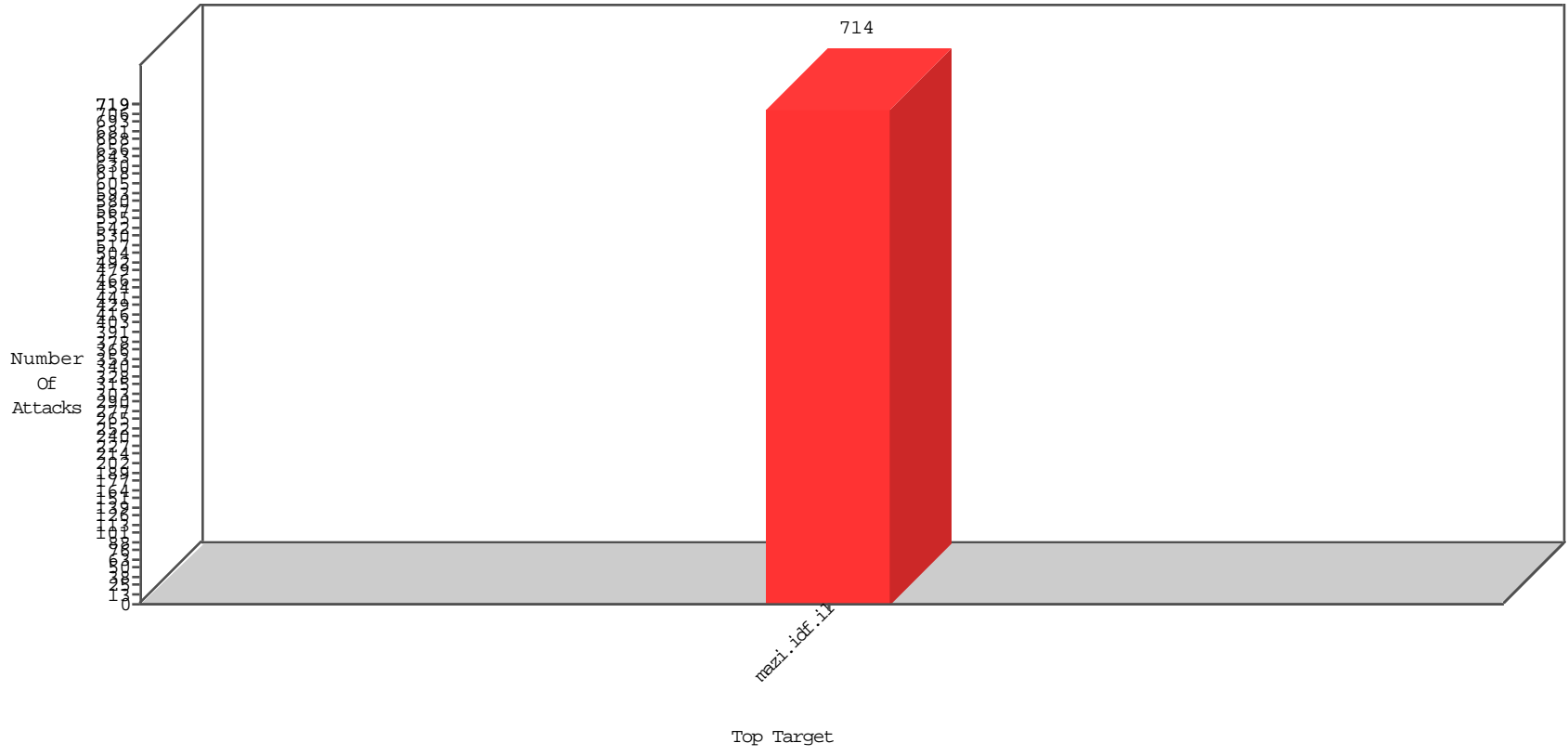


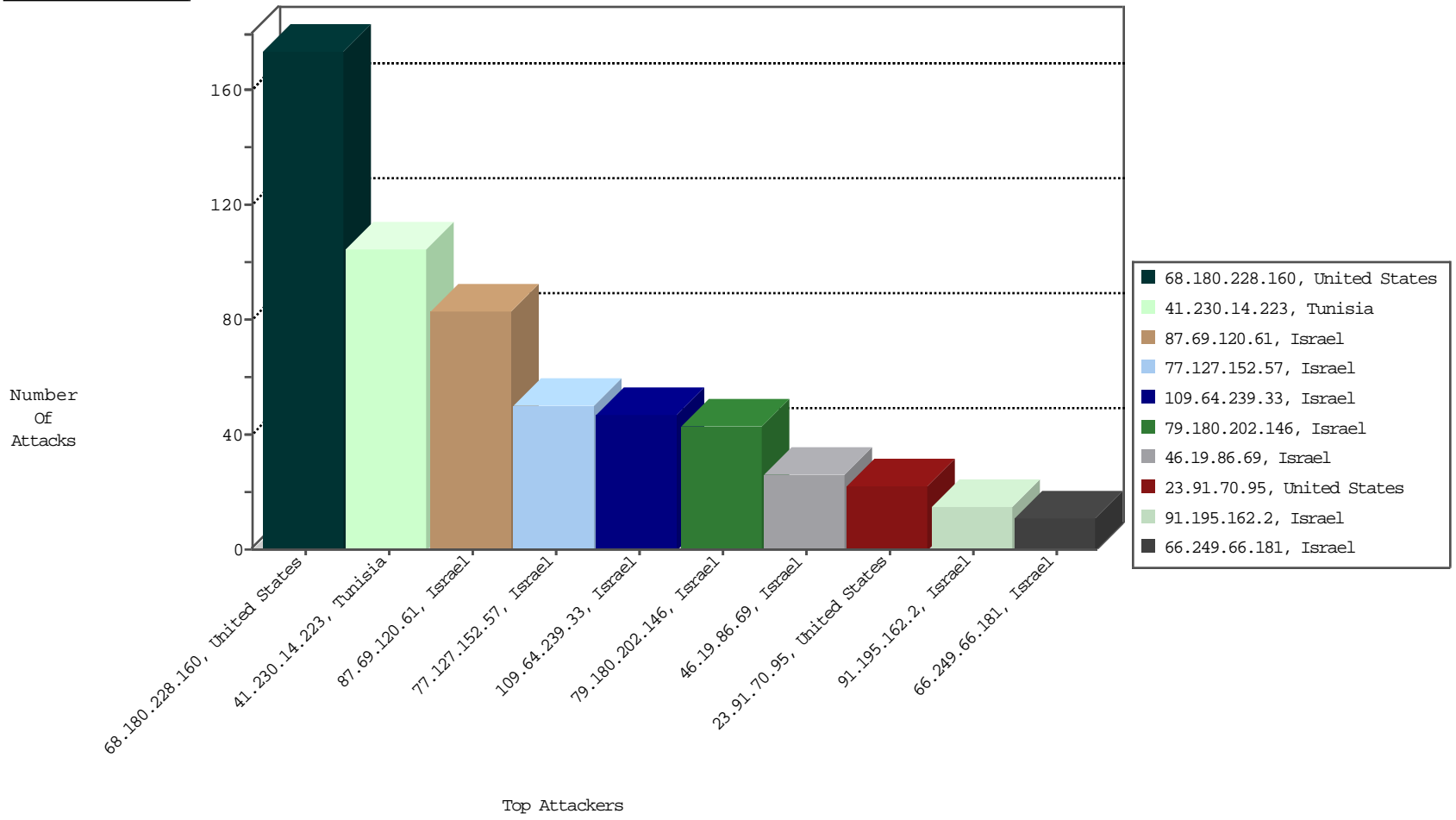
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
54.72.182.187	Ireland	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	NetV-London	3
136.243.48.86	Germany	147.237.77.17	mazi.idf.il	JLM_Purple_Con_Limit_Http	drop	NetV-London	3
136.243.48.86	Germany	147.237.77.17	mazi.idf.il	JLM_Under_Attack_Con_Http	drop	NetV-London	2
89.248.160.132	Netherlands	147.237.77.17	mazi.idf.il	block-sp-trafl	drop	NetV-London	1
184.105.139.100	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
68.180.228.160	United States	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	174
87.69.120.61	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	83
77.127.152.57	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	50
109.64.239.33	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	47
79.180.202.146	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	43
91.195.162.2	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	15
66.249.66.181	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
85.65.24.67	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
2.54.8.118	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
149.88.223.106	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
23.91.70.95	United States	147.237.77.17	mazi.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
23.91.70.95	United States	147.237.77.17	mazi.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
66.249.66.184	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
66.249.66.181	United States	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
66.249.66.187	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
106.38.241.106	China	147.237.77.17	mazi.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
37.26.146.219	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
41.230.14.223	Tunisia	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
80.246.133.19	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
23.91.70.95	United States	147.237.77.17	mazi.idf.il	SQL Injection - Select From	10
13.75.95.104	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -f -sS	1
13.75.95.104	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 3072	1
94.102.48.193	Netherlands	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
162.219.2.60	Canada	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
13.75.95.104	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 2048	1
104.192.0.20	United States	147.237.77.17	mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
209.126.116.147	United States	147.237.77.17	mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
41.230.14.223	Tunisia	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1211
31.168.16.60	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	100
46.19.85.155	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	51
46.19.85.155	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	36
46.19.85.216	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	25
106.38.241.106	China	147.237.77.17	mazi.idf.il	drop	SAM rule	drop	17
46.19.85.231	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
46.19.85.231	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
213.8.204.78	Israel	147.237.77.17	mazi.idf.il	drop	SAM rule	drop	8
79.127.43.222	Iran, Islamic Republic of	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.127.43.222	Iran, Islamic Republic of	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.3.147.179	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
87.69.120.61	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
172.56.42.198	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.102.195.250	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
149.88.126.60	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.69	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
157.55.39.222	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.92	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.127.43.149	Iran, Islamic Republic of	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.22.131.86	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
136.243.5.215	Germany	147.237.77.17	mazi.idf.il	drop	SAM rule	drop	2
85.93.91.84	Germany	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
185.3.147.84	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
87.69.120.61	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
79.127.43.149	Iran, Islamic Republic of	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.19.85.195	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
178.137.209.205	Ukraine	147.237.77.17	mazi.idf.il	drop	SAM rule	drop	2
217.132.97.197	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.46.41.125	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
81.65.166.149	France	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.29.158.249	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
157.55.39.146	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.86.146	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
94.230.86.214	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
41.230.14.223	Tunisia	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
31.154.14.43	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
80.178.157.116	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
157.55.39.224	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.29.44.234	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
69.40.184.98	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
149.78.91.116	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.52	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
109.253.222.126	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
217.132.240.250	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
89.248.160.132	Netherlands	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
207.46.13.176	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
37.142.198.214	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
81.65.166.149	France	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
176.13.21.77	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
41.230.14.223	Tunisia	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 41.230.14.223	Block	98
46.19.86.69	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 46.19.86.69	Block	25
95.86.114.24	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	10
217.132.97.197	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	4
79.181.141.191	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	2
85.93.91.84	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	2
80.246.133.48	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/571-he/igf.aspx	Block	1
207.46.13.176	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/3697-9630-he/igf.aspx 10 x'x x*x'xž'x" 2010	Block	1
141.212.122.129	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to /x	Block	1
66.249.66.184	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/700-he/bayabashaarchive.aspx	Block	1
41.230.14.223	Tunisia	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5551-11516-he/	Block	1
93.172.168.193	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
87.70.48.31	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/xmlrpc.php	Block	1
8.37.71.88	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/113-8000-he/igf.aspx&usg=alkjrhpp7d7zha3pfdmvoozl6fsykua	Block	1
213.57.32.19	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
84.109.3.71	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	NULL Character in Method	Block	1
109.66.13.110	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
46.117.4.116	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-en/igf.aspx	Block	1
89.139.158.254	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
41.230.14.223	Tunisia	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/307-0-he/igf.aspx&send=false&layout=button_count&width=90&show_faces=false&action=like&colorScheme=light&font=arial&height=21	Block	1
5.29.74.167	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
87.70.2.90	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
84.108.186.33	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
207.241.229.222	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/vodchannel/	Block	1
157.55.39.0	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/14-8333-he	Block	1
66.249.66.185	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
41.230.14.223	Tunisia	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5579-7562-he/undefined	Block	1
94.230.93.72	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
89.138.106.196	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
31.154.165.137	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 31.154.165.137	Block	1
213.57.149.169	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
84.109.107.72	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
79.181.141.191	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/xmlrpc.php	Block	1
197.35.225.175	Egypt	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
109.66.13.110	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 109.66.13.110	Block	1
66.249.66.46	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/14-8333-he	Block	1
41.230.14.223	Tunisia	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/3848-5183-he/undefined	Block	1
89.248.160.132	Netherlands	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/xmlrpc.php	Block	1
87.70.2.90	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/xmlrpc.php	Block	1
5.29.74.167	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/xmlrpc.php	Block	1
84.108.186.33	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 84.108.186.33	Block	1
213.8.204.24	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	Abnormally Long Request method	Block	1
66.249.66.188	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3848-5183-he/igf.aspx	Block	1
94.230.93.72	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/xmlrpc.php	Block	1
89.138.106.196	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/xmlrpc.php	Block	1
31.154.165.137	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/1/	Block	1
213.57.149.169	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
84.109.107.72	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
79.181.141.191	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 79.181.141.191	Block	1
197.35.225.175	Egypt	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/xmlrpc.php	Block	1
136.243.48.86	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-5475-he	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
41.230.14.223	Tunisia	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5535-0-he/igf.aspx&send=false&layout=button_count&width=90&show_faces=false&action=like&colorScheme=light&font=arial&height=21	Block	1
93.172.168.193	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
87.70.48.31	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
8.37.70.237	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/4166-he/igf.aspx&usg=alkjrhi9lw0av3czdjutm3fvsj_utqeg-w	Block	1
213.8.204.24	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
84.109.3.71	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	Block	1
68.180.229.218	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/14-8330-he	Block	1
46.19.86.69	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/4/2054.jp	Block	1
89.139.158.254	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1