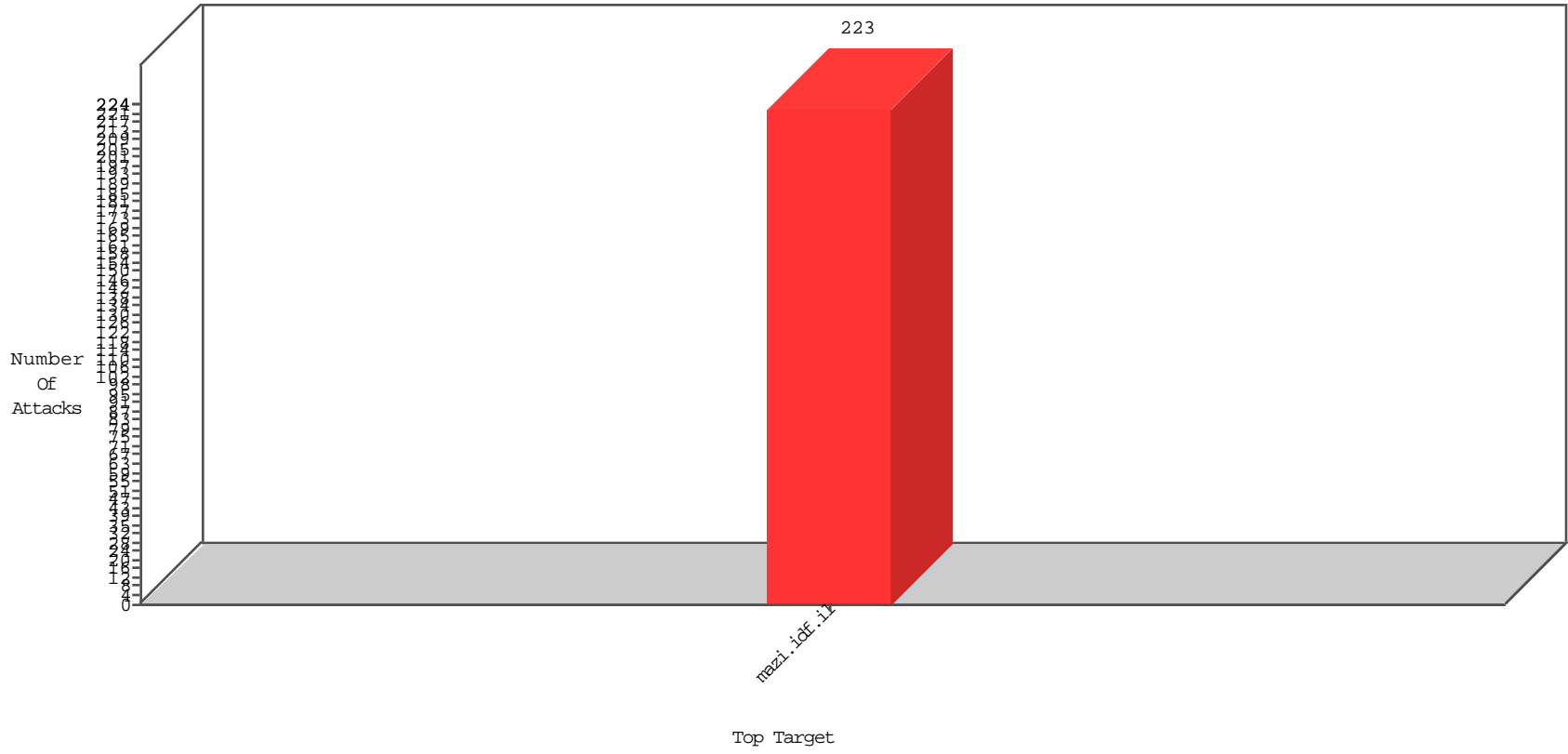


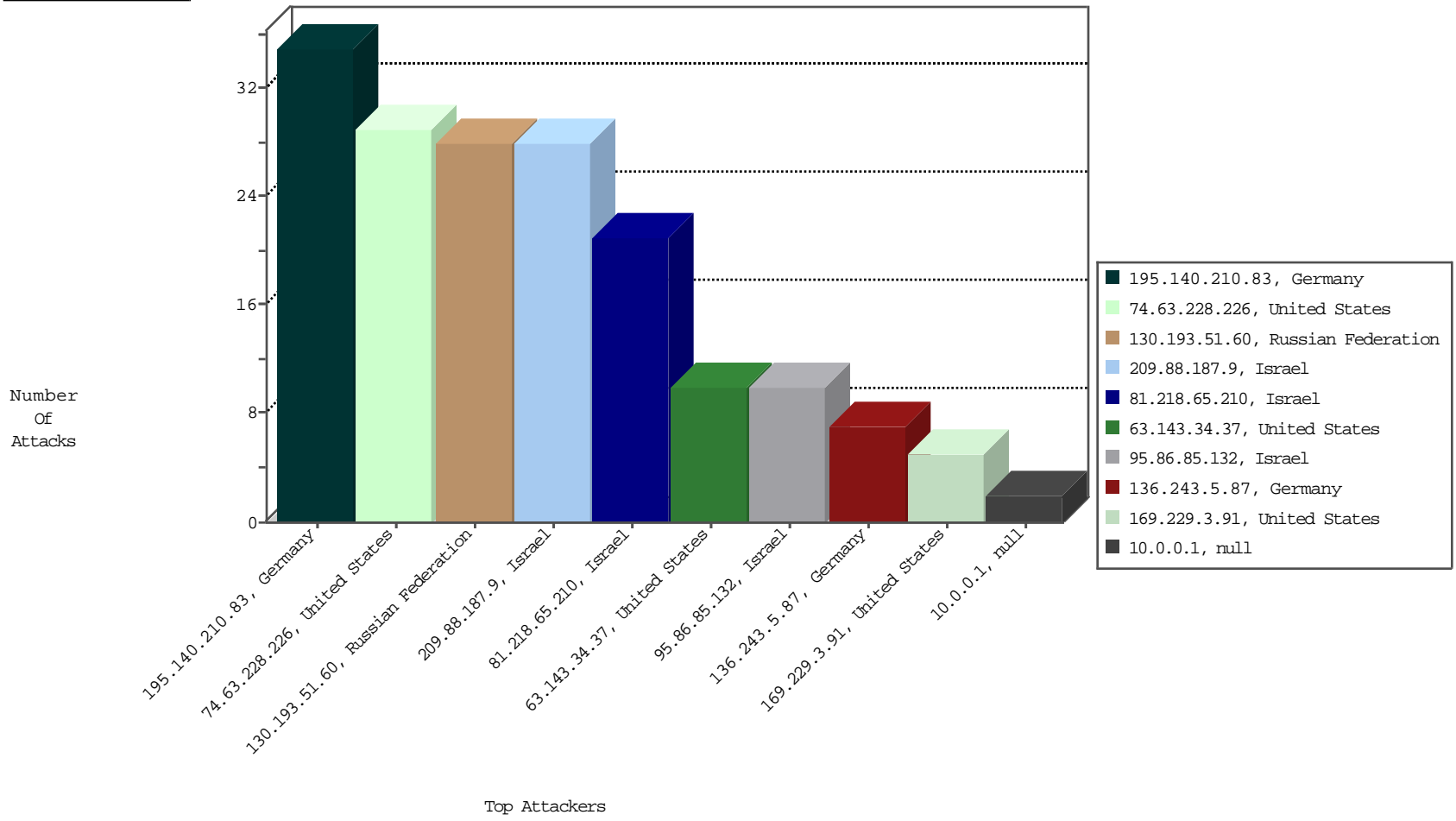
# Focused IP Under Attack Daily Report



## Top Targets



## Top Attackers



03-13-2016 to 03-14-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
81.218.65.210	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	BEL-Israel	21

## Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
209.88.187.9	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	28
130.193.51.60	Russian Federation	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	27
195.140.210.83	Germany	147.237.77.17	mazi.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	26
95.86.85.132	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
74.63.228.226	United States	147.237.77.17	mazi.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	10
136.243.5.87	Germany	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	7
63.143.34.37	United States	147.237.77.17	mazi.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
144.76.12.75	Germany	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	2
87.71.11.106	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
69.30.201.98	United States	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	2
149.78.141.231	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
89.163.148.58	Germany	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	2
10.0.0.1		147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
131.253.25.160	United States	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
74.63.228.226	United States	147.237.77.17	mazi.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2
46.120.156.245	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
109.64.134.131	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
5.255.253.65	Russian Federation	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
207.46.13.10	United States	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
151.80.31.115	Italy	147.237.77.17	mazi.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
157.55.39.193	United States	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

## Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
74.63.228.226	United States	147.237.77.17	mazi.idf.il	SQL Injection - Select From	17
195.140.210.83	Germany	147.237.77.17	mazi.idf.il	SQL Injection - Select From	9
63.143.34.37	United States	147.237.77.17	mazi.idf.il	SQL Injection - Select From	6
101.254.141.27	China	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
115.28.51.141	China	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
188.120.159.43	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	35
46.19.85.31	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
46.19.85.31	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	25
91.200.12.7	Ukraine	147.237.77.17	mazi.idf.il	drop	SAM rule	drop	10
37.46.41.33	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
91.200.12.136	Ukraine	147.237.77.17	mazi.idf.il	drop	SAM rule	drop	7
5.102.242.113	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
176.13.2.98	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
85.130.208.118	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.79.68.161	Netherlands	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
103.1.181.78	Fiji	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.49	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
157.55.39.219	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
84.108.77.78	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
62.210.143.245	France	147.237.77.17	mazi.idf.il	drop	SAM rule	drop	2
67.188.95.73	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
136.243.152.18	Germany	147.237.77.17	mazi.idf.il	drop	SAM rule	drop	2
208.115.113.91	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
157.55.39.77	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
84.108.77.78	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
208.115.113.91	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
77.127.109.251	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.120.156.245	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
149.78.200.77	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
37.26.146.214	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
95.86.85.132	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
87.70.23.252	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
213.57.178.244	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
82.166.140.125	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
66.249.93.16	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
130.193.51.60	Russian Federation	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.87	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.113.91	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
79.182.105.177	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.111	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
149.78.200.77	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.26.148.247	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
87.71.125.88	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
213.57.203.115	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
82.166.140.125	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
200.237.129.78	Brazil	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
159.226.95.66	China	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.49	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
94.230.86.85	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
84.108.208.163	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
81.218.158.53	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.3.147.64	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
66.249.93.16	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
103.1.181.78	Fiji	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

03-13-2016 to 03-14-2016

## Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
212.179.21.194	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage	Block	2
5.29.248.213	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Distributed Unknown HTTP Request Method	Block	1
149.88.44.191	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/2061.jpg	Block	1
81.218.148.60	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4637-5227-he/igf.aspx	Block	1
66.249.65.238	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Distributed Illegal Byte Code Character in Method	Block	1
109.67.136.139	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/resource/userfollowresource/create/	Block	1
77.75.76.165	Czech Republic	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/9/8699.jpg	Block	1
5.29.248.213	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/xmlrpc.php	Block	1
176.13.2.98	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
157.55.39.144	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/4054-he/igf.aspxâ&#x2013;â&#x2013;	Block	1
81.218.158.53	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
66.249.79.148	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/9/8699.jpg	Block	1
213.57.178.244	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/resource/userfollowresource/create/	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Distributed Illegal Byte Code Character in URL	Block	1
130.193.51.60	Russian Federation	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5580-7562-he/igf.asp	Block	1
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	1
66.249.65.18	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/9/8699.jpg	Block	1
188.120.159.43	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3848-5183-he/igf.aspx	Block	1
157.55.39.232	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
85.250.13.34	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5187-he/igf.aspx	Block	1
66.249.79.162	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation PageNum in mazi.idf.il/700-he/igf.aspx	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Distributed Malformed URL	Block	1
149.50.119.45	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
79.177.60.79	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4637-5227-he/igf.aspx	Block	1
66.249.65.231	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
207.241.229.222	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/forums/templates/forums/forums/templates/forums/forumslist.aspx?lang=he	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Distributed Abnormally Long Request	Block	1
107.172.27.22	United States	147.237.77.17	mazi.idf.i	Unauthorized Method HEAD for 147.237.77.17/	Block	1
68.180.228.151	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1

03-13-2016 to 03-14-2016