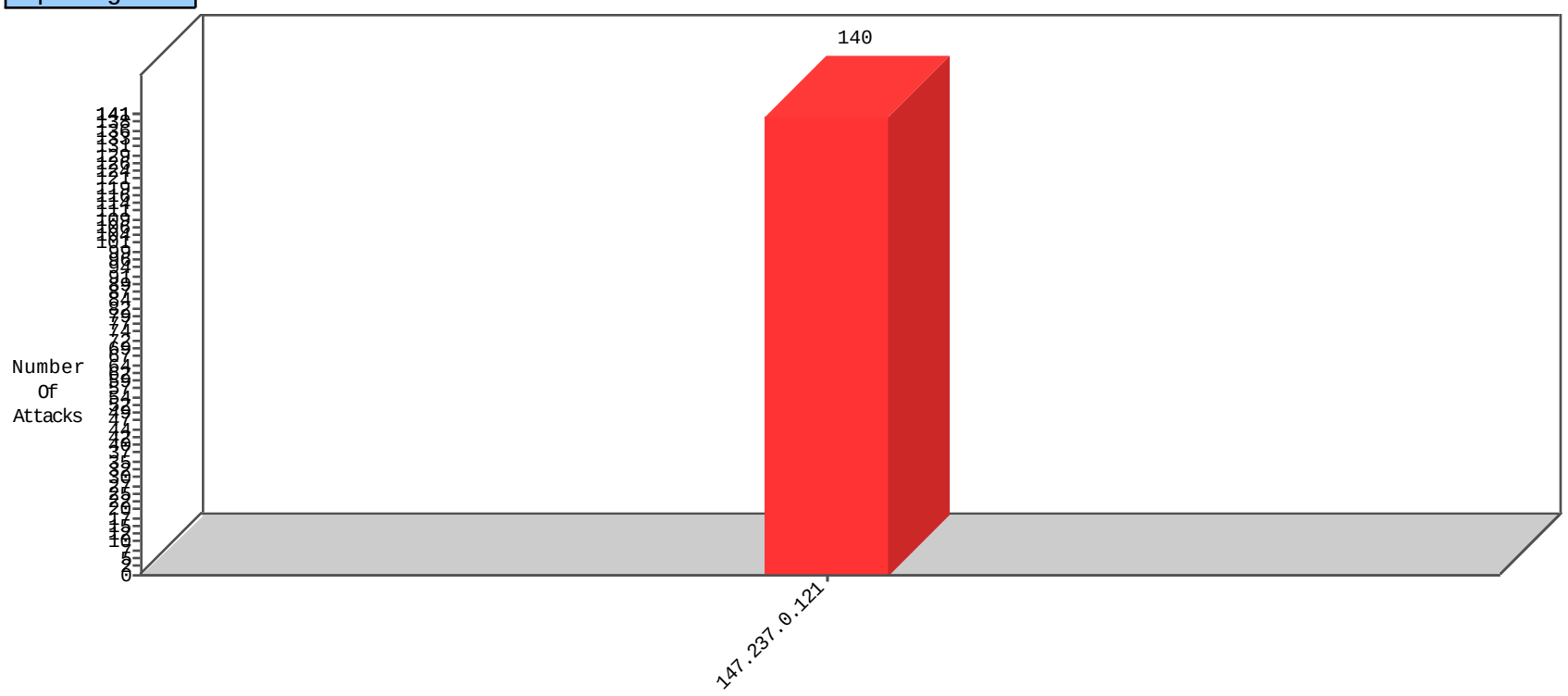
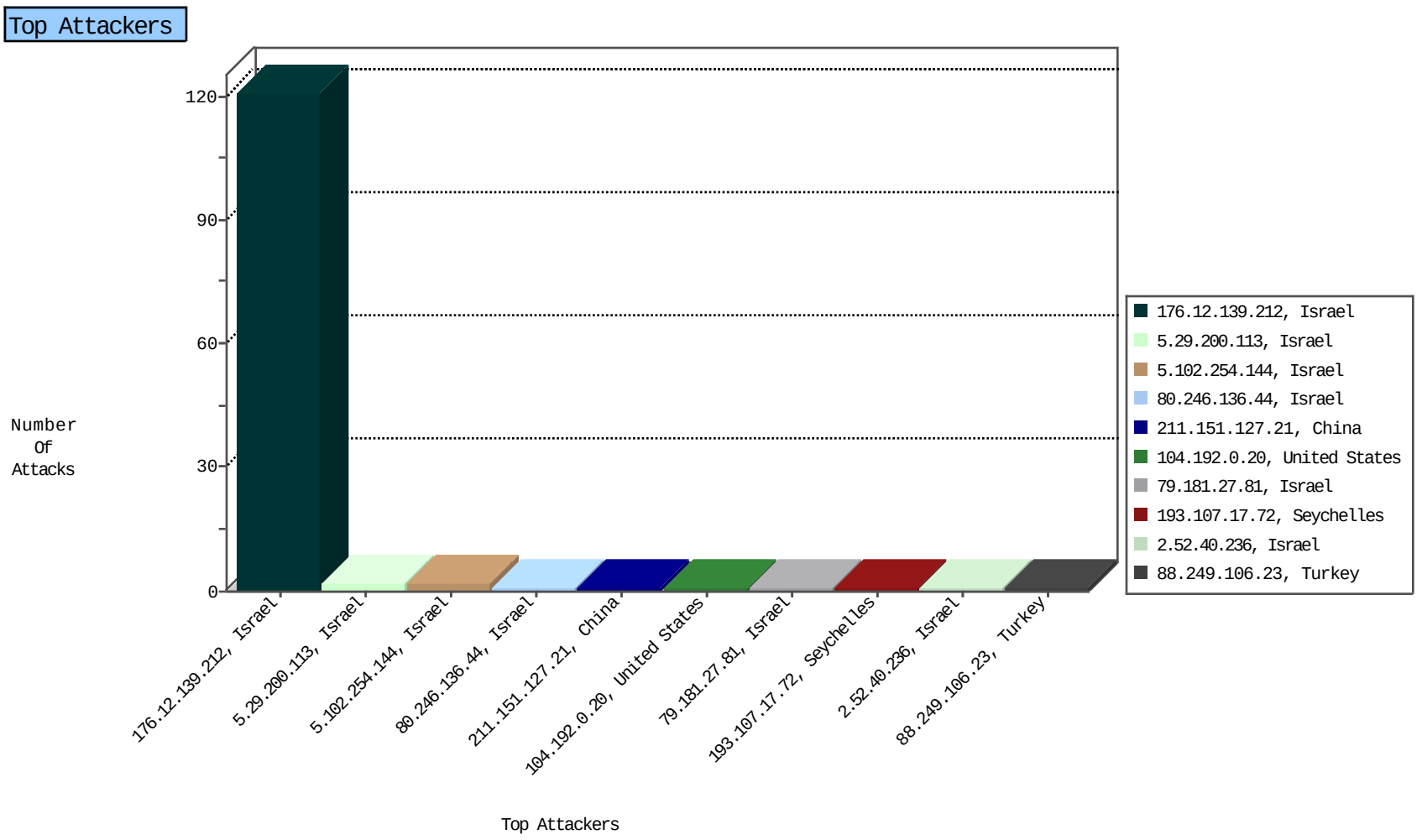
11-13-2015 to 11-14-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



11-13-2015 to 11-14-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
176.12.139.212	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	121

11-13-2015 to 11-14-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

11-13-2015 to 11-14-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
43.229.53.89	Japan	147.237.0.121		ET SCAN Potential SSH Scan	1
88.249.106.23	Turkey	147.237.0.121		ET SCAN NMAP -sS window 1024	1
117.31.224.80	China	147.237.0.121		ET SCAN Potential SSH Scan	1
193.107.17.72	Seychelles	147.237.0.121		ET SCAN NMAP -sS window 1024	1
222.186.34.242	China	147.237.0.121		ET SCAN Potential SSH Scan	1
59.148.238.158	Hong Kong	147.237.0.121		ET SCAN Potential SSH Scan	1
104.192.0.20	United States	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1
163.53.247.165	Macau	147.237.0.121		ET SCAN Potential SSH Scan	1
211.151.127.21	China	147.237.0.121		ET SCAN Potential SSH Scan	1

11-13-2015 to 11-14-2015

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	1696
66.249.93.150	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1335
66.249.93.154	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1204
149.78.27.42	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	521
46.19.85.34	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	242
46.19.85.34	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	240
149.88.202.196	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	225
2.54.139.144	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	225
46.19.85.34	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	159
66.249.93.154	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	156
79.180.22.41	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
82.166.22.25	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	134
66.249.93.150	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	128
66.249.93.146	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	125
149.88.31.37	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	113
149.88.176.226	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	108
149.78.20.93	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	90
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	76
84.111.113.15	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	64
176.13.11.36	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	64
149.78.238.169	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	60
66.102.7.186	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	59
66.249.65.190	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	57
149.78.53.155	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	48
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	47
149.78.227.41	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	46
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	46
81.200.15.10	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	42
109.67.8.47	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	40
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
81.218.146.181	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
176.12.140.137	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	36
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	36
176.12.140.137	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	36
176.13.1.247	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	36
176.13.12.82	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	29
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28
46.19.86.2	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	27
37.142.200.136	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	26
79.176.161.59	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	25
79.176.161.59	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	25
84.108.57.132	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	25
188.120.135.58	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	25
176.13.16.147	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	25
176.13.0.18	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	25
66.249.93.244	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
84.108.57.132	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	25
212.150.31.126	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	25
66.102.9.50	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	24

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
5.29.200.113	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	2
5.102.254.144	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	2
79.181.27.81	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
213.57.241.177	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/newpassword/forgotpassword	Block	1
2.52.40.236	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
80.246.136.44	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 9628273D1701CD8A933AEFD3B5DAB4837E41DFEBC09D87730BAC6D46BF7F19FA8621CB3C78B6485323E60228369A4411921C31F40A9C39E16EB4C51411643E68FF17F7C898139C06E3F9F3985DC2019B649CC73D590836670ABD140BC1562005785F05E189C4C4A0B13B64CC0CE3963A1282E29AD30DAE78C0D28283A3A58EFE, Observed 601A0317418626A131554BC8A32AF45C1FB4CCC4E1671209F2CB276F2D61FA334B2F20A870B975B9F25B6EBB1AF4DA1BC28CF586D1E023ED26A500235F741948405EABE22DEF387504EB4F9A83035B869D8B2BDF9EB3B790D75306800F89FF77A020BB	None	1
82.166.22.36	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
85.250.70.37	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1