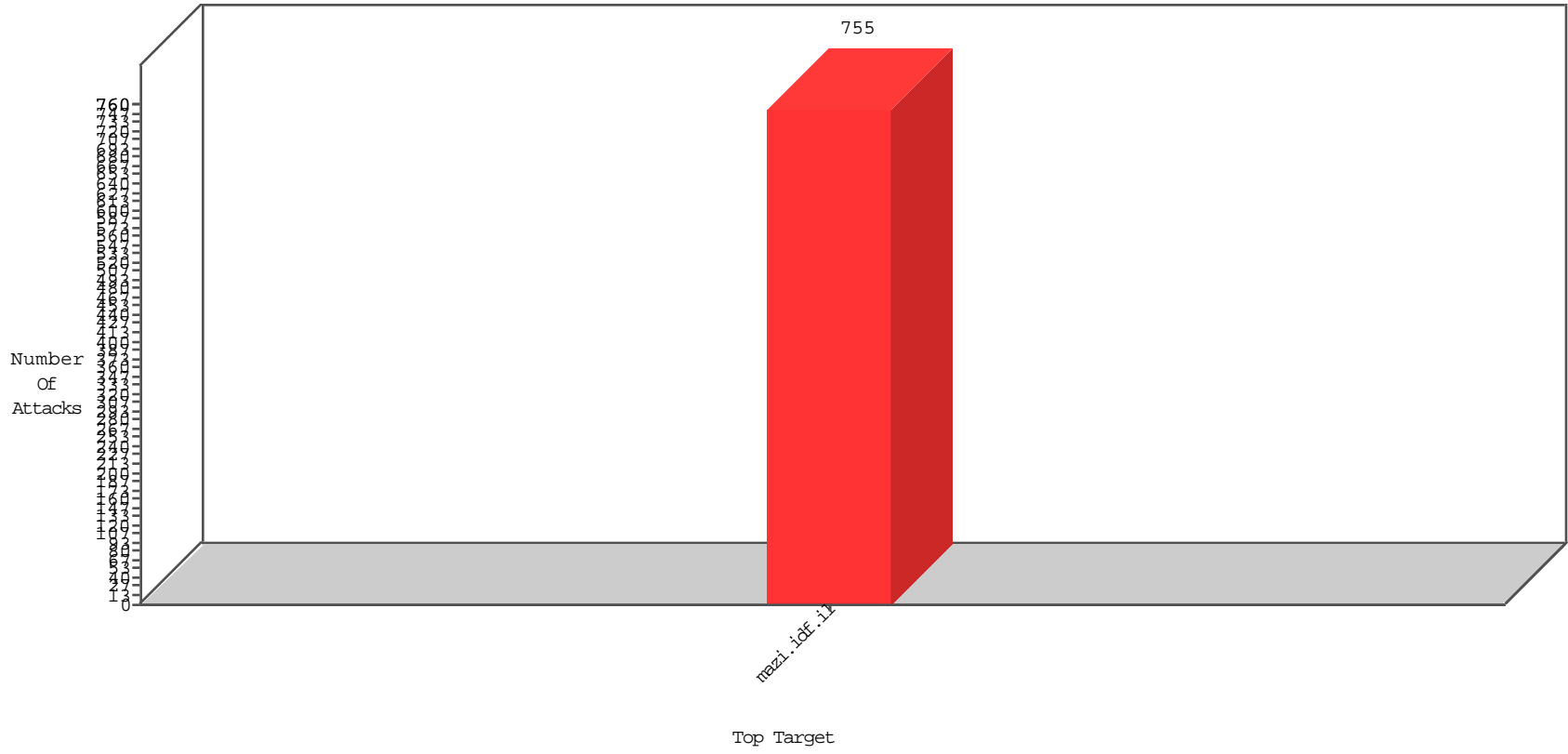


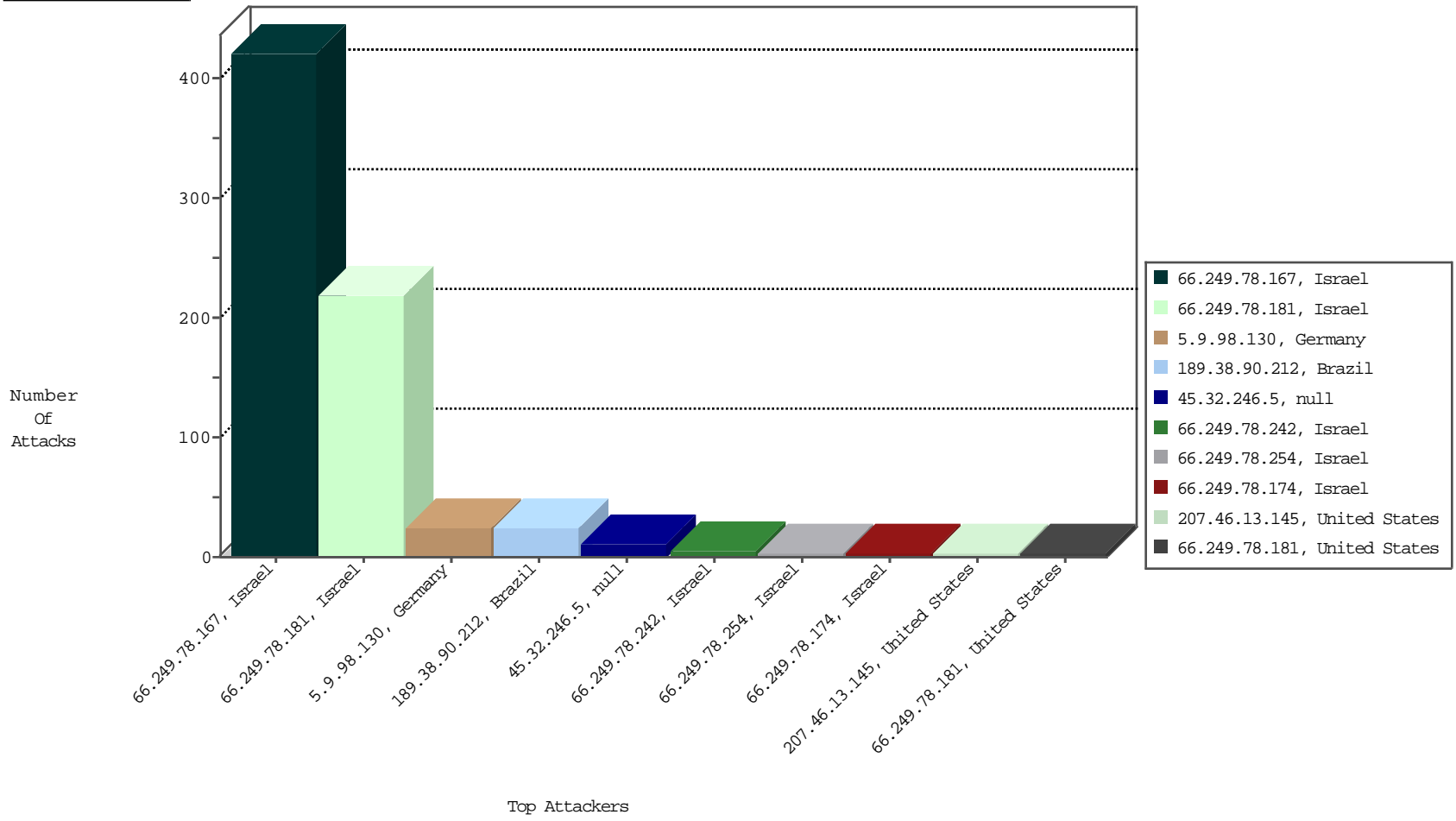
Focused IP Under Attack Daily Report



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	419
66.249.78.181	Israel	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	218
45.32.246.5		147.237.77.17	mazi.idf.il	Invalid TCP Flags	drop	BBL-Frankfurt	5
107.150.43.205	United States	147.237.77.17	mazi.idf.il	block-sp-traf1	drop	BBL-Frankfurt	1

12-08-2015 to 12-09-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
220.156.184.4	India	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	2
185.106.94.91		147.237.77.17	mazi.idf.il	C003: HTTP: phpMyAdmin access	Block	1
188.165.15.231	France	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	1

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
189.38.90.212	Brazil	147.237.77.17	mazi.idf.i	SQL Injection - Select From	24
66.249.78.174	United States	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sA (2)	2
66.249.78.181	United States	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sA (2)	2
45.32.246.5		147.237.77.17	mazi.idf.i	ET SCAN NMAP -f -sS	1
45.32.246.5		147.237.77.17	mazi.idf.i	ET SCAN NMAP -sS window 3072	1
45.32.246.5		147.237.77.17	mazi.idf.i	ET SCAN Potential SSH Scan	1
82.117.208.243		147.237.77.17	mazi.idf.i	ET SCAN NMAP -sS window 1024	1
45.32.246.5		147.237.77.17	mazi.idf.i	ET SCAN NMAP -sS window 2048	1
45.32.246.5		147.237.77.17	mazi.idf.i	ET SCAN NMAP -sS window 4096	1
59.45.79.117	China	147.237.77.17	mazi.idf.i	ET SCAN Potential SSH Scan	1
121.129.45.126	Korea, Republic of	147.237.77.17	mazi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
81.218.148.177	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid sequence number	monitor	53
45.32.246.5		147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	51
45.32.246.5		147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	49
46.19.86.1	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	38
79.182.101.220	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
88.212.40.229	Slovakia	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
5.28.159.7	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
185.106.94.2		147.237.77.17	mazi.idf.il	drop	SAM rule	drop	12
89.139.161.8	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
2.52.58.176	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
37.46.39.124	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.202	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
213.57.134.254	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
89.139.161.8	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	6
207.241.226.39	United States	147.237.77.17	mazi.idf.il	drop	SAM rule	drop	5
46.19.86.1	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.28	Israel	147.237.77.17	mazi.idf.il	SYN Attack		reject	4
85.93.91.84	Germany	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
79.180.62.211	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
109.67.217.250	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
213.57.135.234	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
85.64.215.25	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
128.232.110.28	United Kingdom	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
5.102.254.137	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.221	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.147.194	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.12.149.147	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
41.234.117.145	Egypt	147.237.77.17	mazi.idf.il	drop	SAM rule	drop	2
207.46.13.145	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.29.115	Israel	147.237.77.17	mazi.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
207.46.13.126	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
94.230.86.134	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.26.147.194	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
216.218.206.111	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
207.46.13.140	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.64	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.85.84	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.121.192	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
84.94.32.197	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
2.54.135.42	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.211	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.12.143.107	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.19.85.188	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.28	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
94.230.86.197	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.26.148.232	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
87.69.188.76	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
216.243.31.2	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.29.105.248	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.19.86.117	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
5.9.98.130	Germany	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 5.9.98.130	Block	24
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	2
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	2
89.139.161.8	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4637-5227-he/igf.aspx	Block	2
81.218.241.26	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/trans.gif	Block	1
66.249.78.254	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6578-9991-he/igf.aspx	Block	1
66.249.78.167	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-4980-he	Block	1
188.143.232.26	Russian Federation	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
108.61.211.243	Germany	147.237.77.17	mazi.idf.i	Admin Blocking	Block	1
79.180.140.100	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
66.249.78.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
66.249.78.174	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8334-he	Block	1
207.46.13.140	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8333-he	Block	1
157.55.39.9	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
40.77.167.0	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6221-9268-he/igf.aspx	Block	1
85.64.215.25	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	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 147.237.77.17/3850-5187-he/igf.aspx	Block	1
66.249.78.167	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8333-he	Block	1
188.143.232.41	Russian Federation	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 188.143.232.41	Block	1
108.61.211.243	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/admin	Block	1
5.9.98.130	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/shared/usercontrols/vodchannel/	Block	1
79.180.140.100	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
66.249.78.254	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3834-8928-he/igf.aspx	Block	1
66.249.78.181	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/450-he.aspx	Block	1
207.46.13.145	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8345-he	Block	1
157.55.39.241	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-4983-he	Block	1
40.77.167.0	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
85.93.91.84	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
79.177.128.113	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
66.249.78.174	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8330-he	Block	1
195.62.53.168	Russian Federation	147.237.77.17	mazi.idf.i	Unauthorized URL Access to /css/css	Block	1
131.253.36.205	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/templates/newslist/undefined	Block	1
31.13.100.112	Ireland	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/4634-5228-he/igf.aspx&sandbox=1	Block	1
80.254.120.27	Russian Federation	147.237.77.17	mazi.idf.i	Parameter Type Violation folderid in mazi.idf.il/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
66.249.78.254	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
207.46.13.145	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/common/logininfo.aspx	Block	1
66.249.78.230	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
176.228.186.39	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1
66.249.64.175	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
79.177.128.113	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/xmlrpc.php	Block	1
66.249.78.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5551-9439-he/igf.aspx	Block	1
66.249.78.174	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8331-he	Block	1
207.46.13.140	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 207.46.13.140	Block	1
157.55.39.9	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5010-9094-he/igf.aspx	Block	1
37.46.39.124	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files	Block	1