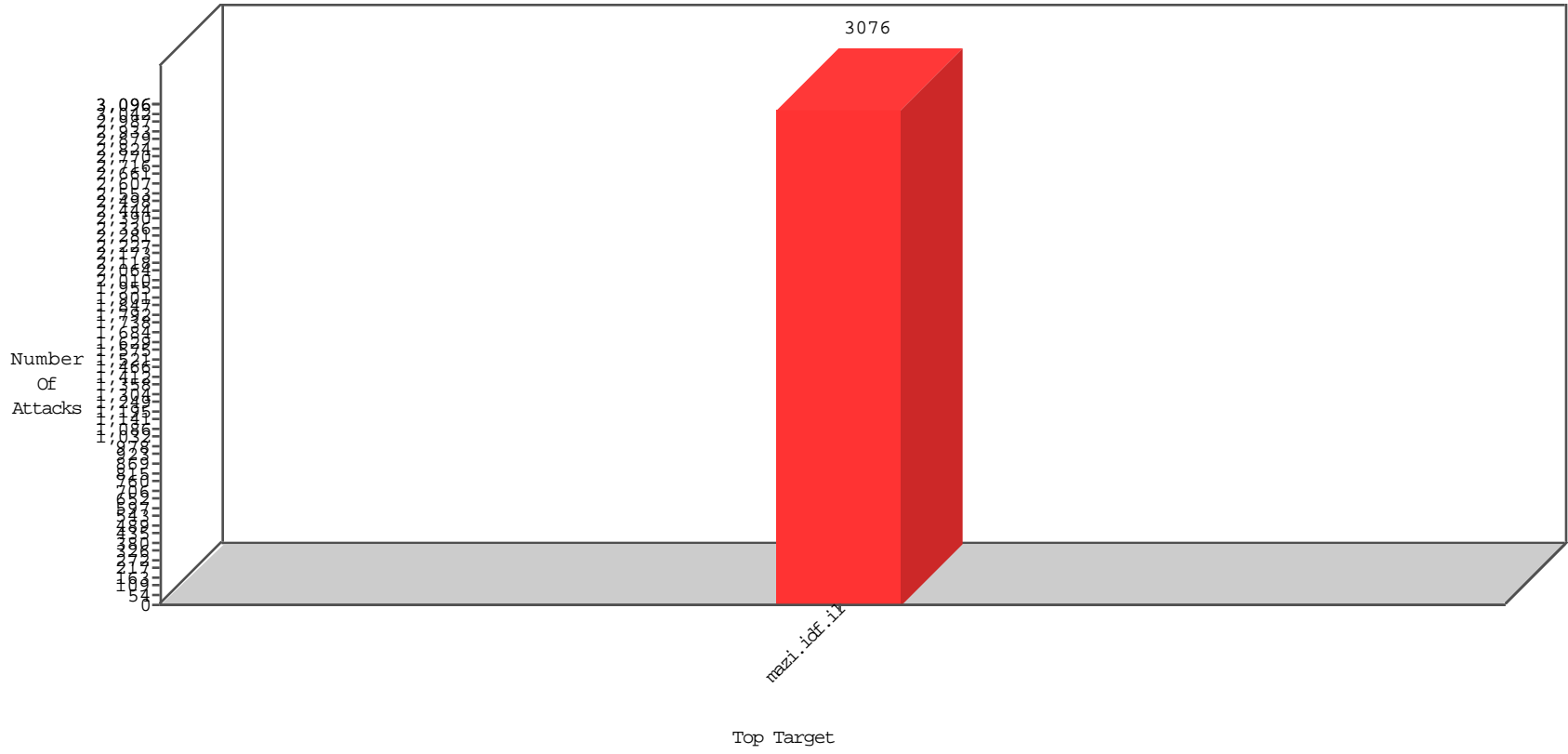


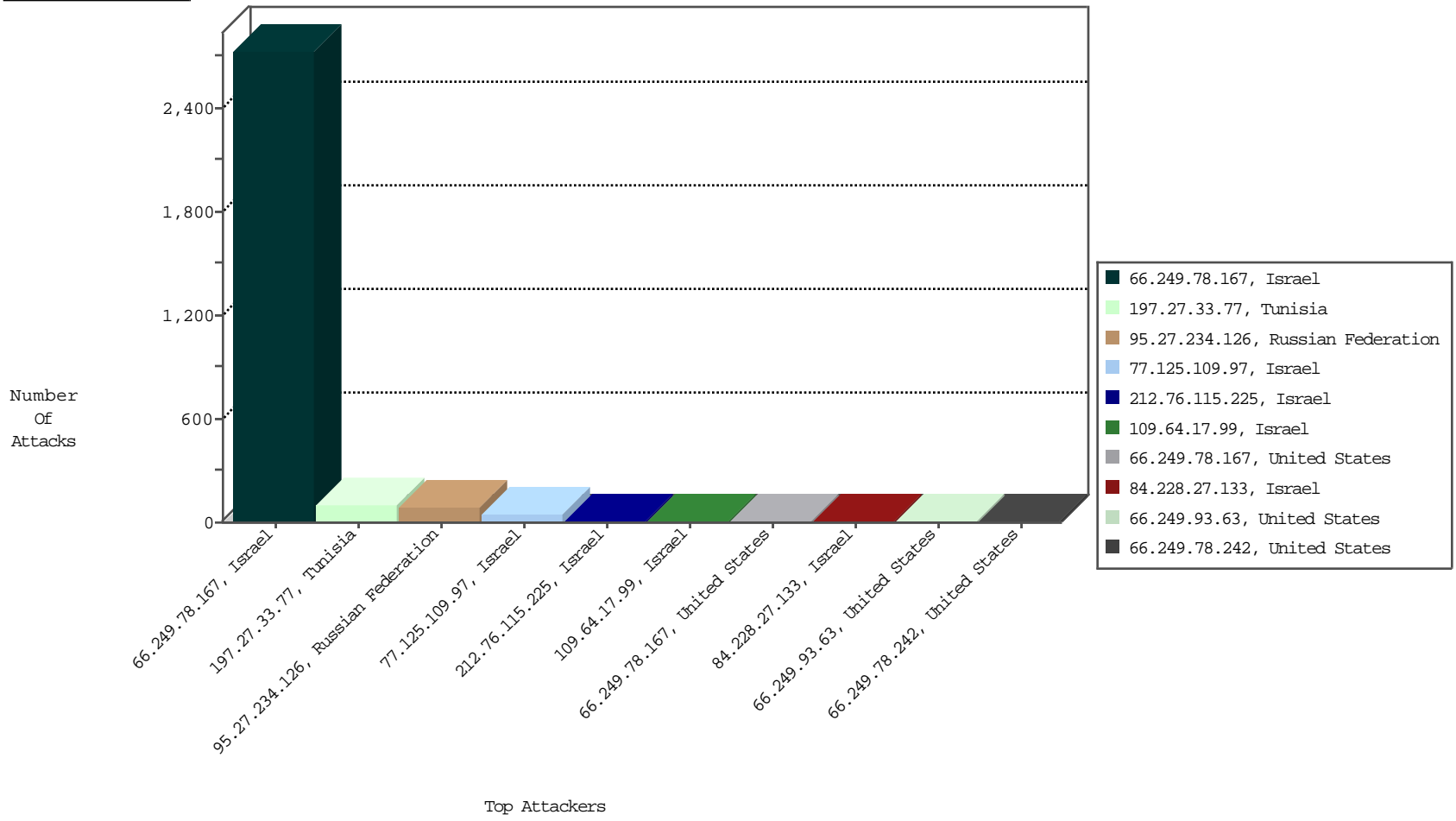
# Focused IP Under Attack Daily Report



## Top Targets



## Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
66.249.78.167	Israel	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	2729
54.72.182.187	Ireland	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	NetV-London	4
114.35.40.191	Taiwan	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	NetV-London	1
180.97.106.36	China	147.237.77.17	mazi.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
184.105.139.114	United States	147.237.77.17	mazi.idf.il	Block_Ntp_All_Net	drop	NetV-London	1

## Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
95.27.234.126	Russian Federation	147.237.77.17	mazi.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	82
77.125.109.97	Israel	147.237.77.17	mazi.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	52
66.249.78.167	Israel	147.237.77.17	mazi.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	8
109.64.17.99	Israel	147.237.77.17	mazi.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	6
66.249.93.63	United States	147.237.77.17	mazi.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	4
173.234.153.122	United States	147.237.77.17	mazi.idf.i	C1000074: HTTP: majestic bot	Block	2
66.249.93.5	Israel	147.237.77.17	mazi.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	2
199.30.24.162	United States	147.237.77.17	mazi.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.93.63	Israel	147.237.77.17	mazi.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	2
203.219.62.28	Australia	147.237.77.17	mazi.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	2
37.26.146.185	Israel	147.237.77.17	mazi.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.93.2	Israel	147.237.77.17	mazi.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	2
40.77.167.51	United States	147.237.77.17	mazi.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.78.168	Israel	147.237.77.17	mazi.idf.i	12890: TCP: Windows TCP/IP Denial-of-Service Vulnerability (ONLY enable when under DoS attack)	Block	1
157.55.39.141	United States	147.237.77.17	mazi.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	1
207.46.13.128	United States	147.237.77.17	mazi.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	1

## Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
66.249.66.181	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.167	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.161	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	1
164.39.11.198	United Kingdom	147.237.77.17	mazi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
195.216.176.244	Latvia	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
164.39.11.198	United Kingdom	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
85.130.243.99	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	102
85.130.243.99	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	99
5.28.186.194	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	69
79.181.2.121	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	64
37.142.153.134	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	52
109.160.160.19	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
46.19.85.117	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	32
46.19.85.48	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	25
46.19.85.48	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
109.160.160.19	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
193.106.54.34	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	16
193.106.54.34	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
46.117.239.72	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
109.160.160.19	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
37.46.38.250	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
77.125.73.75	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
194.90.131.82	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.142.153.134	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.142.153.134	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
87.69.243.141	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.52.35.19	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
193.106.54.34	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.49	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
93.110.20.114	Iran, Islamic Republic of	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.49	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
93.110.20.114	Iran, Islamic Republic of	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
89.139.17.84	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
185.3.147.242	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.46.38.132	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
147.236.34.10	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
89.248.160.136	Netherlands	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
213.57.244.47	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
5.22.134.251	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
85.130.243.99	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.60	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.185	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
149.78.69.146	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
37.164.8.66	France	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.26.146.162	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
212.37.27.58	Sweden	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
84.94.32.197	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
64.125.239.92	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
180.97.106.161	China	147.237.77.17	mazi.idf.il	drop	SAM rule	drop	1
141.212.122.76	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
213.57.244.47	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.22.135.132	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
87.69.165.104	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
186.121.226.64	Bolivia	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
149.78.69.146	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

## Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
197.27.33.77	Tunisia	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 197.27.33.77	Block	96
84.228.27.133	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 84.228.27.133	Block	4
212.76.115.225	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 212.76.115.225	Block	3
212.76.115.225	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	2
84.109.5.111	Israel	147.237.77.17	mazi.idf.i	Unauthorized HTTP Method	Block	2
162.243.92.130	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 162.243.92.130	Block	2
46.19.86.30	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation Master\$ucHeader\$ucSearchControl\$txtSearch in www.mazi.idf.il/6547-he/igf.aspx	Block	2
87.69.229.27	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	2
148.251.21.227	Germany	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 148.251.21.227	Block	2
66.249.78.3	United States	147.237.77.17	mazi.idf.i	Parameter Type Violation PageNum in igf.idf.il/5010-he/igf.aspx	Block	1
207.46.13.125	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/14-8335-he	Block	1
162.243.92.130	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-5475-he	Block	1
66.249.75.160	United States	147.237.77.17	mazi.idf.i	Parameter Type Violation PageNum in igf.idf.il/165-he/igf.aspx	Block	1
66.249.66.40	United States	147.237.77.17	mazi.idf.i	Parameter Type Violation TabNum in igf.idf.il/4941-he/igf.aspx	Block	1
95.86.66.165	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/7322-11795-he/mazi.aspx&sa=u&ved=0ahukewjgk4d_55zlahvbwqkxzexbe0qfggmaw&usq=afqjcn9b9i08tw3fbb41qxjmi_tdvhcb7w	Block	1
79.176.171.173	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
212.76.115.225	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/ajax/updatestatus.php	Block	1
66.249.78.242	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
66.249.78.3	United States	147.237.77.17	mazi.idf.i	Parameter Type Violation Back in igf.idf.il/6051-he/igf.aspx	Block	1
66.249.69.41	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/7343-11581-he/.aspx	Block	1
148.251.21.227	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
84.228.27.133	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
66.249.78.248	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
66.249.78.167	United States	147.237.77.17	mazi.idf.i	Parameter Type Violation PageNum in mazi.idf.il/5013-he/igf.aspx	Block	1
208.115.111.75	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8344-he	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Abnormally Long Request method	Block	1
66.249.75.160	United States	147.237.77.17	mazi.idf.i	Parameter Type Violation TabNum in igf.idf.il/4941-he/igf.aspx	Block	1
66.249.66.182	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
95.153.129.178	Russian Federation	147.237.77.17	mazi.idf.i	Parameter Type Violation ForumId in mazi.idf.il/forums/templates/forums/forum.aspx	Block	1
81.218.241.25	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 81.218.241.25	Block	1
212.235.98.139	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4637-5227-he/igf.aspx	Block	1
66.249.78.242	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4223-he/igf.aspx	Block	1
66.249.78.3	United States	147.237.77.17	mazi.idf.i	Parameter Type Violation Back in igf.idf.il/6053-he/igf.aspx	Block	1
207.46.13.70	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/14-10106-he	Block	1
148.251.21.227	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-4980-he	Block	1
66.249.75.18	United States	147.237.77.17	mazi.idf.i	Parameter Type Violation PageNum in mazi.idf.il/5013-he/igf.aspx	Block	1
87.69.229.27	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 87.69.229.27	Block	1
40.77.167.33	United States	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	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5039-he/igf.aspx	Block	1
66.249.78.167	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/700-he/bayabashaarchive.aspx	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Illegal Byte Code Character in Method	Block	1
66.249.75.168	United States	147.237.77.17	mazi.idf.i	Parameter Type Violation Back in igf.idf.il/6051-he/igf.aspx	Block	1
66.249.66.182	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
132.66.134.6	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
213.151.61.96	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/4634-5228-he/igf.aspx&sa=u&ved=0ahukewiloua10pzlahwdubokhq1mbb aqfggmaw&usq=afqjcn9b9i08tw3fbb41qxjmi_tdvhcb7w	Block	1
66.249.78.242	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1
66.249.78.3	United States	147.237.77.17	mazi.idf.i	Parameter Type Violation PageNum in igf.idf.il/165-he/igf.aspx	Block	1
207.46.13.99	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
66.249.75.160	United States	147.237.77.17	mazi.idf.i	Parameter Type Violation Back in igf.idf.il/6053-he/igf.aspx	Block	1
68.180.229.218	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/14-8347-he	Block	1
66.249.78.167	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
185.112.248.32		147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
66.249.75.176	United States	147.237.77.17	mazi.idf.i	Parameter Type Violation PageNum in igf.idf.il/5010-he/igf.aspx	Block	1
66.249.69.18	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
66.249.78.242	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1