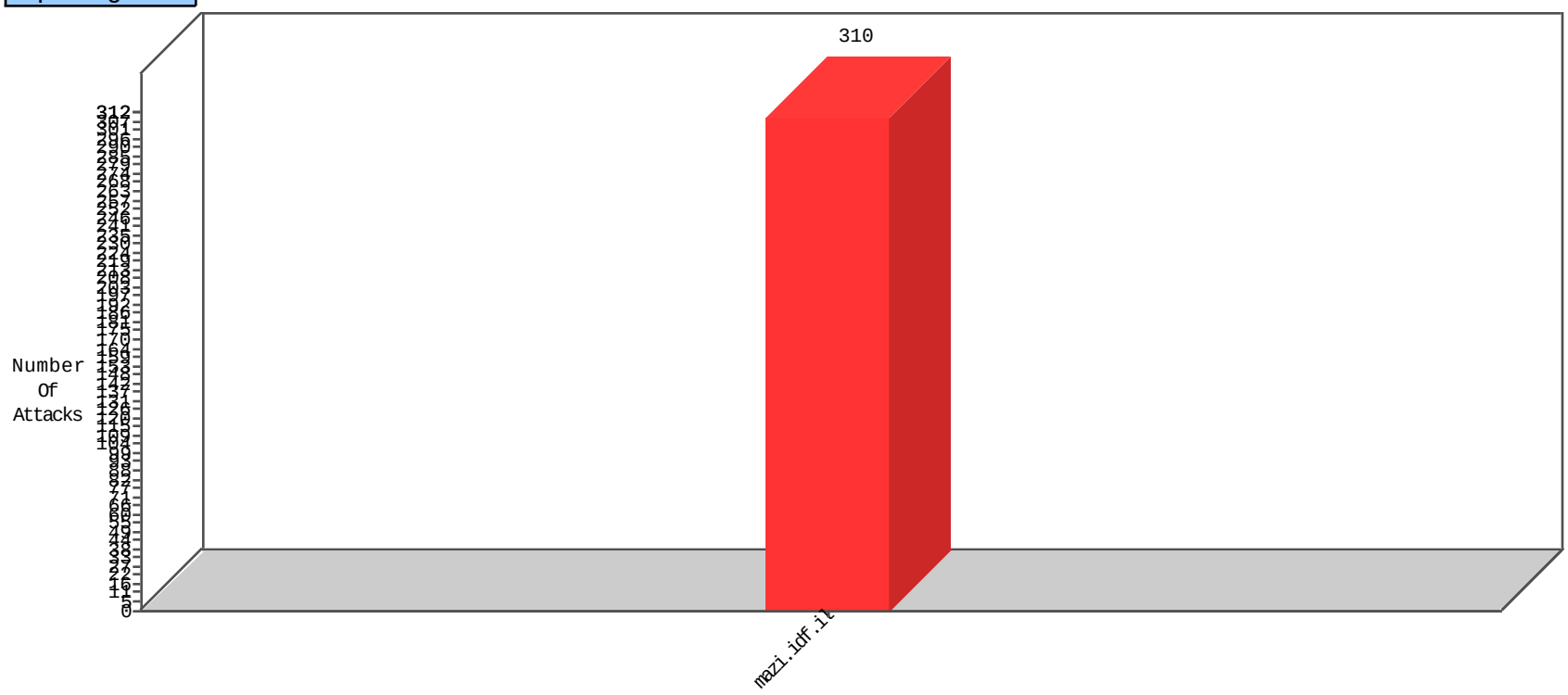
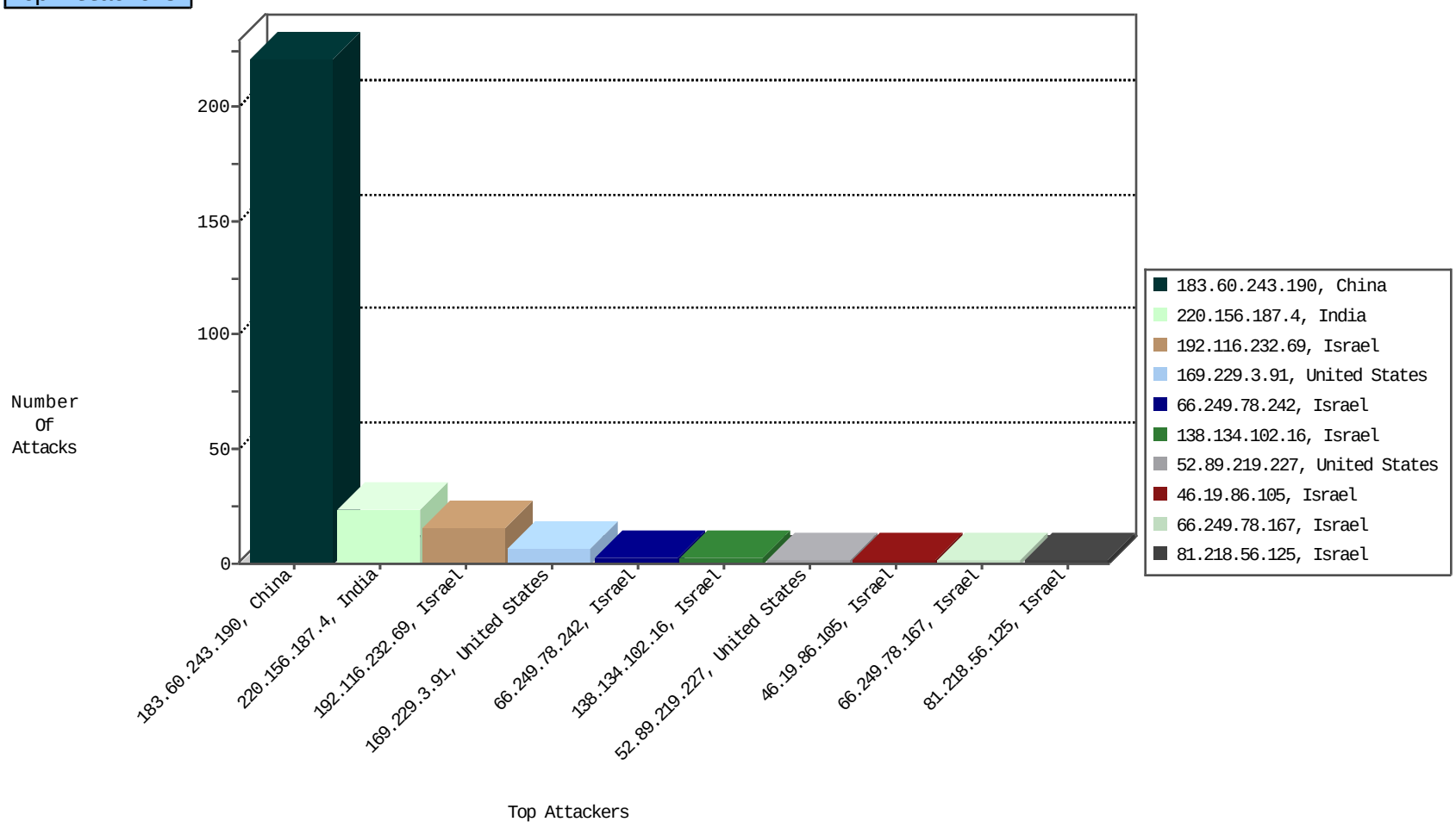
02-03-2016 to 02-04-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



02-03-2016 to 02-04-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
81.218.56.125	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	2
142.54.160.211	United States	147.237.77.17	mazi.idf.il	block-sp-traf1	drop	BBL-Frankfurt	1
146.185.239.100	Russian Federation	147.237.77.17	mazi.idf.il	block-sp-traf1	drop	BBL-Frankfurt	1

02-03-2016 to 02-04-2016

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	24
183.60.243.190	China	147.237.77.17	mazi.idf.il	C003: HTTP: phpMyAdmin access	Block	1

02-03-2016 to 02-04-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
52.89.219.227	United States	147.237.77.17	mazi.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
37.200.225.36	Oman	147.237.77.17	mazi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
89.248.174.81	Netherlands	147.237.77.17	mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.243.190	China	147.237.77.17	mazi.idf.il	SERVER-APACHE Apache Tomcat Web Application Manager access	1
189.219.192.237	Mexico	147.237.77.17	mazi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.60.243.190	China	147.237.77.17	mazi.idf.il	GPL WEB_SERVER WEB-MISC JBoss web-console access	1
183.60.243.190	China	147.237.77.17	mazi.idf.il	SERVER-WEBAPP admin.php access	1
218.246.0.97	China	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1

02-03-2016 to 02-04-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
212.76.127.219	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	189
46.19.85.164	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	81
31.210.186.42	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	27
79.179.219.220	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
212.76.127.10	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	18
195.239.16.53	Russian Federation	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
212.76.127.44	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
195.239.16.40	Russian Federation	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
84.108.175.183	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
8.37.227.68	Anonymous Proxy	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Response out of state	monitor	9
212.76.127.111	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
46.19.85.156	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	9
46.19.85.164	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.28	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.156	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.28	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.206	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
8.37.227.69	Anonymous Proxy	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Response out of state	monitor	4
79.182.24.157	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.160.242.40	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
37.46.38.40	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
195.160.242.40	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
84.108.175.183	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
5.22.131.48	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
216.218.206.70	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
156.158.189.2	Tanzania, United Republic of	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
2.54.27.251	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
5.102.254.60	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
5.22.131.1	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
79.127.43.241	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
62.219.161.150	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
176.228.71.8	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
146.185.239.102	Russian Federation	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.65.97.194	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
66.249.65.18	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.121.210.232	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
176.13.12.165	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
95.86.65.199	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
84.108.127.149	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
5.22.131.81	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
79.176.240.227	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
62.219.168.120	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
176.228.71.8	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.121.28.121	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
46.19.85.147	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
85.65.97.194	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
8.37.227.81	Anonymous Proxy	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Response out of state	monitor	1
80.246.130.97	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
212.179.1.218	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.58	United States	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
183.60.243.190	China	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 183.60.243.190	Block	166
183.60.243.190	China	147.237.77.17	mazi.idf.i	Multiple Admin Blocking from 183.60.243.190	Block	27
183.60.243.190	China	147.237.77.17	mazi.idf.i	PHP Attempt	Block	18
192.116.232.69	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 192.116.232.69	Block	15
183.60.243.190	China	147.237.77.17	mazi.idf.i	Too Many of the Same Response Code (404) in Session from 183.60.243.190	Block	4
138.134.102.16	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	3
46.19.86.105	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage	Block	2
66.249.78.254	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
213.151.58.160	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5551-6165-he/igf.aspx&sa=u&ved=0ahukewi9unwjs9zkahvfpq4khzdbbyyqfggpmam&usg=afqjcnhy2acvcggs65joi5pyg6y1jfdlua	Block	1
66.249.78.167	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	NULL Character in Header Name at	Block	1
157.55.39.135	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
82.81.73.137	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4146-he/igf.aspx	Block	1
194.90.128.185	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/7/6117.jpg	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
157.55.39.76	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/templates/shared/usercontrols/vodchannel/	Block	1
217.118.93.115	Russian Federation	147.237.77.17	mazi.idf.i	Parameter Type Violation pagenum in mazi.idf.il/700-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/5551-11516-he/×ž×©×œ×‘×™×? ×§×″×™×œ×″.aspx	Block	1
183.60.243.190	China	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/cgi-mod/header_logo.cgi	Block	1
66.249.78.167	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
176.13.5.127	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/2061.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
89.138.121.244	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation Master$ucHeader$ucSearchControl$txtSearch in www.mazi.idf.il/582-he/igf.aspx	Block	1
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5477-he/igf.aspx	Block	1
201.245.9.162	Colombia	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/503-en/igf.aspx	Block	1
66.249.65.231	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/55-he/igf.aspx	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Multiple Malformed URL from 169.229.3.91	Block	1
157.55.39.78	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/113-11701-he/×©×¢×ª×? ×©×œ ×″×›×¡×•×™×?.aspx	Block	1
68.180.230.40	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
66.249.78.181	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-4980-he	Block	1
183.60.243.190	China	147.237.77.17	mazi.idf.i	Admin Blocking	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Illegal HTTP Version Â-l	Block	1
98.143.148.107	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/check	Block	1
66.249.78.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/62-he/igf.aspx	Block	1
213.151.37.24	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5216-he/igf.aspx	Block	1
183.60.243.190	China	147.237.77.17	mazi.idf.i	Too Many 404: Response Code per Session	Block	1
66.249.78.17	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/14-8330-he	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
157.55.39.83	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
79.179.219.220	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/120-he/igf.aspx	Block	1
192.116.232.69	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/1.he/general/twitter.gif	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Multiple Abnormally Long Request from 169.229.3.91	Block	1