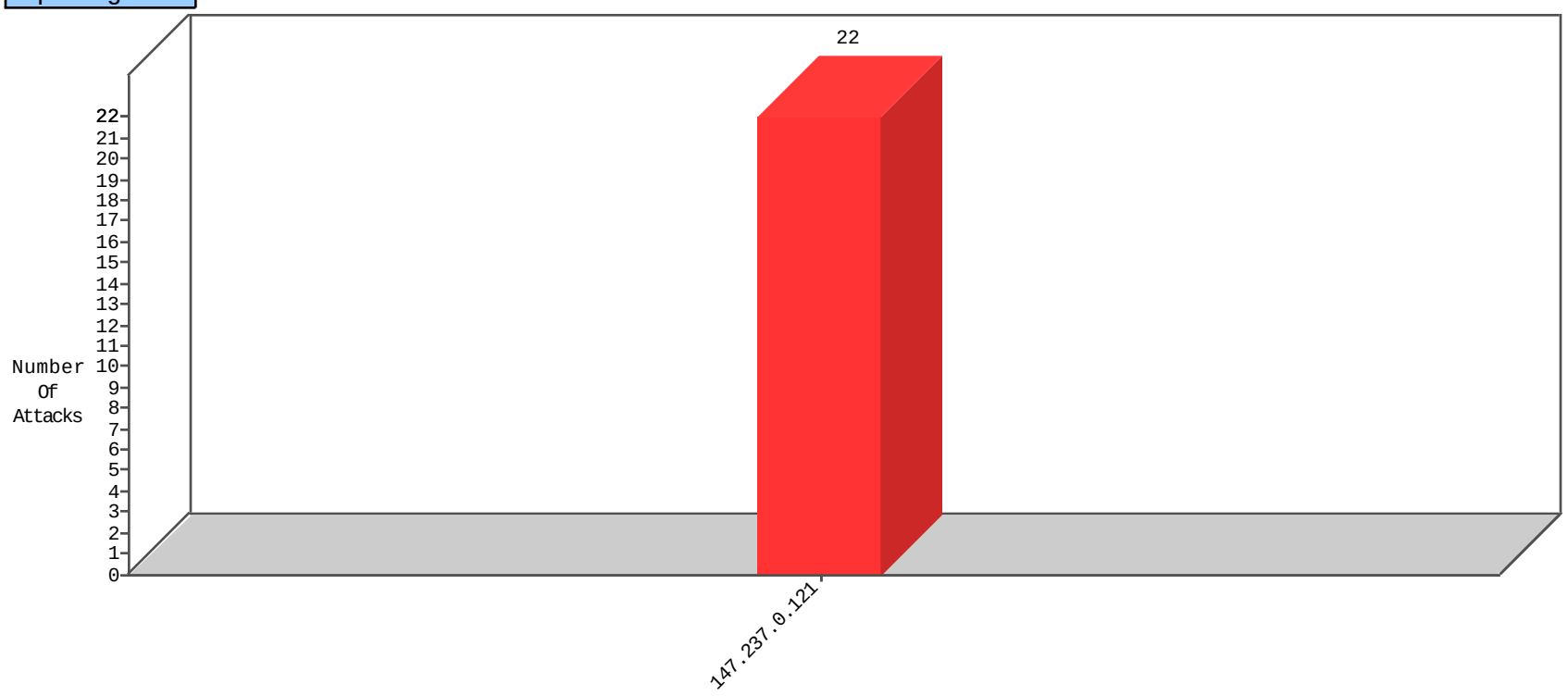
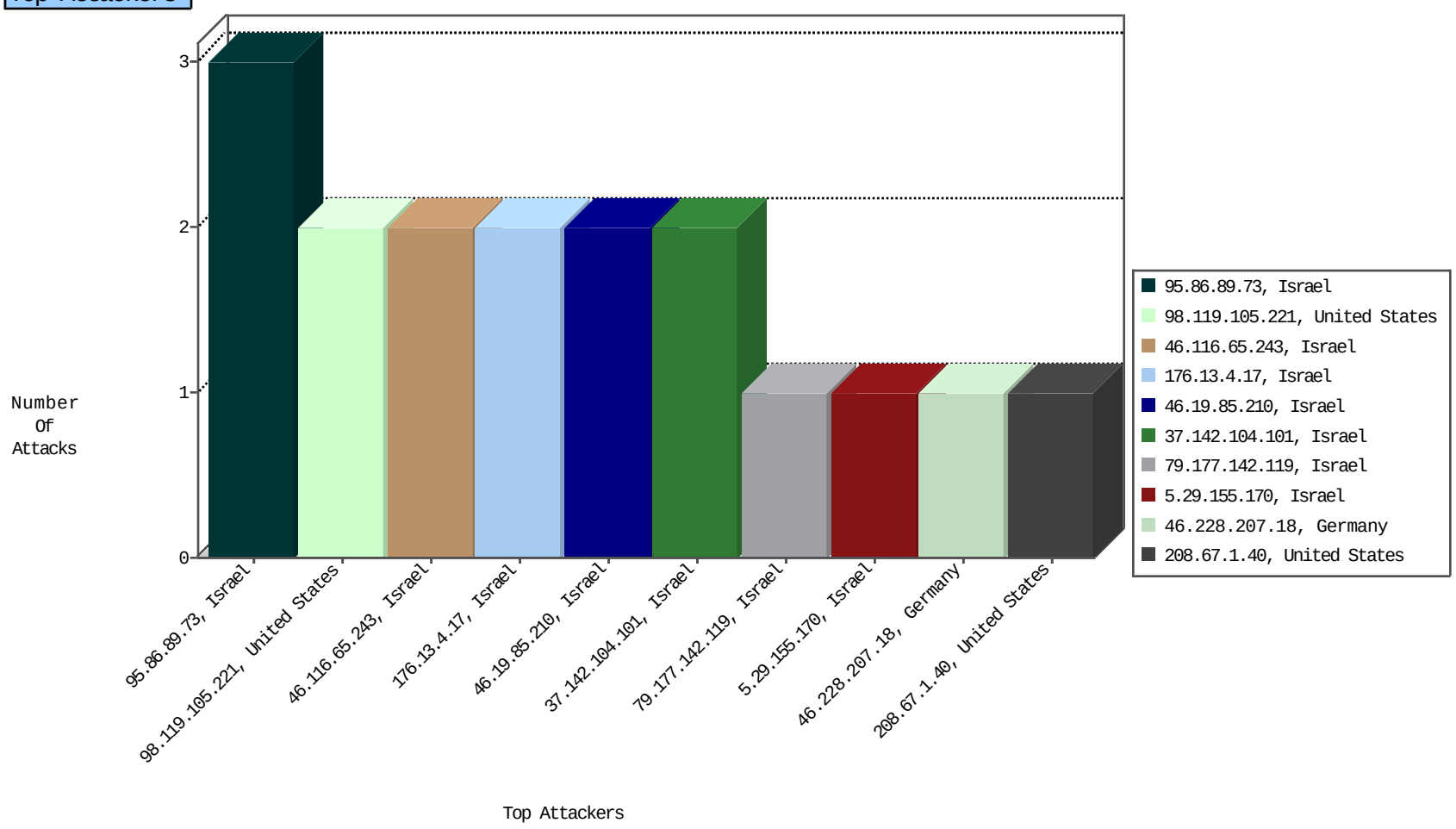
12-05-2015 to 12-06-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



12-05-2015 to 12-06-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count

12-05-2015 to 12-06-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

12-05-2015 to 12-06-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
46.228.207.18	Germany	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1
98.119.105.221	United States	147.237.0.121		ET SCAN NMAP -sS window 4096	1
120.26.205.111	China	147.237.0.121		ET SCAN Potential SSH Scan	1
98.119.105.221	United States	147.237.0.121		ET SCAN NMAP -sS window 3072	1
107.150.20.53	United States	147.237.0.121		ET SCAN Potential SSH Scan	1
208.67.1.40	United States	147.237.0.121		ET SCAN Potential SSH Scan	1

12-05-2015 to 12-06-2015

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	1438
66.249.93.153	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1087
66.249.93.149	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	988
149.88.59.58	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	552
115.84.97.149	Lao People's Democratic Republic	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	376
2.52.178.88	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
149.78.41.56	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	195
66.249.93.149	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	181
149.78.42.1	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	180
66.249.93.145	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	146
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	140
66.249.93.153	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	129
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	122
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	113
50.7.114.113	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	104
149.88.90.189	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	99
194.12.254.131	Bulgaria	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	94
149.78.254.244	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	90
31.168.246.161	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	68
149.78.238.120	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	55
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	55
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	53
149.88.86.121	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	41
149.88.89.180	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	41
217.69.133.253	Russian Federation	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
213.8.204.43	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	36
149.78.50.201	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	36
149.78.233.91	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	32
66.249.66.105	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	30
149.78.176.158	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
149.88.176.226	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
66.249.66.107	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
31.168.246.161	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	26
82.102.169.113	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	25
82.102.169.113	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	25
82.102.169.113	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	25
109.64.179.166	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	25
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	21
188.93.56.124	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	21
173.245.115.77	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	19
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	19
66.249.93.215	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
31.168.246.161	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	18
66.249.81.129	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
66.249.81.238	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
66.249.93.244	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
37.46.39.155	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	17
66.249.81.163	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17

12-05-2015 to 12-06-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
95.86.89.73	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	3
46.116.65.243	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	2
37.142.104.101	Israel	147.237.0.121		Suspicious Response Code	Block	2
79.179.4.70	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNimuk in www.miluim-ishi.aka.idf.il/valtamrequest	Block	1
2.54.143.209	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
176.13.4.17	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
46.19.85.210	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
87.68.56.24	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
5.29.155.170	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected , Observed 83B5A6F6E6C98FC85A69B81ED320051D3AAA5509AC104F2F651D67EDA0B2329686E0DF1AC67753FB2A47D269970A467AC0ADD6E6BD644393D458A8008BB0CA78752FEFAB9F869EE47D006ADB28B17F2243AC5467494541B9A5BEDFC32999B0D32302AAC7C77E50C485FB3637E48E1A8CE6D707EC2B244F6714065B36BC4BE8398DABACB2E2E568B6298FAEA67B7C6966A0A09B6AD16F47D1760E2621FA151B50	None	1
79.177.142.119	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
176.13.4.17	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 176.13.4.17 (sigalgs DoS Attack)	None	1
46.19.85.210	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 46.19.85.210 (sigalgs DoS Attack)	None	1

12-05-2015 to 12-06-2015