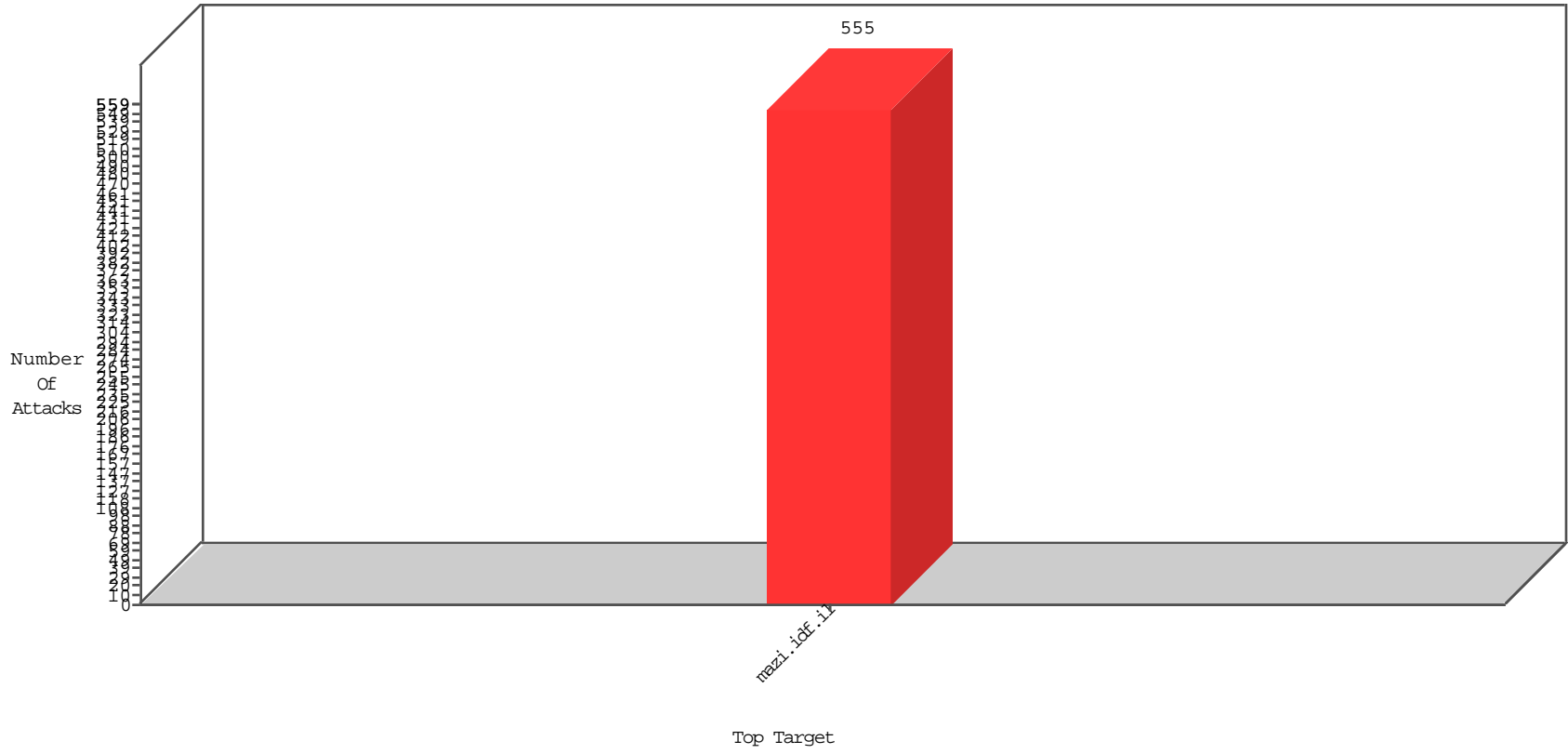


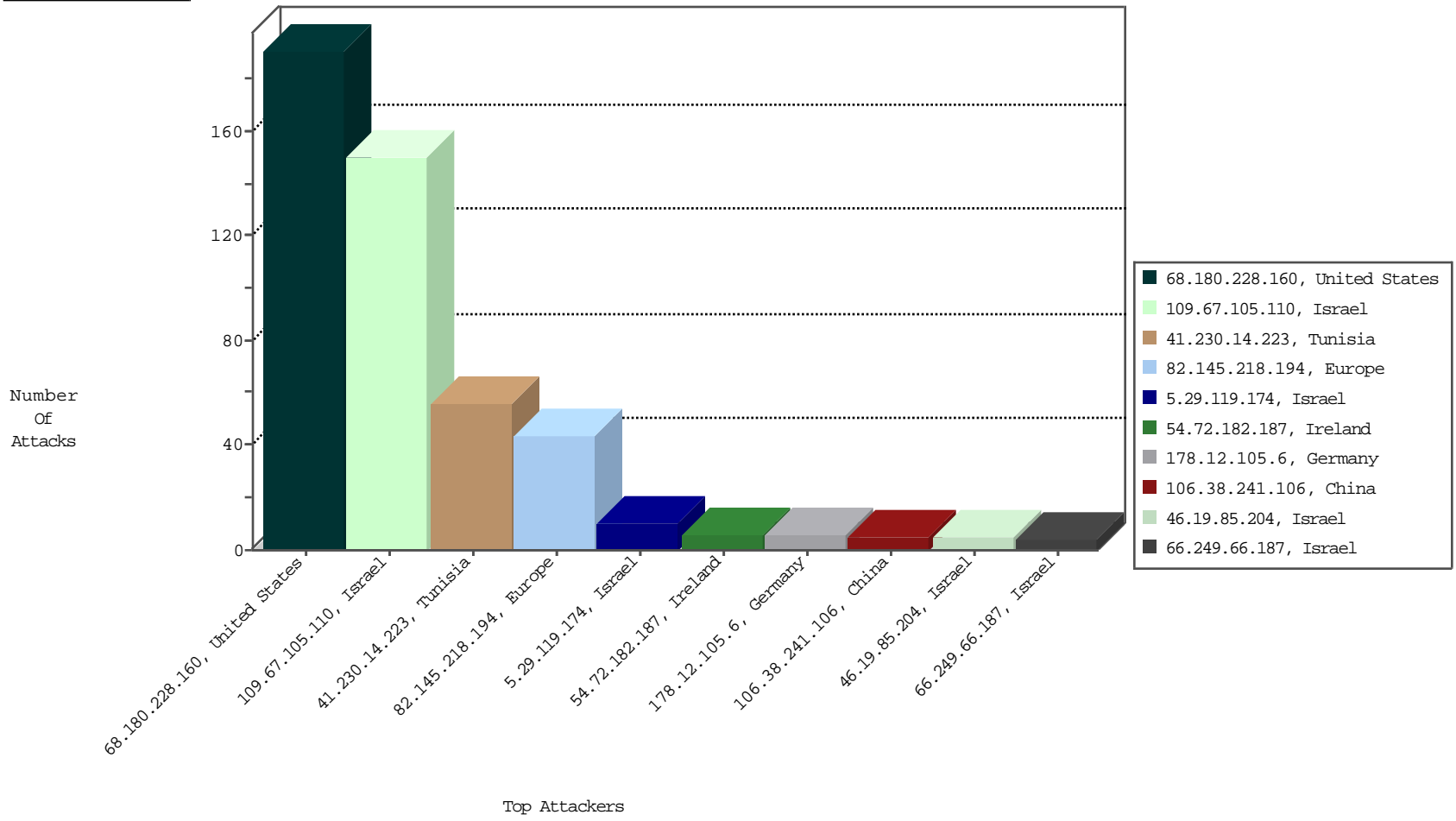
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
82.145.218.194	Europe	147.237.77.17	mazi.idf.il	Block_Ip_Web_In	drop	NetV-London	44
54.72.182.187	Ireland	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	NetV-London	6
134.147.203.115	Germany	147.237.77.17	mazi.idf.il	Block_Ntp_All_Net	drop	NetV-London	2
184.105.139.122	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
68.180.228.160	United States	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	190
109.67.105.110	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	150
5.29.119.174	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
178.12.105.6	Germany	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	6
106.38.241.106	China	147.237.77.17	mazi.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
46.19.85.204	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
207.241.229.222	United States	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
66.249.66.187	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
207.46.13.176	United States	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
157.55.39.122	United States	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.19.85.40	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
77.125.108.183	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
199.30.24.44	United States	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
109.186.154.248	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
151.80.31.152	Italy	147.237.77.17	mazi.idf.il	C1000146: HTTP: AhrefBot crawler	Block	2
91.121.221.15	France	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	2
46.19.86.13	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
199.30.25.84	United States	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
136.243.103.157	Germany	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	2
66.249.75.18	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
54.173.116.45	United States	147.237.77.17	mazi.idf.il	3617: HTTP: Paros Proxy HTTP Request	Block	1
151.80.31.150	Italy	147.237.77.17	mazi.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
66.249.66.184	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
151.80.31.151	Italy	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
98.119.105.221	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 3072	1
209.126.116.147	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
208.67.1.185	United States	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
46.19.85.30	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	25
46.19.85.30	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
106.38.241.106	China	147.237.77.17	mazi.idf.il	drop	SAM rule	drop	19
5.22.135.174	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
85.64.39.201	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
185.3.146.106	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.120.157.131	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.120.157.131	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.210.187.229	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
103.41.177.26		147.237.77.17	mazi.idf.il	drop	SAM rule	drop	4
80.246.133.244	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
109.67.201.176	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
85.64.204.122	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.46.39.197	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
195.154.250.49	France	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
167.114.172.229	Canada	147.237.77.17	mazi.idf.il	drop	SAM rule	drop	1
46.19.86.141	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.102.195.134	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
115.252.43.76	India	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
94.102.48.193	Netherlands	147.237.77.17	mazi.idf.il	drop	SAM rule	drop	1
216.218.206.87	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.28.183.69	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.91	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.67.134.109	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.154	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.102.254.104	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.3.147.45	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
149.88.184.29	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
94.228.34.248	United Kingdom	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
64.125.239.74	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.243.31.2	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.29.147.48	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
172.56.39.7	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.67.201.176	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
85.64.204.122	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.19.86.160	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.3.147.98	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
149.88.184.29	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.48	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.141	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
5.29.147.48	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.111	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
41.230.14.223	Tunisia	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 41.230.14.223	Block	54
79.180.240.6	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/images/transvideocounter.gif	Block	3
85.65.185.40	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/xmlrpc.php	Block	2
85.65.220.174	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	2
77.125.108.183	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	2
85.65.185.40	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	2
66.249.66.185	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/571-he/igf.aspx	Block	1
109.67.229.196	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
79.181.13.2	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/newsgallery/	Block	1
41.230.14.223	Tunisia	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/14-he	Block	1
207.46.13.176	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/templates/newslist/undefined	Block	1
93.172.162.104	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
84.108.88.60	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
79.180.26.12	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
66.249.69.10	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
117.78.13.18	China	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-he	Block	1
79.181.141.191	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
218.255.178.197	Hong Kong	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/images/transvideocounter.gif	Block	1
41.230.14.223	Tunisia	147.237.77.17	mazi.idf.i	Illegal Byte Code Character in URL /14-he/igf.aspx[#20]].	Block	1
93.172.162.104	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
84.108.88.60	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/xmlrpc.php	Block	1
66.249.69.18	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
149.78.139.88	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/2061.jpg	Block	1
89.139.158.254	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
79.181.141.191	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/xmlrpc.php	Block	1
79.178.175.53	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 79.178.175.53	Block	1
218.255.178.197	Hong Kong	147.237.77.17	mazi.idf.i	Parameter Type Violation _EVENTVALIDATION in mazi.idf.il/mazi-site/105-he/igf.aspx	Block	1
95.86.103.252	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
79.181.13.2	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
66.249.75.34	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
40.77.167.35	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/14-5475-he	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Multiple Illegal Byte Code Character in Method from 169.229.3.91	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
80.246.133.244	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/571-he/igf.aspx	Block	1
79.178.175.53	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1