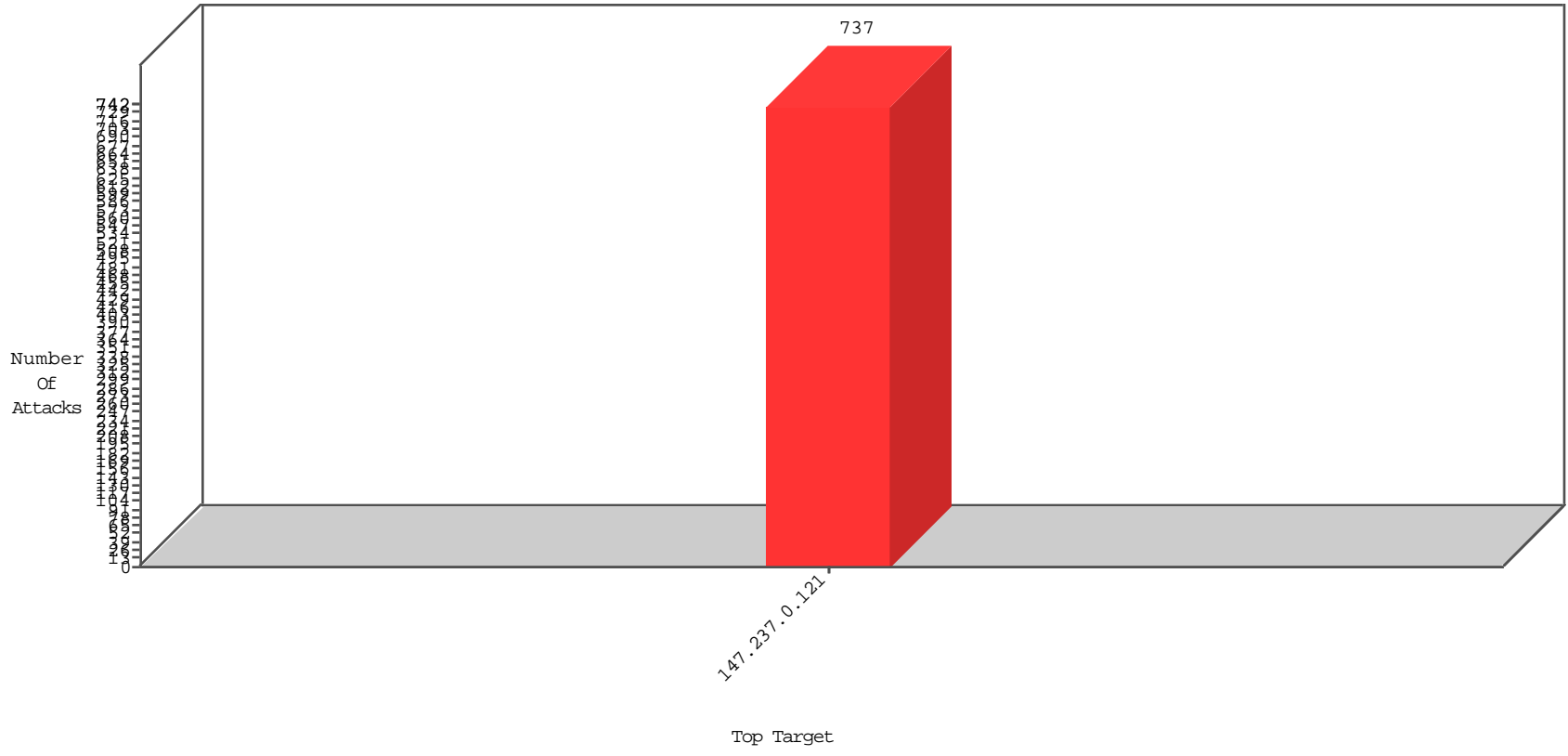


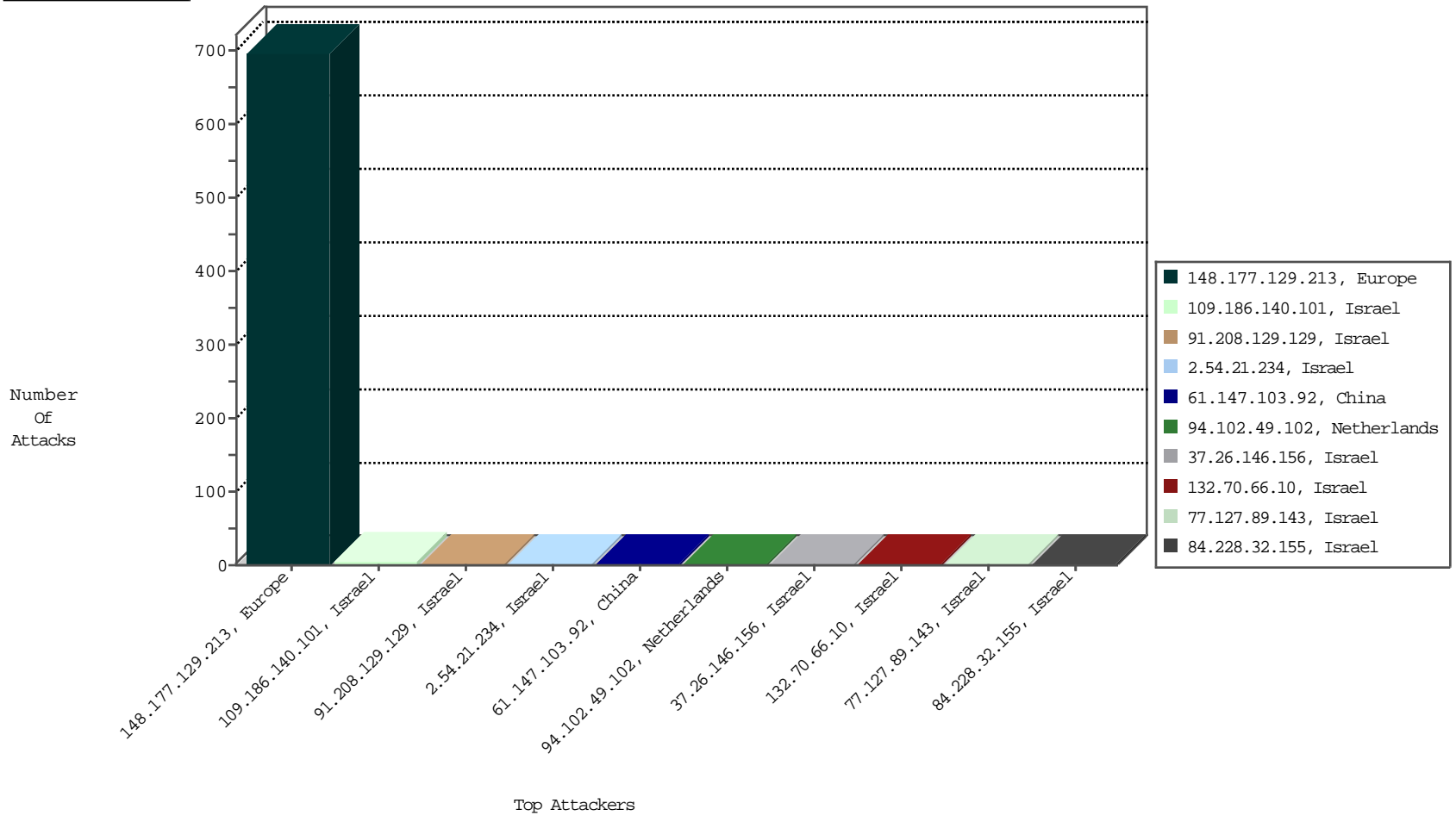
# Focused IP Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
148.177.129.213	Europe	147.237.0.121		TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	698
91.208.129.129	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3
94.102.49.102	Netherlands	147.237.0.121		Frk_Under_Attack_Con_Tcp	drop	BBL-Frankfurt	2
61.147.103.92	China	147.237.0.121		Frk_Under_Attack_Con_Tcp	drop	BBL-Frankfurt	2

11-09-2015 to 11-10-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
37.26.146.156	Israel	147.237.0.121		13840: TLS: OpenSSL Heartbeat Packet	Block	2

11-09-2015 to 11-10-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
59.45.79.117	China	147.237.0.121		ET SCAN Potential SSH Scan	1
84.21.203.130	Bulgaria	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1
31.6.71.154	Poland	147.237.0.121		ET SCAN NMAP -sS window 1024	1
74.117.133.194	United States	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1
176.123.28.153	Moldova, Republic of	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1

## Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site Name	Signature	Device Action	Count
66.102.9.74	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	1496
66.249.93.154	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	1416
66.102.9.97	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	1368
66.102.9.87	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	1162
66.249.81.130	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	947
66.249.81.251	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	883
66.249.93.150	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	846
72.37.140.46	Italy	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	840
66.249.93.146	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	776
66.249.83.208	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	764
66.249.81.254	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	760
2.52.34.55	Israel	147.237.0.121	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	729
66.249.83.212	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	703
149.78.254.181	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	670
66.249.83.216	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	543
149.88.25.125	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	362
149.88.74.190	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	334
198.91.116.182	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	240
149.88.41.145	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	119
64.79.85.205	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	116
67.53.251.122	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	111
66.249.93.154	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	111
66.249.93.146	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	111
66.249.93.150	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	109
66.249.81.130	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	96
54.243.190.43	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	96
149.88.21.216	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	84
66.249.83.208	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	84
149.78.204.142	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	79
66.249.81.251	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	74
66.249.81.254	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	74
66.249.81.168	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	66
149.78.42.30	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	65
66.249.83.216	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	64
149.78.39.110	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	62
66.249.83.212	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	61
66.249.93.241	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	59
66.249.93.247	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	59
134.191.249.39	United Kingdom	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	55
217.69.133.250	Russian Federation	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	50
176.12.138.38	Israel	147.237.0.121	Bad TCP sequence	Invalid ACK number	monitor	49
149.78.221.136	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	48
149.88.5.64	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	48
81.218.105.2	Israel	147.237.0.121	Bad TCP sequence	Invalid ACK number	monitor	45
66.249.81.232	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	42
217.69.133.191	Russian Federation	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	38
66.249.64.165	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	38
149.78.200.202	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	37
31.154.176.123	Israel	147.237.0.121	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
2.54.11.147	Israel	147.237.0.121	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36

11-09-2015 to 11-10-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
109.186.140.101	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/ufi/reaction/	Block	4
132.70.66.10	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	2
77.127.89.143	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/1355-he/miluim.aspx	Block	2
2.54.21.234	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	2
198.20.69.74	United States	147.237.0.121		Unauthorized URL Access to 147.237.0.121/	Block	1
85.64.145.51	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
31.168.240.77	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
212.143.110.33	Israel	147.237.0.121		Unknown Parameter ch in www.miluim-ishi.aka.idf.il/login	Block	1
93.172.158.157	Israel	147.237.0.121		Multiple Unauthorized URL Access from 93.172.158.157	Block	1
37.26.147.247	Israel	147.237.0.121		Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login	Block	1
176.13.21.1	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$Submit1 in www.miluim-ishi.aka.idf.il/changeunit	Block	1
79.180.192.201	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/rules.abe	Block	1
213.57.175.146	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddStudyEmploymentPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
109.66.164.111	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https://www.miluim-ishi.aka.idf.il/	Block	1
45.55.158.46		147.237.0.121		Unauthorized URL Access to /	Block	1
176.13.23.32	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtSmsCode in www.miluim-ishi.aka.idf.il/smsverify	Block	1
84.228.32.155	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https://www.miluim-ishi.aka.idf.il/	Block	1
2.54.160.131	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected , Observed F679031A3EA5E5695DDA7675AA0BBE2B608B8EA40C9A3499DA3B4C321A36B48B9BFEE5560A5BD3FAE931228A3439BF5B58F3D3C5657B793F18B1DC1D1F471D789A4E634E1C2396ECC59A5959EBBF3F80D5DBBED02FE8477F427ECA121E5701A03A95664359C9BE2E21175C46A081DCC0C C75CBC8F48210D66F53277C481C8E9BAC7DC636722760E1426C01B46ED7C09DD89545795E2659A1DF14710A771B4E9F	None	1
46.117.62.166	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 46.117.62.166 (Open Mode)	None	1

11-09-2015 to 11-10-2015