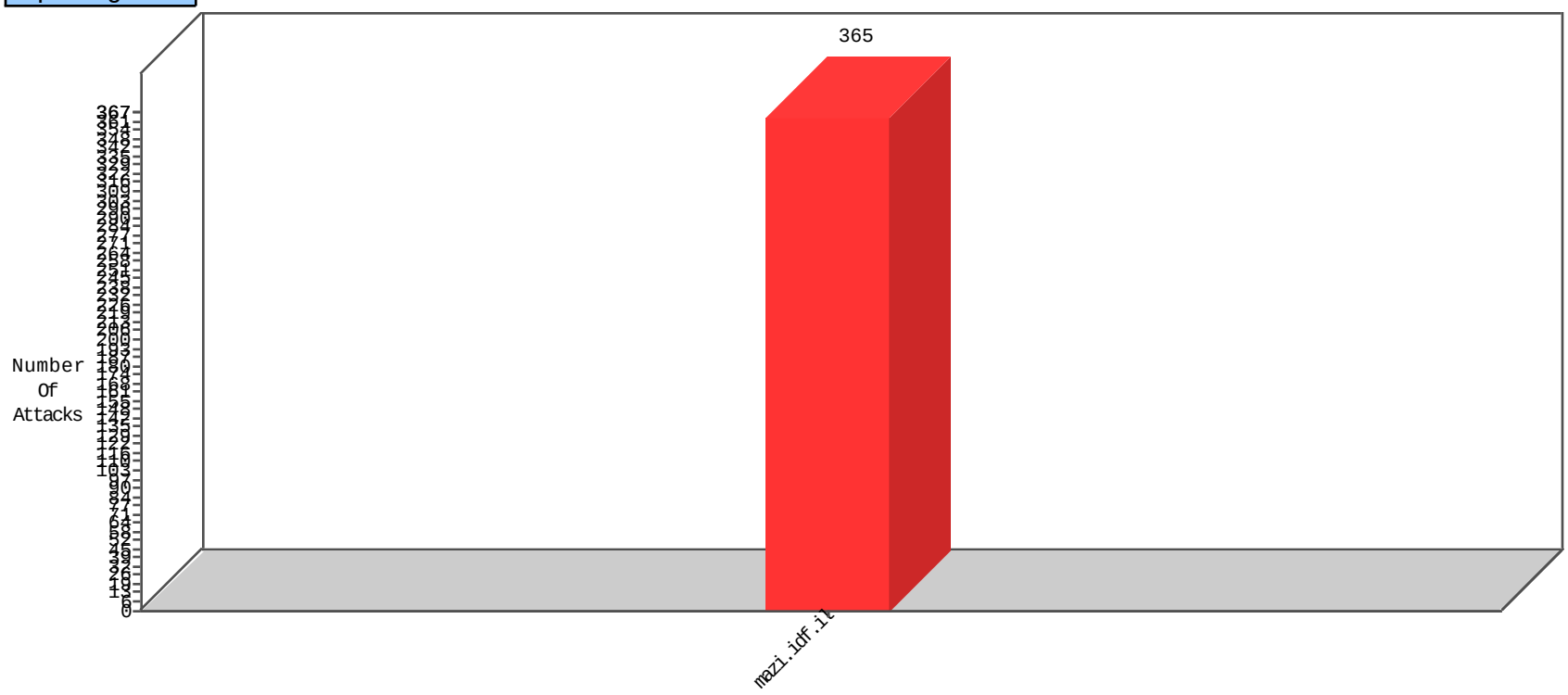
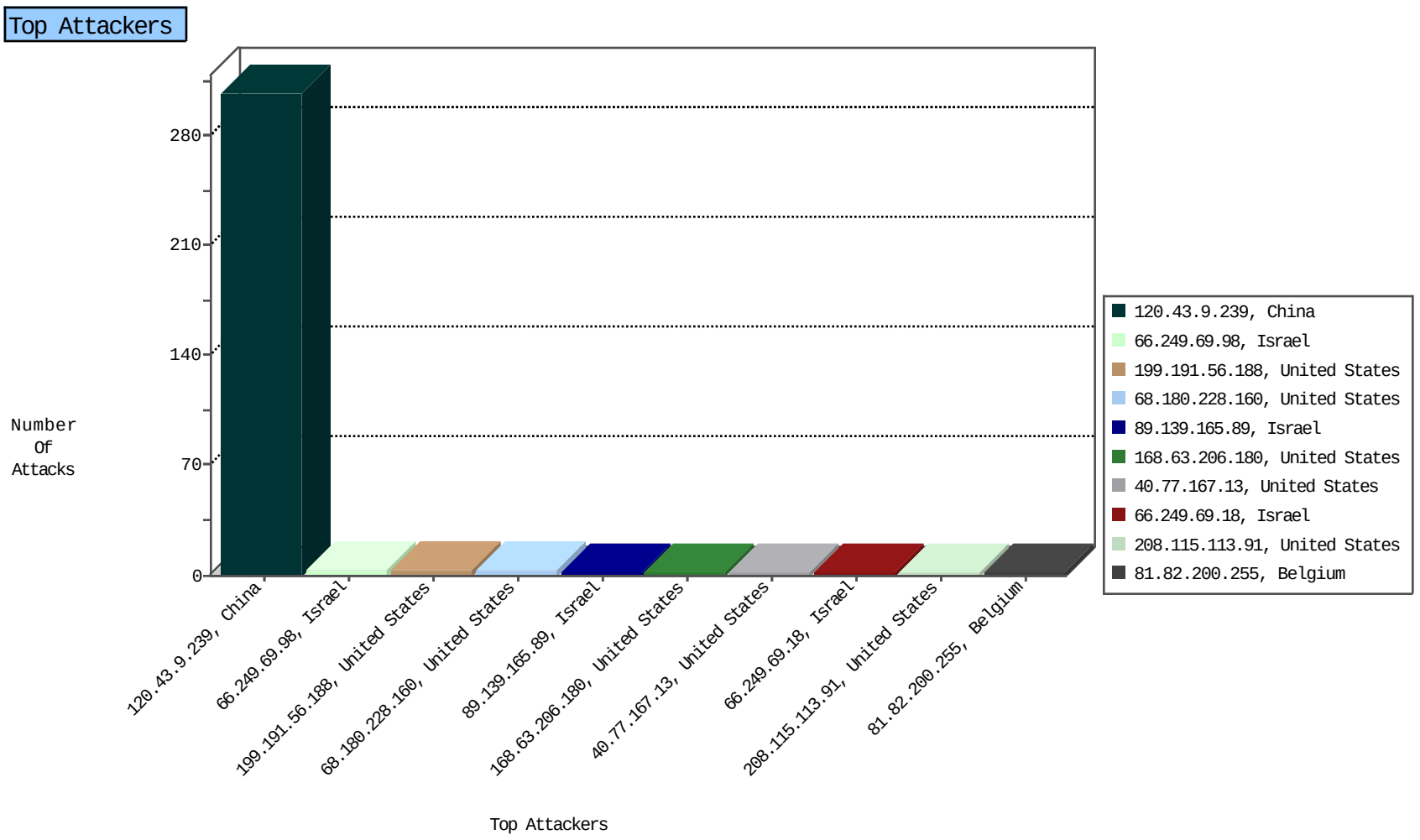
01-08-2016 to 01-09-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



01-08-2016 to 01-09-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
79.180.182.210	Israel	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	1
107.150.60.78	United States	147.237.77.17	mazi.idf.il	block-sp-traf1	drop	BBL-Frankfurt	1
202.112.51.96	China	147.237.77.17	mazi.idf.il	block-sp-traf1	drop	BBL-Frankfurt	1

01-08-2016 to 01-09-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
120.43.9.239	China	147.237.77.17	mazi.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	271
120.43.9.239	China	147.237.77.17	mazi.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1

01-08-2016 to 01-09-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
173.199.74.136	United Kingdom	147.237.77.17	mazi.idf.i	ET SCAN Potential VNC Scan 5900-5920	2
168.63.206.180	United States	147.237.77.17	mazi.idf.i	ET SCAN Potential VNC Scan 5900-5920	2
187.161.132.231	Mexico	147.237.77.17	mazi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
199.191.56.188	United States	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sS window 1024	1
79.177.172.123	Israel	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sS window 4096	1
81.82.200.255	Belgium	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sS window 1024	1
95.156.251.10	Germany	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sS window 1024	1
177.239.212.65	Mexico	147.237.77.17	mazi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
199.191.56.188	United States	147.237.77.17	mazi.idf.i	ET SCAN NMAP -f -sS	1
199.191.56.188	United States	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sS window 2048	1
1.93.129.5	China	147.237.77.17	mazi.idf.i	ET SCAN Potential SSH Scan	1
80.82.69.146	Netherlands	147.237.77.17	mazi.idf.i	ET SCAN Potential SSH Scan	1
81.82.200.255	Belgium	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sS window 3072	1
99.129.251.54	United States	147.237.77.17	mazi.idf.i	ET SCAN Potential SSH Scan	1

01-08-2016 to 01-09-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
216.177.129.140	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2794
216.177.129.140	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	939
212.76.127.111	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	297
120.43.9.239	China	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	289
46.19.85.203	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	100
46.19.85.203	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	100
212.76.127.10	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	54
80.178.6.56	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	49
31.210.188.26	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	37
109.160.166.124	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	26
31.210.188.26	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	26
46.19.85.120	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	25
31.210.188.26	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	25
212.76.127.44	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	18
46.19.85.181	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	18
81.218.251.252	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	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
81.218.251.252	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.120	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.86.237	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	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
212.150.249.184	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
207.46.13.128	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	7
66.249.75.121	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
207.46.13.101	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
85.93.218.204	Luxembourg	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	5
85.93.218.204	Luxembourg	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
207.46.13.141	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.147.254	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
120.43.9.239	China	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
109.160.166.124	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
85.64.240.218	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
149.78.175.179	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
192.243.55.129	Dominica	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
84.108.60.212	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
188.120.148.141	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
109.160.166.124	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	4
85.64.240.218	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
109.65.112.117	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
192.243.55.135	Dominica	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
130.193.51.60	Russian Federation	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
85.64.240.218	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	4
192.243.55.130	Dominica	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
109.160.166.124	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
85.64.156.154	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
133.130.63.178	Japan	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	3
133.130.63.178	Japan	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
207.46.13.13	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.75.8	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
192.243.55.132	Dominica	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3

01-08-2016 to 01-09-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
120.43.9.239	China	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 120.43.9.239	Block	31
120.43.9.239	China	147.237.77.17	mazi.idf.i	PHP Attempt	Block	4
89.139.165.89	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	2
66.249.69.18	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5187-he/igf.aspx	Block	1
31.154.163.169	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
192.243.55.129	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8330-he	Block	1
120.43.9.239	China	147.237.77.17	mazi.idf.i	Multiple Admin Blocking from 120.43.9.239	Block	1
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8335-he	Block	1
66.249.69.98	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-he	Block	1
46.19.85.156	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1
207.46.13.141	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
157.55.39.12	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/widget/clickstream/_rvi	Block	1
84.109.112.187	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage	Block	1
66.249.75.17	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8344-he	Block	1
66.249.69.18	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5010-9220-he/igf.aspx	Block	1
37.26.149.151	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
192.243.55.130	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8331-he	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
66.249.69.106	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8348-he	Block	1
208.115.113.91	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/14-4983-he	Block	1
66.249.69.2	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
157.55.39.212	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/113-11581-he/×œ×œ×? ×'×'×•×œ×•×ª.aspx	Block	1
66.249.75.121	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8350-he	Block	1
66.249.69.98	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 66.249.69.98	Block	1
40.77.167.13	United States	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
192.243.55.137	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-5475-he	Block	1
79.182.7.138	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
66.249.69.114	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8345-he	Block	1
208.115.113.91	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/templates/general/×"	Block	1
66.249.69.10	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
5.29.82.218	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/images/transvideocounter.gif	Block	1
181.215.1.152	Chile	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/forums/temp.....px	Block	1
109.65.112.117	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-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/14-10106-he	Block	1
66.249.69.98	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8346-he	Block	1
40.77.167.13	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/general/inc/css/style.css.php	Block	1
207.46.13.128	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/599-he/totchanim.aspx	Block	1
141.212.122.64	United States	147.237.77.17	mazi.idf.i	Malformed URL proxytest.zmap.io:80	Block	1
80.246.130.206	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
66.249.75.8	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	1

01-08-2016 to 01-09-2016