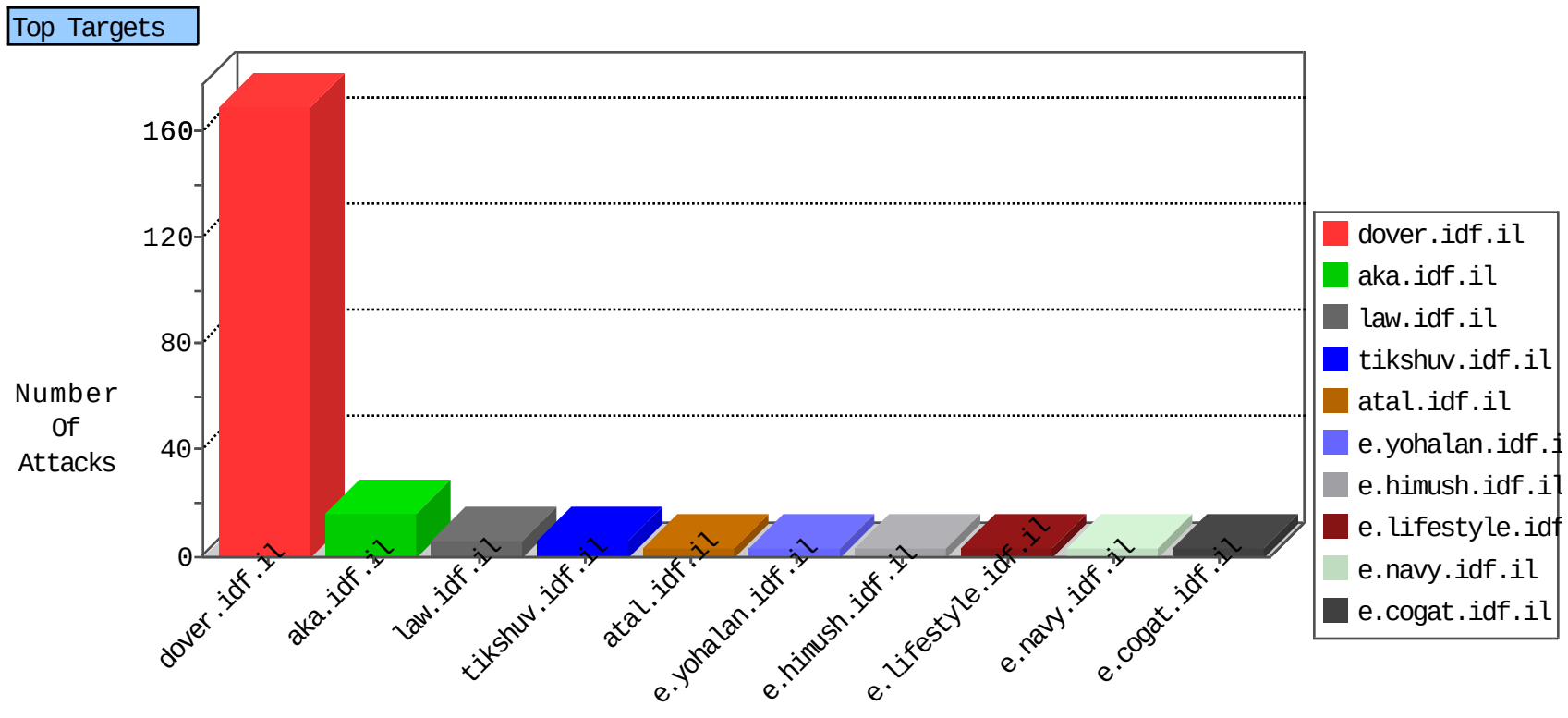
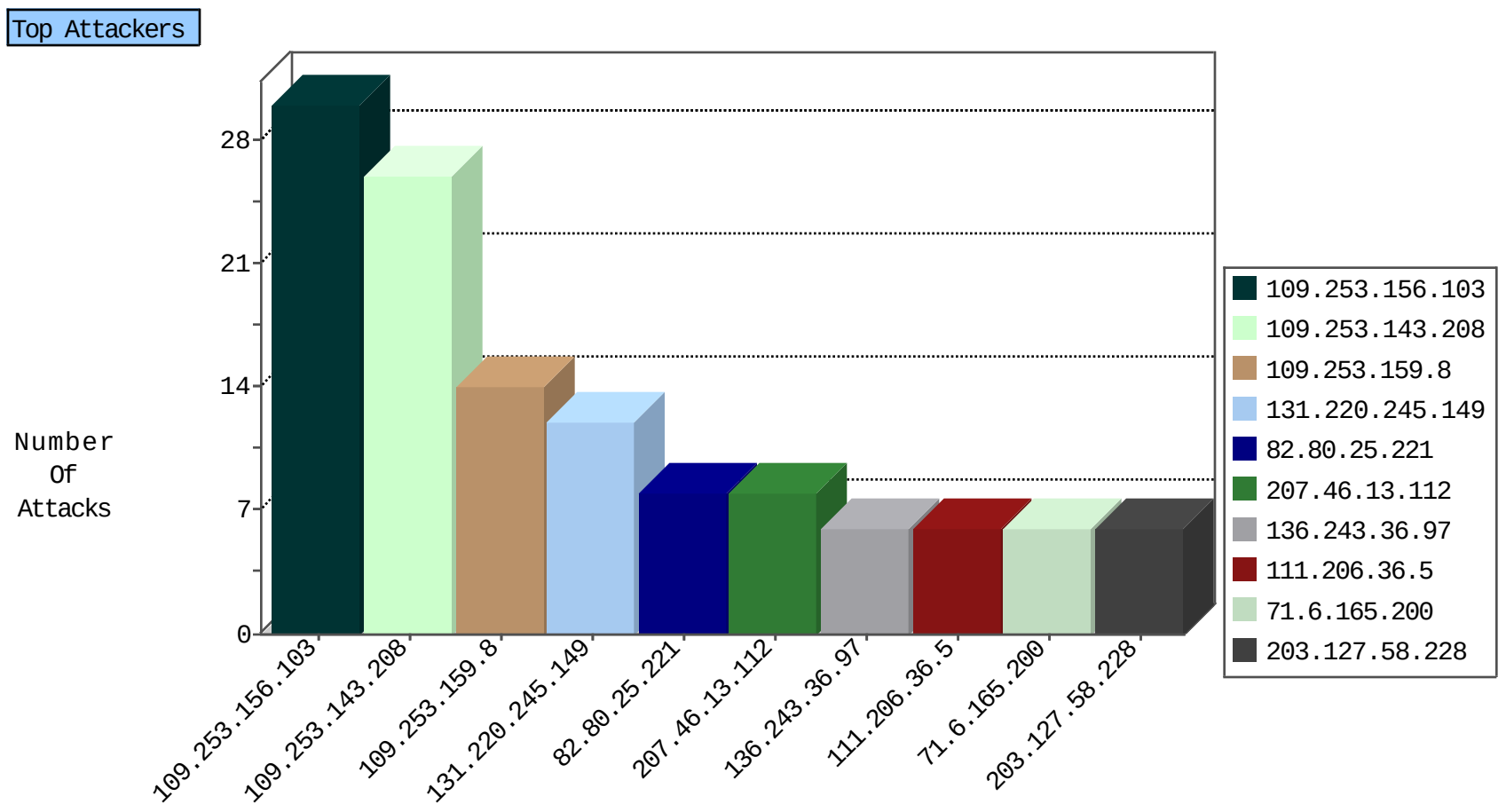
03-31-2015-03:03:07 to 03-31-2015-04:03:07

IDF Under Attack
03-31-2015-03:03:07

Top Targets



Top Attackers



03-31-2015-03:03:07 to 03-31-2015-04:03:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
23.95.248.132	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1

03-31-2015-03:03:07 to 03-31-2015-04:03:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
85.250.146.221	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
77.127.132.2	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
188.138.9.50	Germany	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	2
188.138.9.50	Germany	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	2
131.220.245.149	Germany	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
175.44.5.185	China	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
85.25.43.94	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
23.95.43.76	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
37.130.227.133	United Kingdom	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1

03-31-2015-03:03:07 to 03-31-2015-04:03:07

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	8
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
2.54.32.39	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
27.50.132.60	China	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 4096	1
218.240.7.91	China	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
193.107.16.206	Russian Federation	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
157.55.39.132	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
104.43.14.101		147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1
104.43.14.101		147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.64	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
221.131.111.130	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
218.240.7.91	China	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
27.50.132.60	China	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
157.55.39.227	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
128.61.240.66	United States	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
104.43.14.101		147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.64	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
221.131.111.130	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

03-31-2015-03:03:07 to 03-31-2015-04:03:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
109.253.156.103	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.143.208	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
109.253.159.8	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
131.220.245.149	Germany	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
111.206.36.5	China	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
207.46.13.16	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
207.46.13.112	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
220.255.1.108	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
203.127.58.228	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
220.255.1.152	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
68.180.228.117	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
136.243.36.97	Germany	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
157.55.39.6	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
157.55.39.42	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
203.127.96.217	Singapore	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.14	United States	147.237.77.61	e.cogat.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
188.138.17.205	France	147.237.76.199	e.nakchal.idf.i	Geo-location inbound enforcement	Geo-location enforcement	drop	1
141.212.122.16	United States	147.237.76.199	e.nakchal.idf.i	Geo-location inbound enforcement	Geo-location enforcement	drop	1
190.226.78.192	Argentina	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1
141.212.122.17	United States	147.237.76.200	eitan.aka.idf.i		drop	drop	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	1
141.212.122.11	United States	147.237.76.34	yohalan.idf.il		drop	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
136.243.36.97	Germany	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
188.165.15.196	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.196	Block	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
79.179.26.65	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.160	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/news/kaml	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/asp/rec.asp	Block	1
109.66.176.55	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
74.214.37.228	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//newsite/english/main.stm	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	1
198.204.249.34	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/default.aspx	Block	1
136.243.36.97	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan	Block	1
84.108.86.96	Israel	147.237.72.166	aka.idf.il	Unknown Parameter q in www.aka.idf.il/main/giyus/login.aspx	None	1
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	1
171.96.178.82	Thailand	147.237.77.74	law.idf.il	Distributed Unknown HTTP Request Method	Block	1
125.209.235.184	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm	Block	1
74.214.37.228	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 74.214.37.228	Block	1
36.69.182.153	Indonesia	147.237.77.74	law.idf.il	Distributed Unknown HTTP Request Method	Block	1
207.46.13.112	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
136.243.36.97	Germany	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
84.228.41.17	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
66.249.78.240	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
181.54.159.59	Colombia	147.237.77.74	law.idf.il	Unknown HTTP Request Method COOK in URL www.law.idf.il/14-en/patzar.aspx	Block	1
125.212.121.205	Philippines	147.237.77.74	law.idf.il	Distributed Unknown HTTP Request Method	Block	1
74.214.37.228	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/	Block	1
37.187.93.152	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/	Block	1
207.46.13.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training	Block	1
157.55.39.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
87.68.92.252	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
131.220.245.149	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//894-en/idfgdover.aspx	Block	1
75.37.29.229	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
54.159.134.239	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2000/november/1.stm	Block	1
216.218.206.66	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
157.55.39.130	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
93.172.160.36	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$txtPassword in www.aka.idf.il/main/sachar/	None	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1