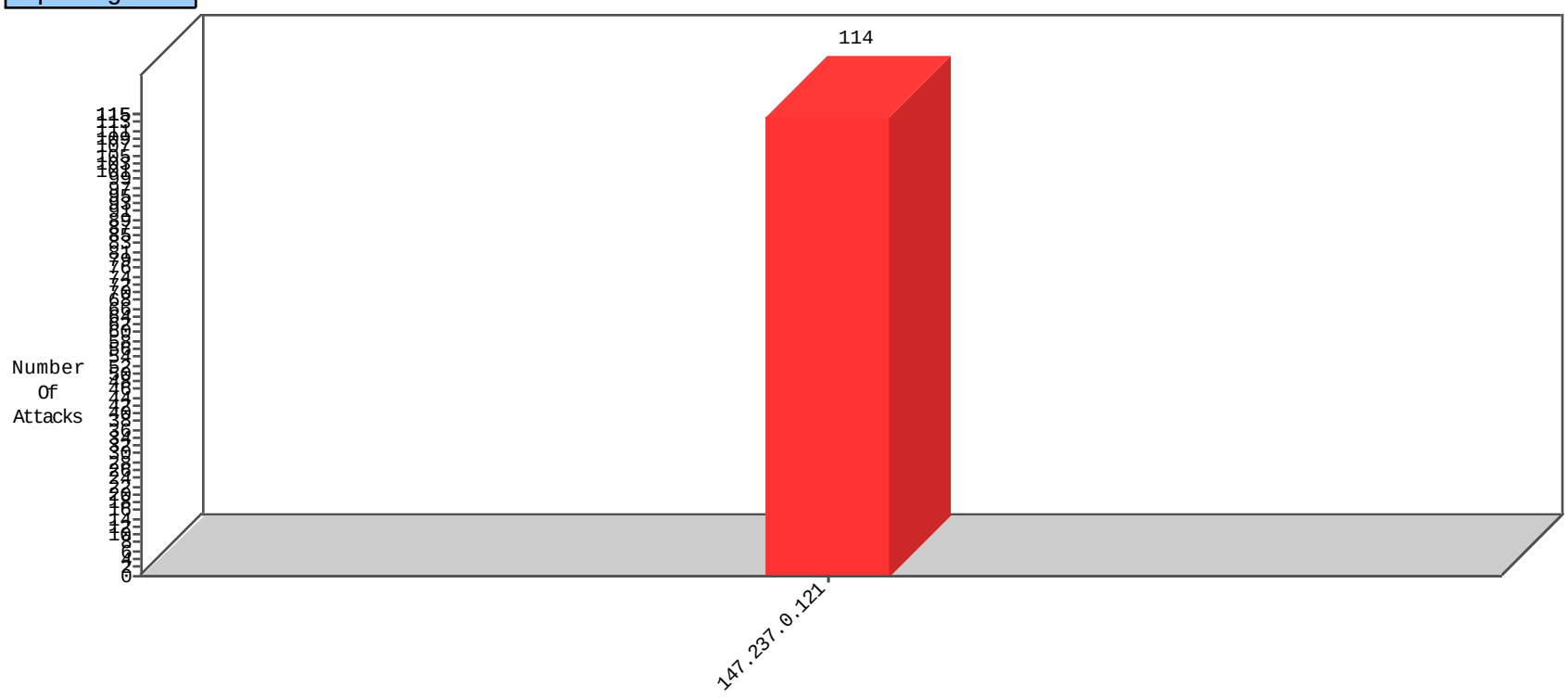
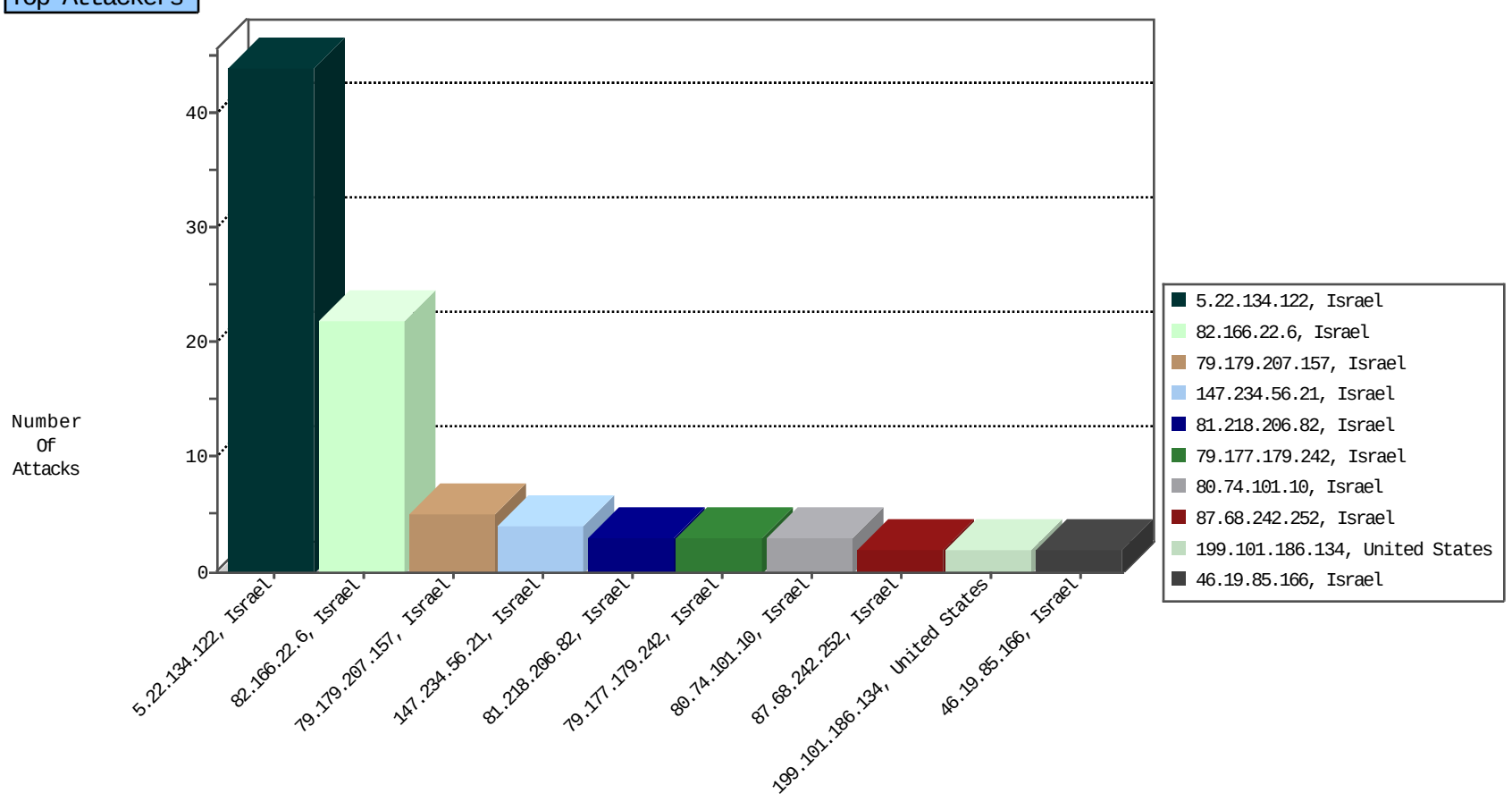
11-08-2015 to 11-09-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



11-08-2015 to 11-09-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
5.22.134.122	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	44
81.218.206.82	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3

11-08-2015 to 11-09-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

11-08-2015 to 11-09-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
104.128.144.131	Canada	147.237.0.121		ET SCAN NMAP -sS window 1024	1
179.217.102.253	Brazil	147.237.0.121		ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
199.101.186.134	United States	147.237.0.121		ET SCAN NMAP -sS window 1024	1
46.166.188.68	Netherlands	147.237.0.121		ET SCAN Potential SSH Scan	1
74.117.133.194	United States	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1
121.40.195.144	China	147.237.0.121		ET SCAN NMAP -sS window 1024	1
182.72.109.162	India	147.237.0.121		ET SCAN NMAP -sS window 1024	1
199.101.186.134	United States	147.237.0.121		ET SCAN NMAP -sS window 3072	1
31.6.71.154	Poland	147.237.0.121		ET SCAN NMAP -sS window 1024	1
61.182.170.38	China	147.237.0.121		ET SCAN Potential SSH Scan	1

11-08-2015 to 11-09-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2160
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2113
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1684
140.101.84.3	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1622
66.249.93.150	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1615
66.249.93.154	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1033
66.249.93.146	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1006
149.88.31.37	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	765
66.249.83.208	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	577
66.249.83.212	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	376
66.102.8.169	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	259
79.183.209.2	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	252
66.249.83.216	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	211
66.249.93.146	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	211
66.249.93.154	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	208
66.249.93.150	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	196
192.116.48.38	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
149.88.26.203	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	110
149.78.19.250	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	97
66.249.93.224	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	89
149.78.227.200	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	82
149.88.21.216	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	67
66.102.7.172	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	63
149.88.77.45	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	63
66.249.93.216	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	61
66.102.7.179	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	52
66.249.93.241	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	52
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	49
66.249.81.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	47
149.88.86.121	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
81.25.53.29	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	41
66.249.83.216	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
149.78.37.178	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	38
66.249.81.238	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	38
66.249.64.170	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	38
66.249.81.164	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
66.102.8.179	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
2.54.27.157	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
84.199.88.155	Belgium	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	36
66.249.83.212	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	34
66.249.93.247	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	33
66.249.93.166	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	32
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	31
64.79.89.130	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	30
190.104.21.197	Bolivia	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	30
17.78.97.150	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	29
66.249.93.244	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	29
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28
66.249.81.251	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28
173.245.115.76	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
82.166.22.6	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddStudyPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	11
82.166.22.6	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddTimetableDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	11
79.179.207.157	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$Submit1 in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	4
79.177.179.242	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/changeunit	Block	3
80.74.101.10	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	3
147.234.56.21	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	2
87.68.242.252	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	2
46.117.177.248	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
147.234.56.21	Israel	147.237.0.121		Multiple Illegal URL Path Encoding from 147.234.56.21	Block	1
83.130.101.29	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
79.178.183.65	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
46.19.85.166	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
212.199.121.196	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
109.67.43.246	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$ctl00$txtOldPass in www.miluim-ishi.aka.idf.il/personalsettings	Block	1
81.218.97.45	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
79.176.145.63	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
84.108.10.220	Israel	147.237.0.121		Unknown Parameter Returnurl / in www.miluim-ishi.aka.idf.il/login	Block	1
46.19.85.229	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected CB520DF1A5ECEA612218301A630091996A5228D1F9FAF02E8F01068412D4FF2703EF8493D30AB6B5FC16411AE2428950F8F94985C9BB379623F925A938D0D2FC7321E126087F4B28CDDD505B41636502F99AAB1D43BBBB5687AB1B9B9AB2B4D868B1B6239280EF6EFC49CCE9028DF52BC2E9CFF5BEFEB56B2819540605496C17, Observed 225A2B3BDED2E25815DCE2D05CD8883AB08E20A609873D2BEACCDEEAE171E20868F1489F653C83C7A7D871AF77B0A24195DE926E0486C8FE23A0F7B12DAF9758F9795FAA038673B600D2311056851F7F4A9E02046FE1AA840E12875C1913208E4BD570	None	1
213.151.32.163	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddIDCardDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
109.186.18.100	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
79.176.186.104	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	1
192.114.91.249	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/templates/personaldetails/	Block	1
85.64.167.54	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/1355-he/miluim.aspx	Block	1
79.179.207.157	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	1
46.117.62.166	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
147.234.56.21	Israel	147.237.0.121		Illegal URL Path Encoding www.miluim-ishi.aka.idf.il/%2	Block	1
46.19.85.166	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 46.19.85.166 (Open Mode)	None	1
212.25.74.27	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	1