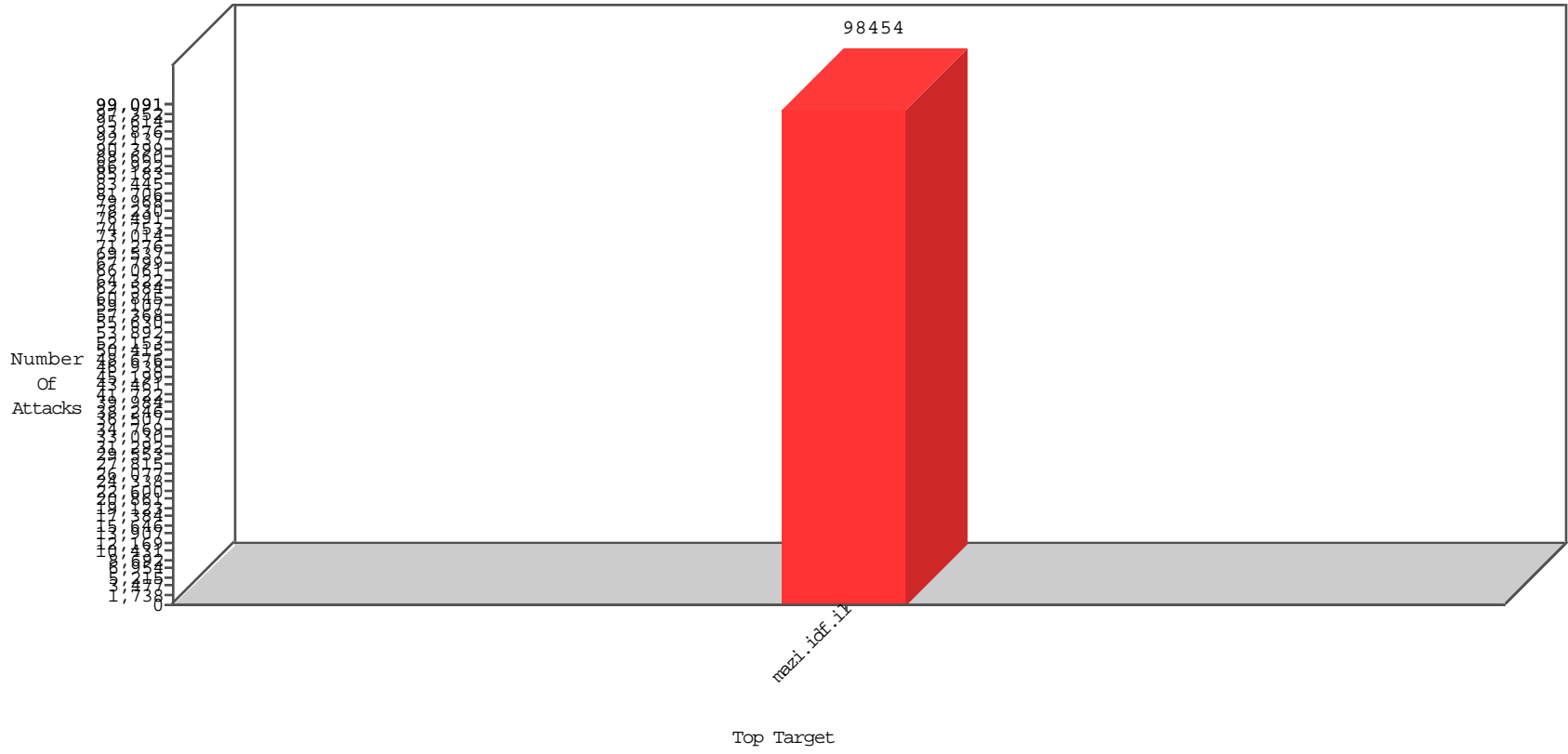


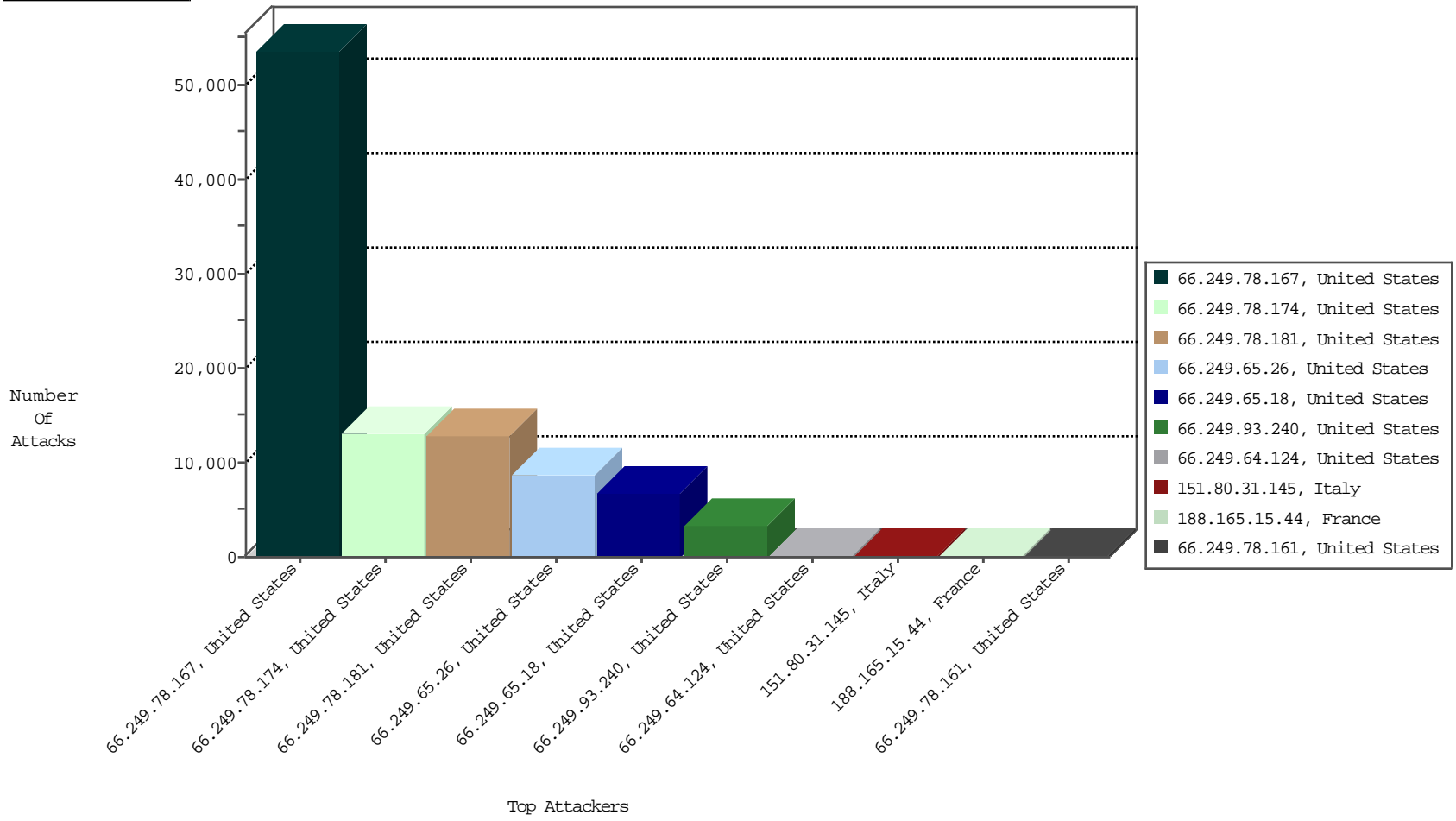
# Focused IP Under Attack Daily Report



## 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	United States	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	53665
66.249.78.174	United States	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	13101
66.249.78.181	United States	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	12773
66.249.65.26	United States	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	8675
66.249.65.18	United States	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	6636
66.249.93.240	United States	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	3273
66.249.64.124	United States	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	118
84.109.114.52	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	3
109.66.37.93	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	2
149.78.135.239	Israel	147.237.77.17	mazi.idf.il	Invalid TCP Flags	drop	BBL-Israel	2

11-12-2015 to 11-13-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
151.80.31.145	Italy	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	60
188.165.15.44	France	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	38
188.165.15.227	France	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	6
220.156.184.4	India	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	3
77.127.225.88	Israel	147.237.77.17	mazi.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
151.80.31.117	Italy	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	1
189.38.90.150	Brazil	147.237.77.17	mazi.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1
189.38.90.150	Brazil	147.237.77.17	mazi.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

## Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
66.249.78.161	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	16
189.38.90.150	Brazil	147.237.77.17	mazi.idf.il	SQL Injection - Select From	5
66.249.65.22	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	4
66.249.78.167	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	4
66.249.65.18	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.181	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	1
172.248.238.74	United States	147.237.77.17	mazi.idf.il	Tehila - Perl LWP with fake user agent	1
210.117.121.60	Korea, Republic of	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 2048	1
66.249.78.174	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	1
88.198.167.80	Germany	147.237.77.17	mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
177.185.214.30	Brazil	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
210.117.121.60	Korea, Republic of	147.237.77.17	mazi.idf.il	ET SCAN NMAP -f -sS	1
210.117.121.60	Korea, Republic of	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 3072	1
59.45.79.117	China	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
54.244.22.103	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	81
77.126.99.23	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	80
54.244.22.103	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	64
73.134.243.249	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid sequence number	monitor	36
46.116.74.116	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid sequence number	monitor	36
73.134.243.249	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	36
46.116.74.116	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	36
68.180.228.160	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	34
46.117.154.217	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
46.120.56.70	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
176.12.141.221	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
46.117.154.217	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid sequence number	monitor	25
216.207.157.78	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
208.115.111.75	United States	147.237.77.17	mazi.idf.il	drop	SAM rule	drop	23
52.33.66.29	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
79.178.122.208	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
79.178.122.208	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid sequence number	monitor	17
46.120.56.70	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
208.115.113.91	United States	147.237.77.17	mazi.idf.il	drop	SAM rule	drop	16
109.64.125.170	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.86.199	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
212.179.21.194	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
109.64.125.170	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid sequence number	monitor	16
212.179.21.194	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
188.120.148.213	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
94.228.34.249	United Kingdom	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
157.55.39.34	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
157.55.39.208	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
68.180.228.160	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
207.46.13.46	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
85.250.20.92	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
109.186.68.201	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid sequence number	monitor	9
85.250.20.92	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid sequence number	monitor	9
192.115.101.101	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
188.120.148.246	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
109.186.68.201	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
141.0.12.190	Norway	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
94.228.34.249	United Kingdom	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
157.55.39.64	United States	147.237.77.17	mazi.idf.il	drop	SAM rule	drop	6
66.249.78.174	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
207.46.13.20	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
207.46.13.56	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.67	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
149.88.59.134	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.115.101.101	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.54.180.200	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
141.0.12.190	Norway	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.131	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.65.26	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
149.88.59.134	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

## Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
81.218.251.251	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	2
66.249.78.3	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/templates/newslist/undefined	Block	2
79.182.12.198	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	2
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3697-10520-he/igf.aspx	Block	1
212.76.119.62	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/4450-he/igf.aspx&sa=u&ved=0ca4qfjacahukewid3jhp14rjahul8xikhtlcat0&sg=afqjcnevz5hduuxeslhq-jtqm06zydwqsa	Block	1
66.249.65.22	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/700-he/bayabashaarchive.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
193.201.224.186	Ukraine	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 193.201.224.186	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
66.249.78.254	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3728-6976-he/igf.aspx	Block	1
66.249.65.238	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
207.46.13.20	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/113-11516-he/xžx@xæx'x™x? x\$x"x™xæx".aspx	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
157.55.39.131	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/	Block	1
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-5475-he	Block	1
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3697-10782-he/igf.aspx	Block	1
213.151.53.59	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/2061.jpg	Block	1
66.249.65.26	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/4	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
193.201.224.186	Ukraine	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
84.94.92.189	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/2061.jpg	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
66.249.78.254	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/700-he/igf.aspx	Block	1
207.46.13.46	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8330-he	Block	1
45.55.41.246		147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 45.55.41.246	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
192.0.100.18	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/3849-5035-he/igf.aspx	Block	1
79.176.188.77	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/2061.jpg	Block	1
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5039-he/igf.aspx	Block	1
216.207.157.78	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
66.249.65.231	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/113-8450-he/igf.aspx	Block	1
31.184.134.21	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
207.46.13.20	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8346-he	Block	1
95.86.95.127	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/6368-9571-he/igf.aspx&sa=u&ved=0ccmqqoubmajqfotci7yztufi8kcfurrfaodnu0fhq&sig2=co31fblrylm_v-juzaeba&usg=afqjcneujm90ac3im9ym6ngdmg5lx9p_gg	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
66.249.78.254	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
66.249.78.174	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
208.115.111.75	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
45.55.41.246		147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/450-he.aspx	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
192.0.100.18	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	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
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4637-5227-he/igf.aspx	Block	1
66.249.65.231	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1
207.46.13.20	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-he/	Block	1
31.184.134.23	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
117.78.13.29	China	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/14-he	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
66.249.93.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1