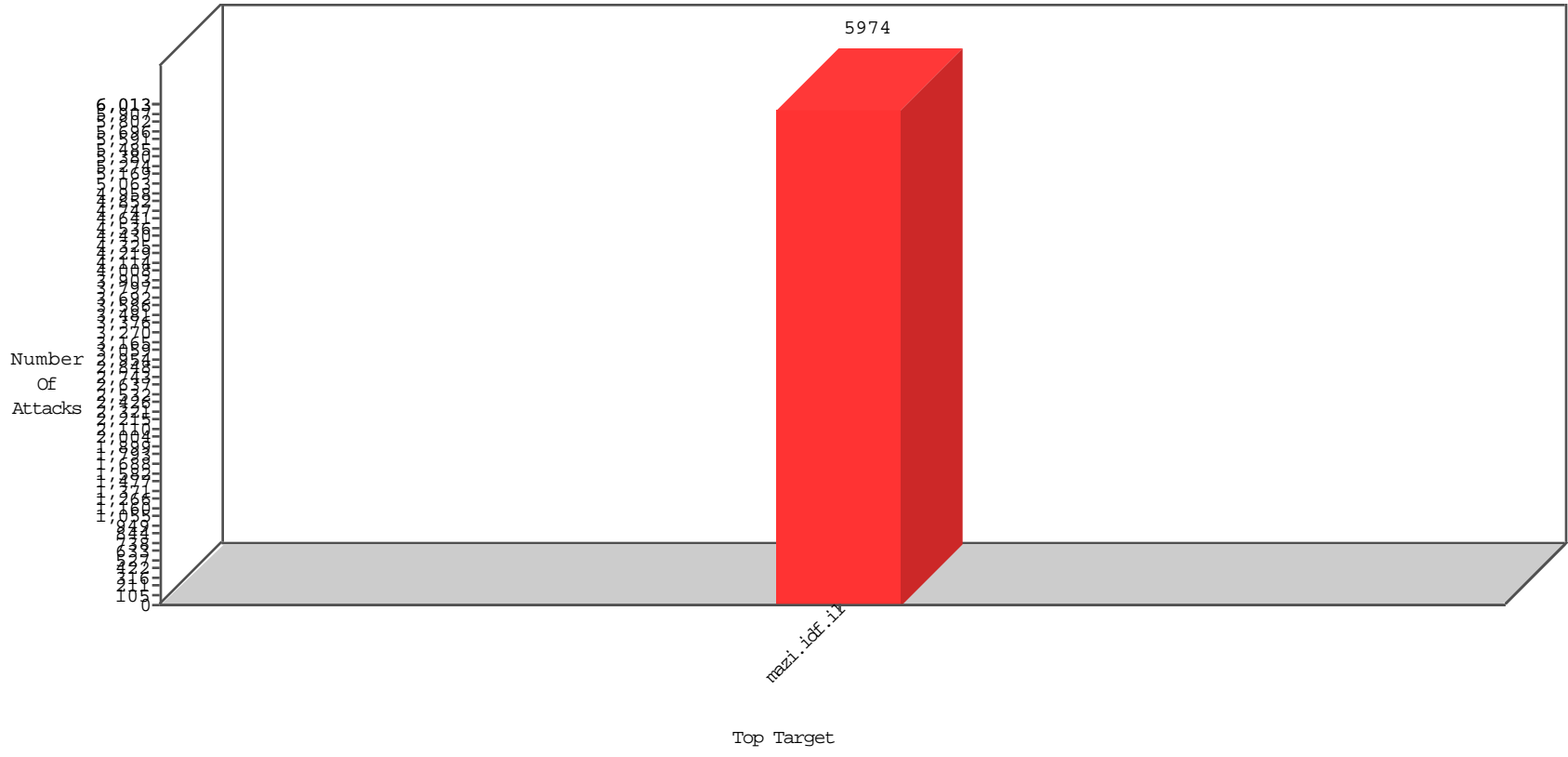


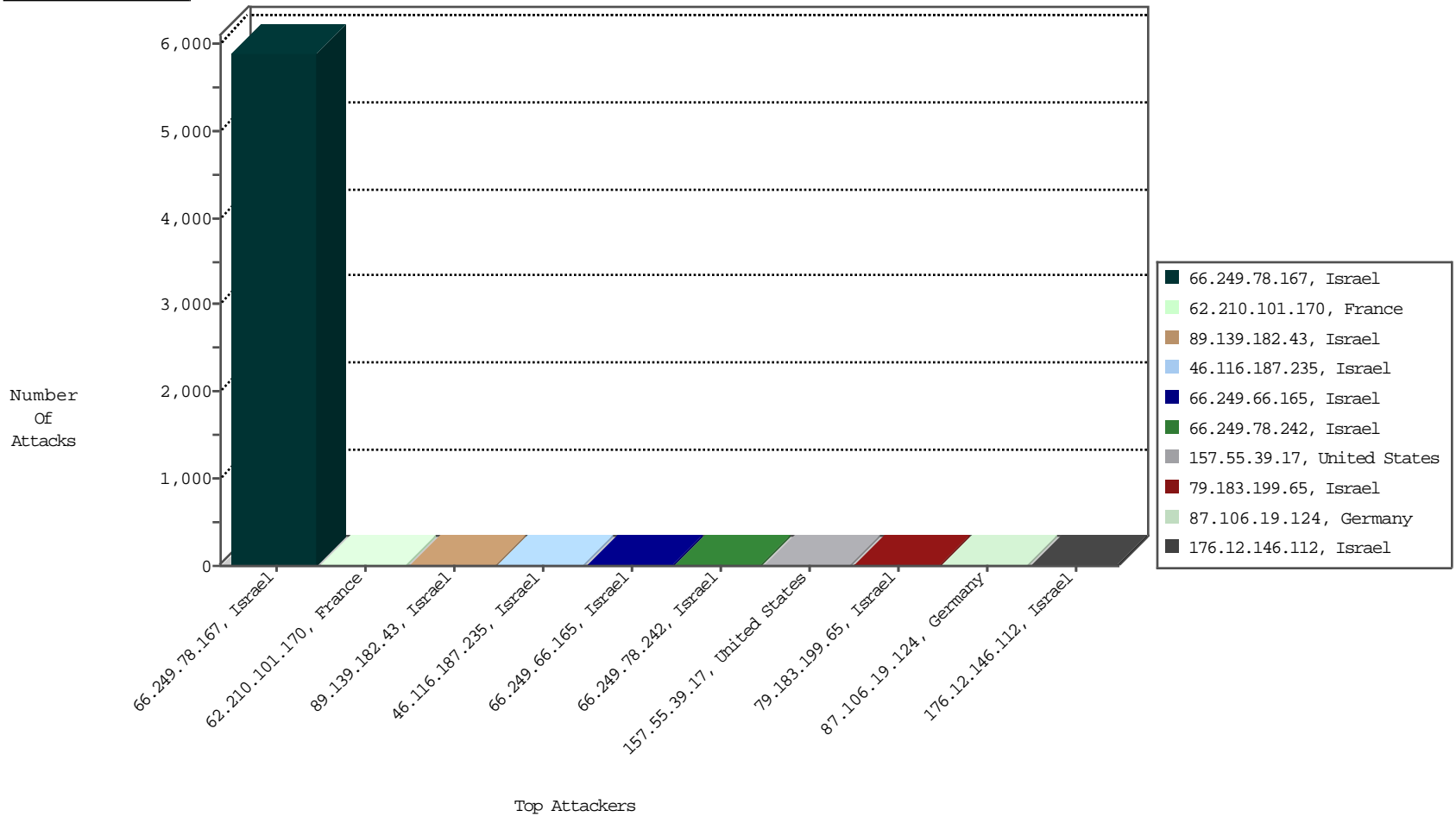
# Focused IP Under Attack Daily Report



## Top Targets



## Top Attackers



12-12-2015 to 12-13-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
66.249.78.167	Israel	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	5912
146.185.239.100	Russian Federation	147.237.77.17	mazi.idf.il	block-sp-trafl	drop	BBL-Frankfurt	1

12-12-2015 to 12-13-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
188.165.15.32	France	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.181	France	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	1

## Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
49.114.225.228	China	147.237.77.17	mazi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
128.199.175.106	Singapore	147.237.77.17	mazi.idf.i	ET DROP Spamhaus DROP Listed Traffic Inbound	1
94.102.60.89	Netherlands	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
90.207.0.33	United Kingdom	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	81
79.180.96.214	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	25
77.126.31.172	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
5.102.254.197	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	18
79.180.96.214	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	16
79.177.207.145	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
156.172.249.167		147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
84.228.54.197	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
85.65.103.23	Israel	147.237.77.17	mazi.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
188.120.148.158	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
185.3.144.157	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
207.241.226.39	United States	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	5
185.3.146.236	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.53	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
223.62.67.141	Korea, Republic of	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
213.57.130.162	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.26.147.181	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence		alert	4
79.180.4.223	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
37.26.147.181	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence		monitor	4
46.19.85.53	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
2.54.57.77	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
46.19.85.95	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
84.109.112.108	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
157.55.39.240	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
80.246.130.26	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
176.12.146.184	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.147.181	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
81.17.16.212	Switzerland	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
208.115.113.91	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
79.178.6.213	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	alert	1
184.105.139.99	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.117.217.160	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
157.55.39.17	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.86.155	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
94.228.34.251	United Kingdom	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
84.109.112.108	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
169.229.3.90	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.170	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
131.253.25.171	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.254	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
84.228.203.129	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.26.147.181	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
81.17.16.212	Switzerland	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
79.178.6.213	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
184.105.247.207	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
66.249.66.40	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
157.55.39.117	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.86.166	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
109.65.108.157	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
80.178.136.122	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1

## Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
89.139.182.43	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	4
62.210.101.170	France	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 62.210.101.170	Block	3
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	3
46.116.187.235	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	2
66.249.78.167	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/ Û..Û^Û,Ø¹	Block	1
207.46.13.90	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/templates/shared/usercontrols/vodchannel/	Block	1
157.55.39.95	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
66.249.66.134	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/700-he/bayabashaarchive.aspx	Block	1
5.141.228.190	Russian Federation	147.237.77.17	mazi.idf.i	Parameter Type Violation lang in mazi.idf.il/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
104.131.147.112	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5187-he/igf.aspx	Block	1
84.111.216.70	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/Û..Û^Û,Ø¹	Block	1
66.249.66.165	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/2061.jpg	Block	1
176.12.146.112	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 176.12.146.112	Block	1
157.55.39.17	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/4054-he/igf.aspxÃfÃçÃèÃéÃâÃçÃ?	Block	1
46.116.187.235	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
79.180.4.223	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3848-5183-he/igf.aspx	Block	1
66.249.78.181	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/vodchannel/	Block	1
207.46.13.106	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/"_	Block	1
157.55.39.156	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
66.249.66.165	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 66.249.66.165	Block	1
37.142.109.35	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/ufi/reaction/	Block	1
109.186.154.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
85.93.91.84	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files	Block	1
76.26.44.151	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
66.249.66.169	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/robots.txt	Block	1
176.12.146.112	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/hi	Block	1
157.55.39.17	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/templates/shared/usercontrols/vodchannel/	Block	1
95.32.202.176	Russian Federation	147.237.77.17	mazi.idf.i	Parameter Type Violation folderid in mazi.idf.il/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
79.183.199.65	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
157.55.39.216	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/14-5475-he	Block	1
66.249.66.165	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
149.88.148.16	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
87.106.19.124	Germany	147.237.77.17	mazi.idf.i	Admin Blocking	Block	1
77.237.138.202	Czech Republic	147.237.77.17	mazi.idf.i	Unauthorized Method HEAD for /	Block	1
66.249.66.189	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/Û..Û^Û,Ø¹	Block	1
183.79.219.168	Japan	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/robots.txt	Block	1
157.55.39.36	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
62.210.101.170	France	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/feed	Block	1
95.175.35.73	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 95.175.35.73	Block	1
79.183.199.65	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/xmlrpc.php	Block	1
66.249.78.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
157.55.39.240	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/"_	Block	1
66.249.66.165	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
46.116.187.235	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 46.116.187.235	Block	1
149.88.160.137	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5216-he/igf.aspx	Block	1
87.106.19.124	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/admin	Block	1
79.178.6.213	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/2061.jpg	Block	1