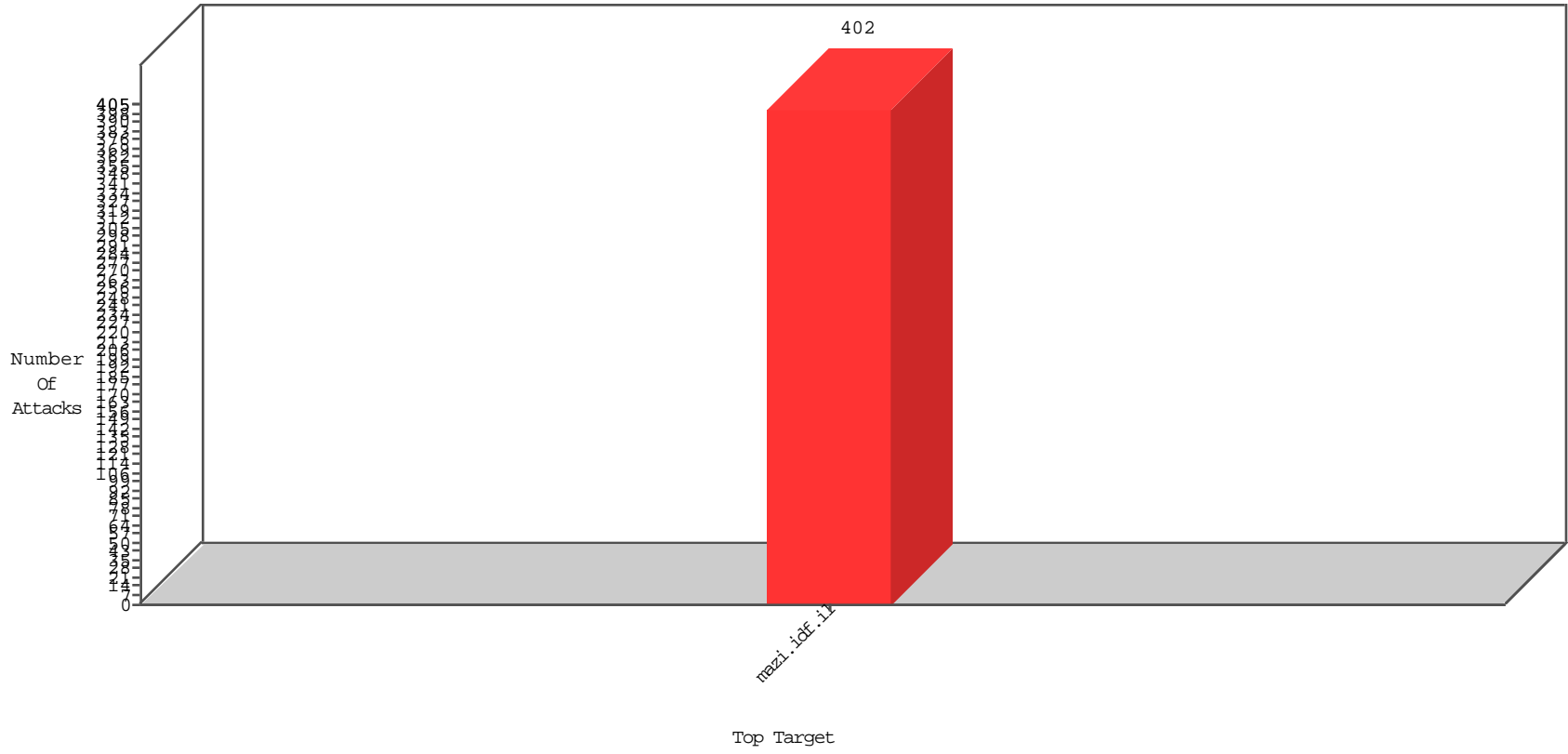


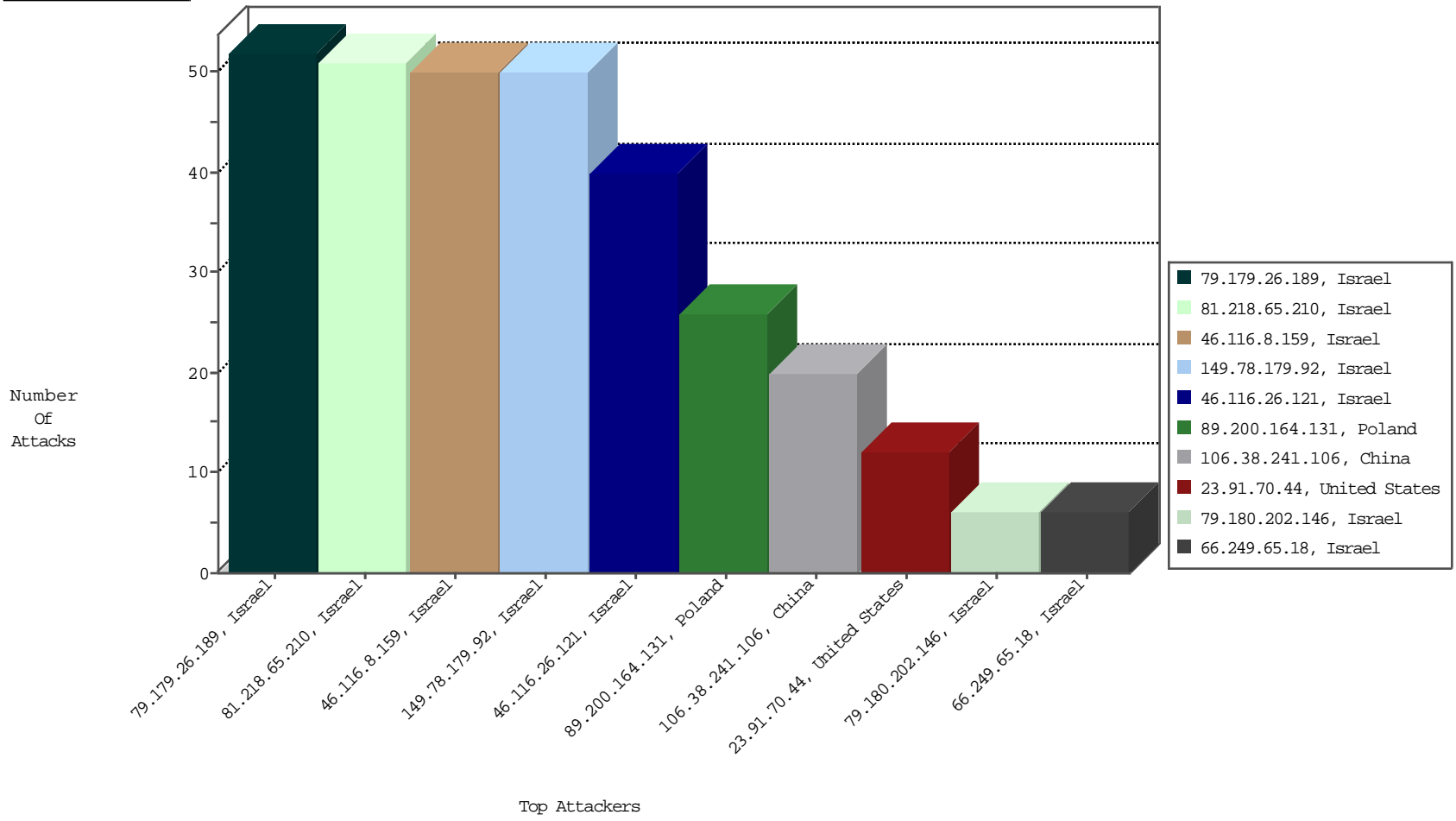
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
81.218.65.210	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	EEL-Isreal	51
159.104.163.18	United Kingdom	147.237.77.17	mazi.idf.il	Invalid TCP Flags	drop	NetV-London	1
159.104.163.17	United Kingdom	147.237.77.17	mazi.idf.il	Invalid TCP Flags	drop	NetV-London	1

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
79.179.26.189	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	52
46.116.8.159	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	50
149.78.179.92	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	50
46.116.26.121	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	40
89.200.164.131	Poland	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	C1000071: HTTP: User Agent Sogou+web+spider	Block	20
79.180.2.176	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
79.180.202.146	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
66.249.65.18	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
23.91.70.44	United States	147.237.77.17	mazi.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
213.244.82.142	Palestinian Territory, Occupied	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
66.249.65.22	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
66.249.65.26	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
51.255.36.85	United Kingdom	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	2
212.199.224.24	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.19.86.43	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
109.65.191.176	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
192.117.150.233	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
5.22.131.12	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
91.121.221.15	France	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	2
151.80.31.140	Italy	147.237.77.17	mazi.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
66.249.65.81	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	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
66.249.78.174	Israel	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

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
23.91.70.44	United States	147.237.77.17	mazi.idf.il	SQL Injection - Select From	6
80.82.79.104	Netherlands	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
185.103.252.60		147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
202.71.25.29	India	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.48.194	Netherlands	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
202.71.25.29	India	147.237.77.17	mazi.idf.il	ET SCAN NMAP -f -sS	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
77.42.180.184	Lebanon	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1785
98.7.73.145	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	68
81.218.28.226	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
46.116.26.121	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
37.26.149.232	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
2.52.129.34	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
2.54.33.127	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
149.78.14.88	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
213.57.151.49	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
213.57.151.49	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
62.90.193.240	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	4
185.3.147.198	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
5.22.135.187	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
207.241.237.223	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
5.102.242.9	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
2.52.130.60	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.85.96	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.6.89	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
5.28.171.247	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.85.114	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.148.35	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
74.82.47.34	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.243.31.2	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
206.45.156.34	Canada	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
93.178.106.254	Russian Federation	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
81.218.251.250	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
64.125.239.54	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
212.40.139.38	Lebanon	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
109.253.201.96	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
84.108.157.182	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.117.175.194	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
23.101.61.176	Ireland	147.237.77.17	mazi.idf.i	Instant Messengers	instant messenger pattern found, application: Skype	monitor	1
184.105.139.112	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
82.80.193.240	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
68.180.229.109	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.114	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
188.120.148.242	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
132.72.10.190	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
84.111.225.33	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
52.13.52.172	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
207.241.237.227	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.3.144.75	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
100.0.213.161	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
82.80.193.240	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.22	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
198.148.27.5	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.102.195.239	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
132.72.10.190	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
85.214.11.209	Germany	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
81.218.251.250	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
109.253.218.36	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/3/11683.jp	Block	3
109.65.12.110	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/sip_storage/files/3/11683.jp	Block	2
197.38.175.202	Egypt	147.237.77.17	mazi.idf.i	PHP Attempt	Block	2
197.38.175.202	Egypt	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	2
95.86.117.73	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 95.86.117.73	Block	2
149.88.59.246	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5187-he/igf.aspx	Block	1
109.253.143.181	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/sip_storage/files/3/11683.jp	Block	1
81.218.28.226	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
54.67.55.75	United States	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
207.241.229.49	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
5.28.191.224	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	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
95.86.117.73	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/4250-he/igf.aspx&sa=u&ved=0ahukewi_05idg8plahwjxiwkhf85bemqfggkmae&usg=afqjcnescoklbk2213hj5fbnbsrzzpwmrpg	Block	1
77.75.79.101	Czech Republic	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/9/8699.jpg	Block	1
31.210.179.25	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation Master\$ucHeader\$ucSearchControl\$txtSearch in mazi.idf.il/55-he/igf.aspx	Block	1
212.116.164.20	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/sip_storage/files/3/11683.jp	Block	1
176.13.14.174	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/sip_storage/files/3/11683.jp	Block	1
109.253.218.36	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/sip_storage/files/3/11683.jp	Block	1
82.166.253.36	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
54.67.55.75	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/wp-login.php	Block	1
5.28.191.224	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
207.241.229.224	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
149.50.36.209	United States	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
79.180.34.127	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 79.180.34.127	Block	1
40.77.167.79	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
212.150.71.177	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage	Block	1
5.22.131.82	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
82.166.253.36	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/xmlrpc.php	Block	1
68.180.229.109	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-5475-he	Block	1
10.67.137.61	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/templates/newslst/undefined	Block	1
208.115.111.75	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8333-he	Block	1
149.50.36.209	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
109.65.208.42	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/599-en/igf.aspx	Block	1
79.180.34.127	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
46.19.85.10	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/sip_storage/files/3/11683.jp	Block	1
5.22.131.82	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
109.253.218.190	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/sip_storage/files/3/11683.jp	Block	1
68.180.229.109	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5676-7827-he/ifg.aspx	Block	1
10.67.137.61	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
212.76.120.188	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/6939-10885-he/igf.aspx&sa=u&ved=0ahukewjqkooovmplahvgwykhal6c3aqqoubcdiwcw&sig2=qn7dkwnc7fuprfljhjyueq&usg=afqjcnhsoptkchjg2k0ymt0xg8hre55soq	Block	1