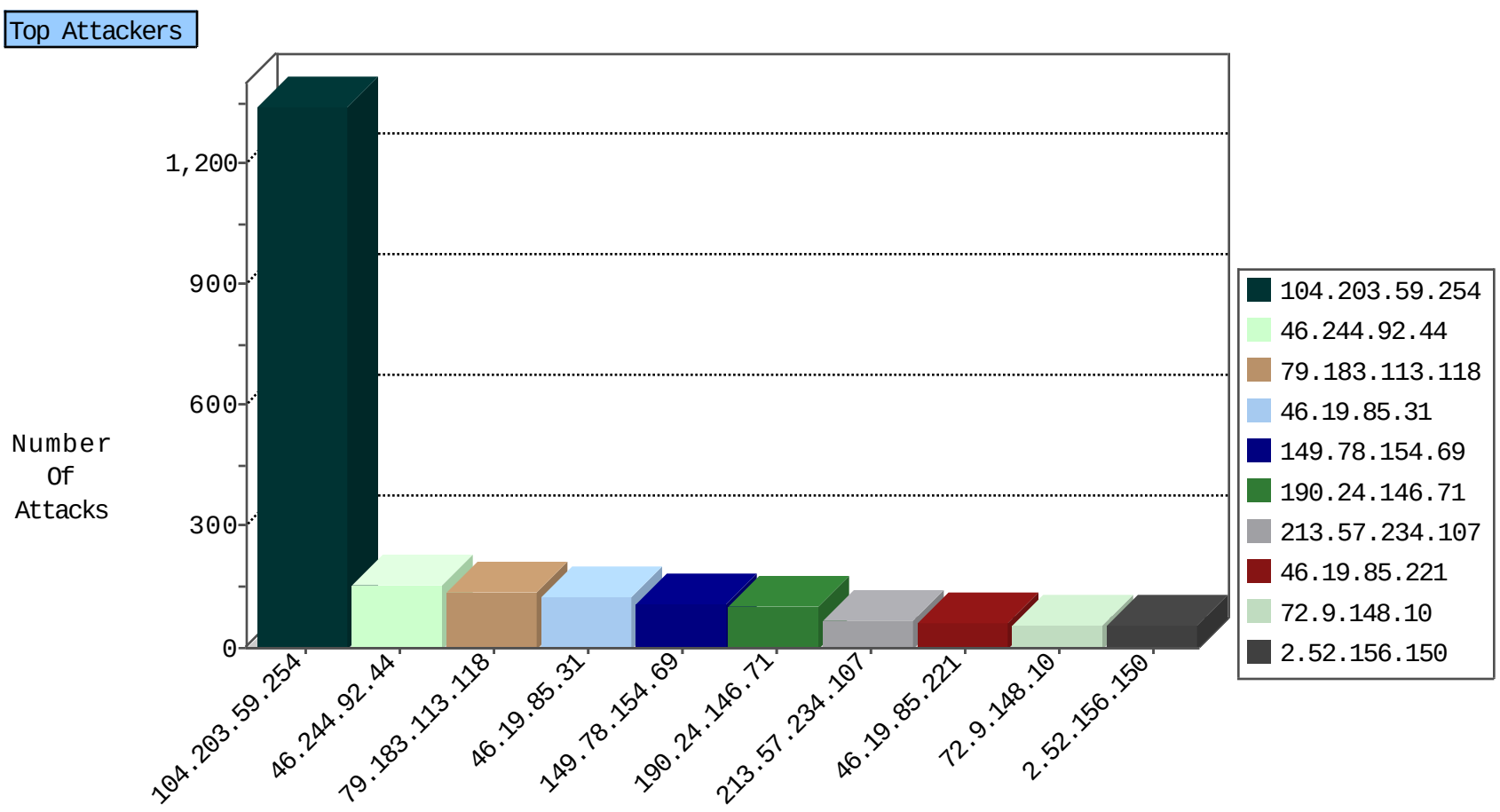
10-27-2015-00:04:04 to 10-27-2015-01:04:04

IDF Under Attack
Daily Report

Top Targets



Top Attackers



10-27-2015-00:04:04 to 10-27-2015-01:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.143.75	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	33
146.137.70.71	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
46.19.86.116	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
37.26.149.230	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	9
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
5.22.131.249	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
5.29.203.75	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
222.186.21.166	China	147.237.76.30	himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
46.19.85.109	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.19.85.250	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.85.109	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
223.67.116.11	China	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
89.248.172.98	Netherlands	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
146.185.239.100	Russian Federation	147.237.0.34	tikshuv.idf.il	block-sp-traf1	drop	1
5.8.66.78	Russian Federation	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.98	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
5.8.66.78	Russian Federation	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
134.173.28.81	United States	147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	1

10-27-2015-00:04:04 to 10-27-2015-01:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
104.203.59.254	United States	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
104.203.59.254	United States	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
104.203.59.254	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	34
104.203.59.254	United States	147.237.77.74	law.idf.il	0854: HTTP: upload* Access	Block	12
104.203.59.254	United States	147.237.77.176	matpash.idf.il	0854: HTTP: upload* Access	Block	12
104.203.59.254	United States	147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Block	11
104.203.59.254	United States	147.237.77.74	law.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
82.158.30.199	Spain	147.237.77.176	matpash.idf.il	C008: HTTP: Xenu UserAgent	Block	1

10-27-2015-00:04:04 to 10-27-2015-01:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	**Signature**	**Count**

10-27-2015-00:04:04 to 10-27-2015-01:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.244.92.44	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	156
79.183.113.118	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	139
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	108
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	100
213.57.234.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
46.19.85.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
2.52.156.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
188.161.104.122	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
84.228.59.6	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
85.168.179.177	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
1.129.96.184	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
46.19.86.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
87.68.72.6	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	22
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.102.8.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
213.61.248.251	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
179.197.229.67	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
54.72.73.168	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	14
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
109.160.221.220	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
174.22.9.129	United States	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	13
206.214.246.4	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
139.162.216.112	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.116	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
202.45.119.33	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.102.8.178	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.10.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.52.143.75	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
77.127.135.43	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.214.56.13	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.54.157.173	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.149.230	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
40.77.167.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
80.40.134.104	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.65.24.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.29.224.174	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
176.13.0.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
149.160.219.32	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
104.203.59.254	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 104.203.59.254	Block	406
104.203.59.254	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 104.203.59.254	Block	350
104.203.59.254	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 104.203.59.254	Block	329
46.19.85.31	Israel	147.237.76.39	mobile.meitav.idf.il	Cookie Tampering on cookie .ASPNETAUTH: Expected 01022617FBD451DED208FE268F3CA054DED20800093300310038003100360037003500310037000012F00FF, Observed 0102CAFE5A3E8FDCD208FECA769C0992DCD20800093300310038003100360037003500310037000012F00FF	None	126
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
2.54.170.100	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	28
31.168.136.250	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	28
104.203.59.254	United States	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 104.203.59.254	Block	28
176.13.6.197	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	28
104.203.59.254	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	28
2.54.157.173	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	28
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
109.186.188.144	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/0/310.pdf -----	Block	14
104.203.59.254	United States	147.237.77.74	law.idf.il	Admin Blocking	Block	14
84.95.110.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
192.126.156.33	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/homepage/	Block	14
50.97.52.130	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/&usg=alkjrhjrgbac-lfq54refbbjysrc1kragq	Block	14
104.203.59.254	United States	147.237.77.176	matpash.idf.il	Multiple Admin Blocking from 104.203.59.254	Block	14
89.138.65.171	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 66.249.78.173	Block	14
176.12.143.141	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	14
17.138.54.77	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	14
104.203.59.254	United States	147.237.77.74	law.idf.il	Multiple Admin Blocking from 104.203.59.254	Block	14
84.95.110.139	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEntrance in madim.atal.idf.il/1088-he/meretz.aspx	Block	14
197.41.94.55	Egypt	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	14
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	14
93.173.142.204	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	14
68.180.229.121	United States	147.237.76.200	eitan.aka.idf.il	Unknown Parameter &SortDir in www.eitan.aka.idf.il/1103-he/eitan.aspx	None	14
176.12.143.141	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.12.143.141	None	14
87.68.72.6	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
66.249.67.143	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	14
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/5/size220x0/17365.jpg	Block	14
94.23.30.222	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
37.239.0.87	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	14
87.69.184.104	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
217.12.204.95	Ukraine	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/9/	Block	14
94.141.38.16	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation PageNum in www.law.idf.il/327-en/patzar.aspx	Block	14
79.176.150.171	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	14
188.143.232.16	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1283-en/dover.aspx	Block	14
104.203.59.254	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/fck/	Block	14
89.138.65.171	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	14

10-27-2015-00:04:04 to 10-27-2015-01:04:04