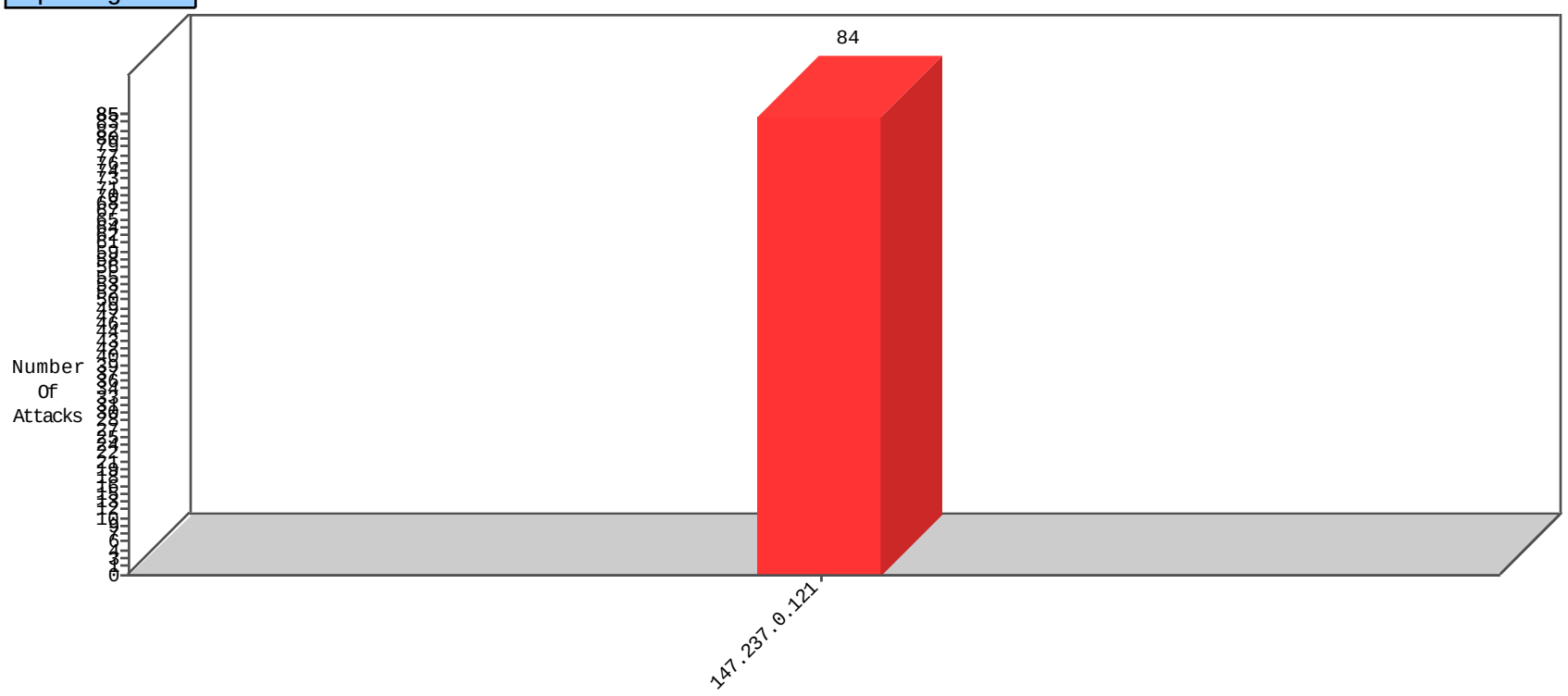
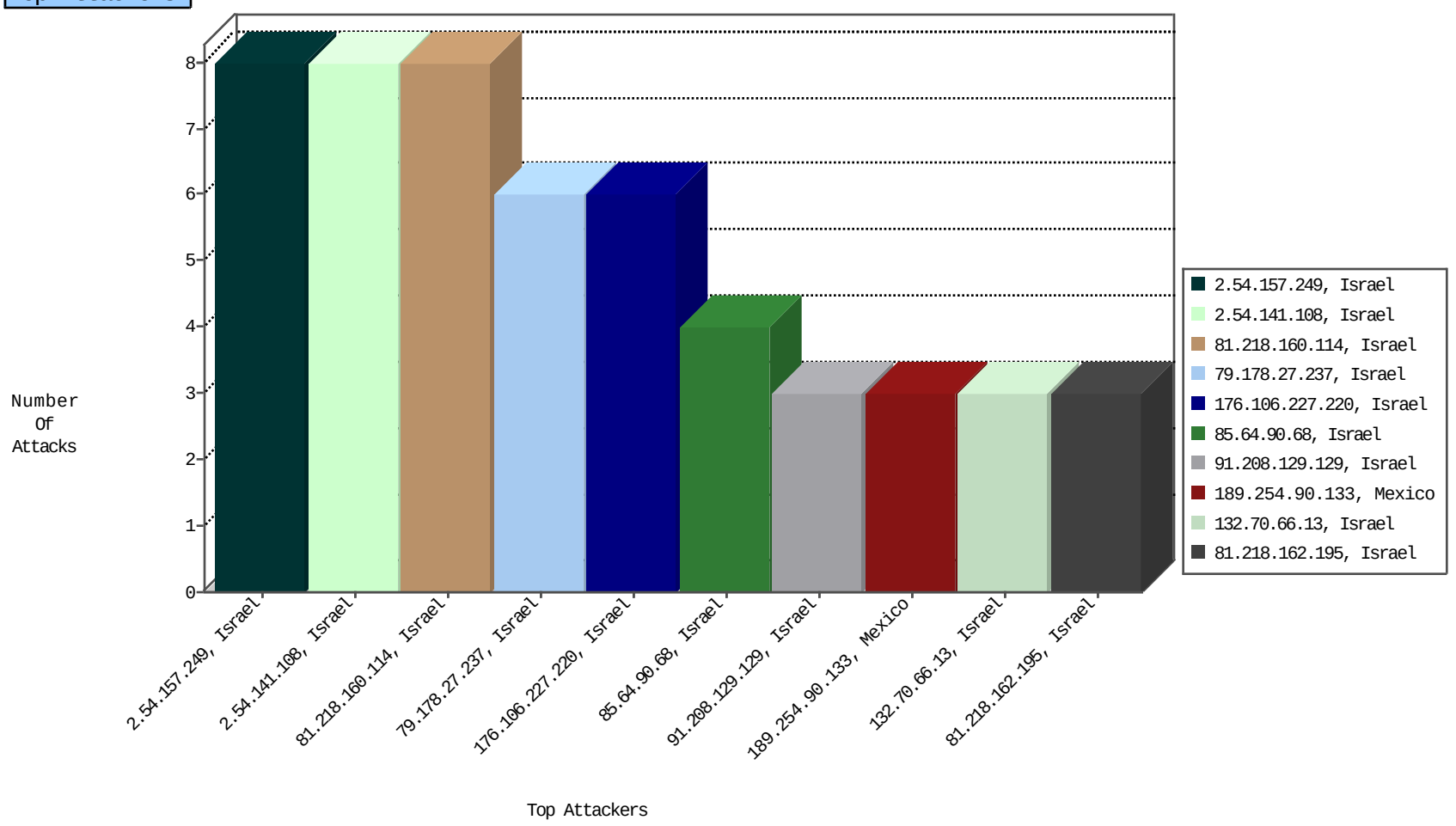
11-25-2015 to 11-26-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



11-25-2015 to 11-26-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
2.54.157.249	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	8
81.218.160.114	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	8
2.54.141.108	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	8
91.208.129.129	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3

11-25-2015 to 11-26-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

11-25-2015 to 11-26-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
183.60.48.25	China	147.237.0.121		ET SCAN Potential SSH Scan	1
189.254.90.133	Mexico	147.237.0.121		ET SCAN NMAP -sS window 2048	1
192.198.151.44	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	1
216.251.24.119	United States	147.237.0.121		ET SCAN NMAP -sS window 2048	1
61.216.2.14	Taiwan	147.237.0.121		ET SCAN NMAP -sS window 1024	1
89.248.174.55	Netherlands	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1
120.55.125.210	China	147.237.0.121		ET SCAN Potential SSH Scan	1
189.254.90.133	Mexico	147.237.0.121		ET SCAN NMAP -f -sS	1
189.254.90.133	Mexico	147.237.0.121		ET SCAN NMAP -sS window 3072	1
216.251.24.119	United States	147.237.0.121		ET SCAN NMAP -f -sS	1
59.45.79.117	China	147.237.0.121		ET SCAN Potential SSH Scan	1
89.248.168.43	Netherlands	147.237.0.121		ET SCAN Potential SSH Scan	1
109.74.226.90	Iran, Islamic Republic of	147.237.0.121		ET SCAN Potential SSH Scan	1

11-25-2015 to 11-26-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.146	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2199
66.249.93.154	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2033
66.249.93.150	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1874
149.78.22.6	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	724
149.78.232.189	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	409
66.249.93.154	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	230
66.249.93.150	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	218
149.78.229.75	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	216
66.249.93.146	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	199
149.78.38.110	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	192
84.253.149.130	Italy	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	184
149.78.136.183	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	183
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	175
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	160
54.243.190.43	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	142
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	140
149.78.22.135	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	130
194.42.67.50	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	116
66.249.81.130	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	109
66.249.81.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	94
188.119.192.14	Spain	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	93
149.88.52.42	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	83
192.114.91.248	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	64
2.54.157.249	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	58
149.88.88.139	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	49
149.88.21.1	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	49
149.78.251.98	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
66.249.66.107	United States	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
66.249.93.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	42
149.78.27.42	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	41
66.249.93.247	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	40
66.249.81.251	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
66.102.9.50	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
149.88.89.180	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	38
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
149.88.81.41	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	36
81.218.160.114	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
2.54.141.108	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
176.13.12.110	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	36
66.249.81.130	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	35
37.142.111.221	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	34
66.249.93.251	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	34
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	33
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	33
66.249.81.254	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	33
84.253.149.138	Italy	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	32
66.102.9.39	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	32
37.142.111.221	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	alert	31

11-25-2015 to 11-26-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
79.178.27.237	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/ufi/reaction/	Block	6
176.106.227.220	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	6
85.64.90.68	Israel	147.237.0.121		Multiple Unauthorized URL Access from 85.64.90.68	Block	4
81.218.162.195	Israel	147.237.0.121		Unknown Parameter ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/smsverify	Block	3
2.54.24.93	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 97BE7DD38373F710D008619B78CA8D51A5AA56B34EDF24BCC8C5154D022D6B1B4F8A354E2A41F1C4983F4B53C72F58217B81A46E19E354DBC36F4ADF82F5A5CF3CE349B1687D455C21BA4A951AF160CD666F48988A1B84ACC3D12C1D7ABA64F2FF5259A32603D5D88A1586C97406E75C0CA577E6322A79446390649027167D3E, Observed 452B3C7EB0DF8727EF2C446C0685B82F7514777A7A959607A67519DEA35DE996DE29030A8A9F230F9633F16F38E5FFE10DD4C5D4AE7DEB0C3F7FF71BA73F082FB1D746128E8B88E6897D1CAF4424AA65E4B8DA6487B58BDC487DD2BE329480BF58D4AF	None	2
132.70.66.13	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesIDs in www.miluim-ishi.aka.idf.il/changeunit	Block	2
176.13.20.106	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
82.80.203.20	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
212.117.143.27	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
109.64.217.212	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/ufi/reaction/	Block	1
81.218.101.2	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/newpassword/forgotpassword	Block	1
31.154.92.154	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddIDCardDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
84.108.224.237	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 84.108.224.237 (Unknown SSL Session)	None	1
79.180.31.246	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
5.22.134.133	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddIDCardDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
37.26.146.203	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	1
185.46.212.69	Switzerland	147.237.0.121		Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login	Block	1
84.108.224.237	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
80.246.138.96	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesIDs in www.miluim-ishi.aka.idf.il/changeunit	Block	1
5.22.134.133	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
132.70.66.13	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
82.80.19.204	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 098AEB6024584318E828FA2E50121B85EFD112812D17B17F9001A9ADF954EC9237551E6C017B76461A580FB0549962BBA23A14BB7FB1F84F33E7ECE71C8640FDE64099943547674262329 0C14E8A35209427BD02AD161013AE285CF48E3F9424BE9318C53C76384026814C07FFF8A12A9B2CB456EE5B6D2B916F4BEE45B57036, Observed 5662110547A529504CF01D910B1E80EBB8CC1E3FCAAC68AEF2DD5543283C9B48B07ABF06F9241BB0F49202E91745D4403D329A1F45B74DEDCAC193042676B3D5A8C306C8BE22148FEFC12B2B2210A58CCF8DFFD41E919B98E03AF26A088100B04E7133	None	1
46.19.86.123	Israel	147.237.0.121		Double URL Encoding - parameter: ReturnUrl in www.miluim-ishi.aka.idf.il/login	Block	1
2.52.16.192	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
212.25.107.145	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
81.218.101.2	Israel	147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	1
31.154.5.181	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1

11-25-2015 to 11-26-2015