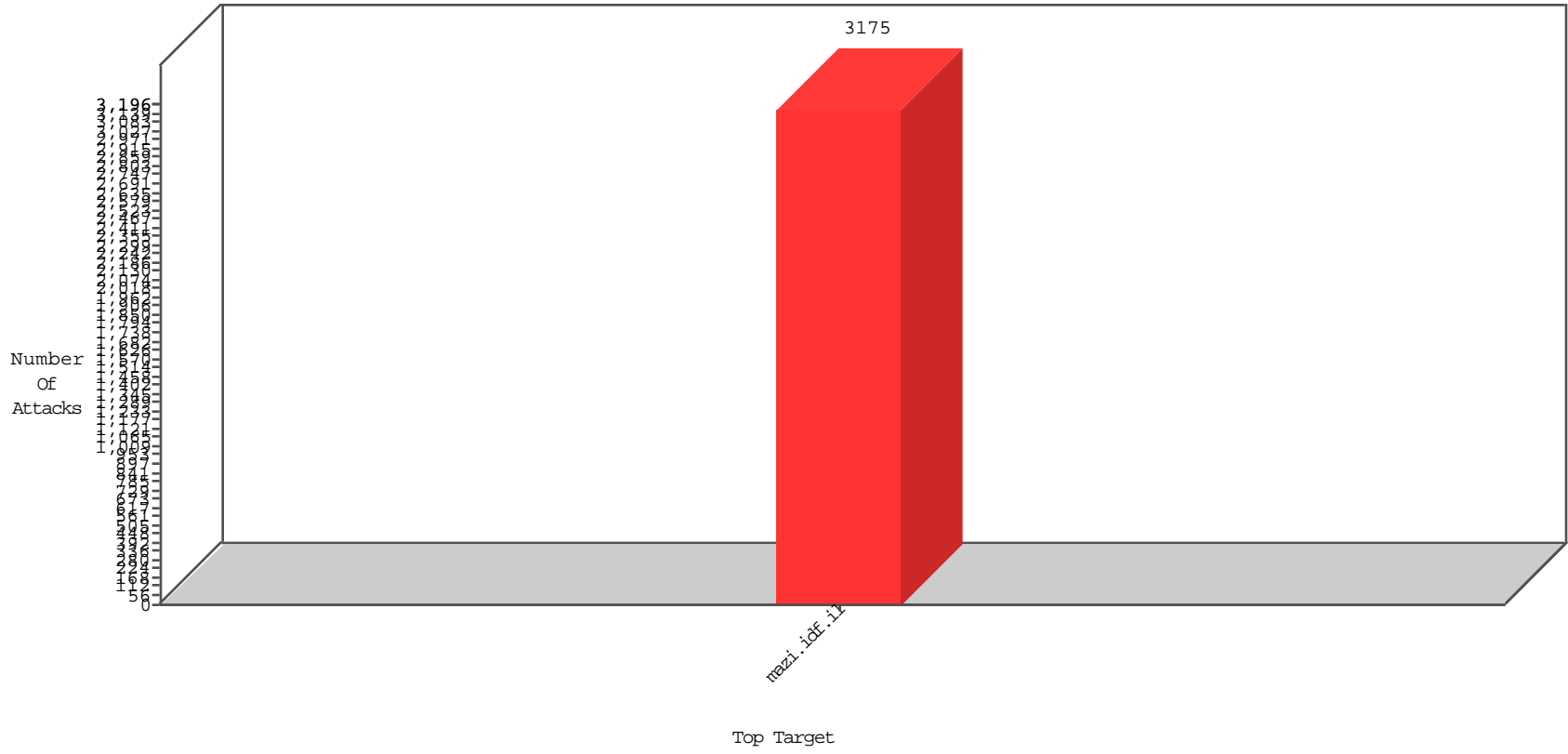


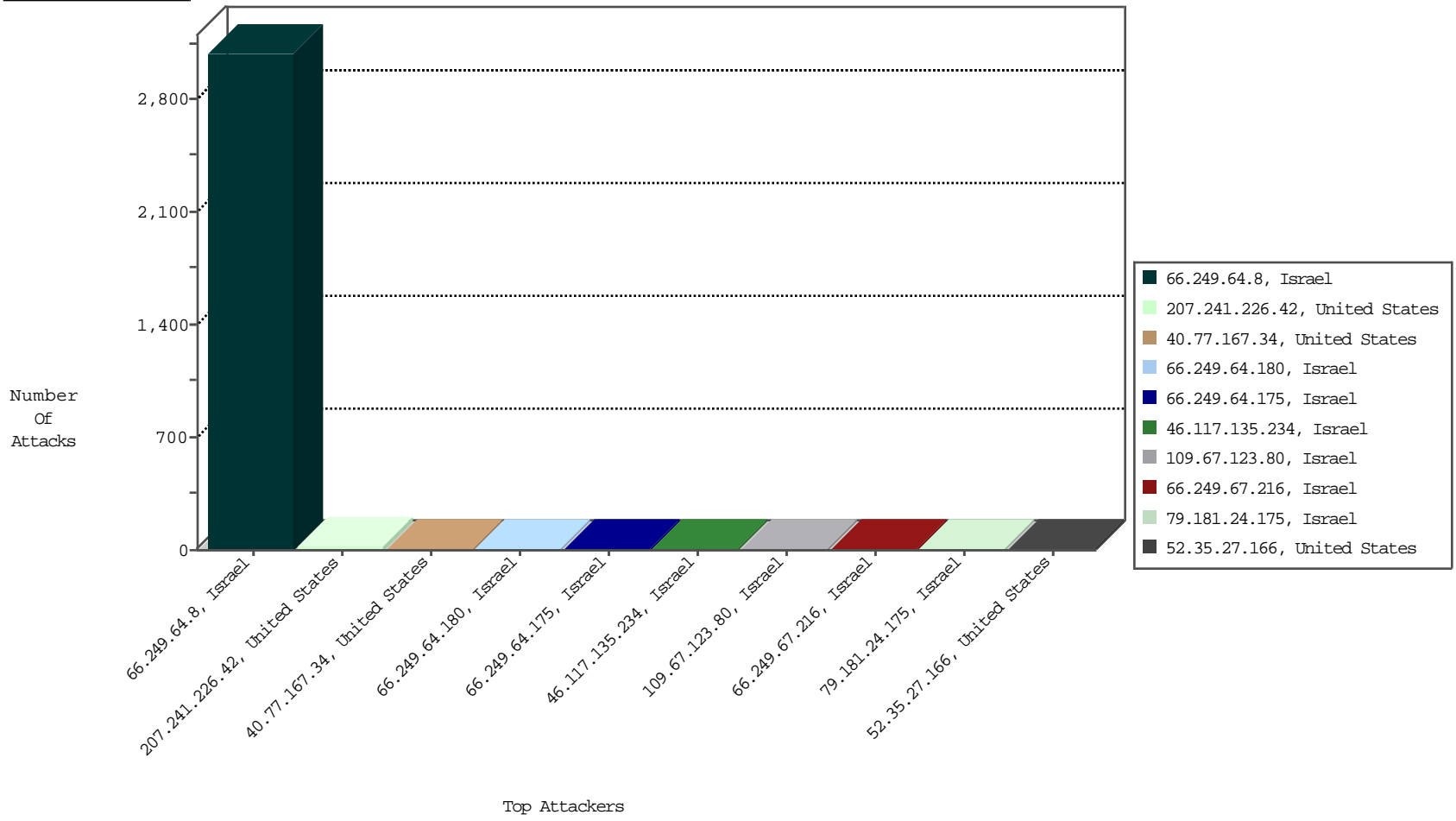
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



11-30-2015 to 12-01-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
66.249.64.8	Israel	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	3092

11-30-2015 to 12-01-2015

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
66.249.64.124	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
76.79.238.254	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	Netherlands	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	Ukraine	147.237.77.17	mazi.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
115.194.42.134	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
79.176.118.70	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	45
46.117.68.11	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	41
46.19.85.212	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	36
46.19.85.212	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	36
46.19.85.178	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	21
79.178.191.188	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
71.66.113.135	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
85.130.176.78	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	18
82.80.193.236	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
46.19.85.77	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
79.176.1.21	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
46.19.85.65	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	13
85.130.176.78	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
106.38.241.106	China	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	12
185.106.94.2		147.237.77.17	mazi.idf.i	drop	SAM rule	drop	10
46.19.86.247	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.86.72	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
46.120.162.189	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
61.216.2.15	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
31.210.186.147	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.178	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
213.57.140.211	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
31.168.164.87	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.109	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.129.81	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
213.57.139.94	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.52.129.81	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
213.57.129.112	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
2.52.129.81	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
94.179.51.113	Ukraine	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.181.143.151	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.65	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
2.52.129.81	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
213.57.129.112	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.86.72	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.52.129.81	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	4
213.57.134.190	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
31.154.91.43	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.247	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
31.168.113.109	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
2.54.42.201	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
46.19.86.114	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.120	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
61.216.2.15	Taiwan	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.46	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
89.138.91.100	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
79.180.138.186	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.142.177.153	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
66.249.67.248	Israel	147.237.77.17	mazi.idf.i	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	1
46.120.162.189	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
207.241.226.42	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 207.241.226.42	Block	11
207.241.226.42	United States	147.237.77.17	mazi.idf.i	PHP Attempt	Block	11
46.117.135.234	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/ufi/reaction/	Block	3
109.67.123.80	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	2
70.194.202.223	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/images/transvideocounter.gif	Block	2
79.181.24.175	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/	Block	2
40.77.167.34	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/4262-he/	Block	2
66.249.64.175	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/	Block	1
207.46.13.182	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
40.77.167.96	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8347-he	Block	1
84.94.119.247	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
66.249.67.216	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5222-6398-he/igf.aspx	Block	1
66.249.64.180	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3728-7059-he/igf.aspx	Block	1
212.150.214.106	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/2061.jpg	Block	1
157.55.39.50	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/113-11581-he/xæxæ? x'x'x*xæx*x^a.aspx	Block	1
52.35.27.166	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/wp-login.php	Block	1
40.77.167.34	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
87.69.18.215	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
66.249.67.200	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5552-7161-he/igf.aspx	Block	1
66.249.64.175	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4223-he/igf.aspx	Block	1
109.226.15.32	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1
84.111.34.68	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/templates/newslst/undefined	Block	1
66.249.67.216	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6300-9396-he/igf.aspx	Block	1
217.132.32.207	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
66.249.64.180	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5039-he/igf.aspx	Block	1
199.203.47.194	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1
61.216.2.15	Taiwan	147.237.77.17	mazi.idf.i	Multiple Illegal Byte Code Character in Method from 61.216.2.15	Block	1
40.77.167.34	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/14-8344-he	Block	1
87.69.62.247	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
66.249.67.208	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
66.249.64.175	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
141.212.122.128	United States	147.237.77.17	mazi.idf.i	Malformed URL proxytest.zmap.io:80	Block	1
46.120.47.239	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
40.77.167.34	United States	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
84.111.184.168	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-4983-he	Block	1
217.132.32.207	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/xmlrpc.php	Block	1
66.249.64.180	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4199-he/igf.aspx	Block	1
66.249.64.124	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-10106-he	Block	1
202.112.51.96	China	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.wooyun.org/	Block	1
95.86.99.127	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/113-11149-he/igf.aspx&sa=u&ved=0ahukewicte2k7ljjahubeg8khhbg_cyqqfggqmai&usq=afqjcnf2-gt7o9rfjg3fr0gxuhjb6n7biq	Block	1
82.80.193.244	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
66.249.67.208	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
66.249.64.180	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/165-6974-he/igf.aspx	Block	1
207.241.226.42	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/	Block	1
157.55.39.15	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslst/undefined	Block	1
52.35.27.166	United States	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
40.77.167.34	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/lifestyle/statcode.php	Block	1
84.111.184.168	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8348-he	Block	1
66.249.64.185	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1