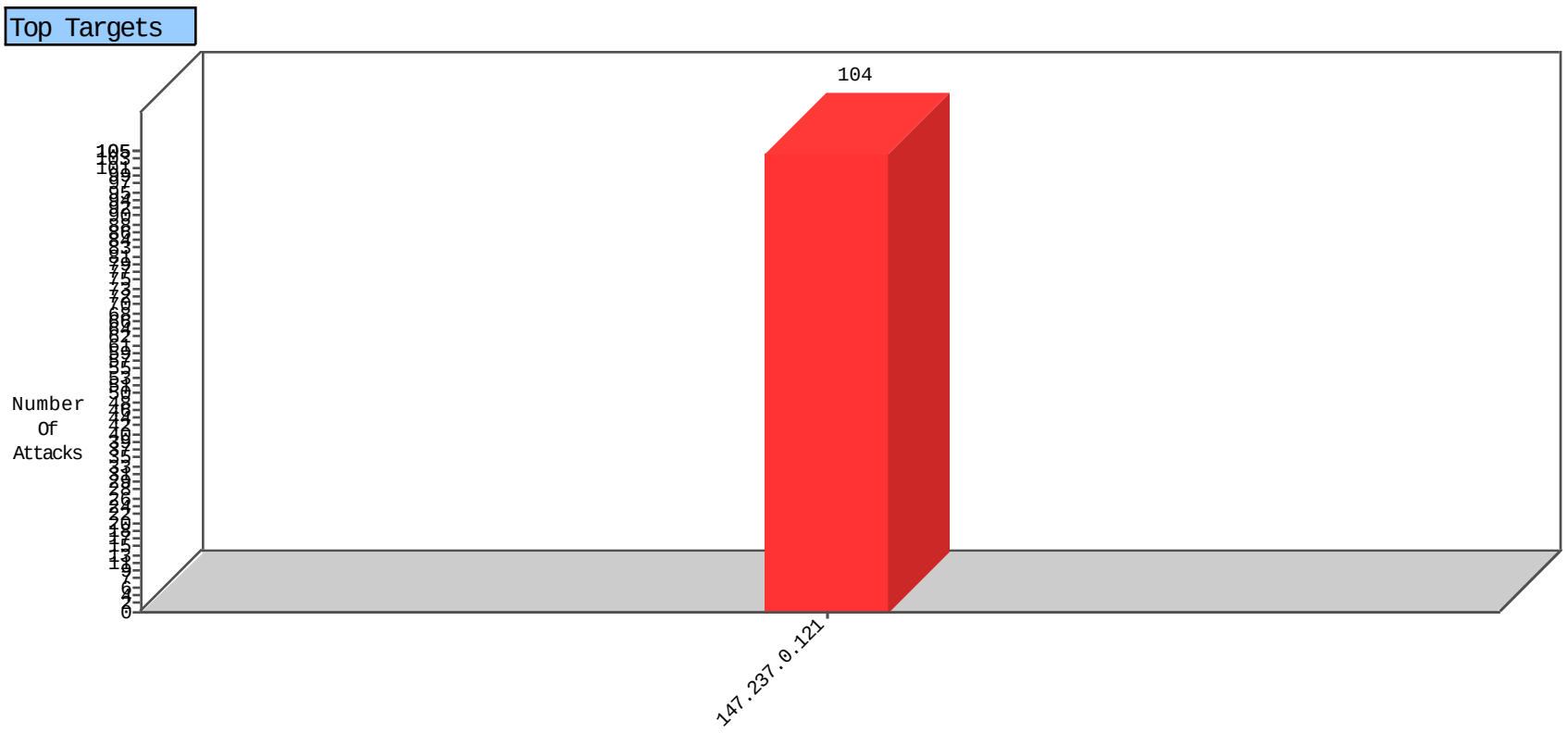
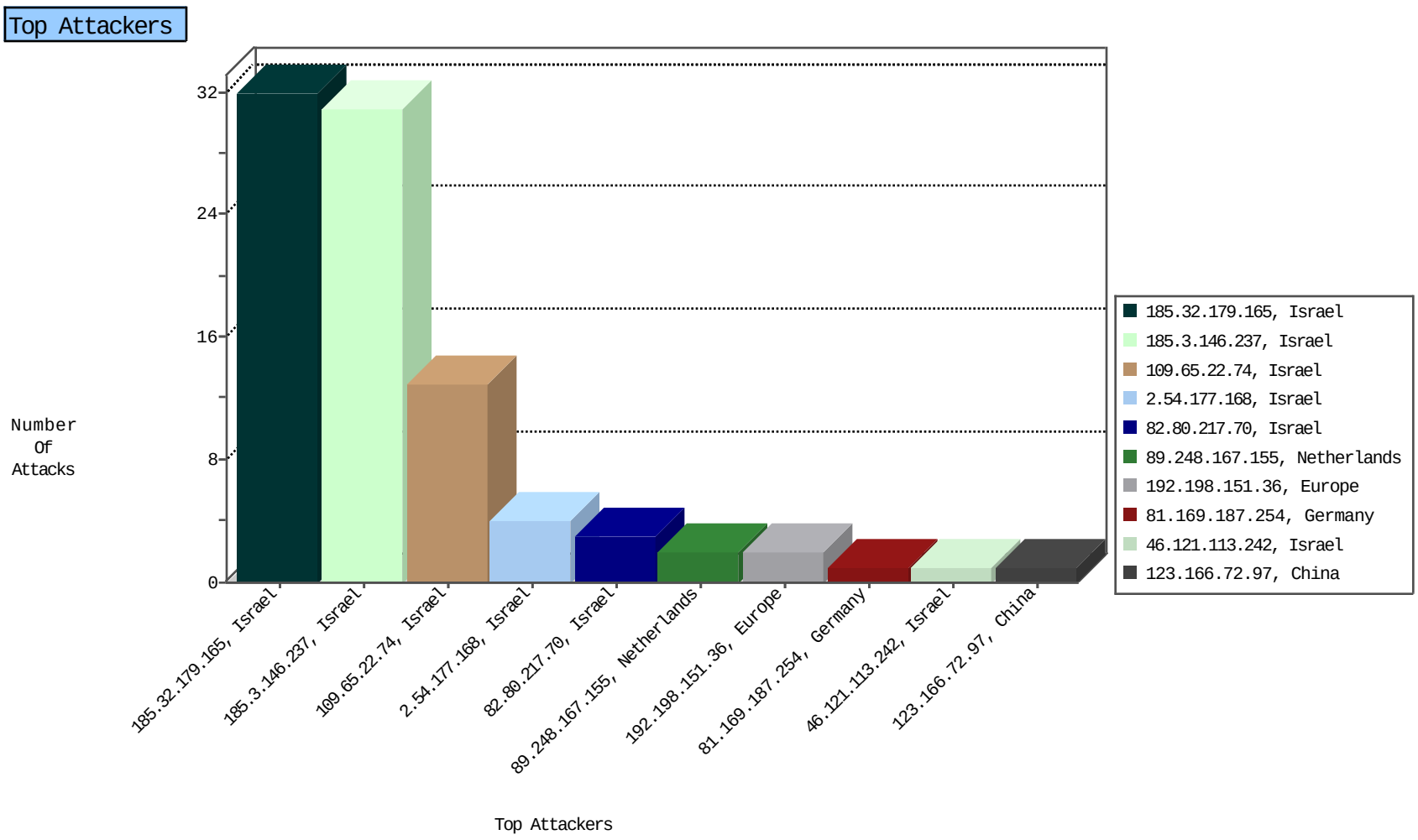
11-16-2015 to 11-17-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



11-16-2015 to 11-17-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
185.32.179.165	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	32
185.3.146.237	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	31
82.80.217.70	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3
89.248.167.155	Netherlands	147.237.0.121		Frk_Under_Attack_Con_Tcp	drop	BBL-Frankfurt	2

11-16-2015 to 11-17-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

11-16-2015 to 11-17-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
192.198.151.36	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	2
45.32.24.122		147.237.0.121		ET SCAN Potential SSH Scan	1
123.166.72.97	China	147.237.0.121		ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
43.229.53.89	Japan	147.237.0.121		ET SCAN Potential SSH Scan	1
81.169.187.254	Germany	147.237.0.121		ET SCAN Potential SSH Scan	1
162.222.185.165	United States	147.237.0.121		ET SCAN Potential SSH Scan	1
218.108.132.58	China	147.237.0.121		ET SCAN NMAP -sS window 1024	1

11-16-2015 to 11-17-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.150	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	3971
66.249.93.146	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	3319
66.249.93.154	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	3179
149.78.28.62	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	452
149.78.253.215	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	386
68.180.229.110	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	378
66.249.93.146	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	357
66.249.93.150	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	325
66.249.93.154	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	304
143.112.144.129	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	288
46.19.85.55	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
149.78.238.95	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	207
149.78.34.111	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	207
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	149
62.219.169.218	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	144
2.54.9.184	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
208.87.233.201	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	127
17.78.71.209	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	126
66.102.7.186	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	118
165.225.72.71	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	116
192.127.94.7	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	113
149.78.221.136	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	101
68.180.228.168	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	96
2.54.161.76	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
64.20.10.221	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	85
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	77
46.19.85.157	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
199.203.223.3	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	72
132.66.40.81	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	72
199.203.223.3	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	72
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	71
193.104.77.4	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	65
37.26.147.134	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	65
62.219.169.218	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	64
89.138.14.251	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	64
149.88.23.98	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	63
212.199.244.112	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	62
37.26.147.134	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	62
149.78.218.9	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	62
66.102.7.179	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	61
149.88.192.21	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	54
176.12.148.162	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	54
190.192.16.26	Argentina	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	53
62.90.214.50	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	52
66.249.81.251	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	50
192.117.103.143	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	47
37.26.147.134	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	46
5.22.134.133	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	41
132.66.40.81	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	41
79.182.206.116	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	40

11-16-2015 to 11-17-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
109.65.22.74	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddDocs&FileToActivate in www.miluim-ishi.aka.idf.il/login	Block	5
109.65.22.74	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddDocs&FilesToCheck in www.miluim-ishi.aka.idf.il/login	Block	5
2.54.177.168	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/medicalcommitteerequest parameter ctl00$ContentPlaceHolder1$txtFilesNames	Block	4
109.65.22.74	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	3
62.90.45.22	Israel	147.237.0.121		Unknown Parameter ch in www.miluim-ishi.aka.idf.il/login	Block	1
2.54.179.159	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	1
147.236.238.55	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
62.128.45.222	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
37.26.148.245	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
185.120.126.60		147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
80.179.194.201	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	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
212.235.98.139	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 578CE58599E8750D35E33EF60BA903DDF3F800555B3F1035D1DA871A13ECE6D96191744AEE86C027283355888B98D18970A14A496B1EA2540696E47A7E1BACFB2310A4D37DB5D7CCA7DB52F9CC7233FF4A63119FE20B03217987D0172FDF1D437E745DF10273ED4139FE325178AB8A47F432D64F94D075449D1F2462ED01DEC5, Observed DC810A3B2493FB2C98ED9482013FD566EC07E9613B7A03A228283A9FA74E05866D5994DF04181E5DB179E7D0CB4FCD7262D3CD79974B34CB8242D46A756B7AFDCFD40704486BE5B44208590B52F7F879D409CD434C8BDFF12BDB50AF62E160F8F2C02F	None	1
80.246.136.49	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
132.70.66.10	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected , Observed 3415E10B04792092D385E195C08A379CEBB076AC1D530CCE04016816CFED26C32E85C0C67D45A085A79033138E5F64E7AAFE56781FE86EF4B83C3ADC57A12C217A0F8F3DDDE7AB9254CBE88E02405DF16EA458D03A9F17D92022D41F35EC9135AADCCE839641C64006315F4535568BD42E64118E778CECD913AC1DE106DB881080C7DED72CF30D95905B4AFC951145958580BCEA0A3AC9EC79B45614E13899F7	None	1

11-16-2015 to 11-17-2015