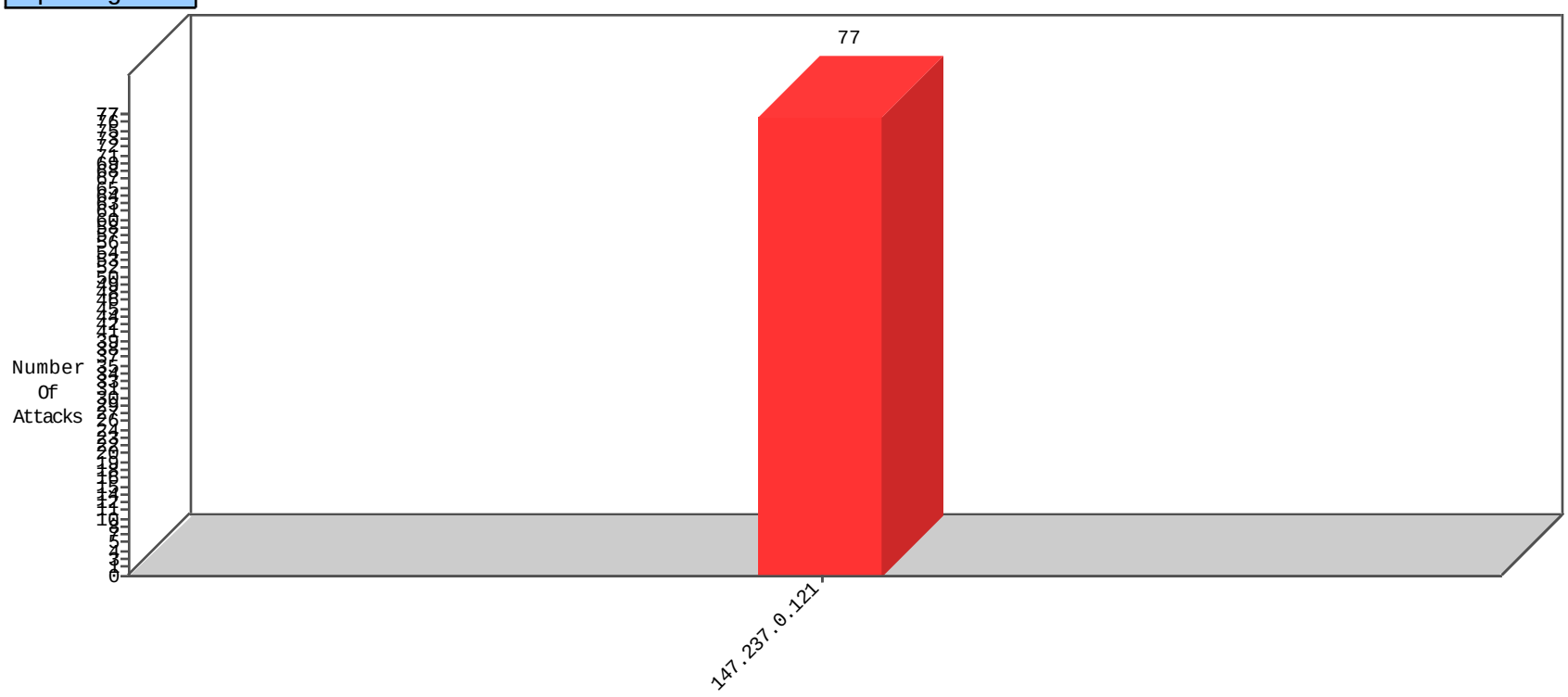
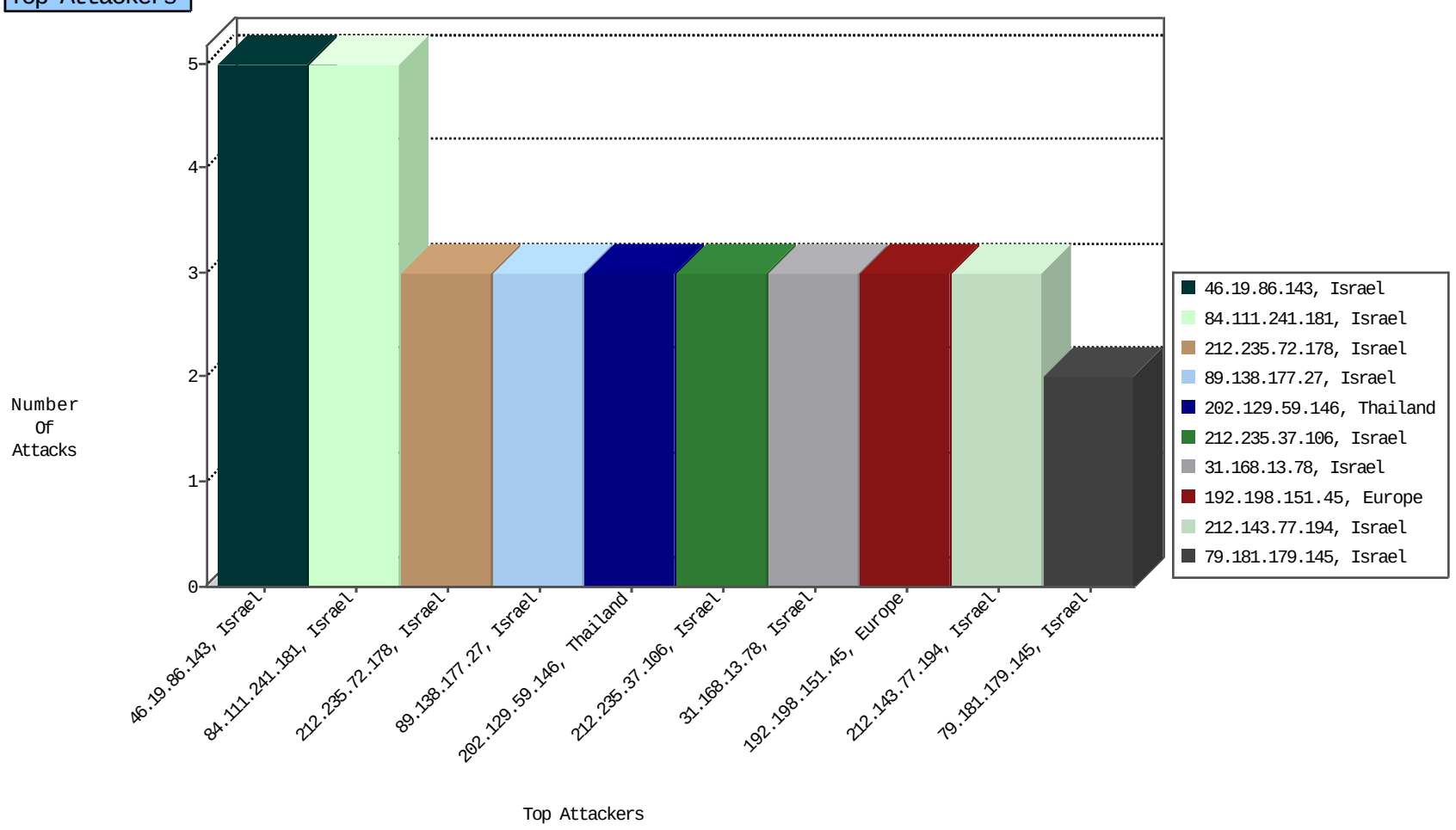
11-29-2015 to 11-30-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



11-29-2015 to 11-30-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
46.19.86.143	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	5
82.80.217.70	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	2

11-29-2015 to 11-30-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

11-29-2015 to 11-30-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
192.198.151.45	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	3
192.198.151.44	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	2
202.129.59.146	Thailand	147.237.0.121		ET SCAN NMAP -f -sS	1
202.129.59.146	Thailand	147.237.0.121		ET SCAN NMAP -sS window 3072	1
179.234.164.182	Brazil	147.237.0.121		ET SCAN Potential SSH Scan	1
202.129.59.146	Thailand	147.237.0.121		ET SCAN NMAP -sS window 2048	1

11-29-2015 to 11-30-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.145	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	3705
66.249.93.153	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	3552
66.249.93.149	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	3550
64.79.85.205	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	518
134.191.232.69	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	512
84.228.176.247	Israel	147.237.0.121		drop	SAM rule	drop	471
66.249.93.149	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	316
66.249.93.153	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	309
66.249.93.145	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	298
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	257
199.207.253.101	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	197
149.88.20.28	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	173
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	165
138.134.192.10	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	141
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	121
106.120.72.69	China	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	108
193.222.161.6	Switzerland	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	89
62.90.70.70	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	85
49.231.254.116	Thailand	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	81
66.249.81.251	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	78
176.13.7.217	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	65
192.127.94.7	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	64
66.249.81.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	58
46.19.85.181	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
66.102.6.153	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	52
66.249.82.147	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	52
212.179.44.27	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	50
149.88.29.145	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	48
15.203.178.34	France	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	48
149.78.51.107	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	48
149.88.13.170	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	48
66.249.81.129	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	46
138.134.102.16	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	46
149.78.39.38	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
134.191.232.68	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	42
2.123.248.131	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
149.88.4.162	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	38
149.88.76.32	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	38
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	38
66.249.81.251	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
66.249.66.109	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	36
212.179.23.10	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	36
66.102.9.22	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	32
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	31
149.78.27.42	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	30
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	29
132.64.24.42	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	29
5.102.254.127	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	28

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
84.111.241.181	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/ufi/reaction/	Block	5
212.143.77.194	Israel	147.237.0.121		Multiple Unauthorized URL Access from 212.143.77.194	Block	3
212.235.37.106	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass2 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	3
79.181.179.145	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/usercontrols/header/	Block	2
89.138.177.27	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	2
212.235.72.178	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPass in www.miluim-ishi.aka.idf.il/login	Block	2
176.13.14.237	Israel	147.237.0.121		Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login	Block	1
89.138.177.27	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 874D418E6367FBAABA738842EC9148384A69D6C873D504208475E14FEAF739A2235C77493C5553139DE0685F9BF6DB8D7F1940BF38E6C0C1237F3EFD67103B5983CBAC9934AD1F0948FC44060866AE8356980B8EB26FA162C1861707BD9C297348259790C18F42FFF8EC995FA4E3ACD878C91350461B0CBEC3DB4E2719E63BE0, Observed CFC6D26E79CBC129FFDC82FC43FEFF69B3899FBA0760FB2C8A71F0B77F8D3C92BC301EF76F86F6FBC6B66479F9ED877BAAA06B264D56EA58BDDFBE6D314F5FC79F1C01B9866BF4E13A04C4499868E0C8AFC3209C653B57E2866AC9487FBA56A659995F	None	1
2.52.186.39	Israel	147.237.0.121		Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login	Block	1
109.186.167.8	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
84.228.60.193	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
62.219.54.250	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
213.57.148.114	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$Submit1 in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
192.115.190.190	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
80.178.206.81	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
31.168.11.194	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/login	Block	1
132.73.200.84	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
84.228.176.247	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddIDCardDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
79.179.217.48	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected CBB0F940FD94788E3DDF9E964B349A75254691A94A3DB8F3AB8C91A94FA3EE5E50813E9F166BAF24D6454A4DD59D86DF96595C29A00D367CE05448A026873B3078C6BE69C8B1B10E77C23F313880D8D683C8EC9E974F2200E32EBA85AE26A0374D52F06E9790A55F0090865DD978C7654C31D42B7753253B589DC78E65EDF92F, Observed 67B5D21CB4F22719ACF9879955394017D66434648C3995190DD9C8A74BE48596AB0A4803FA632EF5F36B83AED5214205CB3DEB84FD8C80711C7DE1F9117D3202C807C2589500D010FEA828DD0D1857C648C9F3EF59451F46DC649AC6F0B69D811F37F6	None	1
192.116.190.250	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/l	Block	1
109.64.101.6	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected , Observed EA6BD58435FC3A478E0DE60F1D45D1978048D9E2A72D9997E1A5B3BB2EF10936361EE59F166CD2D18E0AD78967D4622BC96220186E23F89E5270617A05121B49A0BD74BBA0C280A397677E32E4409730FA6BCBDA8A92D7A5EED8F949A211C89F3D72E33E237EA492754218B81D79A27ECC55652AC1A20A87050680B392BC81718C0E186D42EE7FBB7F74E5FF7938B32CA571B4AD481760C46C3265673B802E01	None	1
80.246.136.63	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
46.117.184.147	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
212.235.72.178	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 940D6929B52770A9FBA844770CEB1834B15C20CC9BE00E325E888ECF8E953BC00F34EBFBA0D133C13D55ACC6FD5C1E5F143EE2ED877212EEC4ED9A7FE7B2244295D0E3C55C7CCAADD74E9817F12F74A7911A0B5A2AA606F71BD5311A09F4E76AFBCE405C7164AD43D9CDB5F13C68966C48E29F02E0C8FE9E81A320E0C76DC504, Observed 1684C84A11968A2ED4CFBE44C6C8C3E8BEAD61FF1627F7D4B6233D38E2E67F87959CBB07064F346E4C4C2441E936B394226B30FB37482025F3BE654FA35E9DD0EAC93241C276EA8DFA055BA3241065AF8C5E04D2F30C4D7D1B1B5A2A354EA2564E4302	None	1
176.13.3.100	Israel	147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	1
84.228.176.247	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
79.181.55.156	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
2.52.186.39	Israel	147.237.0.121		Unknown Parameter ch in www.miluim-ishi.aka.idf.il/login	Block	1
199.203.94.202	Israel	147.237.0.121		Distributed Unknown Parameter on www.miluim-ishi.aka.idf.il/login parameter prm	Block	1
109.64.169.164	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
46.121.113.242	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1

11-29-2015 to 11-30-2015