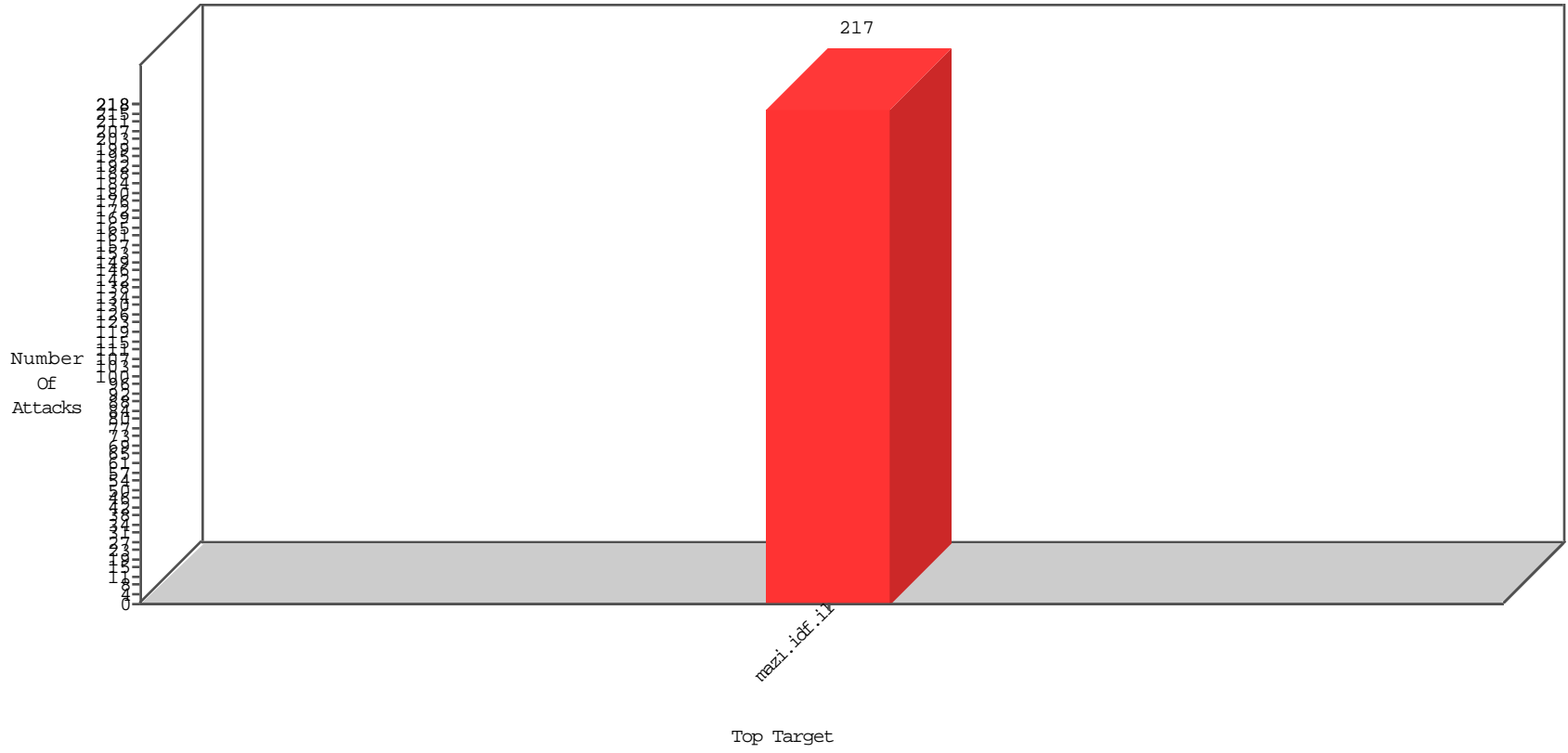


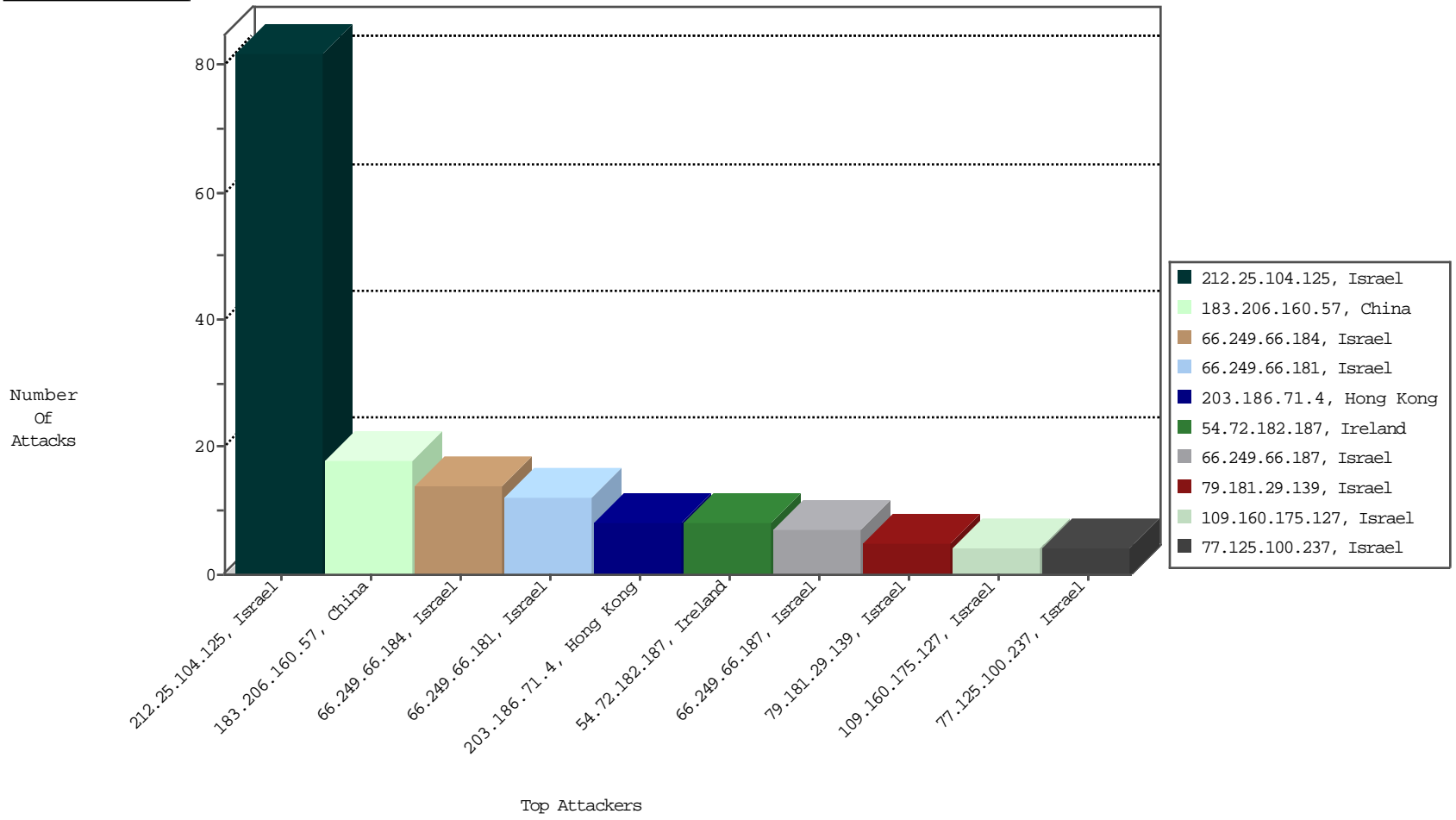
Focused IP Under Attack Daily Report



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	8
71.6.216.48	United States	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	NetV-London	1
104.156.246.165	United States	147.237.77.17	mazi.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
180.97.106.36	China	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	NetV-London	1
185.130.5.224		147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	NetV-London	1
64.79.236.185	United States	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	NetV-London	1

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
212.25.104.125	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	82
66.249.66.184	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
66.249.66.181	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
66.249.66.187	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
109.160.175.127	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
144.76.93.46	Germany	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	2
94.208.145.95	Netherlands	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	2
203.186.71.4	Hong Kong	147.237.77.17	mazi.idf.il	16063: HTTP: Suspicious User-Agent (Opera/8.xx) Likely Win32/Ranbyus	Block	2
144.76.7.107	Germany	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	2
188.165.15.202	France	147.237.77.17	mazi.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
151.80.31.133	Italy	147.237.77.17	mazi.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
157.55.39.222	United States	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
207.46.13.30	United States	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
188.165.15.165	France	147.237.77.17	mazi.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
66.249.66.181	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
81.45.180.180	Spain	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	2
91.201.236.113	Ukraine	147.237.77.17	mazi.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
93.189.26.18	Austria	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	Ukraine	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	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
31.168.23.59	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	64
109.67.112.212	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
46.19.85.200	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
77.126.54.93	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence		monitor	16
37.26.147.142	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
192.243.55.135	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
192.243.55.135	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
192.243.55.135	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.134	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.138	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
188.120.154.51	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.243.55.130	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence		monitor	8
46.117.80.182	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.136	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.130	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
88.253.43.30	Turkey	147.237.77.17	mazi.idf.il	drop	SAM rule	drop	7
192.243.55.135	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
192.243.55.134	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.129	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.131	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.132	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.117.80.182	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.243.55.138	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.134	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence		monitor	4
31.168.209.12	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
2.52.167.116	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
94.230.86.241	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
211.38.165.1	Korea, Republic of	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
192.243.55.138	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.134	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
77.126.54.93	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.138	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence		monitor	4
2.52.167.116	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
192.243.55.136	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
121.105.138.221	Japan	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
213.57.213.218	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
192.243.55.131	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence		monitor	4
71.204.146.106	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.129	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.136	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence		monitor	4
77.126.54.93	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.136	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
98.19.222.133	United States	147.237.77.17	mazi.idf.il	drop	SAM rule	drop	4
192.243.55.136	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.134	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.130	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.52.167.116	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.137	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence		monitor	4
192.243.55.137	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
91.200.12.136	Ukraine	147.237.77.17	mazi.idf.il	drop	SAM rule	drop	3

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
183.206.160.57	China	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 183.206.160.57	Block	10
203.186.71.4	Hong Kong	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 203.186.71.4	Block	5
79.181.29.139	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	5
81.218.8.60	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/images/transvideocounter.gif	Block	4
77.125.100.237	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	4
183.206.160.57	China	147.237.77.17	mazi.idf.i	Multiple Admin Blocking from 183.206.160.57	Block	3
80.74.118.200	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslst/undefined	Block	2
46.117.80.182	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 46.117.80.182	Block	2
212.76.97.63	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/7322-11795-he/mazi.aspx&sa=u&ved=0ahukewjqwpwi0k_lahwok5okhybuc3yqfggemak&usg=afqjcn9i08tw3fbb4lqxjmi_tdvhcb7w	Block	2
84.108.88.60	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 84.108.88.60	Block	1
77.75.76.162	Czech Republic	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/9/8699.jpg	Block	1
62.219.113.61	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
183.206.160.57	China	147.237.77.17	mazi.idf.i	Admin Blocking	Block	1
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-7710-he	Block	1
212.235.8.225	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/2061.jpg	Block	1
40.77.167.85	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/robots.txt	Block	1
183.206.160.57	China	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/includes/fckeditor/editor/	Block	1
85.65.185.40	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
77.75.76.167	Czech Republic	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/9/8699.jpg	Block	1
66.249.66.182	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3848-5183-he/igf.aspx	Block	1
203.186.71.4	Hong Kong	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/wepdwulltelnzuzwnzilndrkza=	Block	1
2.52.162.27	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage	Block	1
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files	Block	1
183.206.160.57	China	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/scripts/fckeditor/editor/	Block	1
85.65.185.40	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/xmlrpc.php	Block	1
66.249.66.185	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5034-he/igf.aspx	Block	1
207.241.229.222	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
5.22.134.215	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
84.108.88.60	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
68.180.229.218	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/14-8331-he	Block	1
46.117.80.182	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslst/undefined	Block	1
183.206.160.57	China	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/admin/fckeditor/editor/	Block	1
156.170.29.4		147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4637-5227-he/igf.aspx	Block	1
66.249.66.185	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
5.22.134.215	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
183.206.160.57	China	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/fckeditor/editor/	Block	1