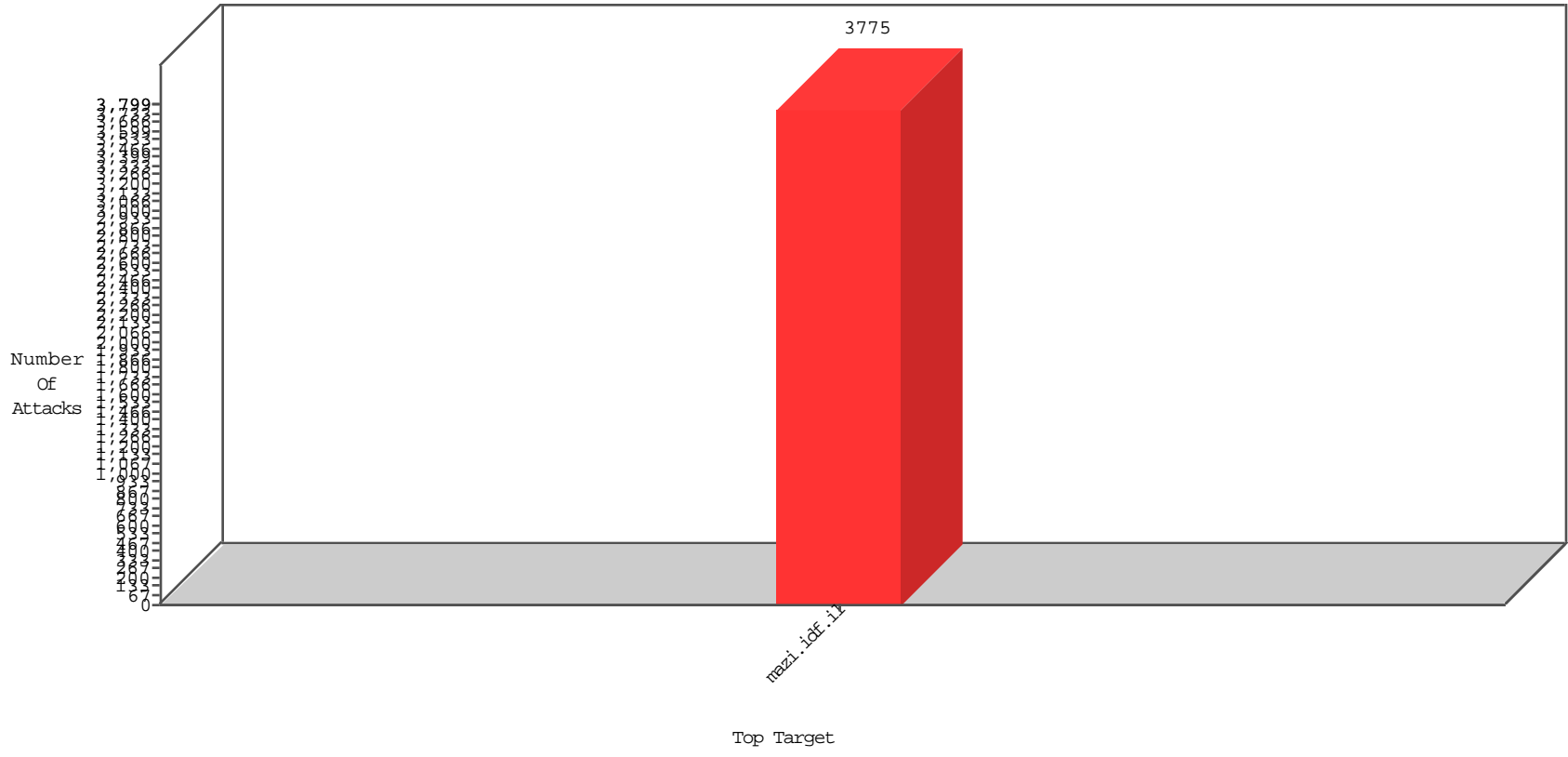


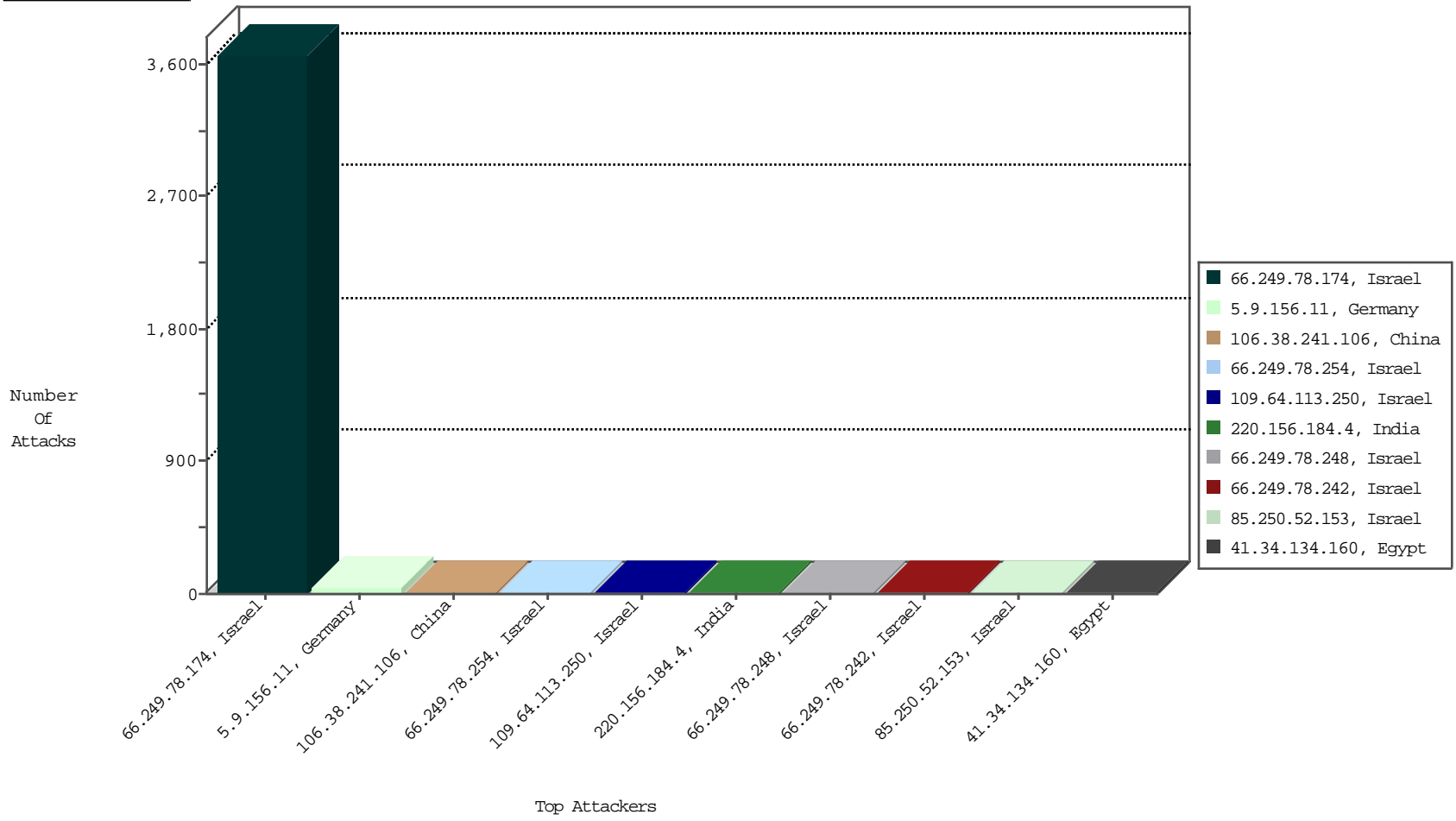
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
66.249.78.174	Israel	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BEL-Frankfurt	3666
109.64.113.250	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	BEL-Israel	5
202.112.51.96	China	147.237.77.17	mazi.idf.il	block-sp-trafl	drop	BEL-Frankfurt	1

12-05-2015 to 12-06-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.17	mazi.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	6
220.156.184.4	India	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	3

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
85.97.38.244	Turkey	147.237.77.17	mazi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
138.121.34.52		147.237.77.17	mazi.idf.i	ET SCAN Potential SSH Scan	1
93.158.215.45	Netherlands	147.237.77.17	mazi.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
151.236.217.221	United Kingdom	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
185.112.102.211		147.237.77.17	mazi.idf.il	drop	SAM rule	drop	204
79.183.49.213	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	79
109.65.50.128	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	64
87.69.79.45	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	52
2.54.141.245	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
185.3.144.54	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid sequence number	monitor	20
188.120.148.150	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.86.72	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
46.19.86.105	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
79.176.102.168	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
46.19.86.72	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
5.22.131.152	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.196	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.196	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
2.54.141.245	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.19.86.105	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.252	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
109.186.18.45	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
37.46.39.112	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
217.132.91.252	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
213.8.204.47	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
46.19.85.166	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.154	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.166	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
5.9.156.11	Germany	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
206.253.226.22	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
66.249.78.167	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.102.254.54	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.8.93	Israel	147.237.77.17	mazi.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
46.19.85.216	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.28	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
68.180.228.160	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.78.167	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
74.82.47.52	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.90	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
46.19.86.133	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.121.192	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.4	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
93.173.139.97	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.111.224.55	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
202.112.51.96	China	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
66.249.78.248	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.117.36.178	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
151.236.217.221	United Kingdom	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.183	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
213.57.251.198	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
85.65.71.107	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
208.115.111.75	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
37.142.64.23	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
195.60.232.57	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

12-05-2015 to 12-06-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
5.9.156.11	Germany	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 5.9.156.11	Block	43
2.52.180.149	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	2
85.250.52.153	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	2
5.107.167.116	United Arab Emirates	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/xmlrpc.php	Block	1
151.241.113.122	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Multiple Malformed URL from 151.241.113.122	Block	1
79.183.49.213	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1
66.249.78.254	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3848-5222-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
198.20.69.74	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/robots.txt	Block	1
37.142.64.73	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/xmlrpc.php	Block	1
5.9.156.11	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5676-7827-he/ifg.aspx	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
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8331-he	Block	1
66.249.78.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5010-7632-he/igf.aspx	Block	1
64.79.85.205	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/shared/usercontrols/vodchannel/	Block	1
31.210.187.202	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
157.55.39.22	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6221-9268-he/igf.aspx	Block	1
85.64.57.175	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
66.249.78.254	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5551-5809-he/igf.aspx	Block	1
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/165-8946-he/igf.aspx	Block	1
206.253.226.22	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/robots.txt	Block	1
41.34.134.160	Egypt	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
5.9.156.11	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/7247-11477-he/404.aspx	Block	1
141.212.122.64	United States	147.237.77.17	mazi.idf.i	Malformed URL proxytest.zmap.io:80	Block	1
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/vodchannel/	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
66.249.64.175	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
157.55.39.22	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
31.210.187.202	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 31.210.187.202	Block	1
66.249.78.254	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 147.237.77.17/6752-10682-he/igf.aspx	Block	1
206.253.226.23	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
41.34.134.160	Egypt	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
5.107.167.116	United Arab Emirates	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
151.236.217.221	United Kingdom	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
79.176.102.168	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/571-he/igf.aspx	Block	1
66.249.78.254	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3728-10383-he/igf.aspx	Block	1
66.249.78.164	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/7343-11581-he/xœxœ? x'x'x•xœx•x^a.aspx	Block	1
157.55.39.214	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5374-he/igf.aspx	Block	1
37.142.64.73	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
109.67.139.27	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5035	Block	1
5.9.156.11	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-7707-he	Block	1
66.249.78.254	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
66.249.78.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/120-he/mazi.aspx	Block	1
207.46.13.20	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/113-11618-he/igf.aspx	Block	1
46.19.86.181	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/571-he/igf.aspx	Block	1

12-05-2015 to 12-06-2015