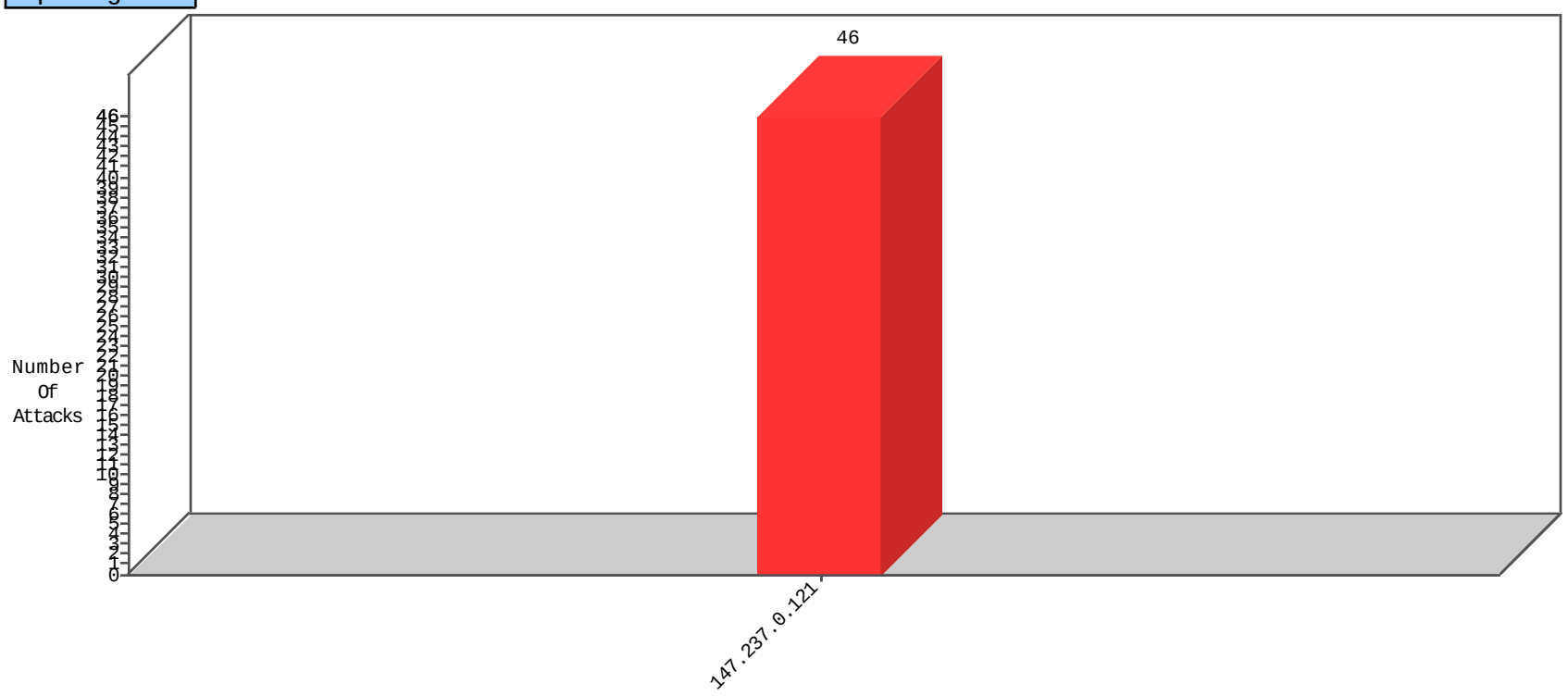
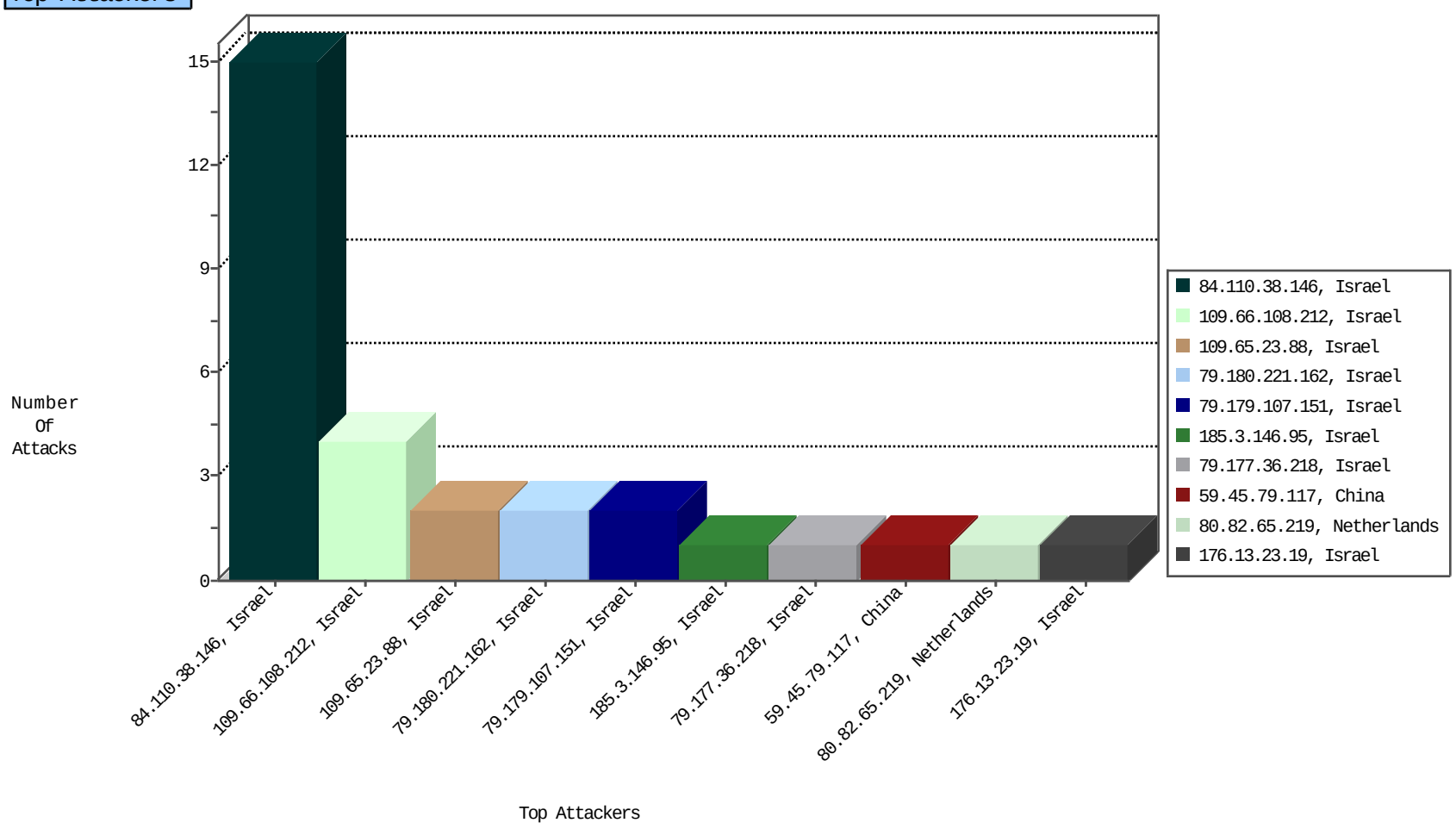
11-19-2015 to 11-20-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



11-19-2015 to 11-20-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count

11-19-2015 to 11-20-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

11-19-2015 to 11-20-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
80.82.65.219	Netherlands	147.237.0.121		ET SCAN Potential SSH Scan	1
110.20.7.193	Australia	147.237.0.121		ET SCAN Potential SSH Scan	1
43.229.53.89	Japan	147.237.0.121		ET SCAN Potential SSH Scan	1
61.182.170.38	China	147.237.0.121		ET SCAN Potential SSH Scan	1
74.117.209.136	United States	147.237.0.121		ET SCAN NMAP -sS window 1024	1
101.4.136.68	China	147.237.0.121		ET SCAN Potential SSH Scan	1
191.243.51.34	Brazil	147.237.0.121		ET SCAN Potential SSH Scan	1
59.45.79.117	China	147.237.0.121		ET SCAN Potential SSH Scan	1
74.117.209.135	United States	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1

11-19-2015 to 11-20-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
212.25.84.200	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	5058
66.249.93.150	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	4630
66.249.93.154	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	3626
66.249.93.146	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2815
212.25.84.200	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	400
66.249.93.146	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	335
15.203.162.37	France	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	290
149.88.185.151	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	289
77.125.84.209	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
66.249.93.154	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	280
66.249.93.150	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	275
13.21.125.9	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	231
2.52.28.2	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	216
149.78.244.147	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	200
149.88.59.30	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	185
149.78.18.50	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	173
13.17.125.9	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	172
15.203.178.33	France	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	162
59.149.187.128	Hong Kong	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	150
212.25.84.200	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	138
149.78.246.250	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	122
58.104.74.252	Australia	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	108
149.78.32.196	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	105
138.134.192.10	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	99
149.78.134.165	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	90
149.88.192.21	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	67
66.102.9.39	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	65
149.88.92.99	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	64
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	62
2.54.135.158	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	61
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	59
149.78.2.63	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	56
2.54.12.102	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	54
14.0.207.53	Hong Kong	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	53
66.249.81.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	52
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	52
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	52
50.97.184.196	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	51
149.88.216.249	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	49
91.228.248.251	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	49
192.115.177.203	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	49
66.249.66.105	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	46
46.19.86.26	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
201.31.215.129	Brazil	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
87.68.159.170	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	37
199.203.226.21	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	37
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
66.102.7.186	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
2.54.135.158	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	36

11-19-2015 to 11-20-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
84.110.38.146	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/ufi/reaction/	Block	13
109.66.108.212	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/ufi/reaction/	Block	4
79.180.221.162	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected E70F24B1F410AEAEEC7B536D642AB2447F170E9D77153FFC09749C246C688D6DC8AC17AA5ACB884B3BCCCF87FE915D880D8D827756167191B5C745E56BF51139DF4A9689F443C71AF240CB903CB50A9E583D59F09D542720D3C7DCD304F602DD3B51D34017DC135AE90C69259E4D0A15FD099183D55C12A3C8E3ADEDA92EBFB8, Observed 59E8D696221C4BE3207831029A58A7BEEC56B99616B4089B3A336CF7C7189D29F4F4659147212126D7F4C02308A74378DC7DADACD9F280AC6DDE6BF5F882285D6F9DB671AE36AE172BE29F511F8F1A13A809EA9E99C6117405D0480DF27A3E34899F3A	None	2
109.65.23.88	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/ufi/reaction/	Block	2
79.179.107.151	Israel	147.237.0.121		Unknown Parameter ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/smsverify	Block	2
185.120.125.4		147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
85.250.194.138	Israel	147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	1
79.177.36.218	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	1
109.67.152.4	Israel	147.237.0.121		Parameter Type Violation __EVENTVALIDATION in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
2.54.29.56	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected , Observed 215DBCB56447556AAB45AF8BD84E5AB25250A314B83AF20C5F9DFD9D6B32C5A09186559B3483AB8A7EFBC240600DAD7FA92455242DAEB3F220DE09FA448150E995B0813F5282774A1E04D363F550EF12551F0596F8BFBC296C64A9501F22A92500669ECAA2DED3442C3F068B980EE371DB6ABA623CCB04F54B62EA83B03CD6D25B5699D67922BE74276B556F2869F11A60BB93D47564935983385E9FD229851C	None	1
192.115.94.2	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
94.230.86.245	Israel	147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	1
79.178.155.191	Israel	147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	1
176.13.23.19	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 9C27070B0E117B6395803F3289040C56F437BCA2531C6282C8FECDA17DBF64E9375548640F6E6CF23D48DE1F690ACBDB4A908DCAED1C14A72CD80355359F115AF92B8E6545D53B2404FF900CA085838A590FD0170A9D3E1019BD7FD2A7674210813C325AD45CE565448CE971F16772807092E97BDEC19BB50D6DFA7D7230A4F5, Observed 93DF67EBA5AC526F6B3B07CE488099DF1EB03353E1E68005A75493182354886728A5D6D4AC928D343C559F742FA8BDDAAB1F454AC5DAF9C8357B6AD9D271CF1210CCA848589DC437F3F167609E5F86F3EB1C00A222C3D017298B9FE75F3290F5BC5BAE	None	1
84.110.38.146	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
46.19.86.86	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/newpassword/firstlogin	Block	1
185.3.146.95	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
84.110.38.146	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddStudyEmploymentPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
62.0.113.48	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1

11-19-2015 to 11-20-2015