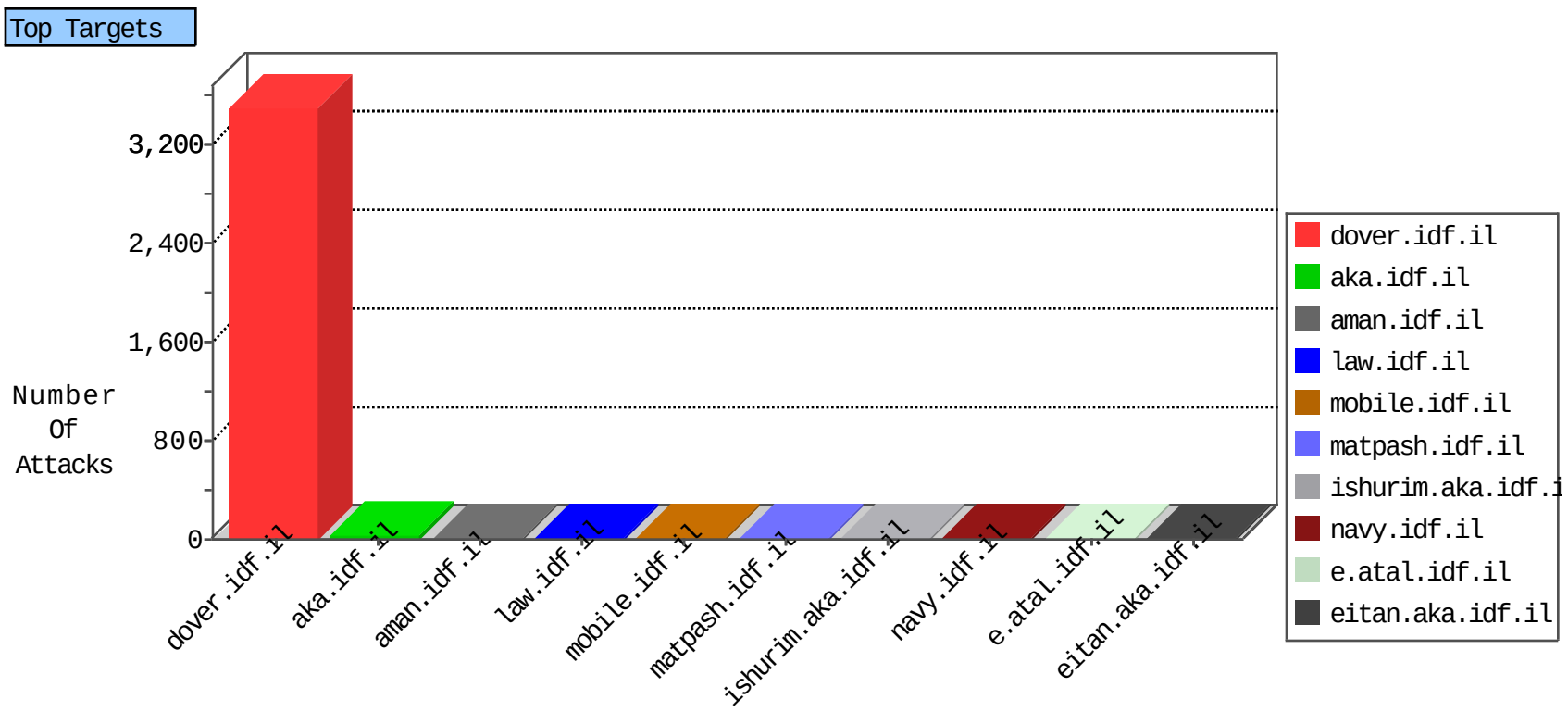
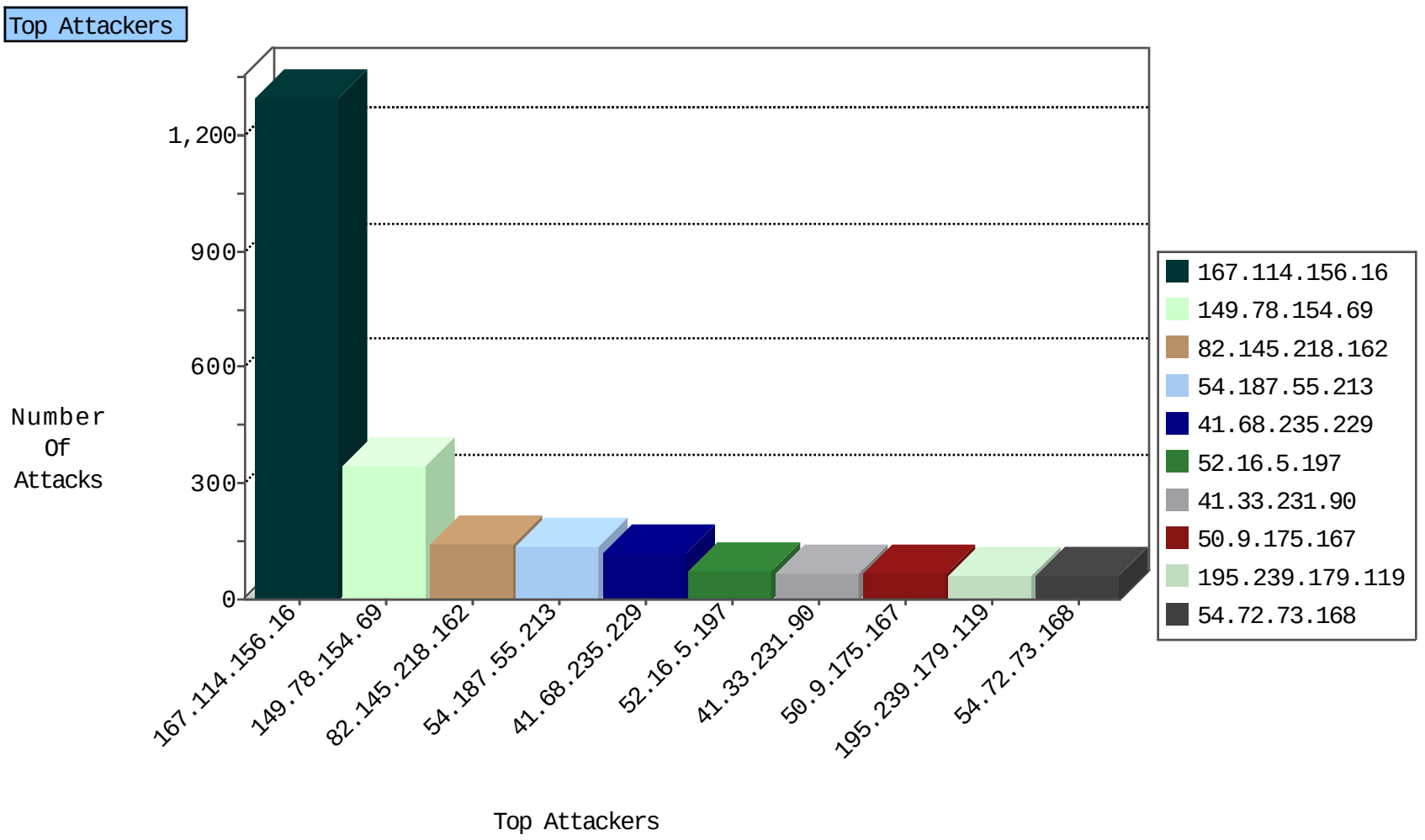
11-02-2015-05:04:07 to 11-02-2015-06:04:07

IDF Under Attack
Daily Report

Top Targets



Top Attackers



11-02-2015-05:04:07 to 11-02-2015-06:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.75.68	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2861
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2337
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	721
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	6
85.64.119.137	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
75.166.221.21	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
185.32.179.187	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
141.212.122.169	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1

11-02-2015-05:04:07 to 11-02-2015-06:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-02-2015-05:04:07 to 11-02-2015-06:04:07

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	9
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.69.76	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.69.84	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
61.188.189.8	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
210.61.150.154	147.237.76.200	Taiwan	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1
50.87.144.145	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
188.240.46.86	147.237.8.27	Romania	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.8.66.101	147.237.77.179	Russian Federation	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
119.10.8.133	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
103.232.35.106	147.237.72.217	Hong Kong	e.idf.il	ET SCAN NMAP -sS window 1024	1
61.244.49.137	147.237.77.212	Hong Kong	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
61.188.189.8	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
61.188.189.8	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
210.61.150.154	147.237.76.200	Taiwan	eitan.aka.idf.il	ET SCAN NMAP -sS window 2048	1
61.188.189.8	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
185.82.201.17	147.237.77.216		dover.idf.il	ET DOS SSL Bomb DoS Attempt	1
103.232.35.106	147.237.72.217	Hong Kong	e.idf.il	ET SCAN NMAP -sS window 3072	1
100.33.159.233	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
61.244.49.137	147.237.8.46	Hong Kong	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
61.188.189.8	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
210.61.150.154	147.237.76.200	Taiwan	eitan.aka.idf.il	ET SCAN NMAP -sS window 3072	1

11-02-2015-05:04:07 to 11-02-2015-06:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	346
82.145.218.162	Europe	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	142
54.187.55.213	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	134
41.68.235.229	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	121
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	65
50.9.175.167	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	65
195.239.179.119	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	60
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	58
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	57
181.171.218.173	Argentina	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	56
205.203.135.1	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	54
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	54
2.54.155.244	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	47
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
212.179.21.194	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
46.19.86.1	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29
2.54.47.45	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
37.26.149.217	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
151.80.31.112	Italy	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
99.231.51.115	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
46.19.86.243	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
104.231.116.185		147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
75.166.221.21	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
66.249.78.159	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.121.193.57	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
66.102.8.233	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.78.173	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
198.58.102.155	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
40.77.167.13	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
216.121.135.123	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
173.180.3.196	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
79.178.112.130	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
66.249.78.159	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
70.196.135.227	United States	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
141.164.162.2	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
70.196.135.227	United States	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid sequence number	monitor	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop		drop	9
68.190.249.150	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
207.46.13.180	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
66.102.8.243	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
54.244.22.103	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
157.55.39.248	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
66.102.7.226	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
93.173.232.157	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
66.102.8.238	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.121.246.26	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	4
54.227.89.194	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
176.228.214.151	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	3
176.228.214.151	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	3
54.205.77.224	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
54.211.215.47	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
79.183.144.61	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
184.72.152.246	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
95.35.142.252	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
77.126.229.195	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
79.177.150.38	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
109.66.29.7	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
54.91.130.61	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
91.231.192.149	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
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	2
176.228.214.151	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
149.88.31.247	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
217.132.50.199	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
176.12.140.49	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
54.145.183.23	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
92.47.112.59	Kazakstan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
75.166.221.21	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
2.52.172.238	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
149.88.72.234	Israel	147.237.76.86	navy.idf.il	Cookie Tampering on cookie __atrfs: Expected ab/	None	1
80.246.136.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
176.13.6.121	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
54.161.128.99	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
184.73.15.230	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
37.187.114.171	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to /xmii/illuminator	Block	1
157.55.39.52	United States	147.237.72.166	aka.idf.il	Unknown Parameter pageNum in aka.idf.il/patzar/klali/default.asp	None	1
85.250.51.8	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Unknown SSL Session	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
54.166.98.113	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
108.89.134.115	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-em-dover.aspx	Block	1
66.249.74.96	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/coordinationgaza/news_gaza/archiv/pages/agregatim25456.aspx	Block	1
185.32.179.165	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
157.55.39.245	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
91.231.192.149	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1
79.183.144.61	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
66.249.75.54	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/1078-6106-he/patzar.aspx	Block	1
195.239.179.119	Russian Federation	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
176.12.136.235	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1

11-02-2015-05:04:07 to 11-02-2015-06:04:07