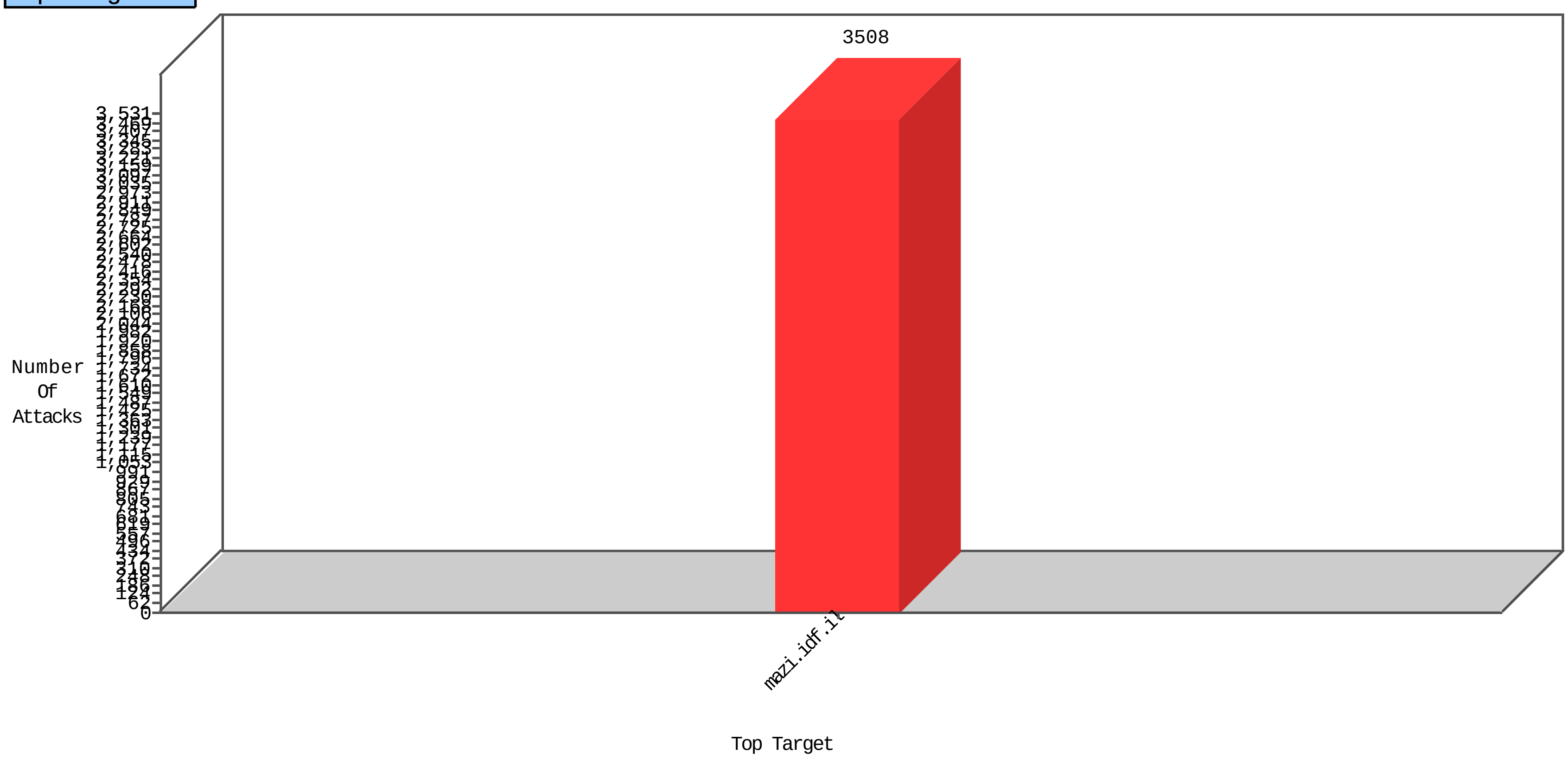
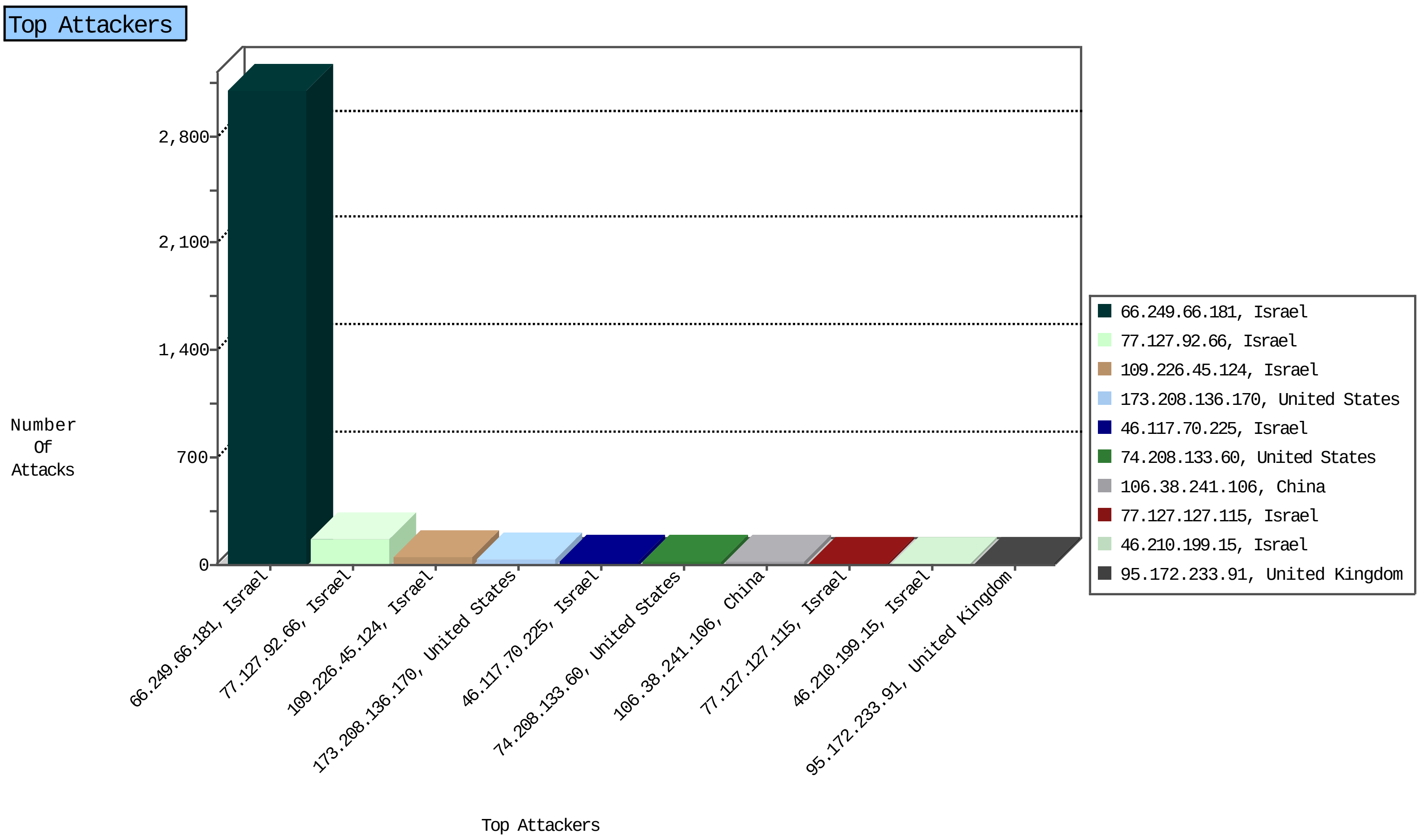
02-21-2016 to 02-22-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



02-21-2016 to 02-22-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
66.249.66.181	Israel	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	3096
81.218.130.69	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	3

02-21-2016 to 02-22-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
77.127.92.66	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	171
109.226.45.124	Israel	147.237.77.17	mazi.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	50
46.117.70.225	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	26
106.38.241.106	China	147.237.77.17	mazi.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	13
77.127.127.115	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
66.249.66.181	Israel	147.237.77.17	mazi.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	10
46.210.199.15	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
5.29.189.86	Israel	147.237.77.17	mazi.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	4
164.138.113.83	Israel	147.237.77.17	mazi.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	2
95.35.21.21	Israel	147.237.77.17	mazi.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	2
147.235.185.74	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.66.184	Israel	147.237.77.17	mazi.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.17	mazi.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	2
66.249.66.181	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
149.202.48.240	Germany	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	2
46.4.32.75	Germany	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	2
151.80.31.126	Italy	147.237.77.17	mazi.idf.il	C1000228: HTTP: AhrefBot crawler	Block	1
66.249.66.184	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
188.165.15.66	France	147.237.77.17	mazi.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

02-21-2016 to 02-22-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
74.208.133.60	United States	147.237.77.17	mazi.idf.il	SQL Injection - Select From	18
66.249.66.181	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
185.130.5.165		147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
91.223.25.134	Russian Federation	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
125.212.232.144	Vietnam	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 4096	1
202.152.254.236	Indonesia	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
125.212.232.144	Vietnam	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1

02-21-2016 to 02-22-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
173.208.136.170	United States	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	2984
37.26.148.246	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	652
37.26.148.246	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	650
89.138.89.160	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	121
199.203.111.231	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	43
199.203.8.2	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	36
199.203.8.2	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	36
2.52.153.156	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
192.115.83.5	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	21
192.115.83.5	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	12
79.176.169.28	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
95.172.233.91	United Kingdom	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
89.163.251.200	Germany	147.237.77.17	mazi.idf.i	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	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
46.117.193.207	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
185.120.126.89		147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
46.120.32.155	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
5.102.254.32	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
85.64.60.166	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
79.182.171.196	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.26.146.190	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.117.193.207	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
79.176.49.75	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
95.35.151.223	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.130.118	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.141.214	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
31.13.113.85	Ireland	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
84.94.64.146	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
194.114.146.227	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
5.22.135.101	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.78	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.253.134.21	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.215	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
91.135.102.188	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
87.69.243.141	Israel	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
81.218.148.177	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	1
192.114.20.101	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
78.137.66.241	Yemen	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	1
46.117.244.162	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
37.46.41.205	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
89.163.251.200	Germany	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.92	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
31.210.187.240	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
84.94.64.146	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
195.154.226.90	France	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	1
5.22.135.195	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
185.3.144.82	Israel	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
173.208.136.170	United States	147.237.77.17	mazi.idf.i	Multiple Admin Blocking from 173.208.136.170	Block	39
95.172.233.91	United Kingdom	147.237.77.17	mazi.idf.i	Suspicious Response Code	Block	6
31.44.137.250	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	4
62.219.212.22	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation Master$ucHeader$ucSearchControl$txtSearch in mazi.idf.il/5675-7811-he/igf.aspx	Block	2
149.88.36.9	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage	Block	2
199.203.111.231	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	2
31.184.133.24	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	2
95.86.105.224	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/4166-he/igf.aspx&sa=u&ved=0ahukewie7f2esynlahxdca8khb0fdzcqfggkmae&sig2=jnqydkjzqdyu8qfuurs98a&usg=afqjcnf3ixvex2h5tkxc87mhi8p2qlwu5q	Block	2
37.160.176.216	France	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/571-he/igf.aspx	Block	2
208.115.111.75	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8338-he	Block	1
66.249.66.188	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5034-he/igf.aspx	Block	1
68.180.230.245	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/templates/shared/usercontrols/vodchannel/	Block	1
208.115.111.75	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-he	Block	1
89.163.251.200	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to /myadmin/scripts/setup.php	Block	1
66.249.66.181	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5551-11516-he/×ž×©×œ×‘×™×? ×§×”×™×œ×”.aspx	Block	1
208.115.113.92	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/4070-11595-he/×ž×—×œ×§×ª ×ª×›× ×•×Ÿ ×•×‘×§×¨×”.aspx	Block	1
157.55.39.145	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5676-7827-he/ifg.aspx	Block	1
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/450-he.aspx	Block	1
208.115.111.75	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 208.115.111.75	Block	1
66.249.66.182	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
173.208.136.170	United States	147.237.77.17	mazi.idf.i	Admin Blocking	Block	1
68.180.229.218	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/14-8330-he	Block	1

02-21-2016 to 02-22-2016