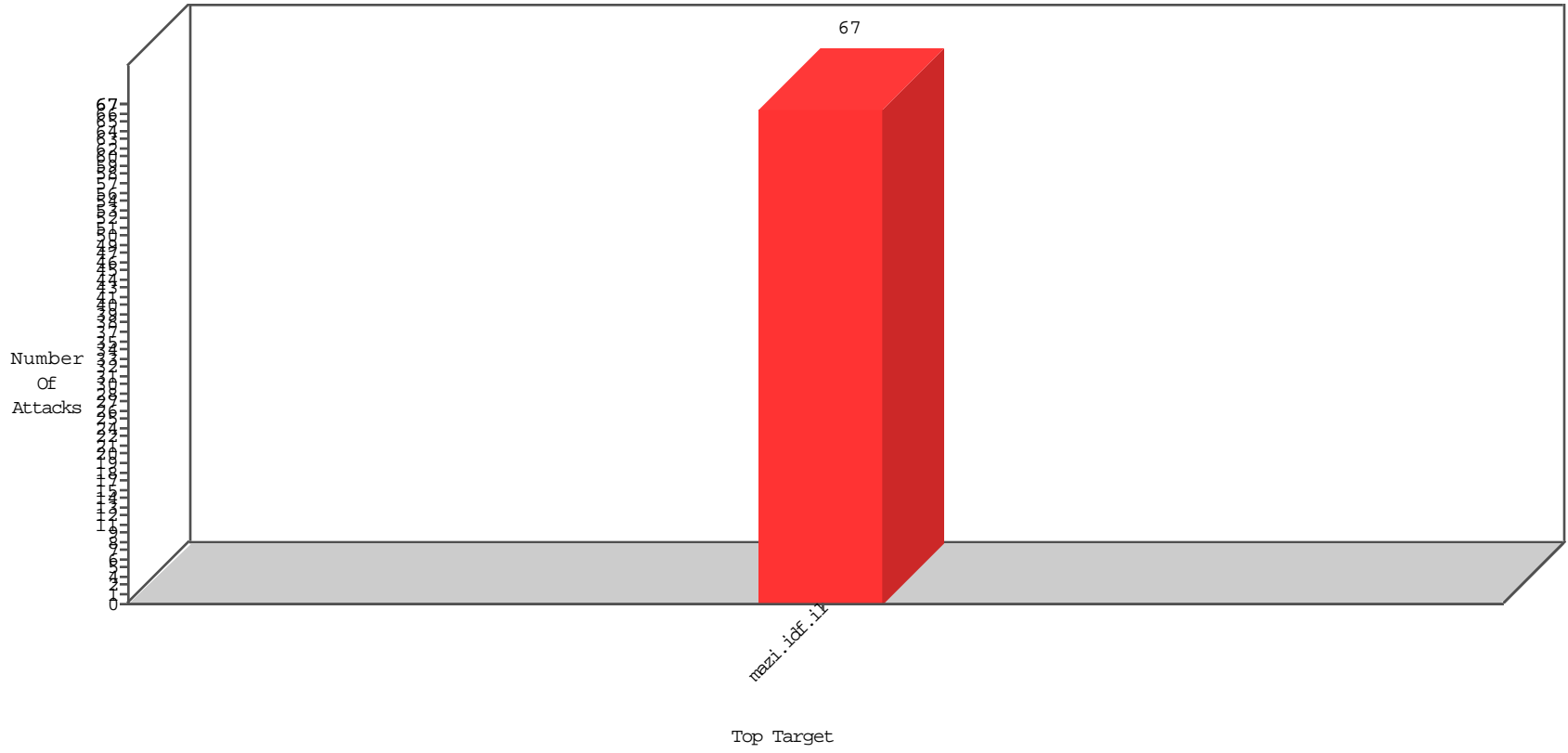


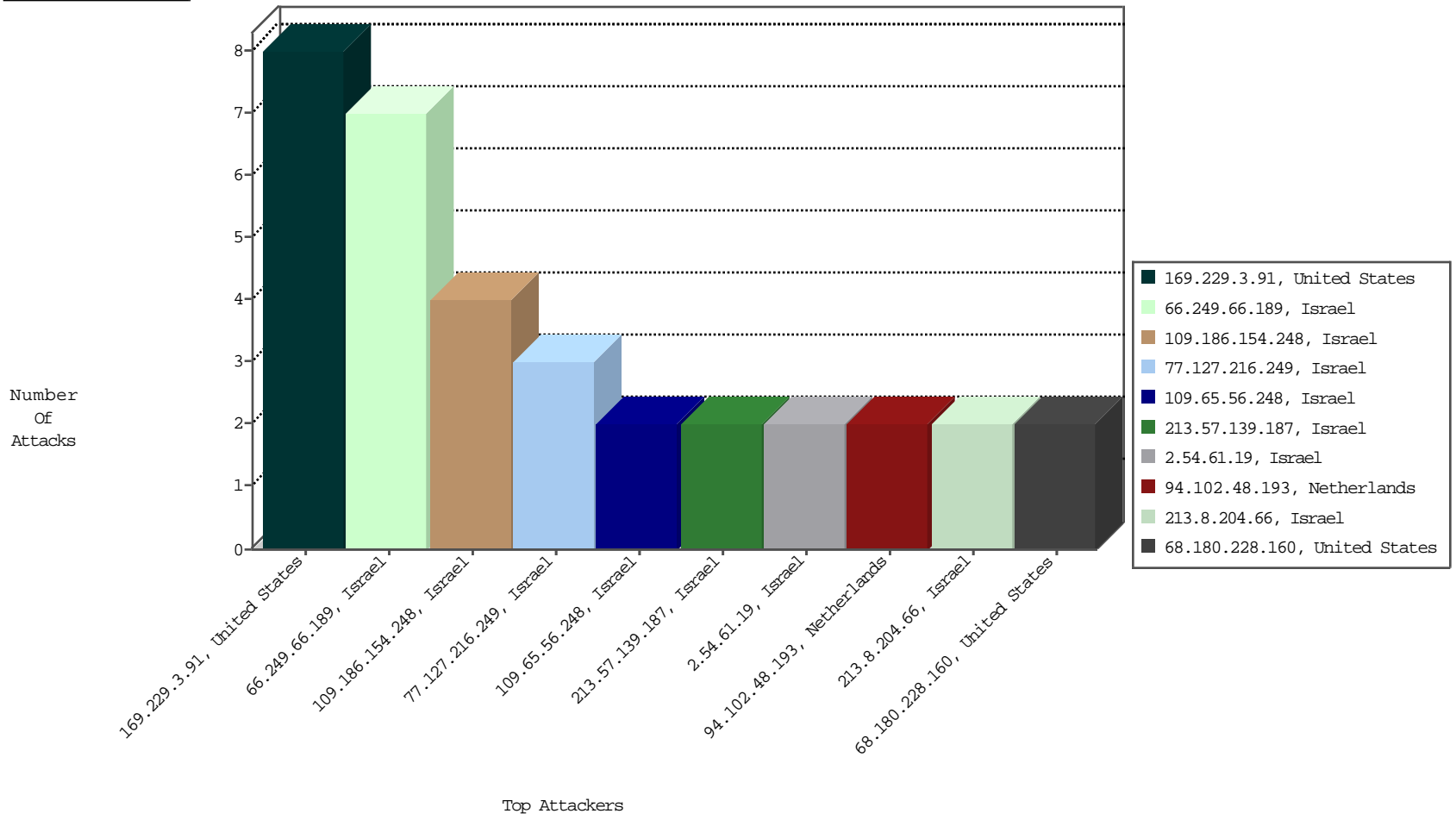
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
66.249.66.189	Israel	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	6
37.26.148.247	Israel	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	1

02-13-2016 to 02-14-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
151.80.31.123	Italy	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.234	France	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	1

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
94.102.48.193	Netherlands	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	2
66.102.9.111	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
122.152.54.168	Bangladesh	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.231		147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	China	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
66.192.6.154	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
112.124.10.141	China	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
125.227.64.115	Taiwan	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
213.8.204.48	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	71
212.76.127.10	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	45
212.76.127.44	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	36
213.151.35.218	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	36
213.8.204.50	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	31
80.179.91.165	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
46.19.85.12	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.85.12	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	16
212.199.63.46	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
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
212.76.127.111	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
37.46.38.236	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.45	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
212.76.127.219	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
84.228.180.188	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
176.42.67.66	Turkey	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	7
5.22.131.29	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
37.46.38.155	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
213.8.204.48	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	alert	6
37.26.148.148	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
79.127.43.14	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	5
79.127.43.14	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
89.139.13.42	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.117.177.144	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
91.200.12.136	Ukraine	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	4
2.52.39.227	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
91.200.12.143	Ukraine	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	4
120.52.72.46	China	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	3
5.22.129.255	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
85.64.35.36	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	2
199.168.142.24	United States	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	2
85.64.35.36	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
185.3.147.227	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
77.125.111.138	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.190	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
95.82.115.131	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.58	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
85.64.132.111	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
82.80.140.226	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
64.125.239.97	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
149.78.169.140	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.142	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
79.181.101.194	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
77.126.225.224	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.207	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.68	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
87.69.154.159	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
213.8.204.19	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
84.0.124.54	Hungary	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	1

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
109.186.154.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	4
77.127.216.249	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	3
2.54.61.19	Israel	147.237.77.17	mazi.idf.i	Suspicious Response Code	Block	2
217.132.48.152	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	2
5.22.135.153	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
213.8.204.48	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Illegal HTTP Version	Block	1
149.50.87.20	United States	147.237.77.17	mazi.idf.i	Suspicious Response Code	Block	1
79.181.193.104	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
213.57.139.187	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
66.249.66.169	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/571-he/igf.aspx	Block	1
207.46.13.164	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-4983-he	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Illegal Byte Code Character in Header Value	Block	1
109.65.56.248	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
5.22.135.153	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
213.8.204.50	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Malformed URL gq•ox'k	Block	1
157.55.39.222	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
84.228.180.188	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4947-8221-he/igf.aspx	Block	1
213.57.139.187	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
66.249.66.173	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
208.115.113.91	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-5475-he	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Illegal Byte Code Character in Method 3'f','	Block	1
77.125.87.0	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
213.8.204.66	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
37.26.148.148	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Unknown HTTP Request Method 3'f','	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Abnormally Long Request method	Block	1
85.60.135.196	Spain	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/7/1087.jpg	Block	1
66.249.66.189	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
5.22.129.255	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1
208.115.113.91	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8334-he	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Illegal Byte Code Character in URL gq•ox'k	Block	1
141.212.122.177	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
213.8.204.66	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
54.147.176.220	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3848-5222-he/igf.aspx	Block	1
180.250.50.253	Indonesia	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/cgi-bin/test.sh	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Illegal Byte Code Character in Header Name 7=1k'f'b'Kf',c[[#1]]'f'-	Block	1
109.65.56.248	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/14-10105-he	Block	1