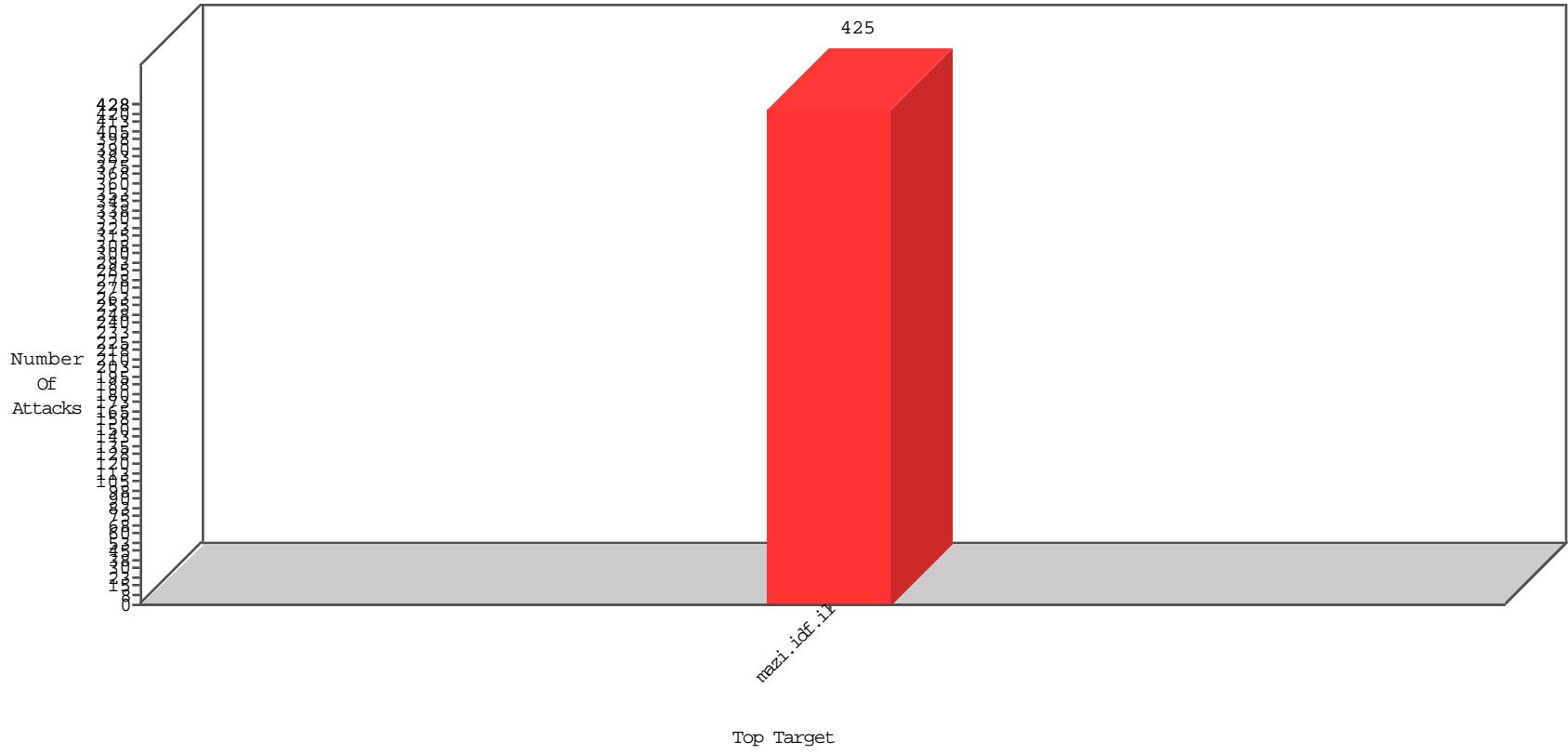


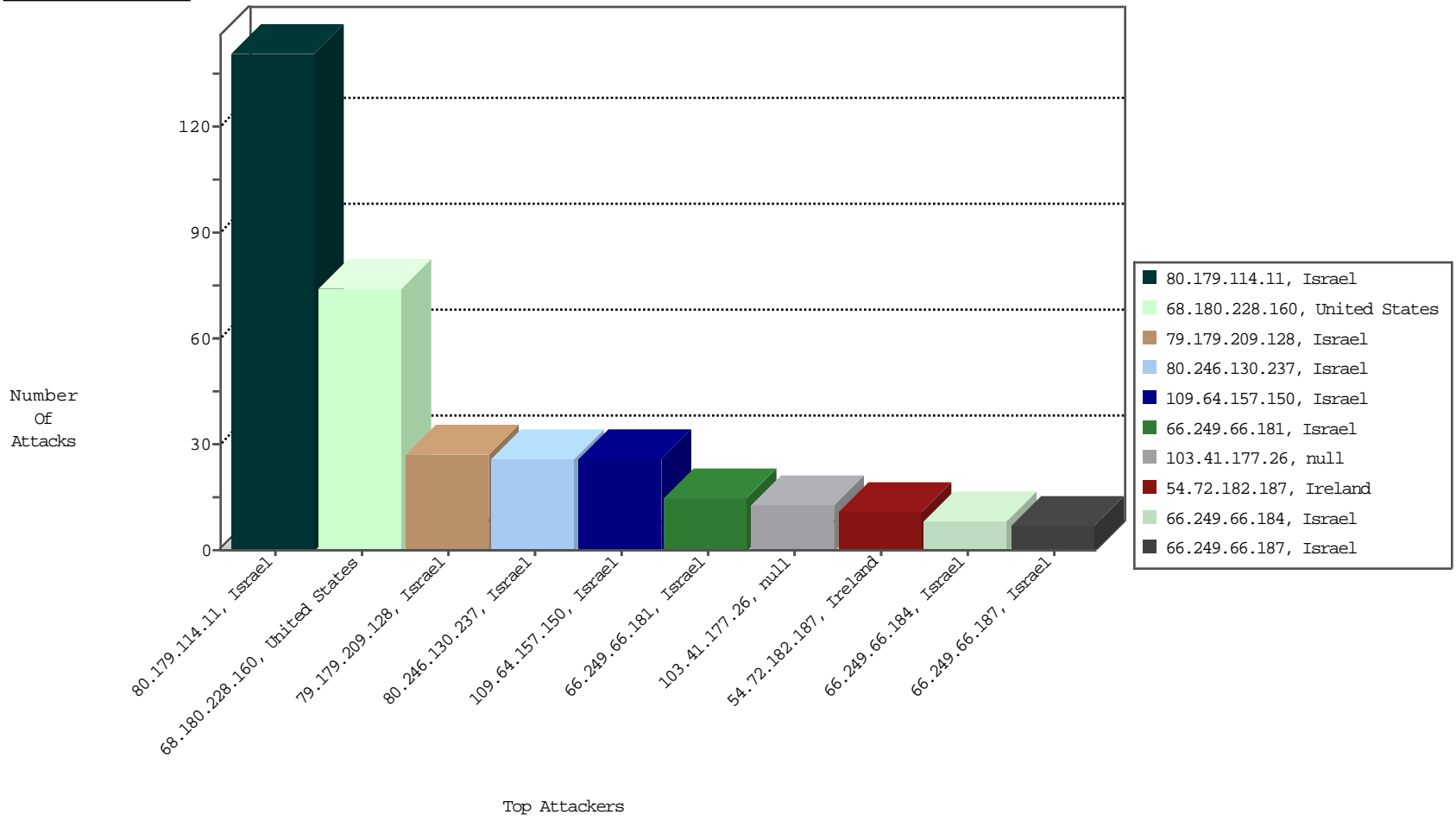
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
54.72.182.187	Ireland	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	NetV-London	11
108.186.168.25	United States	147.237.77.17	mazi.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
184.105.139.100	United States	147.237.77.17	mazi.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
209.126.105.33	United States	147.237.77.17	mazi.idf.il	Block_Ntp_All_Net	drop	NetV-London	1

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
80.179.114.11	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	141
68.180.228.160	United States	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	74
109.64.157.150	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	26
80.246.130.237	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	26
79.179.209.128	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	25
66.249.66.181	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	15
66.249.66.184	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
66.249.66.187	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
81.109.65.38	United Kingdom	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	5
84.108.31.210	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
79.182.97.19	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
162.210.196.100	United States	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	4
79.177.181.10	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
37.26.149.169	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
213.8.58.181	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
37.26.149.170	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
37.26.149.210	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
79.183.56.185	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
157.55.39.222	United States	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

03-07-2016 to 03-08-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
218.108.132.58	China	147.237.77.17	mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
40.76.55.204	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 4096	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
212.235.28.71	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid sequence number	monitor	36
46.19.85.144	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
46.19.85.144	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
46.19.85.186	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
79.179.33.205	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.85.186	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
37.26.147.236	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
5.22.130.229	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.81	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.111	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.70.67.66	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
5.102.242.191	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
149.88.213.100	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
87.70.67.66	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
87.70.67.66	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
40.77.167.35	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.111.1.129	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.148.146	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.69	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.148.146	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
151.80.31.151	Italy	147.237.77.17	mazi.idf.il	drop	SAM rule	drop	2
46.19.85.191	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.253.145.97	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.22.131.45	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
77.237.138.202	Czech Republic	147.237.77.17	mazi.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
216.243.31.2	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.71	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.93.185.246		147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
149.88.213.100	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
2.52.53.55	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
84.94.32.197	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
68.51.127.204	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
207.46.13.55	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.232	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
137.226.113.7	Germany	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
85.65.22.139	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.113	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
195.160.242.40	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
103.41.177.26		147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.22.130.225	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
84.94.32.197	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
68.51.127.204	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
207.46.13.55	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.3.146.231	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.81	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
149.88.74.125	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
80.179.114.11	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.19.86.180	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
195.160.242.40	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.142.233.116	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
2.70.7.169	Sweden	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	4
103.41.177.26		147.237.77.17	mazi.idf.i	Multiple Abnormally Long Request from 103.41.177.26	Block	4
103.41.177.26		147.237.77.17	mazi.idf.i	Multiple Illegal HTTP Version from 103.41.177.26	Block	4
50.93.198.232	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 50.93.198.232	Block	2
96.44.141.19	United States	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	2
79.179.209.128	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	2
50.93.198.232	United States	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	2
89.139.158.254	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
212.143.38.222	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
66.249.66.182	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
40.77.167.4	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
185.24.76.132	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/xmlrpc.php	Block	1
104.236.244.67		147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 104.236.244.67	Block	1
103.41.177.26		147.237.77.17	mazi.idf.i	Abnormally Long Request request version	Block	1
77.75.77.36	Czech Republic	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/9/8699.jpg	Block	1
207.232.29.186	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 207.232.29.186	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
103.41.177.26		147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 103.41.177.26	Block	1
89.139.158.254	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
66.249.66.182	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
46.19.86.84	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation Master\$ucHeader\$ucSearchControl\$txtSearch in www.mazi.idf.il/14-he/igf.aspx	Block	1
194.114.146.227	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 194.114.146.227	Block	1
104.236.244.67		147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/magento_version	Block	1
103.41.177.26		147.237.77.17	mazi.idf.i	Illegal HTTP Version + _nucjs + ".nuconomy.com/n.js HTTP/1.1	Block	1
77.237.138.202	Czech Republic	147.237.77.17	mazi.idf.i	Unauthorized Method HEAD for /	Block	1
207.232.29.186	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
52.37.168.145	United States	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
31.168.31.178	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
149.78.243.186	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/handas	Block	1
103.41.177.26		147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/joinmailinglist.aspx	Block	1
68.180.230.40	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
46.19.86.100	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
196.221.237.247	Egypt	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
109.65.175.36	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
212.143.38.222	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
52.37.168.145	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/wp-login.php	Block	1
31.168.31.178	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
185.24.76.132	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
103.41.177.26		147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/joinmailinglist.aspx	Block	1
96.44.141.19	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 96.44.141.19	Block	1
77.75.77.11	Czech Republic	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/9/8699.jpg	Block	1
196.221.237.247	Egypt	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
109.65.175.36	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/xmlrpc.php	Block	1
2.52.5.75	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/7343-11581-he/.aspx	Block	1