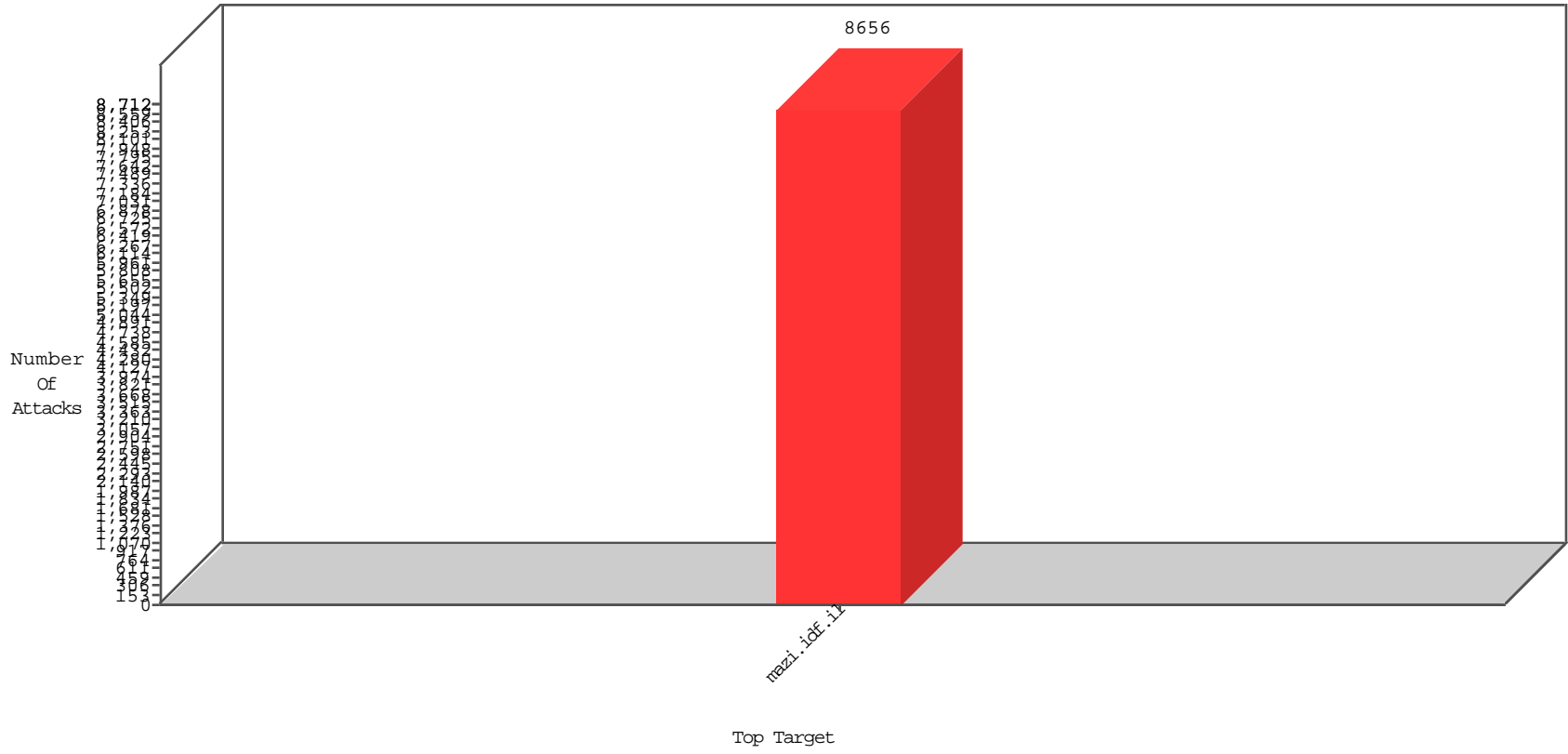


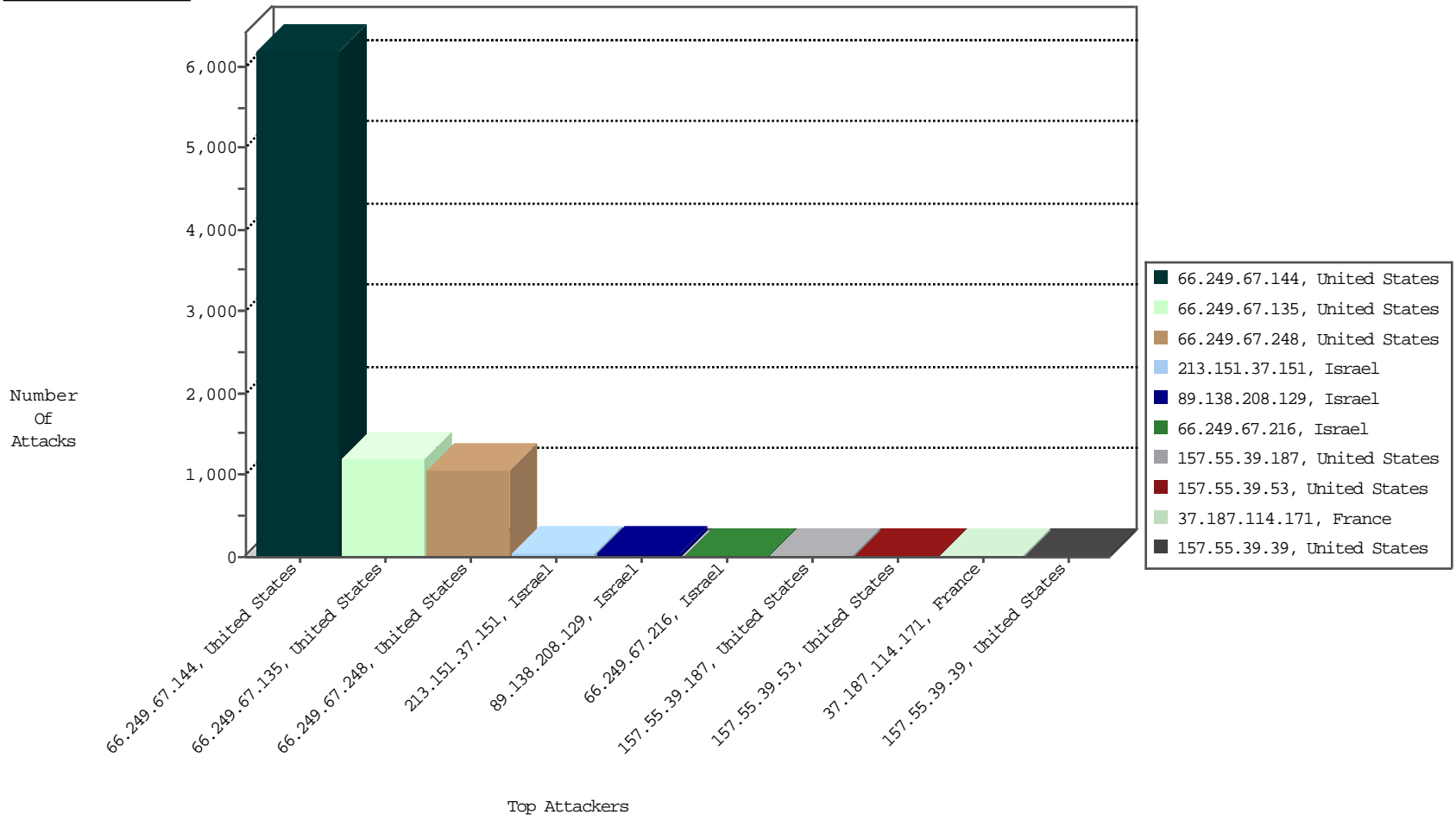
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
66.249.67.144	United States	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BEL-Frankfurt	6193
66.249.67.135	United States	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BEL-Frankfurt	1210
66.249.67.248	United States	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BEL-Frankfurt	1040

11-02-2015 to 11-03-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
82.166.247.98	Israel	147.237.77.17	mazi.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
66.249.67.248	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	9
66.249.67.144	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	7
201.249.199.91	Venezuela	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
5.8.66.101	Russian Federation	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
66.249.67.135	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	1
5.8.66.101	Russian Federation	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	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
80.178.13.254	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	42
85.130.220.178	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	34
46.19.85.238	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	16
46.19.85.238	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.85.133	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.85.224	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
85.130.183.30	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.104	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.54	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.4	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.14	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.146.174	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.162	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.50.124	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.178	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.181	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.251	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.146.174	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	4
62.90.201.181	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
5.22.130.124	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
5.22.130.116	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
2.52.55.187	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	2
2.54.177.119	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
46.19.85.79	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
2.52.55.187	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
2.52.55.187	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	2
46.19.86.109	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
176.12.149.50	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
5.22.129.135	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
77.127.55.231	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.248	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
212.143.134.129	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
87.69.109.252	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
5.29.228.42	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
82.80.16.226	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
2.52.146.240	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.249	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.133	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
178.173.171.236	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
85.130.220.178	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
212.143.134.129	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.133	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
87.69.166.14	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
82.80.16.226	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
54.244.22.103	United States	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	1
46.19.86.140	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
178.173.171.236	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
81.218.48.37	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
46.19.86.239	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
155.178.180.11	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
213.151.37.151	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	32
89.138.208.129	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	30
157.55.39.39	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	15
157.55.39.53	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/templates/general/x"	Block	15
37.187.114.171	France	147.237.77.17	mazi.idf.i	Unauthorized URL Access to /xmii/illuminator	Block	15
157.55.39.187	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/14-8331-he	Block	15
66.249.67.216	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5198-he/igf.aspx	Block	15
77.126.151.204	Israel	147.237.77.17	mazi.idf.i	Suspicious Response Code	Block	8
149.78.234.208	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	3
77.75.78.168	Czech Republic	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/9/8699.jpg	Block	2
66.249.67.216	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/	Block	2
66.249.67.200	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/	Block	2
94.159.155.16	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/images/transvideocounter.gif	Block	2
79.183.167.233	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	2
2.54.147.241	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/	Block	2
85.250.142.142	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	2
66.249.67.135	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-4983-he	Block	1
93.173.186.87	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 93.173.186.87	Block	1
80.178.13.254	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/robots.txt	Block	1
194.90.116.27	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/7/1087.jpg	Block	1
66.249.67.200	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6510-9854-he/igf.aspx	Block	1
2.54.173.59	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/sip_storage/files/7/1087.jpg	Block	1
66.249.67.200	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/robots.txt	Block	1
93.173.186.87	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/ajax/updatestatus.php	Block	1
84.95.59.213	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-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/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
207.46.13.99	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
66.249.67.208	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/	Block	1
157.55.39.0	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
93.158.178.198	Russian Federation	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/9/8699.jpg	Block	1
66.249.67.216	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4941-he/igf.aspx	Block	1
85.65.165.205	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/	Block	1
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/4070-11595-he/xžx-xæx\$xa xax x x•xŸ x•x'x\$xx".aspx	Block	1
207.46.13.130	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
66.249.67.208	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/113-8118-he/igf.aspx	Block	1
40.77.167.33	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
157.55.39.7	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
93.173.186.87	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
176.106.226.193	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 147.237.77.17/3834-9547-he/igf.aspx	Block	1
133.130.49.166	Japan	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4637-5227-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/5580-7562-he/igf.asp	Block	1
207.46.13.165	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
66.249.67.216	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/4944-he/igf.aspx	Block	1