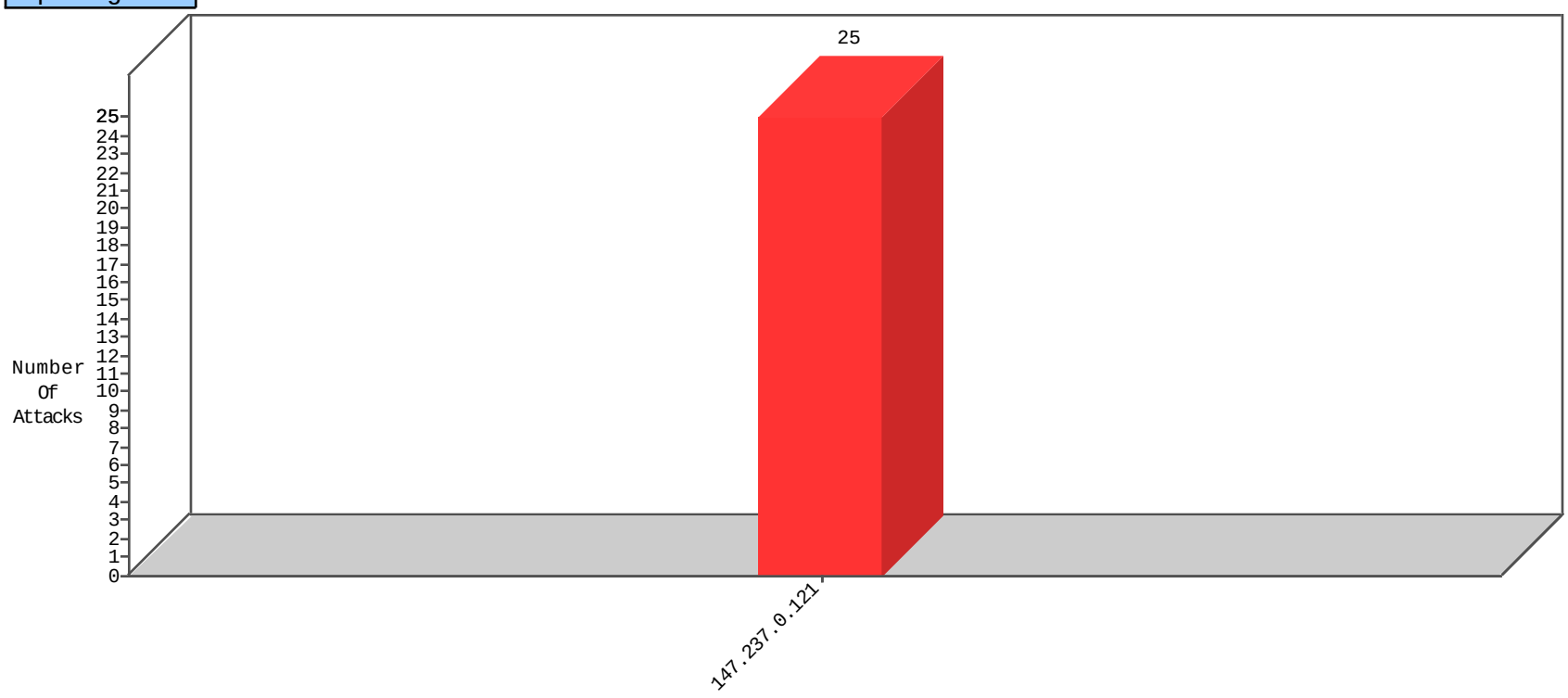
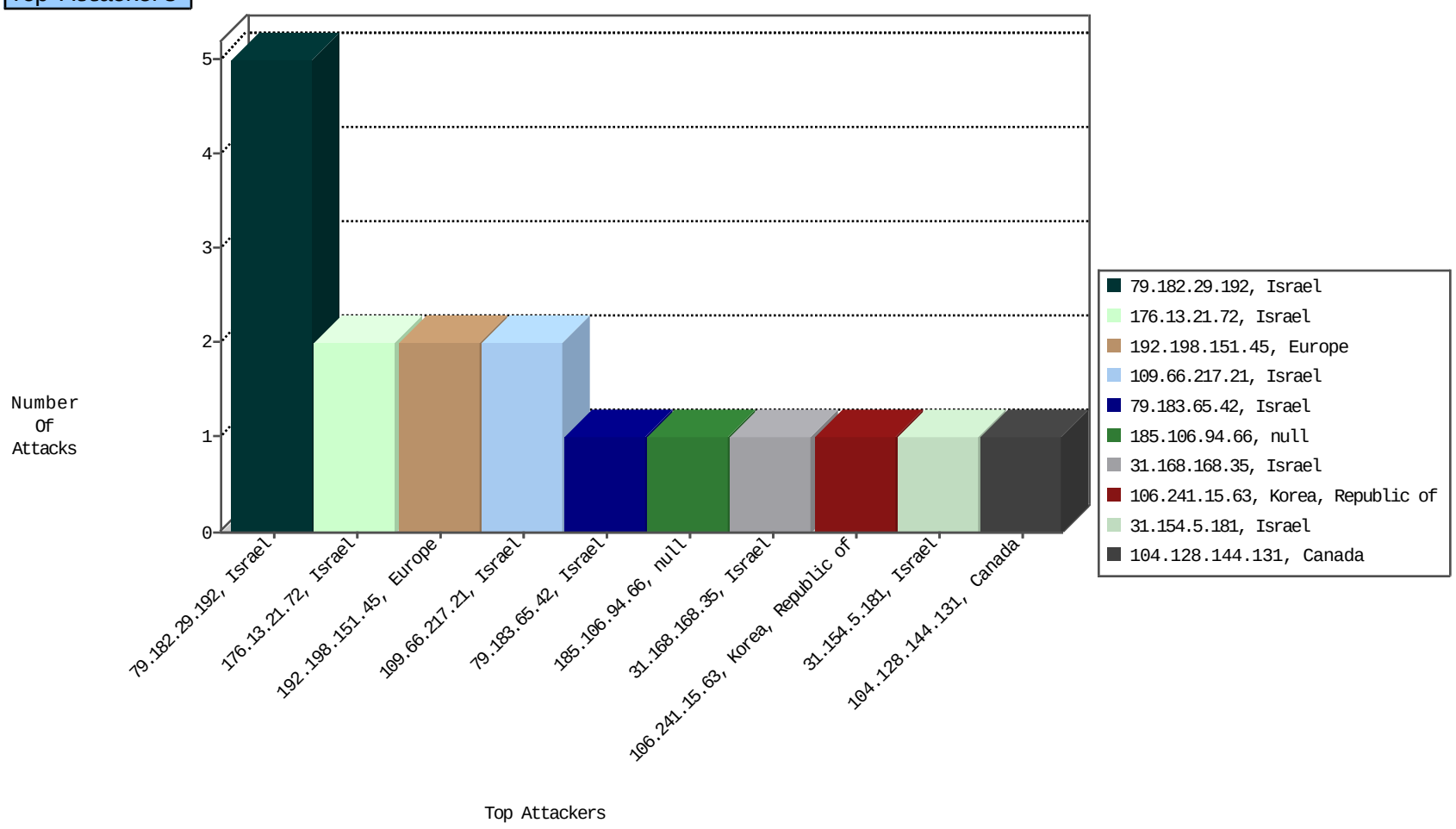
12-11-2015 to 12-12-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



12-11-2015 to 12-12-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
79.182.29.192	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	5

12-11-2015 to 12-12-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

12-11-2015 to 12-12-2015

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)	2
61.216.2.14	Taiwan	147.237.0.121		ET SCAN NMAP -sS window 1024	1
104.128.144.131	Canada	147.237.0.121		ET SCAN NMAP -sS window 1024	1
185.106.94.66		147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1
85.236.191.80	Russian Federation	147.237.0.121		ET SCAN Potential SSH Scan	1
106.241.15.63	Korea, Republic of	147.237.0.121		ET SCAN Potential SSH Scan	1
185.111.76.132		147.237.0.121		ET SCAN Potential SSH Scan	1

12-11-2015 to 12-12-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
149.78.134.165	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1751
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1210
66.249.93.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	896
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	776
217.149.140.193	Netherlands	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	680
66.249.93.93	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	326
157.55.39.61	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	281
149.78.81.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	278
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	166
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	157
2.52.21.215	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	126
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	121
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	116
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	93
2.54.22.217	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
89.139.179.241	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	82
89.139.179.241	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	81
94.44.254.68	Hungary	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	65
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	51
149.78.62.113	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	49
212.235.98.139	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	46
149.78.240.184	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	40
149.88.189.146	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
149.78.233.91	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	36
79.182.29.192	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
149.78.200.202	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	36
2.54.134.89	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
149.88.221.238	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	23
77.125.92.184	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	22
66.249.93.23	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
66.249.93.93	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	21
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
66.102.9.33	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	19
64.120.28.235	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
66.249.93.17	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
5.102.254.69	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	17
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	11
31.13.102.110	Ireland	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	10
52.90.119.174	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	10
66.249.93.51	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	9
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	9
66.249.66.109	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	9
66.249.66.105	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	9
66.249.81.129	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	9
149.88.86.126	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	8

12-11-2015 to 12-12-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
109.66.217.21	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	2
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
79.183.65.42	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
176.12.142.144	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
31.168.168.35	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
84.228.177.225	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.21.72	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 176.13.21.72 (sigalgs DoS Attack)	None	1
46.117.158.135	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
109.66.180.137	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected , Observed 5761578EEC0796723F22652D2E8684AF9810CD3F0FE2EA708CDEC5A9258C875410BE6750615047C95C7975F1621364427AC86A73B9B0A8B02DAFCDF0FB5E80372F674DB819B95FD1FEDFD441EA532D5058A0A3D3E353E15DC5512D9012B8A4B1F102A39871F41ABACB751814261B4033CF2363983DE488BA62B7169865EB31ED1DC6F01D10FFCB7C8FF22DEA1F1DC0F04D3A50E94FA0E17F9DB7BD351A196FE7	None	1
176.13.21.72	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
46.120.184.147	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1

12-11-2015 to 12-12-2015