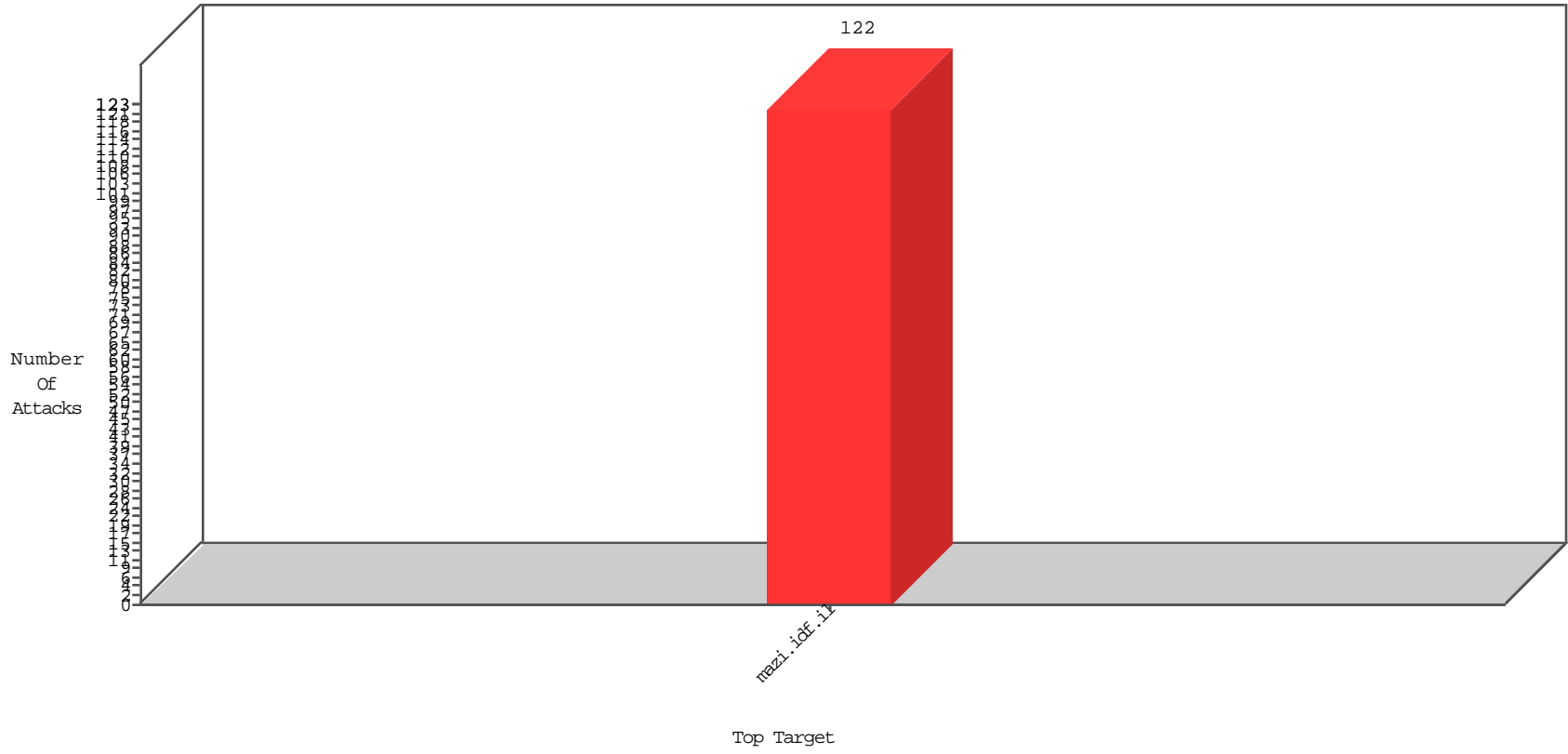


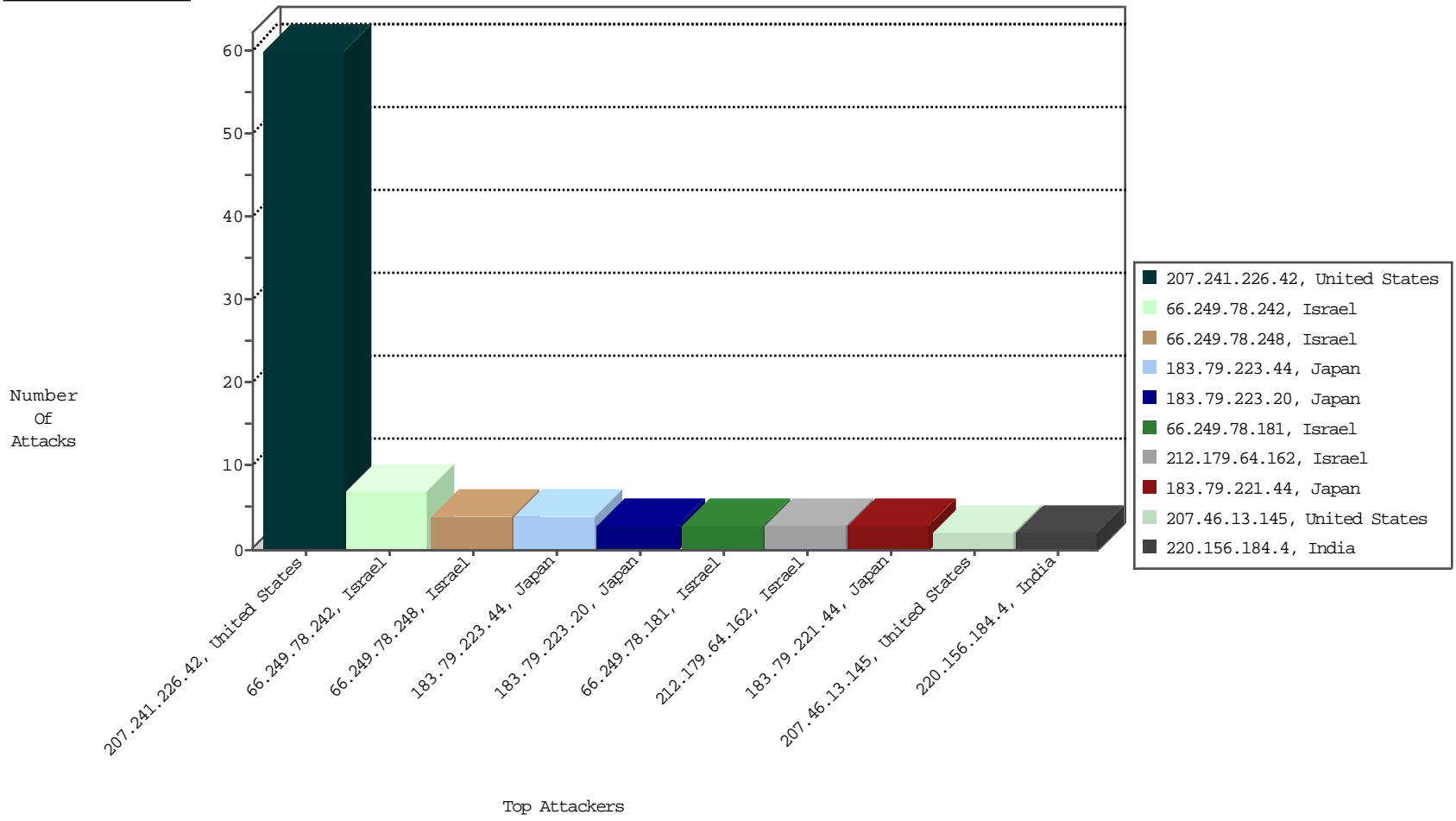
# Focused IP Under Attack Daily Report



## Top Targets



## Top Attackers



12-09-2015 to 12-10-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
212.179.64.162	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	BEL-Israel	3

12-09-2015 to 12-10-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
220.156.184.4	India	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	2
69.12.70.34	United States	147.237.77.17	mazi.idf.il	21609: HTTP: pChart Directory Traversal Vulnerability	Block	1

## Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
66.249.78.174	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
93.174.93.9	Netherlands	147.237.77.17	mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
119.73.228.130	Singapore	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 3072	1
221.2.43.66	China	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
92.43.70.181	United Kingdom	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
119.73.228.130	Singapore	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
133.130.118.109	Japan	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1

12-09-2015 to 12-10-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
85.130.245.195	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	251
85.130.245.195	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	188
37.26.147.162	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	41
82.81.240.91	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	31
46.19.85.23	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	25
46.19.85.23	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	25
173.162.34.45	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
37.58.80.11	Netherlands	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	12
46.19.86.124	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	9
213.57.135.234	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
46.19.86.124	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
79.177.120.234	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
5.28.156.232	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
185.3.146.223	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
82.81.240.91	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	5
5.28.156.232	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
46.19.85.35	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
85.93.91.84	Germany	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
46.19.86.130	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.86.225	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.121.64.106	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
37.46.39.124	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
46.121.103.245	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	2
2.54.169.25	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
91.200.12.7	Ukraine	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	2
213.57.133.192	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
207.46.13.140	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.147.186	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	2
46.19.86.184	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.121.103.245	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.176.200	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
207.46.13.140	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
37.26.147.186	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
128.232.110.28	United Kingdom	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
41.234.117.145	Egypt	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	2
31.154.149.53	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
207.46.13.145	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
65.55.212.76	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.90	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.253	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.121.177	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.162	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
95.108.158.145	Russian Federation	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.243.31.2	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.156	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
208.115.111.75	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.15	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.45.254.227	Russian Federation	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
157.55.39.106	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
46.19.86.208	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

12-09-2015 to 12-10-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
207.241.226.42	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 207.241.226.42	Block	35
207.241.226.42	United States	147.237.77.17	mazi.idf.i	PHP Attempt	Block	13
207.241.226.42	United States	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	11
183.79.223.44	Japan	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 183.79.223.44	Block	3
183.79.223.20	Japan	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 183.79.223.20	Block	2
149.78.157.154	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	2
183.79.221.44	Japan	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 183.79.221.44	Block	2
66.249.78.181	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8347-he	Block	1
157.55.39.7	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5676-7827-he/igf.aspx	Block	1
85.93.91.84	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
66.249.78.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4384-7935-he/igf.aspx	Block	1
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	1
65.55.212.70	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
183.79.221.44	Japan	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/a	Block	1
141.212.121.176	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
77.75.77.200	Czech Republic	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/9/8699.jpg	Block	1
212.235.98.139	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-he	Block	1
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5221-6390-he/igf.aspx	Block	1
66.249.78.181	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/591-he/handasa.aspx	Block	1
183.79.223.44	Japan	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/a	Block	1
157.55.39.9	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
40.77.167.31	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/robots.txt	Block	1
104.131.123.215	United States	147.237.77.17	mazi.idf.i	Unauthorized Method HEAD for 147.237.77.17/	Block	1
66.249.78.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6752-10378-he/igf.aspx	Block	1
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/165-5908-he/igf.aspx	Block	1
66.249.78.167	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8335-he	Block	1
149.78.112.74	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5187-he/igf.aspx	Block	1
79.177.63.181	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
207.46.13.145	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8331-he	Block	1
66.249.78.181	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/700-he/bayabashaarchive.aspx	Block	1
157.55.39.87	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
40.77.167.84	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
104.131.147.112	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5216-he/igf.aspx	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
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4223-he/igf.aspx	Block	1
66.249.78.174	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/4384-6059-he	Block	1
183.79.223.20	Japan	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
84.228.20.43	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
66.249.78.248	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/robots.txt	Block	1
207.46.13.145	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/common/logininfo.aspx	Block	1
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/14-he/igf.aspx	Block	1
46.19.85.75	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
131.253.24.158	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/templates/newslist/undefined	Block	1
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8346-he	Block	1
207.241.226.42	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/113-11973-he/piwik.php	Block	1
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4945-he/igf.aspx	Block	1

12-09-2015 to 12-10-2015