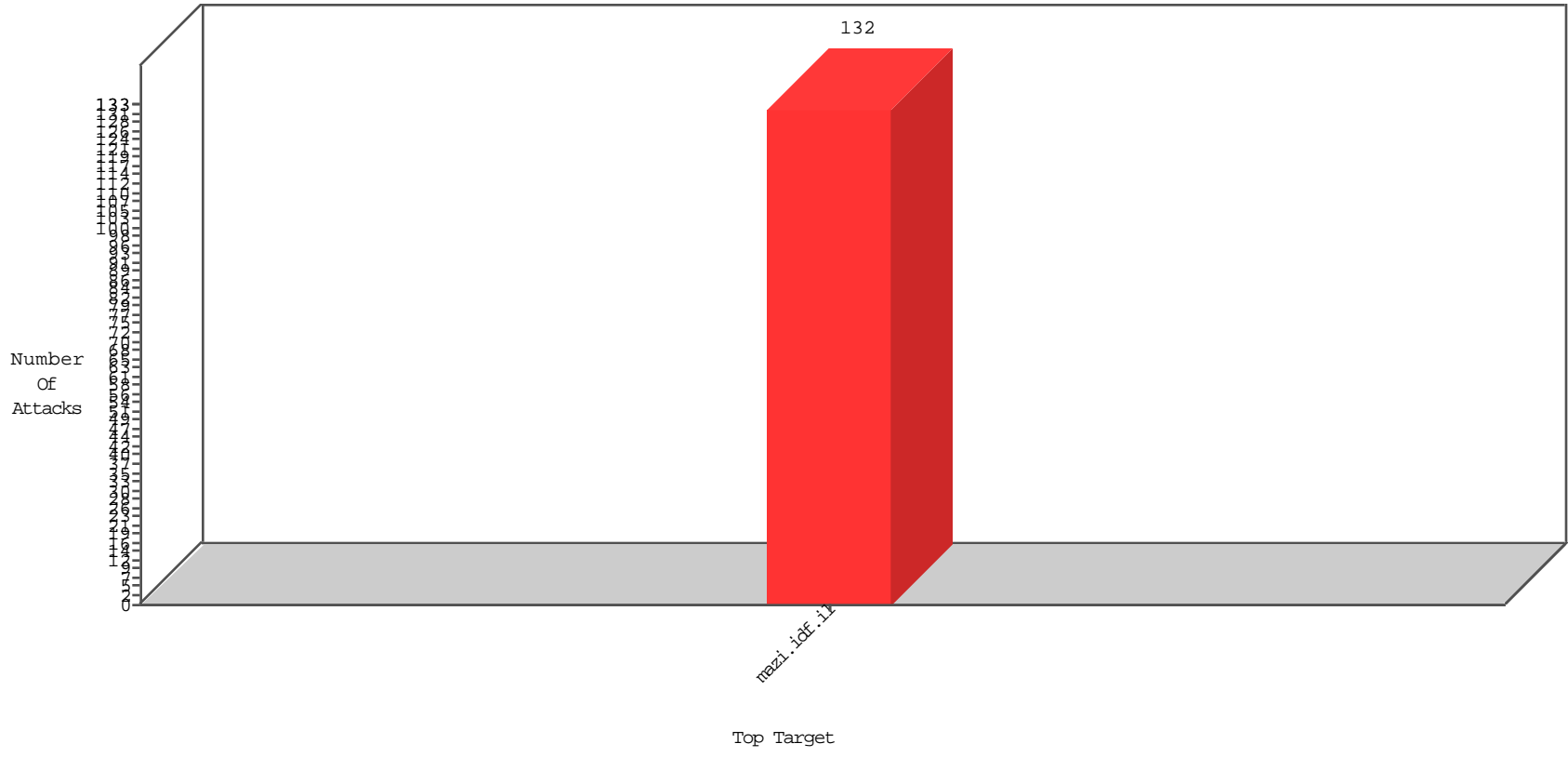


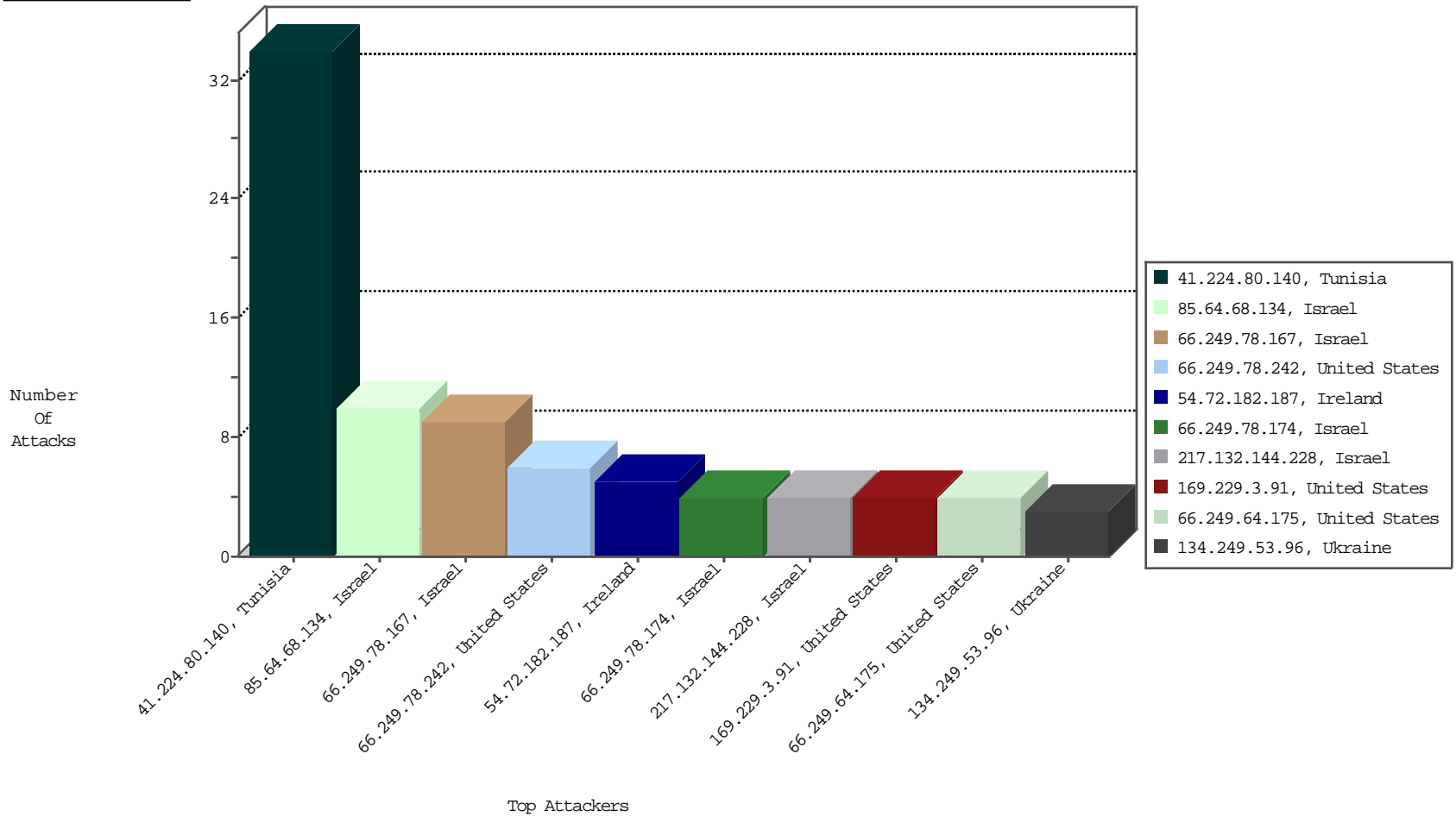
Focused IP Under Attack Daily Report



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	5
151.225.249.172	United Kingdom	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	NetV-London	1
184.105.139.98	United States	147.237.77.17	mazi.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
184.105.139.104	United States	147.237.77.17	mazi.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
89.248.160.138	Netherlands	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
85.64.68.134	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
66.249.78.167	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
66.249.78.174	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
5.9.89.170	Germany	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	2
66.249.64.2	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.78.181	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.64.124	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
134.249.53.96	Ukraine	147.237.77.17	mazi.idf.il	C1000016: HTTP: administrator in URI	Block	1
157.55.39.135	United States	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
66.249.64.8	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
66.249.93.63	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.16	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
104.255.65.207		147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
185.106.92.142		147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
180.150.177.188	China	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
223.71.251.11	China	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
109.65.208.233	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1225
83.170.93.32	United Kingdom	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	54
46.32.170.122	Azerbaijan	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	48
46.19.85.189	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	16
46.19.85.189	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
5.102.254.60	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
37.46.39.112	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
88.212.40.229	Slovakia	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	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
195.239.16.53	Russian Federation	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
46.120.151.41	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
203.133.168.83	Korea, Republic of	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.120.151.41	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
79.181.199.208	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
185.3.147.237	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
79.183.117.151	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.31	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.146.188	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
2.54.134.78	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
185.3.147.131	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
109.253.201.151	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
80.178.163.239	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
192.116.175.162	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	illegal header format detected: Malformed HTTP format in request	monitor	1
5.29.238.106	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
2.52.157.5	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
79.178.25.254	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
46.19.86.174	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
46.19.85.116	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.26.147.243	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
109.253.223.104	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
5.22.131.81	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
83.170.93.32	United Kingdom	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
41.224.80.140	Tunisia	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.88	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.39.93.143	France	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
94.230.86.236	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
2.52.157.5	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.174	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
216.243.31.2	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.175	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	alert	1
37.26.149.194	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
114.112.90.54	China	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	1
5.28.130.233	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
64.125.239.228	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.86.31	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
46.19.85.45	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
184.105.139.106	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.54.133.127	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.175	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
41.224.80.140	Tunisia	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 41.224.80.140	Block	34
217.132.144.228	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation Master\$ucHeader\$ucSearchControl\$txtSearch in mazi.idf.il/5221-6393-he/igf.aspx	Block	3
66.249.78.242	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	2
83.170.93.32	United Kingdom	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	2
66.249.78.242	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5479-he/igf.aspx	Block	1
217.132.144.228	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation Master\$ucHeader\$ucSearchControl\$txtSearch in mazi.idf.il/5374-he/igf.aspx	Block	1
66.249.64.175	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
46.19.85.175	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/571-he/igf.aspx	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Unknown HTTP Request Method [[#2]]É[[#24]]#012	Block	1
134.249.53.96	Ukraine	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
66.249.78.254	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6054-he/igf.aspx	Block	1
66.249.69.18	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6050-he/igf.aspx	Block	1
212.76.119.192	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/3539-he/igf.aspx&sa=u&ved=0ahukewjdi5gg3pjlaxhd0rqkxhzrd8yqfggfmag&usq=afqjcnedawkvlguvfunk50jifvawpjddq	Block	1
66.249.64.175	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Illegal Byte Code Character in Method [[#2]]É[[#24]]#012	Block	1
89.42.216.25	Romania	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/wordpress/wp-admin/	Block	1
66.249.78.242	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5528-he/igf.aspx	Block	1
66.249.64.180	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
46.32.170.122	Azerbaijan	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4637-5227-he/igf.aspx	Block	1
185.82.200.91		147.237.77.17	mazi.idf.i	Unauthorized Method HEAD for 147.237.77.17/	Block	1
134.249.53.96	Ukraine	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/wp-login.php	Block	1
66.249.78.254	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
66.249.78.242	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/113-he/igf.aspx	Block	1
213.151.41.61	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
66.249.64.175	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/582-he/igf.aspx	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Illegal Byte Code Character in URL "f[[#5]]0 4 n&6,6[[]] #23[[]]#2-]]4#[[^\xenbž]] 1[[#26]][[#4]]vŷŮt tzi{ [[#24]]@ *s[[#7]]q=;n9[[#2]]·g@[[#14]]k	Block	1
46.19.85.35	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
89.107.186.233	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/old/wp-admin/	Block	1
66.249.78.242	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5536-he/igf.aspx	Block	1
66.249.69.2	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4169-he/igf.aspx	Block	1
64.71.32.29	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/test/wp-admin/	Block	1
198.105.221.6	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/blog/wp-admin/	Block	1
139.162.10.19	Netherlands	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/wp/wp-admin/	Block	1
77.237.138.202	Czech Republic	147.237.77.17	mazi.idf.i	Unauthorized Method HEAD for /	Block	1
66.249.64.175	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/62-he/igf.aspx	Block	1
46.19.85.70	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Malformed URL "f[[#5]]0 4 n&6,6[[]] #23[[]]#2tŮŷv]]4#[[]]62#[[[]]1-]]4#[[^\xenbž]] tzi{ [[#24]]@ *s[[#7]]q=;n9[[#2]]·g@[[#14]]k	Block	1
98.130.0.152	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/wp-admin/	Block	1
66.249.78.254	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/120-he/igf.aspx	Block	1
66.249.69.10	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4166-he/igf.aspx	Block	1
65.55.218.32	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/templates/newslist/undefined	Block	1
207.46.13.183	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
157.55.39.135	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/113-11516-he/.aspx	Block	1
37.142.68.77	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3848-5222-he/igf.aspx	Block	1