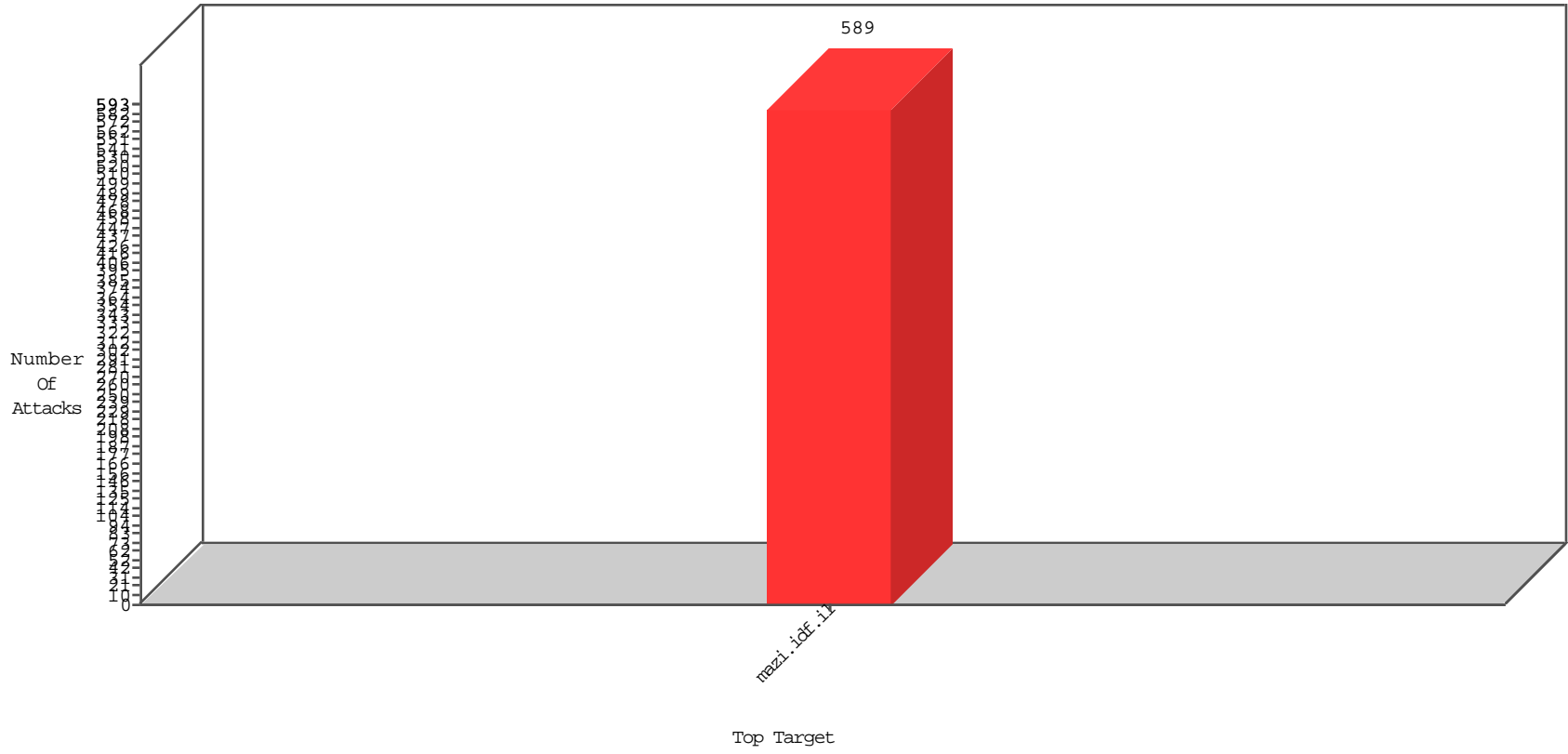


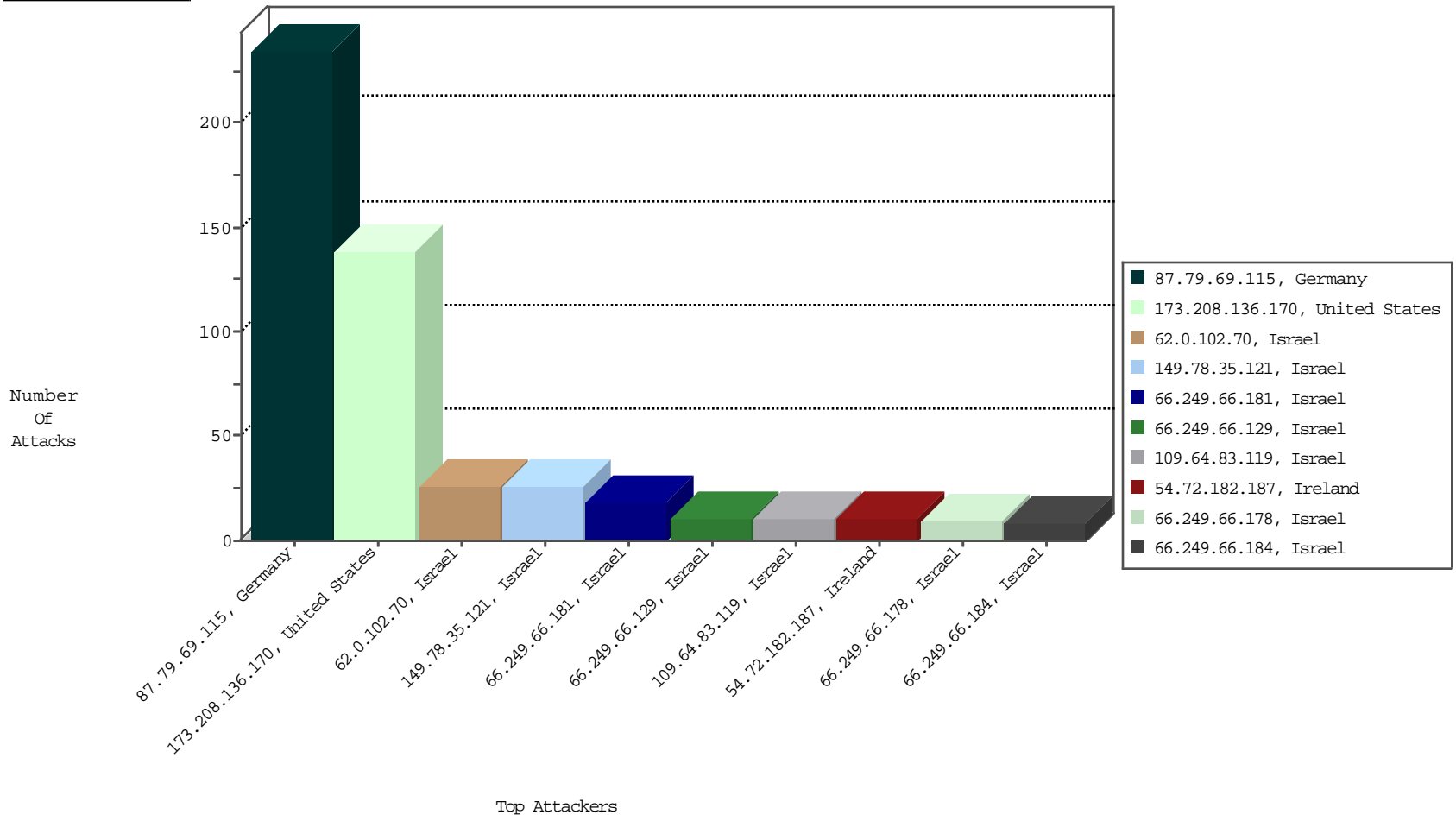
Focused IP Under Attack Daily Report



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	10
212.143.254.66	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	DP-Tehila	3
23.228.107.104	United States	147.237.77.17	mazi.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
64.94.45.65	United States	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	NetV-London	1
64.94.45.66	United States	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	NetV-London	1
65.196.5.13	United States	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	NetV-London	1
141.255.164.234	Switzerland	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
184.105.139.118	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
87.79.69.115	Germany	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	235
149.78.35.121	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	26
62.0.102.70	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	26
66.249.66.181	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	18
66.249.66.178	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
66.249.66.184	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
66.249.66.129	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
66.249.93.5	United States	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
66.249.93.63	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
31.168.113.160	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.93.5	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.19.85.29	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
212.251.221.118	Norway	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	2
157.55.2.164	United States	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
66.249.66.133	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
89.216.115.6		147.237.77.17	mazi.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	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
66.249.75.18	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
66.249.93.2	Israel	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
66.249.66.181	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
104.197.254.53	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 2048	1
104.197.254.53	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -f -sS	1
104.197.254.53	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 3072	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
192.243.55.130	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	51
192.243.55.138	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	50
87.79.69.115	Germany	147.237.77.17	mazi.idf.il	drop	SAM rule	drop	50
192.243.55.136	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	48
192.243.55.134	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	44
192.243.55.136	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	44
192.243.55.133	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	42
192.243.55.132	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	38
192.243.55.137	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	38
192.243.55.130	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence		monitor	36
192.243.55.130	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	36
192.243.55.131	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	35
192.243.55.129	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	34
192.243.55.130	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	34
192.243.55.138	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	32
46.19.85.161	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	32
192.243.55.136	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	32
192.243.55.135	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	31
192.243.55.134	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
192.243.55.133	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	29
192.243.55.134	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	28
192.243.55.134	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence		monitor	28
192.243.55.137	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	27
192.243.55.138	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	26
93.173.141.108	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
192.243.55.137	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
192.243.55.135	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
192.243.55.132	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence		monitor	24
192.243.55.129	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
192.243.55.133	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence		monitor	24
192.243.55.136	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	23
192.243.55.132	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
192.243.55.131	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
192.243.55.133	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	21
192.243.55.131	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	21
192.243.55.131	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence		monitor	20
192.243.55.136	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence		monitor	20
192.243.55.135	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence		monitor	20
192.243.55.135	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	19
192.243.55.130	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	19
192.243.55.129	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	19
192.243.55.138	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
192.243.55.133	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	17
192.243.55.134	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	17
192.243.55.138	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence		monitor	16
87.69.149.147	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
192.243.55.135	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
192.243.55.129	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
87.69.149.147	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
192.243.55.132	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13

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 Unauthorized URL Access from 173.208.136.170	Block	121
173.208.136.170	United States	147.237.77.17	mazi.idf.i	Multiple Admin Blocking from 173.208.136.170	Block	17
109.64.83.119	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	10
183.206.160.57	China	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 183.206.160.57	Block	5
50.93.198.132	United States	147.237.77.17	mazi.idf.i	PHP Attempt	Block	4
79.179.218.170	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	4
50.93.198.132	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 50.93.198.132	Block	4
183.206.173.99	China	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 183.206.173.99	Block	3
79.180.222.198	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	2
2.52.147.195	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/templates/newslist/undefined	Block	1
183.206.160.57	China	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/editor/editor/	Block	1
87.70.48.31	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/3697-9630-he/igf.aspx 10 2010	Block	1
192.243.55.130	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8330-he	Block	1
176.204.180.97	United Arab Emirates	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
109.67.43.83	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
81.218.241.25	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/1.he/sidebar/sb_over_bg.gif	Block	1
192.243.55.136	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8331-he	Block	1
66.249.66.129	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
37.26.149.179	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3848-5222-he/igf.aspx	Block	1
87.70.48.31	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/vodchannel/	Block	1
54.152.3.137	United States	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
192.243.55.131	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-5475-he	Block	1
141.212.122.209	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
85.65.185.40	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
208.115.111.75	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
66.249.66.129	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
38.81.65.42	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
183.206.173.99	China	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/editorold/editor/	Block	1
173.208.136.170	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/acg-nwl/assetmanager/assetmanager.asp	Block	1
192.243.55.131	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8333-he	Block	1
54.152.3.137	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/wp-login.php	Block	1
183.206.160.57	China	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/editor/fckeditor/editor/	Block	1
156.173.103.230		147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4637-5227-he/igf.aspx	Block	1
85.65.185.40	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/xmlrpc.php	Block	1
213.8.46.1	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
66.249.66.165	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4170-he/igf.aspx	Block	1
192.243.55.129	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/www.idiegogo.com/projects/121440	Block	1
176.204.180.97	United Arab Emirates	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
109.67.43.83	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
192.243.55.132	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/vodchannel/	Block	1
66.249.66.40	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/14-7708-he	Block	1