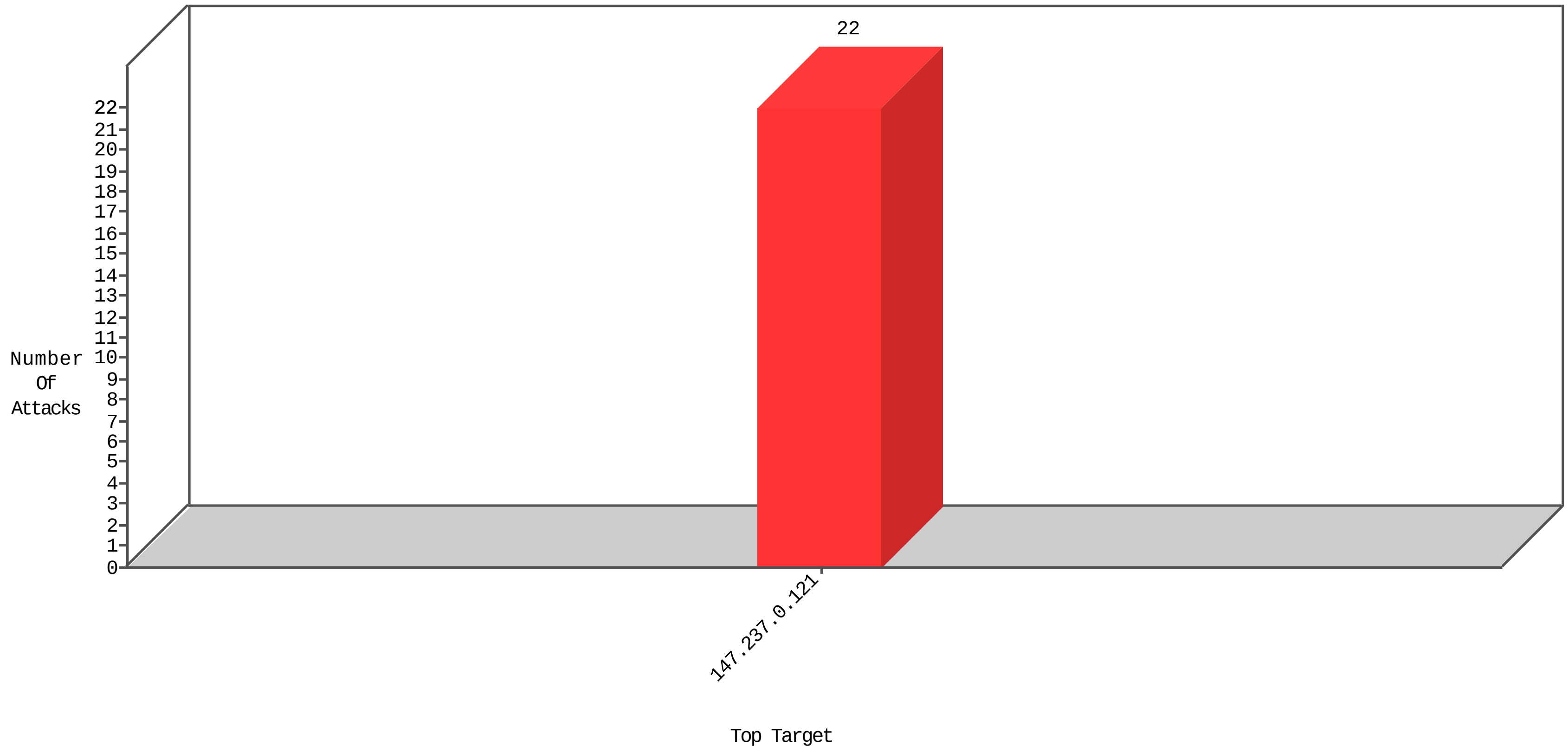
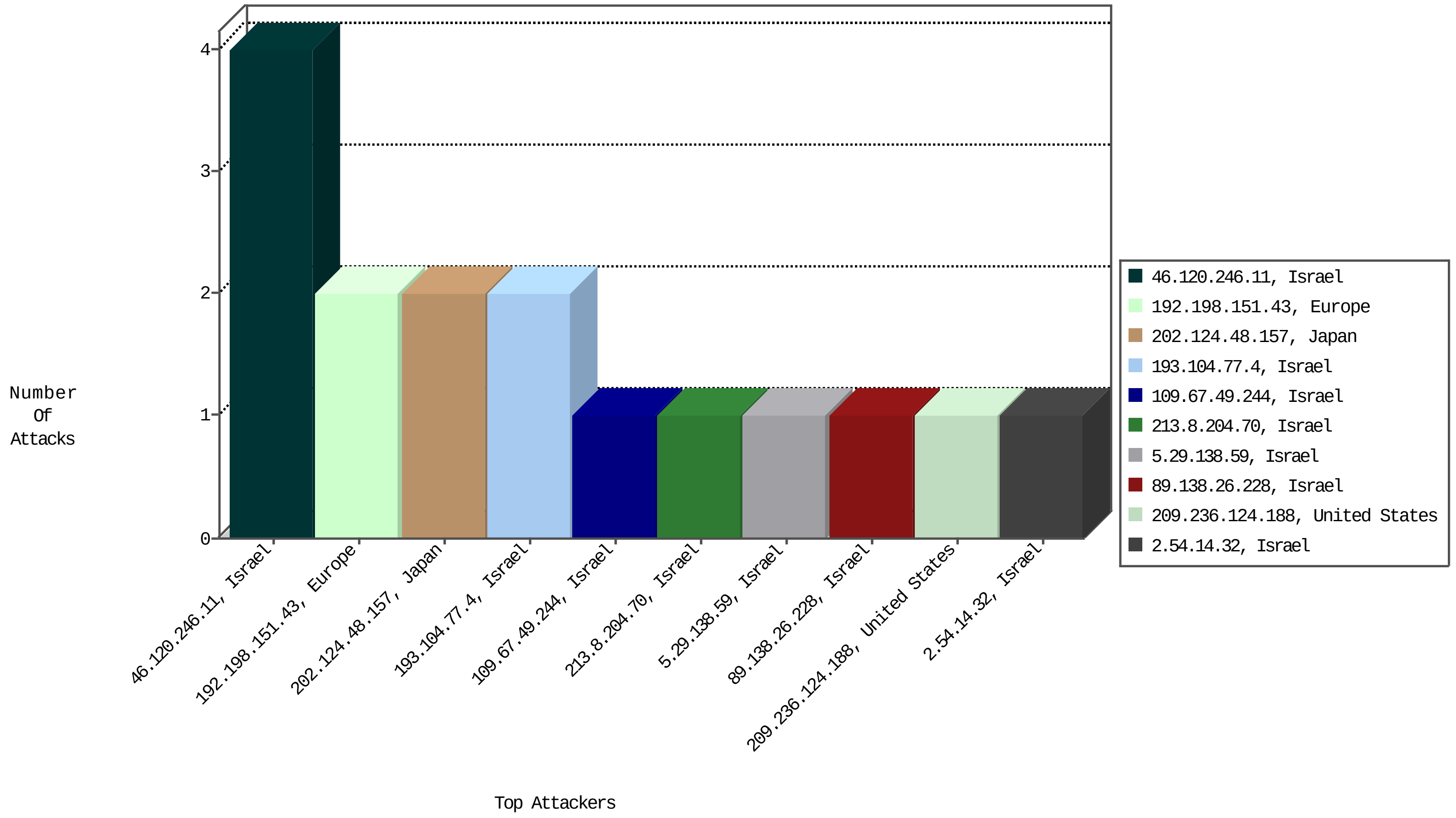
12-26-2015 to 12-27-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



12-26-2015 to 12-27-2015

Top Attackers In DDoS-Defence

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

12-26-2015 to 12-27-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

12-26-2015 to 12-27-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
59.45.79.117	China	147.237.0.121		ET SCAN Potential SSH Scan	1
199.191.56.187	United States	147.237.0.121		ET SCAN NMAP -sS window 3072	1
202.124.48.157	Japan	147.237.0.121		ET SCAN NMAP -sS window 4096	1
123.143.79.107	Korea, Republic of	147.237.0.121		ET SCAN Potential SSH Scan	1
202.124.48.157	Japan	147.237.0.121		ET SCAN NMAP -sS window 1024	1
209.236.124.188	United States	147.237.0.121		ET SCAN NMAP -sS window 1024	1

12-26-2015 to 12-27-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	951
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	852
66.249.93.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	816
64.79.85.205	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	526
217.171.42.130	Italy	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	486
149.78.239.141	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	332
149.78.194.90	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	307
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	169
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	165
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	153
149.78.23.130	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	143
149.78.109.90	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	132
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	123
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	117
2.52.131.246	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	92
157.55.39.178	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	73
149.88.61.157	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	69
149.88.142.227	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	58
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	57
149.88.176.226	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	43
85.228.31.123	Sweden	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
46.19.85.213	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	36
5.138.110.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	33
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	33
207.46.13.2	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	33
46.120.239.231	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	30
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	29
149.50.76.114	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	29
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28
149.78.50.201	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28
212.116.166.10	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	27
212.116.166.10	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	27
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
66.249.69.165	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	24
85.64.18.157	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	21
149.50.82.115	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
157.55.39.179	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
66.249.69.170	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
185.3.144.165	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	16
66.102.9.33	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13
149.78.136.136	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	12
149.88.65.252	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	11
141.8.183.14	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	9
95.108.158.159	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	9
66.249.93.208	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	9
66.249.69.98	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	9

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
192.198.151.43	Europe	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	2
46.120.246.11	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 46.120.246.11 (Open Mode)	None	2
109.67.49.244	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
2.54.14.32	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
193.104.77.4	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 193.104.77.4 (sigalgs DoS Attack)	None	1
46.120.246.11	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
185.3.146.89	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 3B7CCD6E4C9EBD76F6A899634AD8BB532501B01D98B289E88BC2D78636091C61F8F6B65EEF77A011D962E7022A43D321A7D13A205A1A05764DD14577999196A0596FD1838C0D669CC4FAC41190A78084B3D0116598213947C2E30E96411A8F1F0FED2BBA4204FA0BC6D1DE5338C2CCCC00DB79A83119D7E2F29170E13E949E7B, Observed 908C01A1E160D03B135A1F6750872E0B040CDA0BDB1FA1A3FF727AB4810256728D36BBF4D9597F3E28B95985BF127D61FCC50EAB0AA14504C1BF3B32E8BC67B98163D5E327985808FD6B822DB6D90337DAA90D297114EC6E246C26361F6817600705E4	None	1
5.29.138.59	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
193.104.77.4	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
84.94.33.224	Israel	147.237.0.121		Unknown Parameter _ in www.miluim-ishi.aka.idf.il/newpassword/firstlogin	Block	1
185.3.146.247	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
46.120.246.11	Israel	147.237.0.121		Double URL Encoding - parameter: ReturnUrl in www.miluim-ishi.aka.idf.il/login	Block	1
213.8.204.70	Israel	147.237.0.121		Double URL Encoding - parameter: ReturnUrl in www.miluim-ishi.aka.idf.il/login	Block	1
89.138.26.228	Israel	147.237.0.121		Double URL Encoding - parameter: ReturnUrl in www.miluim-ishi.aka.idf.il/login	Block	1

12-26-2015 to 12-27-2015