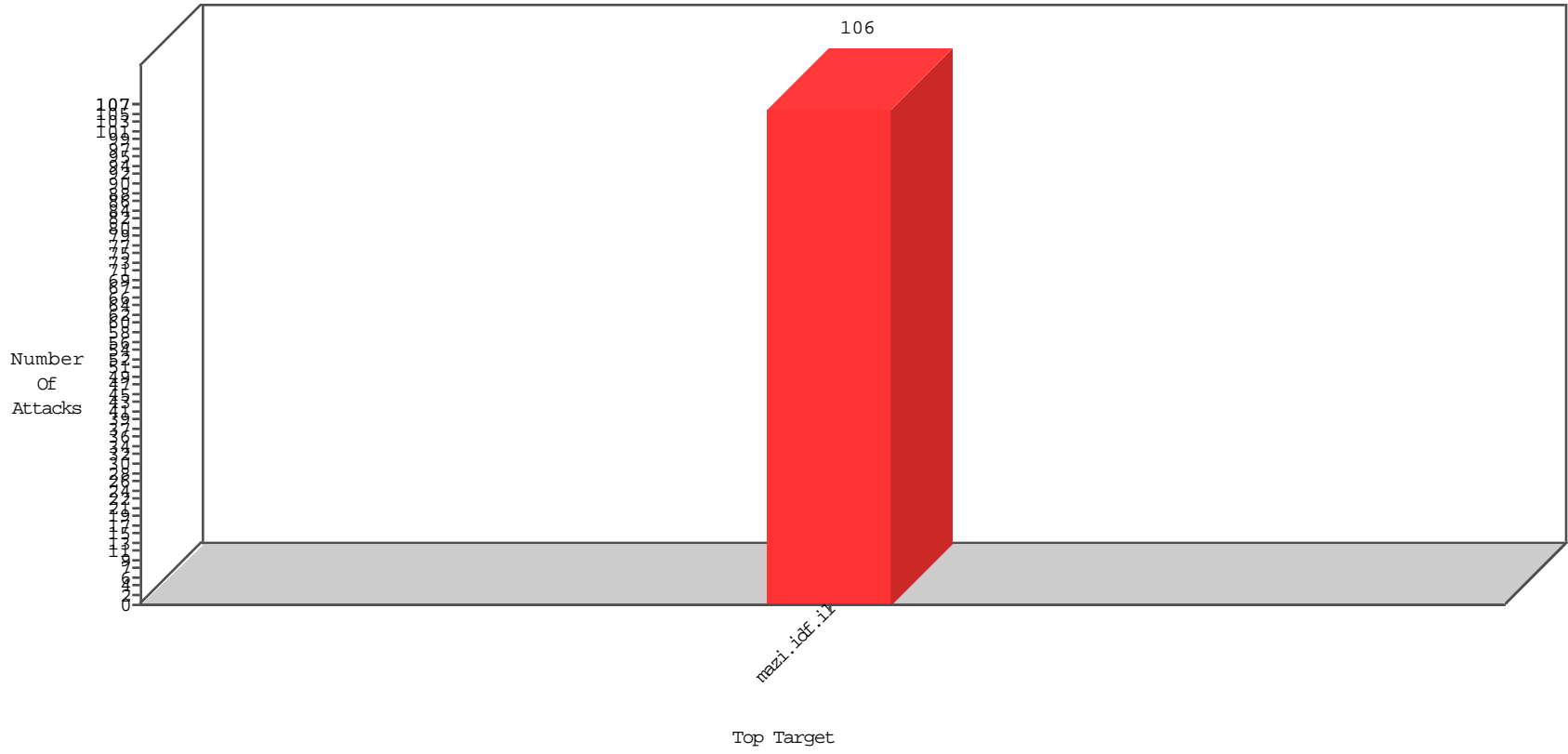


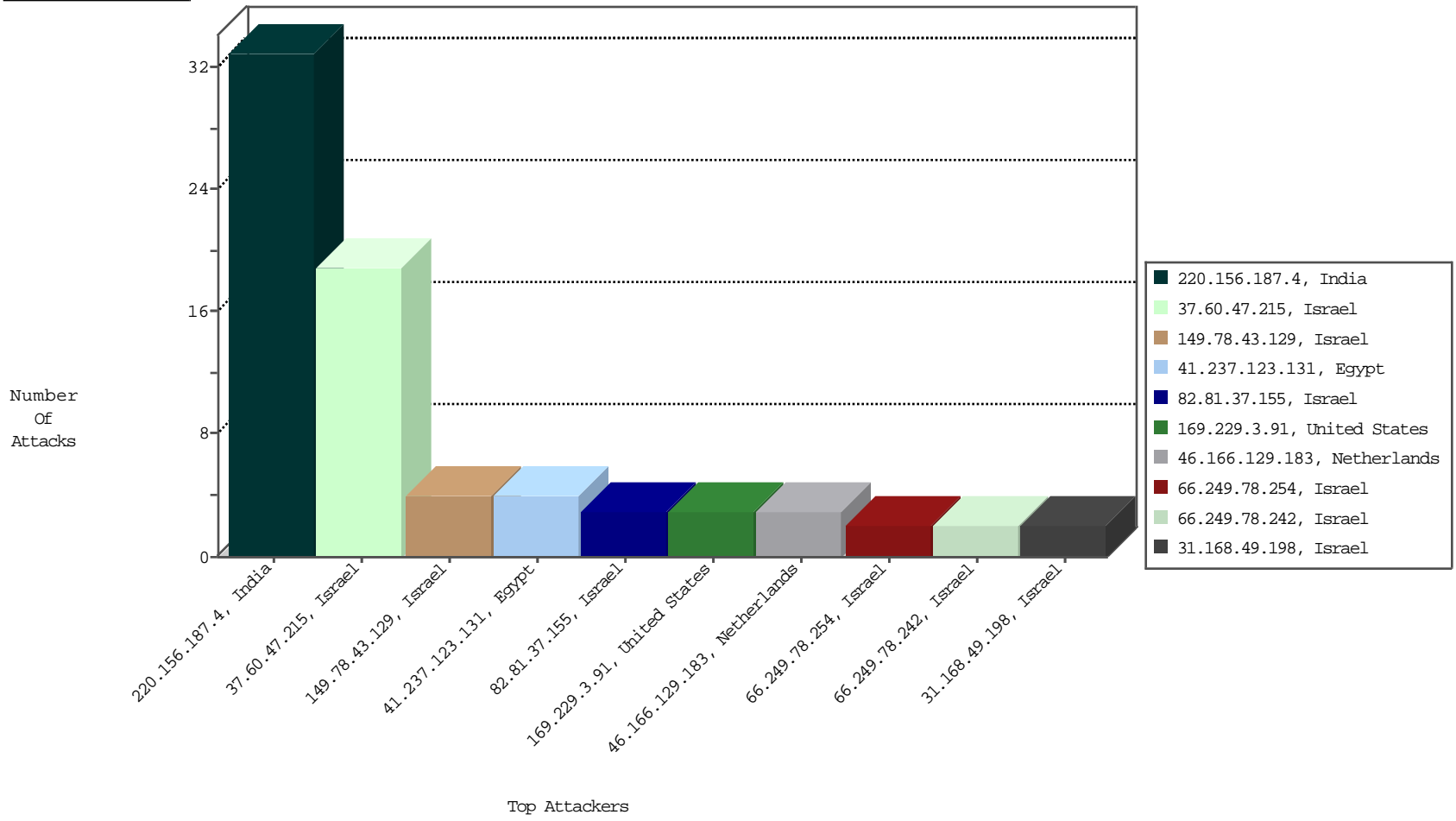
# Focused IP Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
82.81.37.155	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	3
185.130.215.3		147.237.77.17	mazi.idf.il	I4 Source or Dest Port Zero	drop	BBL-Frankfurt	2

## Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
220.156.187.4	India	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	33
208.52.161.99	United States	147.237.77.17	mazi.idf.il	C003: HTTP: phpMyAdmin access	Block	1
188.165.15.66	France	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.241	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
46.166.129.183	Netherlands	147.237.77.17	mazi.idf.il	ET SCAN NMAP -f -sS	1
46.166.129.183	Netherlands	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 4096	1
158.130.6.191	United States	147.237.77.17	mazi.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
209.126.116.147	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
46.166.129.183	Netherlands	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.65	China	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
168.62.238.153	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
89.139.167.227	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	49
190.95.243.229	Ecuador	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	25
74.208.77.114	United States	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	25
46.19.85.167	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
46.19.85.157	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
79.183.171.130	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
46.117.207.178	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
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
46.19.85.167	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
109.160.224.249	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
109.160.224.249	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
109.65.221.17	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
91.200.12.141	Ukraine	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	4
31.168.49.198	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
71.204.146.106	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.86.5	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.7	Ukraine	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	4
212.199.251.227	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
212.199.251.227	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	2
84.94.32.197	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
206.116.145.8	Canada	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.59	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.235	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
146.185.234.48	Russian Federation	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
41.237.123.131	Egypt	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	1
216.243.31.2	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.39.93.143	France	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
87.68.73.82	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
79.176.111.188	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.121.28.121	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
157.55.2.133	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
130.193.51.60	Russian Federation	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
37.26.148.186	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
84.111.102.115	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
180.97.106.36	China	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	1
46.117.123.179	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
149.78.56.175	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
87.69.232.91	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
64.125.239.89	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
157.55.2.133	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.5	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
146.185.234.48	Russian Federation	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
37.26.148.186	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
98.143.148.107	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.52.14.236	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.228.30.131	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
77.201.201.147	France	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.98	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

## Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
37.60.47.215	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	19
149.78.43.129	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslst/undefined	Block	4
41.237.123.131	Egypt	147.237.77.17	mazi.idf.i	PHP Attempt	Block	2
37.147.33.61	Russian Federation	147.237.77.17	mazi.idf.i	Parameter Type Violation ForumId in mazi.idf.il/forums/templates/forums/forum.aspx	Block	1
157.55.39.76	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/14-8344-he	Block	1
80.178.195.236	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
66.249.78.174	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-5475-he	Block	1
41.237.123.131	Egypt	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
212.76.103.235	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
31.168.49.198	Israel	147.237.77.17	mazi.idf.i	Unauthorized HTTP Method	Block	1
141.212.122.177	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-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
66.249.75.146	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/14-8334-he	Block	1
37.147.33.61	Russian Federation	147.237.77.17	mazi.idf.i	Parameter Type Violation lang in mazi.idf.il/forums/templates/forums/forum.aspx	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Abnormally Long Request method	Block	1
2.52.20.186	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage	Block	1
82.9.7.103	United Kingdom	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/7/1087.jpg	Block	1
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
46.19.85.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
37.26.149.193	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/idf	Block	1
146.185.234.48	Russian Federation	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/templates/newslst/newslst.in.aspxundefined	Block	1
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/vodchannel/	Block	1
66.249.75.164	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/14-8331-he	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Illegal Byte Code Character in Method Ã[[#8]]Ã,m!Ã}Ã'[[#17]][[#4]]Ã>ÃÃÃ@vÃ*h!Ã~[[#1]];Ã»IjÃ'Ã*ÃÃÃ"ÃÃ.ÃuiÃ*rÃfÃÃÃ?Ã°[[#14]]pÃtÃÃ[[#30]]ÃÃj[[#23]]eÃ?cÃÃeÃÃÃ[[#5]]ÃÃÃ}Ã vÃy	Block	1
31.44.133.76	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/images/transvideocounter.gif	Block	1
95.86.106.29	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5566-he/igf.aspx&sa=u&ved=0ahukewjfxuwf_djkahxczw8khqajdg4qfgggm ac&usg=afqjcnerylfwe5cpla8u-jomyfthvpsag	Block	1
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/571-he/igf.aspx	Block	1
46.120.97.101	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslst/undefined	Block	1
80.178.195.236	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
66.249.78.10	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/templates/newslst/undefined	Block	1
41.237.123.131	Egypt	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/xmlrpc.php	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Unknown HTTP Request Method Ã[[#8]]Ã,m!Ã}Ã'[[#17]][[#4]]Ã>ÃÃÃ@vÃ*h!Ã~[[#1]];Ã»IjÃ'Ã*ÃÃÃ"ÃÃ.ÃuiÃ*rÃfÃÃÃ?Ã°[[#14]]pÃtÃÃ[[#30]]ÃÃj[[#23]]eÃ?cÃÃeÃÃÃ[[#5]]ÃÃÃ}Ã vÃy in URL	Block	1
31.168.49.198	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 31.168.49.198	Block	1
95.135.13.241	Ukraine	147.237.77.17	mazi.idf.i	Parameter Type Violation PageNum in mazi.idf.il/4040-he/igf.aspx	Block	1
66.249.78.254	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1
66.249.69.98	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslst/undefined	Block	1