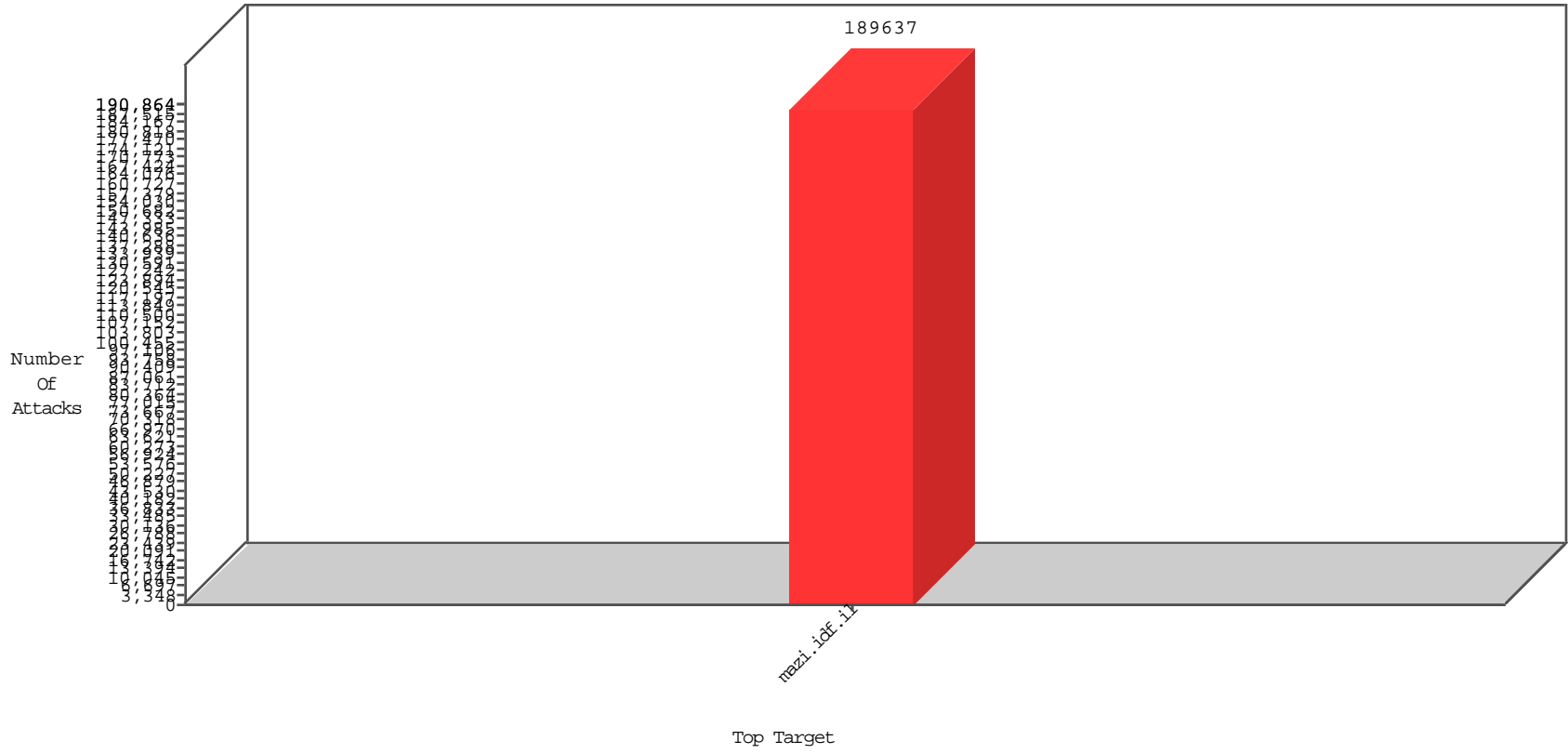


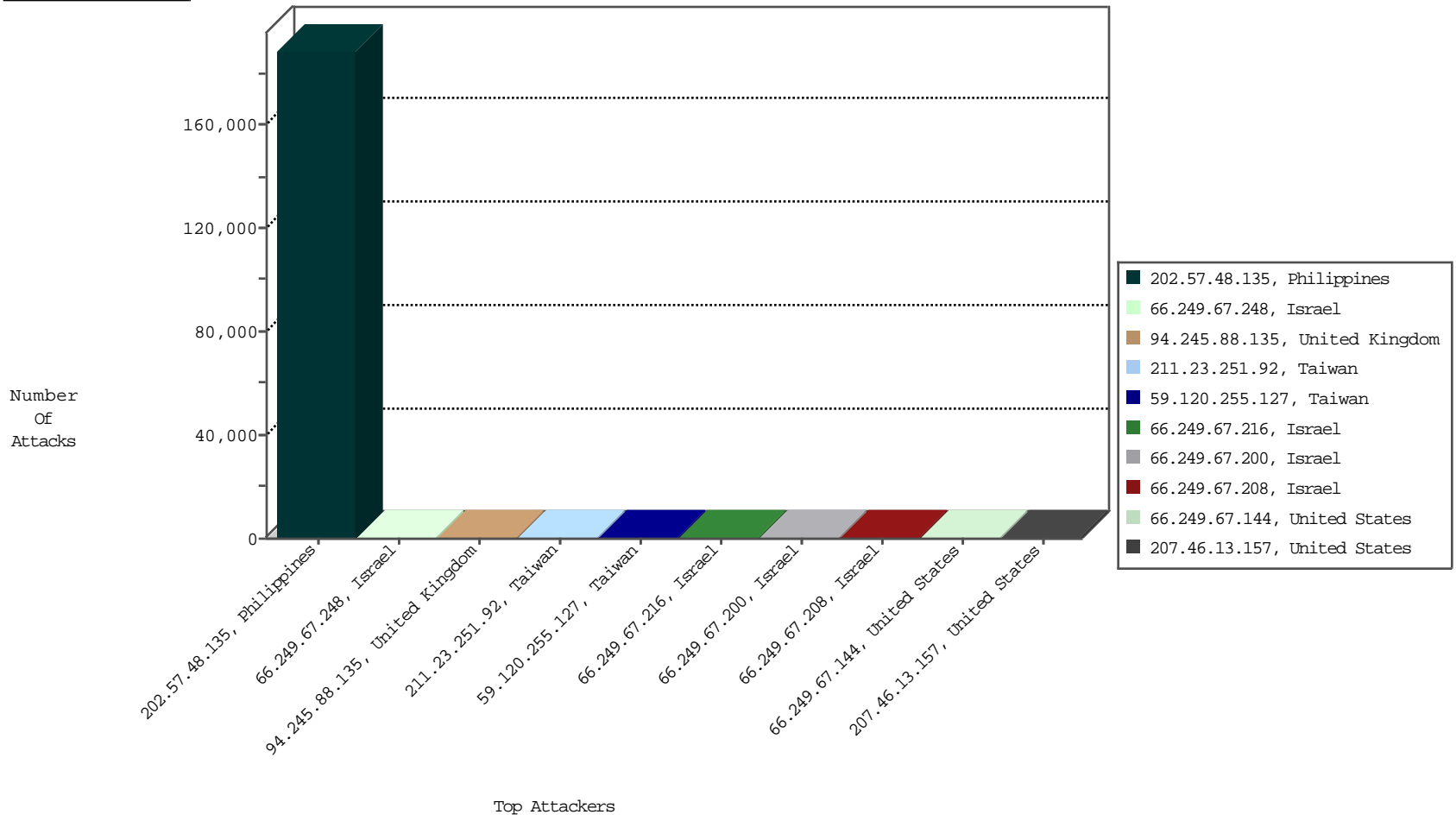
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
202.57.48.135	Philippines	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	189179
66.249.67.248	Israel	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	277

12-01-2015 to 12-02-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
94.245.88.135	United Kingdom	147.237.77.17	mazi.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	28
94.245.88.135	United Kingdom	147.237.77.17	mazi.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	19
211.23.251.92	Taiwan	147.237.77.17	mazi.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	7
59.120.255.127	Taiwan	147.237.77.17	mazi.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	3
188.165.15.223	France	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	1
94.245.88.135	United Kingdom	147.237.77.17	mazi.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1

12-01-2015 to 12-02-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
94.245.88.135	United Kingdom	147.237.77.17	mazi.idf.i	SQL Injection - Select From	18
211.23.251.92	Taiwan	147.237.77.17	mazi.idf.i	SQL Injection - Select From	15
59.120.255.127	Taiwan	147.237.77.17	mazi.idf.i	SQL Injection - Select From	9
66.249.67.144	United States	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sA (2)	4
66.249.67.135	United States	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sA (2)	2
122.194.13.249	China	147.237.77.17	mazi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
209.126.116.147	United States	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sS window 1024	1

12-01-2015 to 12-02-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
46.19.85.90	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	36
46.19.86.238	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	36
46.19.85.90	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	36
46.19.85.98	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	26
46.19.85.98	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	25
46.19.85.142	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	25
46.19.85.142	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	25
46.19.85.209	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	23
213.8.174.14	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
79.176.216.40	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
93.172.166.73	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
192.117.13.30	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
37.58.75.46	Netherlands	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	14
46.19.85.209	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	11
87.68.61.66	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
84.108.180.168	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	9
79.183.183.164	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
84.108.180.168	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
61.216.2.13	Taiwan	147.237.77.17	mazi.idf.i	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	9
106.38.241.106	China	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	8
87.69.38.214	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
185.3.146.219	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
213.57.130.29	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
84.95.198.7	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
5.102.254.88	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
109.65.75.168	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.214	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
128.232.110.28	United Kingdom	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
213.57.136.37	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
212.96.178.162	Czech Republic	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
85.250.28.99	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
185.3.146.95	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
157.55.39.125	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
2.54.178.214	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
87.69.38.214	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	2
37.60.147.198	Palestinian Territory, Occupied	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
195.60.232.57	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
91.253.19.84	Italy	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.29	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
202.112.51.96	China	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
64.125.239.11	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
188.120.148.142	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.44	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.87	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
210.186.53.248	Malaysia	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
193.106.54.21	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
61.216.2.13	Taiwan	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.215	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.45	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
207.46.13.66	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
176.13.4.209	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	2
31.168.170.190	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/	Block	2
66.249.67.208	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/templatecontrols/pictureinfo/pictureinfo.aspx	Block	2
79.176.213.214	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslst/undefined	Block	2
207.46.13.157	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 207.46.13.157	Block	2
109.67.28.178	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/ufi/reaction/	Block	2
79.182.219.240	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/images/transvideocounter.gif	Block	2
5.29.111.83	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslst/undefined	Block	2
157.55.39.84	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/vodchannel/	Block	1
66.249.66.46	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation TabNum in igf.idf.il/3793-he/igf.aspx	Block	1
31.184.133.24	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/3850-5187-he/igf.aspx	Block	1
95.86.107.246	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/397-he/igf.aspx&sa=u&ved=0ahukewii4ocpgbvjahugvrokhd9wby4qqoubccmwag&sig2=cyrklot_gbtn9tirwn4ddw&usq=afqjcneiptgljix0maat04tm3dvokhy9g	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
31.184.131.21	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/3850-5187-he/igf.aspx	Block	1
207.46.13.184	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6221-9268-he/igf.aspx	Block	1
66.249.67.216	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3728-6770-he/igf.aspx	Block	1
66.249.67.200	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3847-he/igf.aspx	Block	1
109.67.168.165	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/xmlrpc.php	Block	1
54.173.19.39	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-he/	Block	1
31.184.132.24	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/3850-5187-he/igf.aspx	Block	1
84.95.198.7	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5187-he/igf.aspx	Block	1
66.249.67.216	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6752-10691-he/igf.aspx	Block	1
207.46.13.47	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/glp	Block	1
66.249.67.200	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 66.249.67.200	Block	1
157.55.39.90	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/pg/api/getsimblog/	Block	1
31.184.134.21	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5187-he/igf.aspx	Block	1
104.131.147.112	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5216-he/igf.aspx	Block	1
31.184.131.24	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/3850-5187-he/igf.aspx	Block	1
212.179.21.194	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 212.179.21.194	Block	1
66.249.67.216	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4476-he/igf.aspx	Block	1
66.249.67.200	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
193.41.209.2	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
131.162.130.180	Canada	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/	Block	1
61.216.2.13	Taiwan	147.237.77.17	mazi.idf.i	Illegal Byte Code Character in Method	Block	1
31.184.133.21	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/3850-5187-he/igf.aspx	Block	1
86.104.162.55	Romania	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
66.249.67.216	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
31.184.130.33	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/3850-5187-he/igf.aspx	Block	1
66.249.67.216	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/	Block	1
66.249.67.200	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/113-9528-he/igf.aspx	Block	1
157.55.39.125	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslst/js/common_functions.cfm	Block	1
31.184.134.23	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/3850-5187-he/igf.aspx	Block	1
79.182.191.24	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation PageNum in mazi.idf.il/113-he/igf.aspx	Block	1
31.184.132.21	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/3850-5187-he/igf.aspx	Block	1
212.179.21.194	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/vodchannel/	Block	1
66.249.67.216	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6072-8876-he/igf.aspx	Block	1
66.249.67.208	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/113-9895-he/igf.aspx	Block	1
197.35.117.192	Egypt	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
149.88.58.47	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/4070-11595-he/xžx-xæx\$xa xaxx xaxx x*xŸx*x'x\$xx".aspx	Block	1
66.249.66.43	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation TabNum in igf.idf.il/4941-he/igf.aspx	Block	1
31.184.133.23	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/3850-5187-he/igf.aspx	Block	1
86.104.162.55	Romania	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/xmlrpc.php	Block	1
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/113-11581-he/xæxæx? x'x'xæxæxæx^a.aspx	Block	1
31.184.130.35	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/3850-5187-he/igf.aspx	Block	1
207.46.13.157	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/gen_204	Block	1
66.249.67.216	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/113-10370-he/igf.aspx	Block	1
66.249.67.200	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3697-6779-he/igf.aspx	Block	1
157.55.39.139	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/legacy	Block	1
109.67.168.165	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
31.184.134.24	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/3850-5187-he/igf.aspx	Block	1
31.184.132.23	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/3850-5187-he/igf.aspx	Block	1
66.249.67.216	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6510-9854-he/igf.aspx	Block	1
197.35.117.192	Egypt	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
66.249.67.208	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3845-he/igf.aspx	Block	1