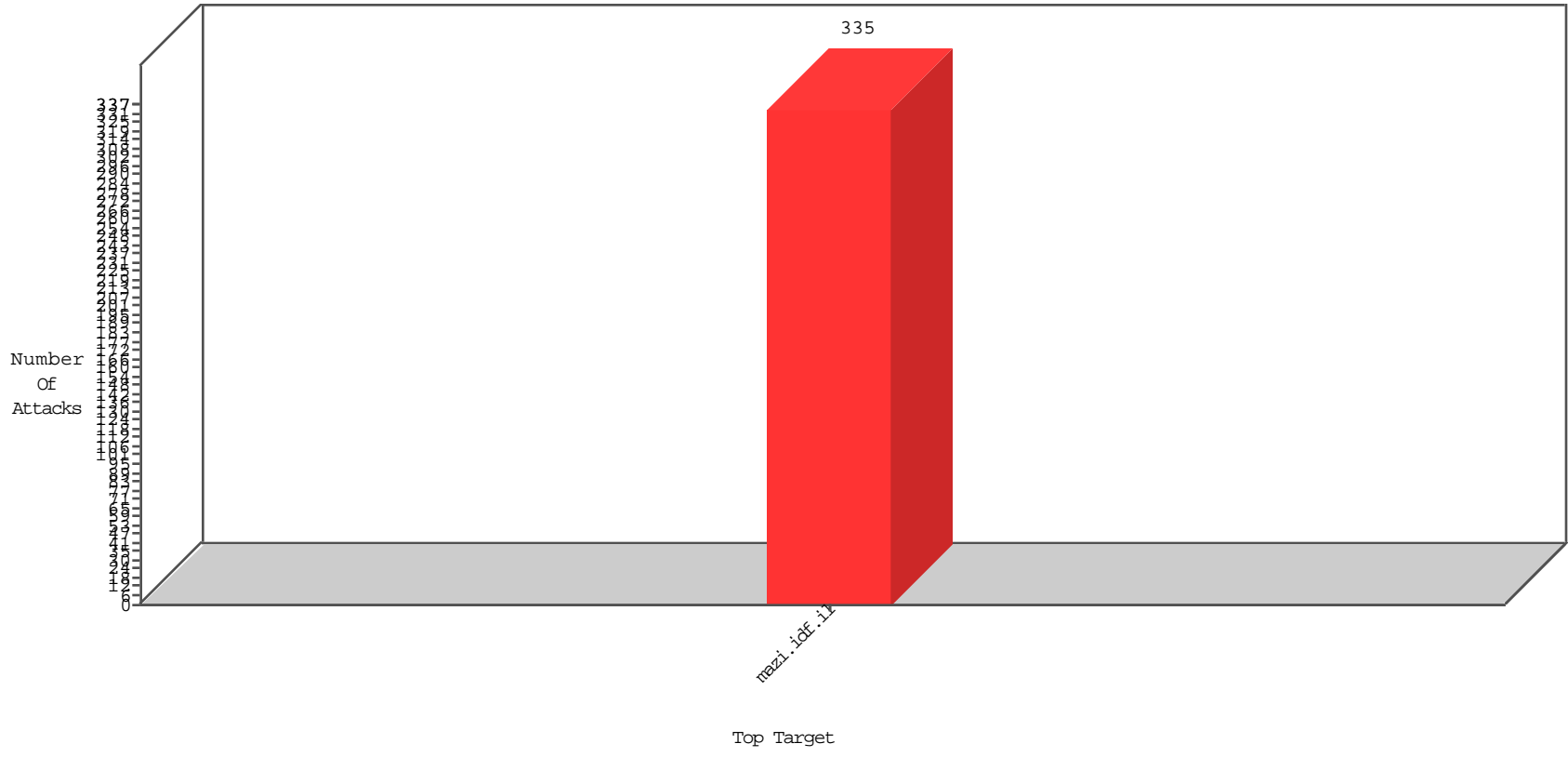


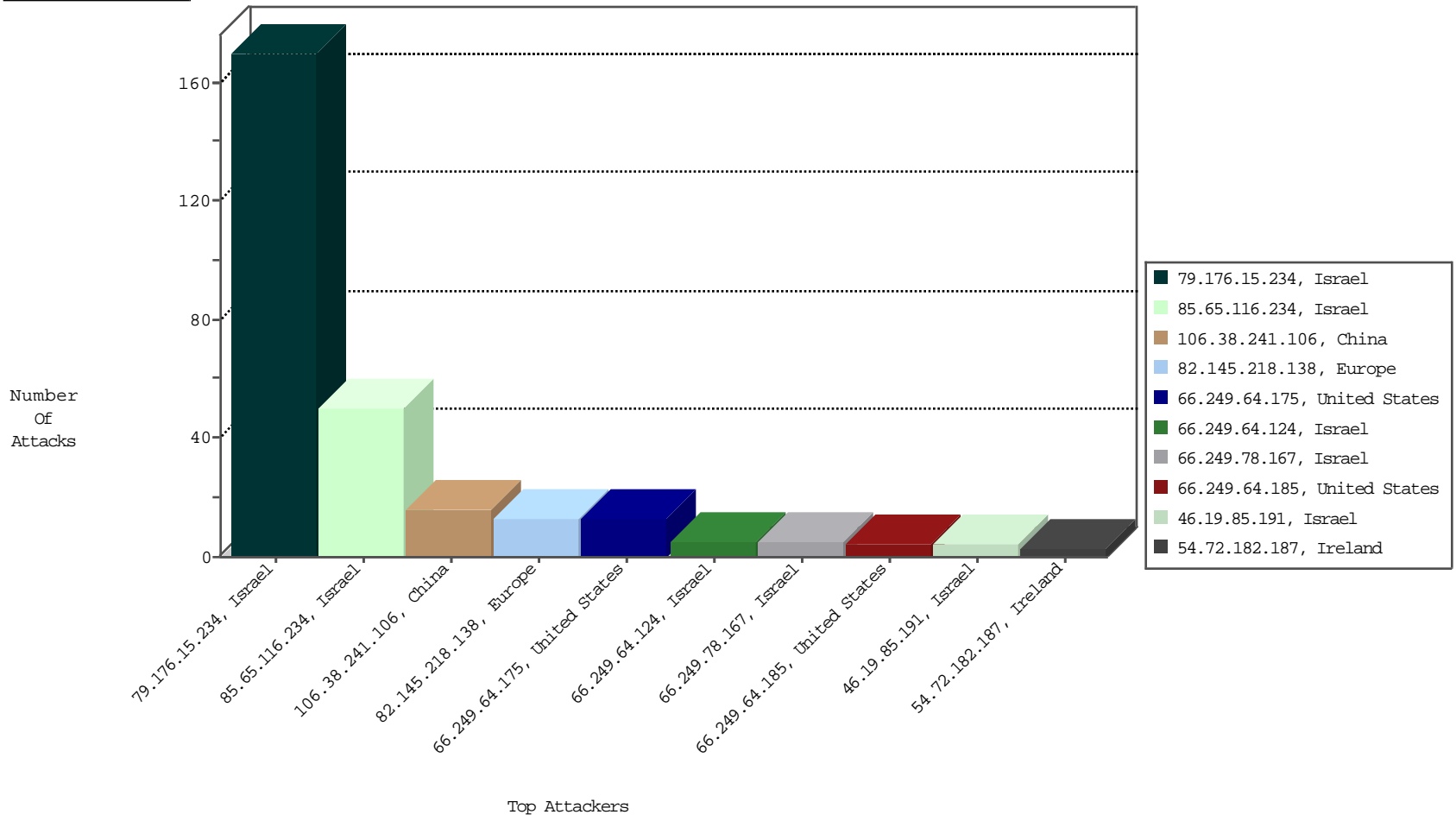
# Focused IP Under Attack Daily Report



## Top Targets



## Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
82.145.218.138	Europe	147.237.77.17	mazi.idf.il	Block_Ip_Web_In	drop	NetV-London	13
54.72.182.187	Ireland	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	NetV-London	3
64.94.179.60	United States	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	NetV-London	1
123.203.72.247	Hong Kong	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	NetV-London	1
184.105.139.110	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
79.176.15.234	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	170
85.65.116.234	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	50
106.38.241.106	China	147.237.77.17	mazi.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	16
66.249.78.167	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
66.249.64.124	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
66.249.64.2	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
62.210.107.201	France	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.215.130	United States	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	2
66.249.78.174	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
66.249.64.8	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

## Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
66.249.64.16	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.21	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
93.174.93.144	Netherlands	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
40.113.118.99	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 2048	1
59.45.79.117	China	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
146.185.250.2	Russian Federation	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
40.113.118.99	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -f -sS	1
40.113.118.99	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 3072	1

## Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
46.32.170.122	Azerbaijan	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	82
77.126.167.182	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
212.76.127.219	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
61.216.2.14	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
109.67.223.62	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	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
106.38.241.106	China	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	7
192.243.55.136	Dominica	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.131	Dominica	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.136	Dominica	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
46.120.74.223	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
46.120.74.223	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.136	Dominica	147.237.77.17	mazi.idf.i	Bad TCP sequence		monitor	4
192.243.55.132	Dominica	147.237.77.17	mazi.idf.i	Bad TCP sequence		monitor	4
37.26.148.222	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
109.253.158.191	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
87.69.231.58	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
192.243.55.136	Dominica	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	3
192.243.55.136	Dominica	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
61.216.2.14	Taiwan	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
192.243.55.129	Dominica	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
192.243.55.137	Dominica	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
192.243.55.131	Dominica	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
192.243.55.138	Dominica	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
192.243.55.131	Dominica	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
192.243.55.132	Dominica	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
37.46.41.183	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.190	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
198.54.90.200	United States	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	1
2.52.175.6	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
66.249.81.219	Israel	147.237.77.17	mazi.idf.i	Directory Traversal	directory traversal overflow	monitor	1
192.243.55.134	Dominica	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
46.121.57.149	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.181	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.126	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.243.31.2	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.22.135.174	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
109.253.208.185	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
192.243.55.138	Dominica	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
87.69.235.203	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
61.216.2.14	Taiwan	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Response out of state	monitor	1
192.243.55.132	Dominica	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
192.243.55.130	Dominica	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
37.142.142.136	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
149.78.219.2	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
2.52.175.6	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	1
106.38.241.106	China	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
192.243.55.138	Dominica	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
192.243.55.135	Dominica	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1

## Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
66.249.64.175	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	2
79.180.14.116	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
46.19.85.191	Israel	147.237.77.17	mazi.idf.i	Illegal HTTP Version push_time_start=1456478814875	Block	1
66.249.78.242	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6051-he/igf.aspx	Block	1
66.249.64.180	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/599-he/igf.aspx	Block	1
157.55.39.178	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
66.249.64.175	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5039-he/igf.aspx	Block	1
61.216.2.14	Taiwan	147.237.77.17	mazi.idf.i	Multiple Illegal Byte Code Character in Method from 61.216.2.14	Block	1
109.64.48.94	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3848-5183-he/igf.aspx	Block	1
5.39.222.159	Netherlands	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/rom-0	Block	1
66.249.81.219	United States	147.237.77.17	mazi.idf.i	URL is Above Root Directory m.mazi.idf.il/./images/body.jpg	Block	1
66.249.64.185	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/96-he/igf.aspx	Block	1
66.249.64.175	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/671-he/igf.aspx	Block	1
66.249.64.175	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/41-he/igf.aspx	Block	1
148.251.21.227	Germany	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 148.251.21.227	Block	1
91.196.50.33	Poland	147.237.77.17	mazi.idf.i	Unauthorized URL Access to testp2.czar.bielawa.pl/testproxy.php	Block	1
46.19.85.191	Israel	147.237.77.17	mazi.idf.i	Malformed URL k_visit=2;	Block	1
66.249.78.248	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6056-he/igf.aspx	Block	1
66.249.64.180	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/707-he/igf.aspx	Block	1
157.55.39.179	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6216-he/igf.aspx	Block	1
66.249.64.175	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5478-he/igf.aspx	Block	1
66.249.64.175	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/101-he/igf.aspx	Block	1
109.253.158.191	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/favicon.ico	Block	1
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5676-7827-he/igf.aspx	Block	1
40.77.167.46	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
66.249.64.185	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
66.249.64.175	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/70-he/igf.aspx	Block	1
66.249.64.175	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4275-he/igf.aspx	Block	1
148.251.21.227	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
94.199.151.22	United Kingdom	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5676-7827-he/igf.aspx	Block	1
46.19.85.191	Israel	147.237.77.17	mazi.idf.i	Unknown HTTP Request Method 6478784862; in URL k_visit=2	Block	1
66.249.78.254	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4275-he/igf.aspx	Block	1
66.249.64.185	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5374-he/igf.aspx	Block	1
208.115.111.75	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/14-5475-he	Block	1
66.249.64.175	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/55-he/igf.aspx	Block	1
113.76.90.196	China	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
77.126.167.182	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
46.19.85.191	Israel	147.237.77.17	mazi.idf.i	Distributed Abnormally Long Request	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
66.249.64.180	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4419-he/igf.aspx	Block	1
157.55.39.68	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/4085-he/	Block	1
66.249.64.175	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5013-he/igf.aspx	Block	1
107.178.38.31	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
46.32.170.122	Azerbaijan	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4637-5227-he/igf.aspx	Block	1
2.54.42.66	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1
66.249.78.254	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
66.249.64.185	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5551-he/igf.aspx	Block	1
66.249.64.175	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6216-he/igf.aspx	Block	1
66.249.64.175	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3433-he/igf.aspx	Block	1
141.212.122.177	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1