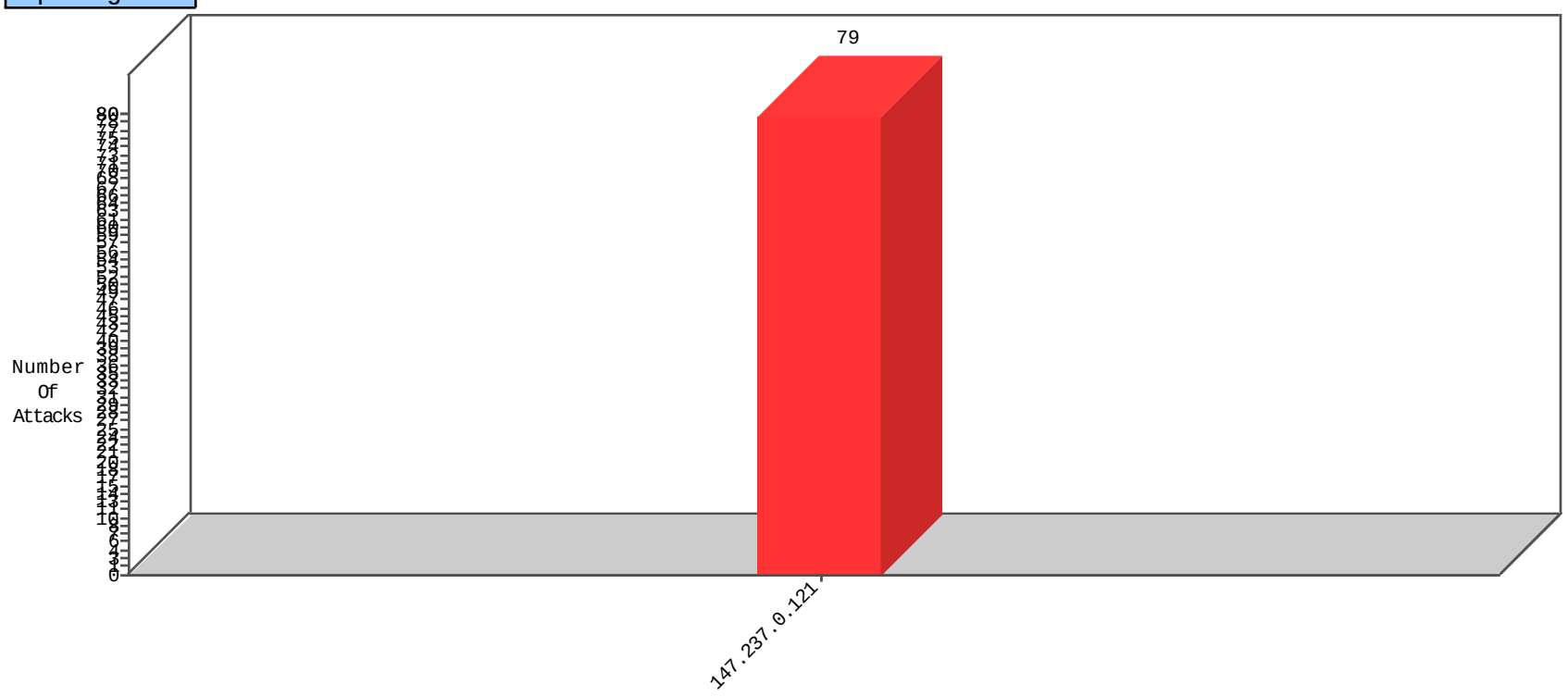
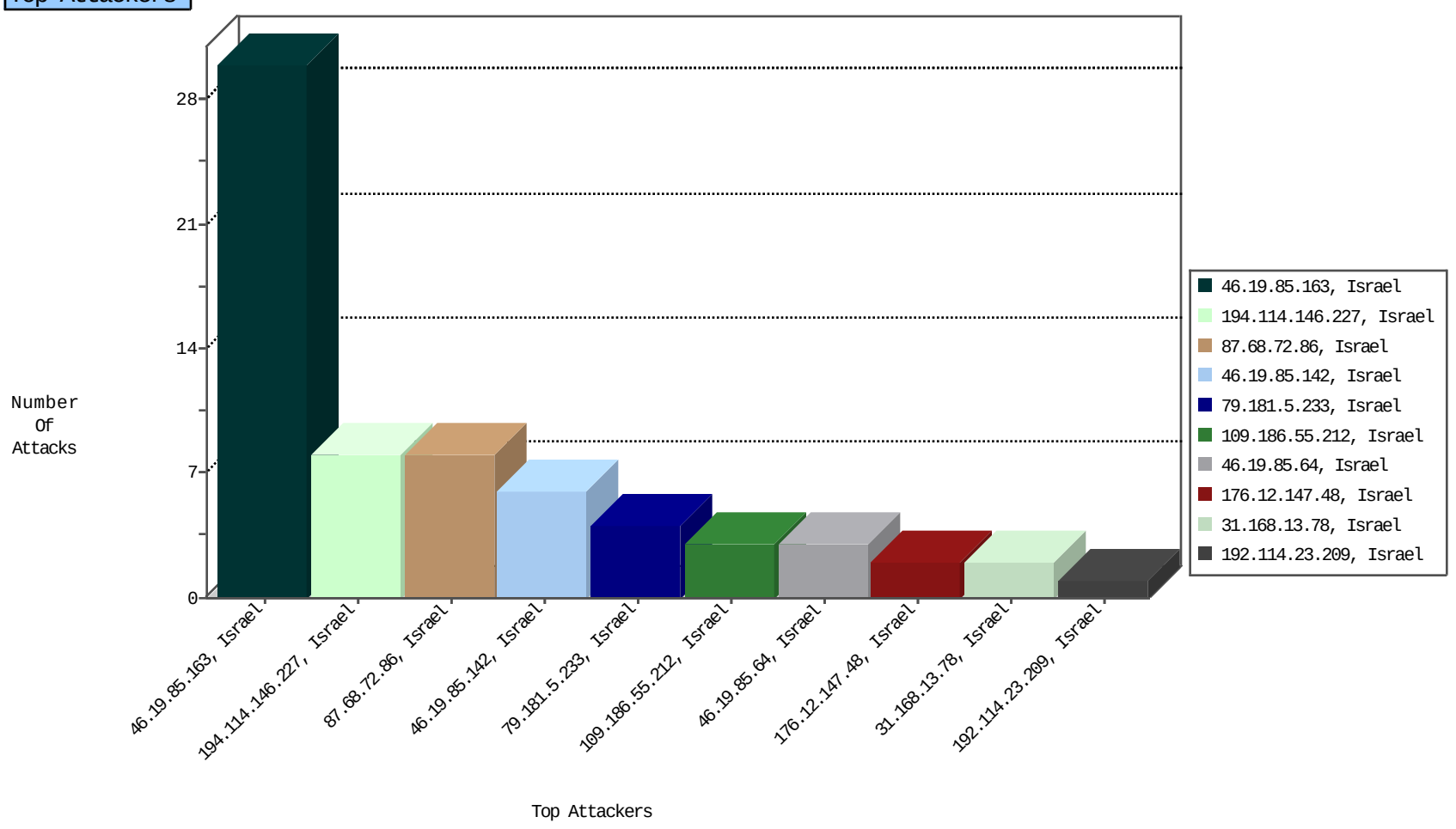
11-11-2015 to 11-12-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



11-11-2015 to 11-12-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
87.68.72.86	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	8

11-11-2015 to 11-12-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

11-11-2015 to 11-12-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
61.182.170.38	China	147.237.0.121		ET SCAN Potential SSH Scan	1
112.33.8.23	China	147.237.0.121		ET SCAN Potential SSH Scan	1

11-11-2015 to 11-12-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.154	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2769
66.249.93.150	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2319
66.249.93.146	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2216
68.180.229.110	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	342
66.249.81.130	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	305
149.78.181.213	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	288
95.90.206.79	Germany	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	286
66.249.81.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	282
66.249.93.150	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	248
66.249.93.154	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	232
66.102.6.153	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	226
66.249.93.146	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	209
66.249.81.251	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	202
149.78.255.14	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	185
176.106.227.18	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	141
149.78.228.207	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	126
149.88.25.125	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	118
46.19.85.26	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
67.53.251.122	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	106
149.88.92.106	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	102
192.146.6.2	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	100
68.180.228.168	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	79
69.248.240.127	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	68
149.78.59.197	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	65
66.102.7.172	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	56
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	52
66.249.65.190	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	51
66.249.65.176	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	50
66.249.81.254	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	46
149.78.19.250	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
149.78.221.136	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
149.78.27.42	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	41
66.249.93.244	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
79.177.129.67	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
87.68.72.86	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
192.198.151.45	Europe	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	36
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	35
192.114.105.254	Israel	147.237.0.121		Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	34
81.200.15.10	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	34
66.249.81.238	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	34
66.249.81.130	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	32
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	31
66.249.81.164	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	29
66.249.65.190	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28
66.102.9.50	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
66.249.81.168	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
46.19.86.138	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	25
66.249.81.235	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	24

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
46.19.85.163	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 8808403612764309DE89F2B9E70DA08BEF5BBD9C58C40921A93DB5837FAFDC82DF914C0995625F19C4DB7D03935873083E68B0873B5428EAB222C33BE3EC29F15CB0568C3609532CE54312D3C3972F9E914744C80CAABAEE6AA332CDFCB32C9631FD595878E6696ABAB5EBD8A06C01EECE3C8E60FFDFAD51FBE65870A91F9AD2, Observed 370B7935B32DB7D0006FF229438CAA8EF833544EA8F0F8C0DFB5718A1389DEA6B7818E3C939ADE1D7158A8CA9FBA52428FD4194BB38F77C2C0564CE1E856FE85388EB0B41F1A763DA09CFB07E4FD2EAD8FCC3B8F2A44D186E9CADE221136671C023274	None	30
194.114.146.227	Israel	147.237.0.121		Unauthorized HTTP Method	Block	8
46.19.85.142	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected AEB83ED98AD865FAACCAD1E1ABCDD49EB74D0C7491E217BEEC108B2C81FE45BEC5D5510125D55B242F53E390F343AC188C83EC35807848CA4142A768E7900390EB9F4266811957D64CE6EC9B623FEC796CB2288C4DC054768D864283D3D140B2690EE30D62BA8240DCC99FC02578C25221B81E9CBF8A10561C8A45127FC9B424, Observed FAD30B6751F3B6117C780ABF94C35AEEBEECC6481C8BE72F060B2B270A727AEFF1A4B182795269148762ACA3D7DC05B01306C5B2A4A60E4D641821D2883D0655AF83A3BB892DAA2E4667552DFA5D91AB1D963A38871FE85D1789B8F1E017600710E052	None	6
46.19.85.64	Israel	147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	3
109.186.55.212	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/ufi/reaction/	Block	3
79.181.5.233	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddStudyEmploymentPermitDocs&FilesToCheck in www.miluim-ishi.aka.idf.il/login	Block	2
176.12.147.48	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	2
79.181.5.233	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddStudyEmploymentPermitDocs&FileToActivate in www.miluim-ishi.aka.idf.il/login	Block	2
2.54.8.178	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
192.114.23.209	Israel	147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	1
138.134.102.15	Israel	147.237.0.121		Unknown Parameter tzav in www.miluim-ishi.aka.idf.il/login	Block	1
46.19.86.241	Israel	147.237.0.121		Unknown Parameter returnurl in www.miluim-ishi.aka.idf.il/login	Block	1
31.168.13.78	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 31.168.13.78 (Open Mode)	None	1
192.198.151.43	Europe	147.237.0.121		Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 192.198.151.43	Block	1
94.188.248.70	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/changepassword/	Block	1
46.120.32.218	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
31.168.13.78	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
185.32.179.56	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected A8A92D4A8D2685B2F3402C91C8A59D08C6062372CB9714655B24A7E3250B67C62AE9CF112BA853C85E50BB6D23E4AC0846F49D3228A2D871A180B93BBAC4957721903992B9950E718A890581FE98F69C448AF98B93519A31E67A116BCFFCD30D24EDD99CD4361CE6CCBA2C1D7D5332075E3213BDF06CD15BD00A9E7ACADE9A40, Observed 6C6A487B02466DC7BD58568569EFF98CEDAA7F8FB8569FD292DA96C6F1DE5478B3B50B5EE9393016C4EDF97DB1244782903FF3F0DFAA05BC12D3EA3EB70D0769A08679AB711CE3B45A0799FBDF89569D9C82D0BC1780A99E126B63573727E58F2ED942	None	1
46.19.85.56	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 67A8DCE5B4082A467829FC0D4C6BF11A0EDB18EEF4F5C34625EE00A74F307164D26DE91843CB4120260A0FE813A903AD3804A12EAFBC8CA523163DBB970715FD57402D2897BB5C6DAAF01C85D845101A34E67F90E8C416FFC07F9D03225D622439EEC1058EF8EB9B204042FBD326C27425EFAB81AB9FDBF8BD538804090DB5EF, Observed 4BC0BFE1675D46FFB2F51A52AF19CB944FD862740075F3BCD6366CE3D47EADAE80A0F9DF5CFEBB1131F05EE54352C9BE28A49211BBD5DB530CD4D2B16779F13F8ABDC64C32E30349249D28B549578E7FCBF780D7D6D108203E67650A6FCAA35E364B7F	None	1
132.70.66.12	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
46.19.85.236	Israel	147.237.0.121		Distributed Double URL Encoding	Block	1