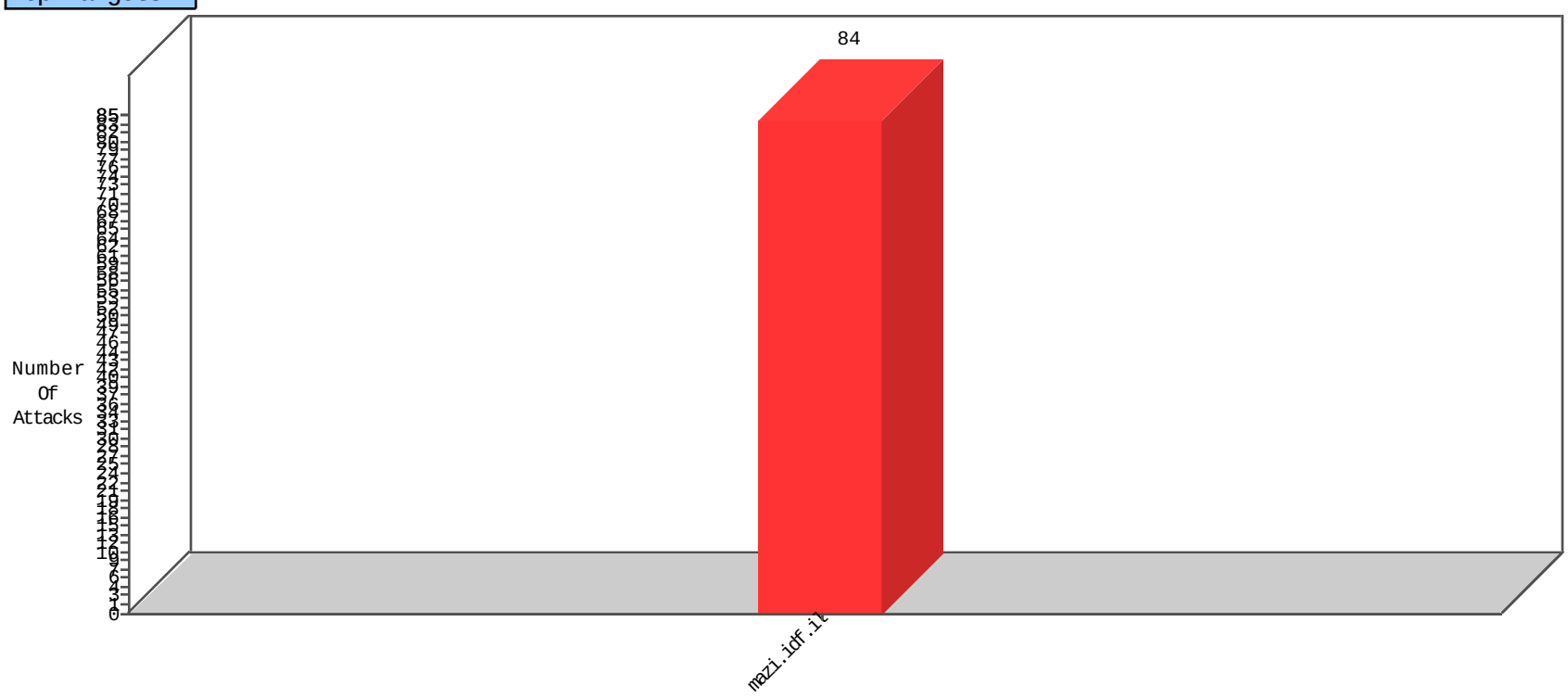
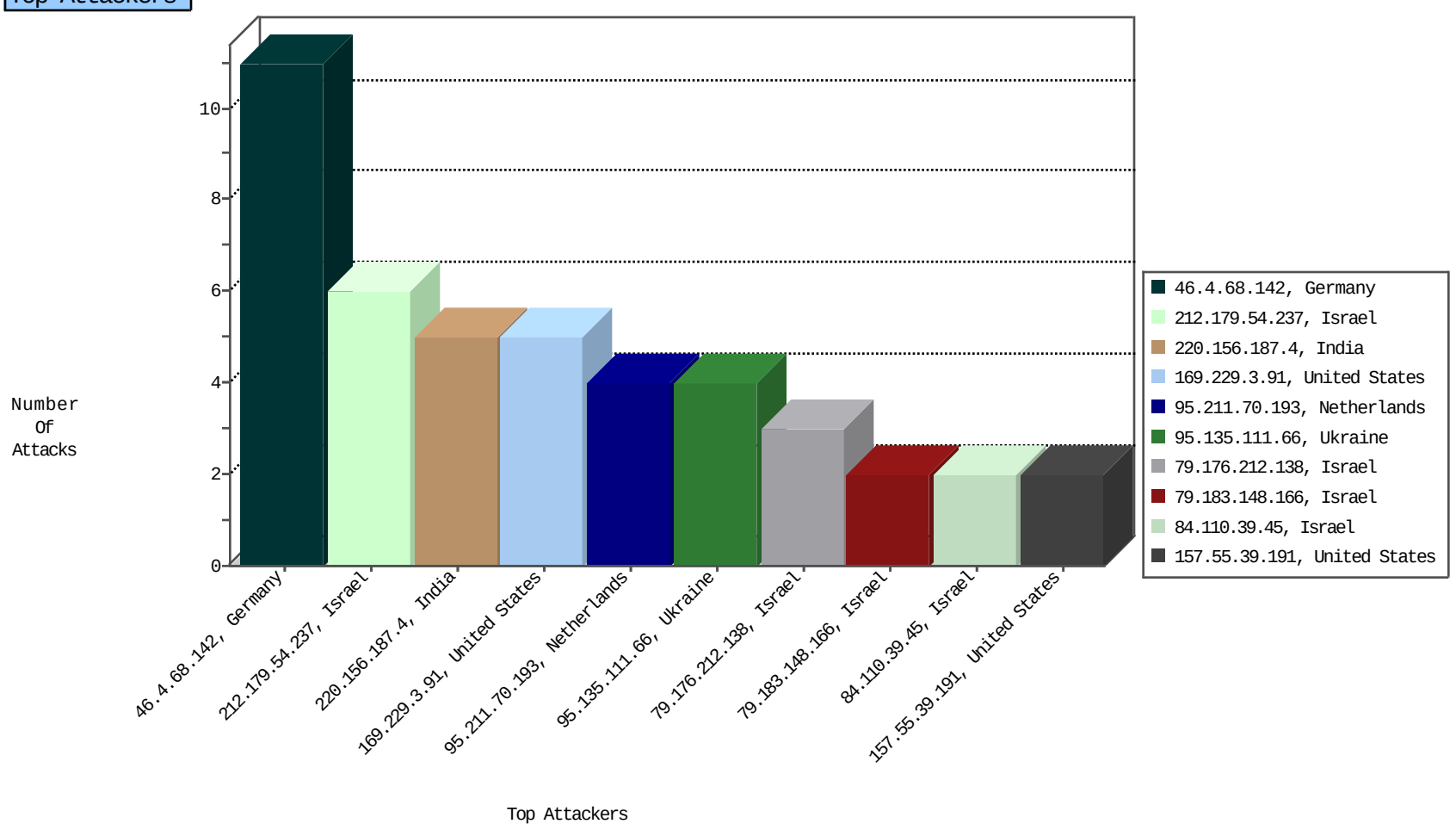
01-21-2016 to 01-22-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



01-21-2016 to 01-22-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
212.179.54.237	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	6
79.176.212.138	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	3
107.150.60.244	United States	147.237.77.17	mazi.idf.il	block-sp-traf1	drop	BBL-Frankfurt	1

01-21-2016 to 01-22-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
220.156.187.4	India	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	5
95.211.70.193	Netherlands	147.237.77.17	mazi.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

01-21-2016 to 01-22-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
95.211.70.193	Netherlands	147.237.77.17	mazi.idf.il	SQL Injection - Select From	3
66.249.66.134	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
91.218.113.195	Russian Federation	147.237.77.17	mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
168.62.238.153	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1

01-21-2016 to 01-22-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
62.0.102.94	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	529
62.0.102.94	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	49
62.0.102.94	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	49
46.19.85.71	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	36
94.230.86.236	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	36
46.19.85.71	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	36
46.19.85.80	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	25
79.182.197.64	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
2.52.6.242	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
176.13.2.64	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
37.26.146.219	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
213.57.214.183	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
195.239.16.40	Russian Federation	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
195.239.16.53	Russian Federation	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
46.19.86.153	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
217.132.127.160	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
152.115.70.227	Denmark	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	8
2.52.163.171	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.86.122	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.163.171	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.153	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.52.163.171	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	4
46.19.85.30	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
217.132.127.160	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.30	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
217.132.127.160	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
85.64.115.15	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.163.171	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
206.253.226.23	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
203.133.168.35	Korea, Republic of	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
195.160.242.40	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
86.104.160.99	Romania	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	2
217.132.127.160	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
2.54.33.124	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
5.22.131.18	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
188.120.148.171	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.1	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
207.46.13.122	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.85.167	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
94.230.86.249	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.8	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.114.127.80	Palestinian Territory, Occupied	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
5.29.122.103	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
81.218.251.252	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
2.54.28.141	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.240	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.70	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.121.192	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
93.172.129.58	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	1
85.64.126.226	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
207.46.13.127	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.22.130.239	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
46.4.68.142	Germany	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 46.4.68.142	Block	8
66.249.65.231	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	2
149.78.37.10	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/templates/newslist/undefined	Block	2
157.55.39.191	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	2
81.218.140.160	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
208.90.57.196	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/joinmailinglist.aspx	Block	1
79.178.31.109	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Illegal Byte Code Character in Method `Ã˜[[#23]]Ã®[[#31]]Ã†Â´Â”[[#24]]n>QÂŸ 'Ã¨[[#17]]Â”C	Block	1
95.135.111.66	Ukraine	147.237.77.17	mazi.idf.i	Parameter Type Violation lang in mazi.idf.il/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
41.233.17.133	Egypt	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
84.110.39.45	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
79.183.148.166	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	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
66.249.66.173	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/113-9193-he/igf.aspx	Block	1
46.4.68.142	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/templates/homepage/404.aspx	Block	1
157.55.39.224	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
95.135.111.66	Ukraine	147.237.77.17	mazi.idf.i	Parameter Type Violation DocID in mazi.idf.il/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
2.54.42.69	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
82.80.133.53	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
212.179.42.227	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation PageNum in mazi.idf.il/3697-he/igf.aspx	Block	1
79.178.31.109	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
66.249.65.238	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3834-7123-he/igf.aspx	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Malformed URL	Block	1
104.128.144.131	Canada	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/redirect.php	Block	1
41.233.17.133	Egypt	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 41.233.17.133	Block	1
84.110.39.45	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
79.183.148.166	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 79.183.148.166	Block	1
207.232.55.134	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
79.177.22.48	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
46.4.68.142	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/templates/newslist/undefined	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Abnormally Long Request method	Block	1
95.135.111.66	Ukraine	147.237.77.17	mazi.idf.i	Parameter Type Violation FileID in mazi.idf.il/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
5.28.154.193	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
82.80.133.53	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/xmlrpc.php	Block	1
79.178.110.143	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Unknown HTTP Request Method `Ã˜[[#23]]Ã®[[#31]]Ã†Â´Â”[[#24]]n>QÂŸ 'Ã¨[[#17]]Â”C	Block	1
66.249.65.245	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
89.138.95.227	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
81.218.140.160	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
207.232.55.134	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/xmlrpc.php	Block	1
79.177.22.48	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
46.19.86.21	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Illegal Byte Code Character in Header Name	Block	1
95.135.111.66	Ukraine	147.237.77.17	mazi.idf.i	Parameter Type Violation folderid in mazi.idf.il/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
8.37.70.253	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/6072-8874-he/igf.aspx&usg=alkjrhgnqhknnrkfn8_fjypzsohpr3b2oa	Block	1
84.94.169.160	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
79.178.110.143	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/xmlrpc.php	Block	1
176.13.2.64	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
66.249.66.169	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3728-7059-he/igf.aspx	Block	1
46.4.68.142	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/113-11581-he/×œ×œ×? ×’×‘×•×œ×•×ª.aspx	Block	1
94.230.86.236	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1

01-21-2016 to 01-22-2016