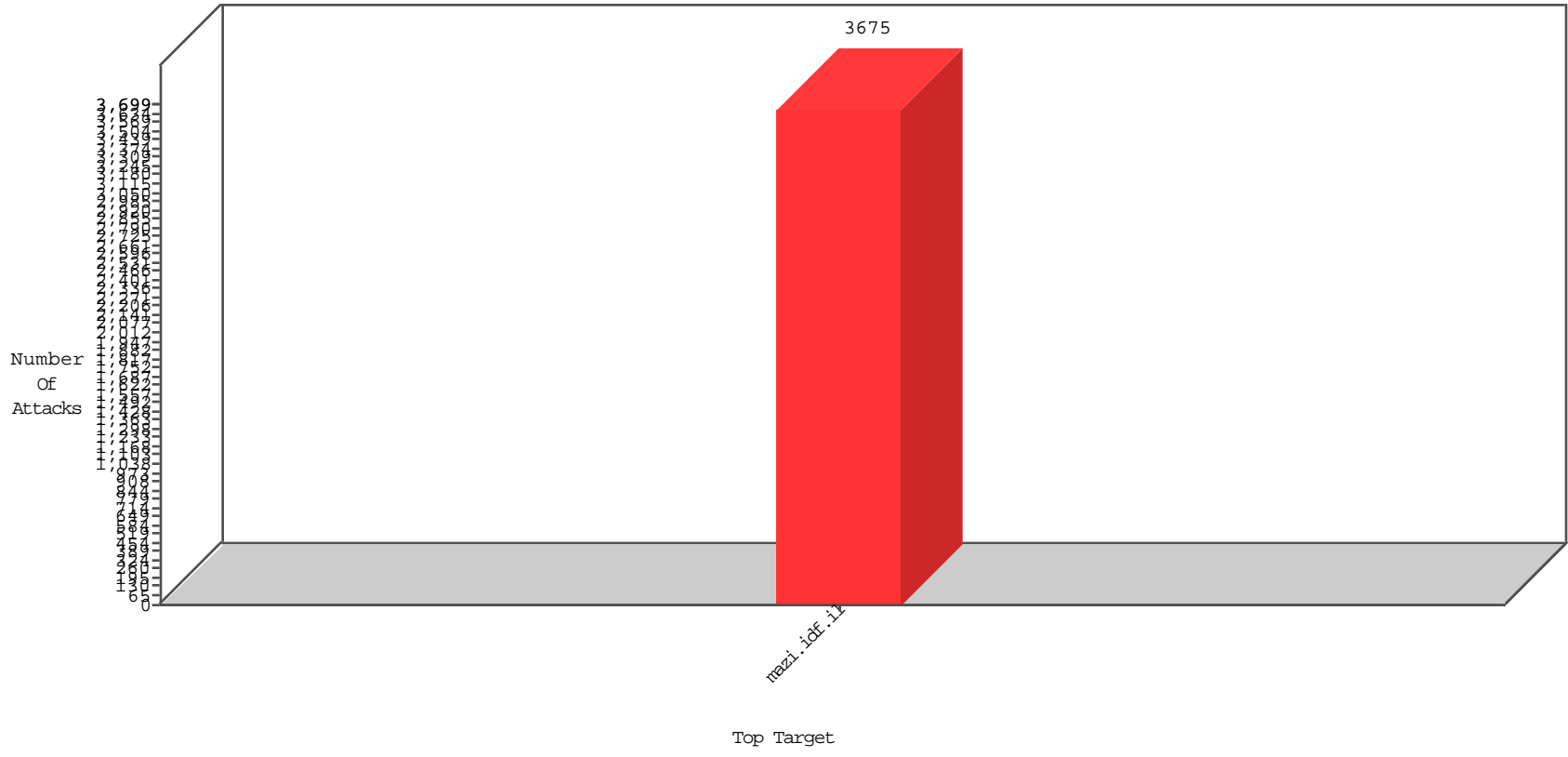


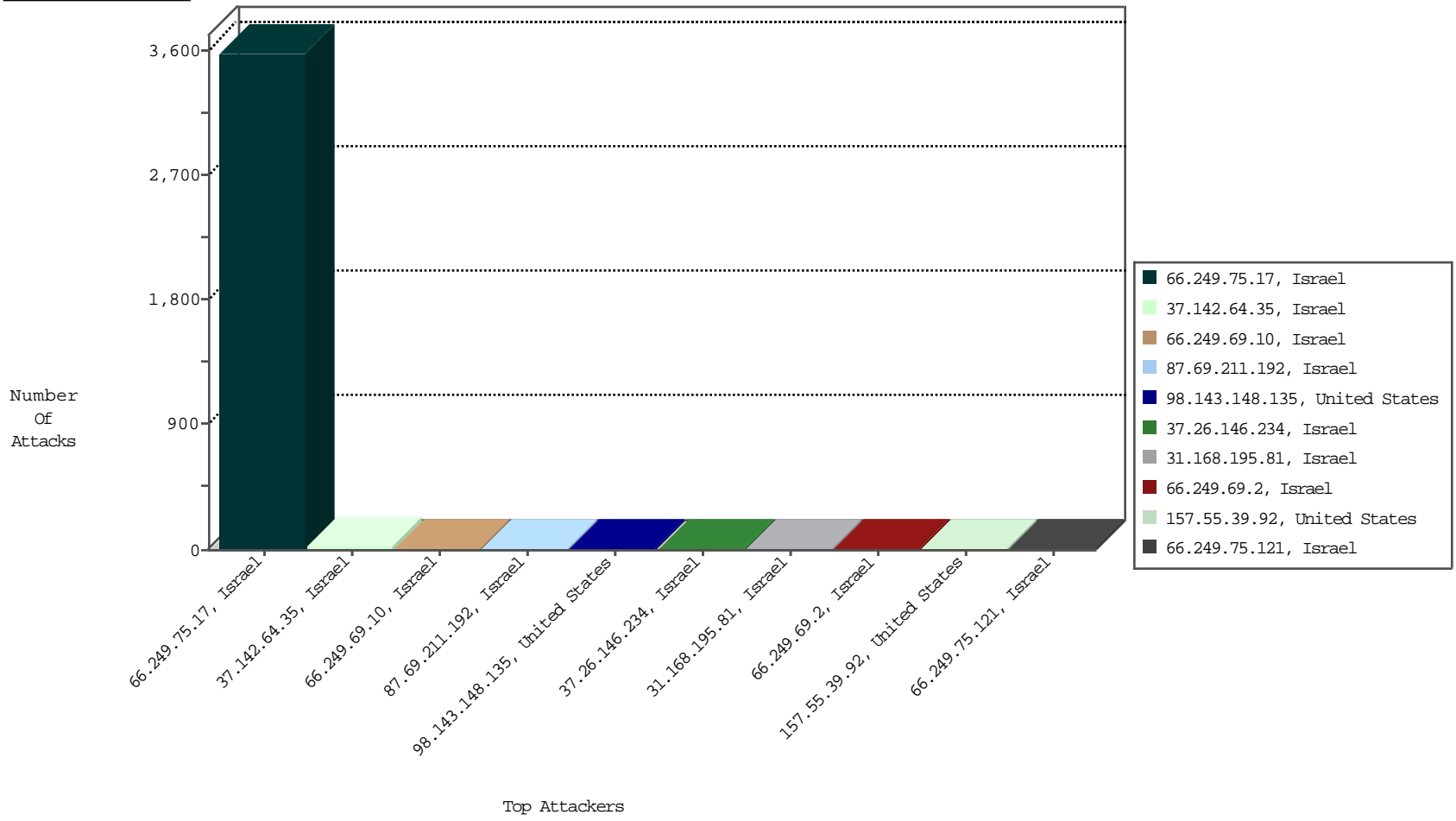
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



12-27-2015 to 12-28-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
66.249.75.17	Israel	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	3595

12-27-2015 to 12-28-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
------------------	--------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
89.248.174.28	Netherlands	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
104.197.83.150	United States	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.56		147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
218.1.31.135	China	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
104.192.0.226	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.178.31		147.237.77.17	mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.88		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
46.121.253.23	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1225
46.19.86.126	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	64
213.57.128.210	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	48
46.19.85.205	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
95.227.11.162	Italy	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	36
61.216.2.13	Taiwan	147.237.77.17	mazi.idf.i	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	36
195.189.193.1	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	33
128.127.107.123	Netherlands	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	30
79.178.127.87	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	29
46.19.86.126	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	25
46.19.85.101	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	22
46.19.86.26	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
46.19.85.101	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
31.210.186.157	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
212.76.127.10	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
24.38.192.108	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	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
195.239.16.53	Russian Federation	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
192.0.80.128	United States	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
165.225.76.55	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
213.57.140.221	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
86.57.167.45	Belarus	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
213.57.140.181	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.86.188	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
213.57.135.234	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
37.26.149.205	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.86.188	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
212.25.107.145	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
213.57.134.79	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.86.188	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	4
46.19.86.98	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
149.88.93.150	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
213.57.140.181	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
37.46.39.10	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
212.25.107.145	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
213.57.134.79	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.86.188	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
86.57.167.45	Belarus	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
213.57.140.181	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
109.65.128.166	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.188	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
79.183.29.81	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
213.57.135.234	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.26.149.205	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.188	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
213.8.204.51	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
84.109.96.11	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.86.26	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
176.13.7.214	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
2.181.231.149	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
37.142.64.35	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/xmlrpc.php	Block	9
37.142.64.35	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	5
37.142.64.35	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	4
149.88.93.150	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	2
31.168.195.81	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	2
37.26.146.234	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/4070-11595-he/xžx-xæx\$xa xax>x x*xÿ x*x'x\$xx".aspx	Block	2
157.55.39.92	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/templates/homepage	Block	2
2.54.31.51	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	2
66.249.69.18	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5477-he/igf.aspx	Block	1
61.216.2.13	Taiwan	147.237.77.17	mazi.idf.i	Illegal Byte Code Character in Method	Block	1
176.13.17.37	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/7343-11581-he/xæxæx? x'x'x*xæx*x ^a .aspx	Block	1
85.250.93.1	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
66.249.79.232	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
212.25.107.145	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation __EVENTVALIDATION in mazi.idf.il/mazi-site/105-he/igf.aspx	Block	1
66.249.69.10	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1
40.77.167.74	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 40.77.167.74	Block	1
157.55.39.169	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
98.143.148.135	United States	147.237.77.17	mazi.idf.i	Unknown HTTP Request Method [[#1]]I20100 in URL	Block	1
77.75.79.101	Czech Republic	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/9/8699.jpg	Block	1
66.249.75.121	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
207.46.13.141	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/robots.txt	Block	1
66.249.69.2	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/robots.txt	Block	1
157.55.39.25	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/watch_fragments_ajax	Block	1
95.86.90.222	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
66.249.79.245	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3697-9347-he/igf.aspx	Block	1
217.194.204.190	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation Master\$ucHeader\$ucSearchControl\$txtSearch in mazi.idf.il/120-he/igf.aspx	Block	1
66.249.69.10	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5675-7805-he/igf.aspx	Block	1
40.77.167.74	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/external/wpages/v12/directory/js/googlemapsjavascript.aspx	Block	1
157.55.39.232	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/599-he/igf.aspx&sa=u&ei=thgitootlm_goikmqlsf&ved=0cbqqfjad&usq=afqjcne_k0jl7d6l9f-7frdrpk8wb6topw	Block	1
104.131.147.112	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5216-he/igf.aspx	Block	1
84.229.191.20	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1
66.249.75.121	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/www.idiegogo.com/projects/121440	Block	1
207.46.13.168	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/9/8699.jpg	Block	1
66.249.69.2	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
40.77.167.9	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on www.mazi.idf.il/templates/homepage	Block	1
98.143.148.135	United States	147.237.77.17	mazi.idf.i	Illegal Byte Code Character in Method [[#1]]I20100	Block	1
68.180.230.40	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
66.249.69.18	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3834-6694-he/igf.aspx	Block	1
46.19.85.101	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
176.13.2.55	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/hi	Block	1
149.88.14.157	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
85.65.173.48	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
66.249.79.231	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
208.115.113.91	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-10105-he	Block	1
66.249.69.10	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3834-9547-he/igf.aspx	Block	1
40.77.167.61	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/3697-9630-he/igf.aspx 10 x³xÿ ÆçÄ½x³Ä x³xÿÄçÄ½x³xÿÄçÄ½x³xÿÄçÄ½x³xÿÄçÄ½x³xÿÄçÄ½x³Ä" 2010	Block	1
157.55.39.168	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/707-he/igf.aspx	Block	1
98.143.148.135	United States	147.237.77.17	mazi.idf.i	Malformed URL	Block	1
77.75.78.164	Czech Republic	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/9/8699.jpg	Block	1