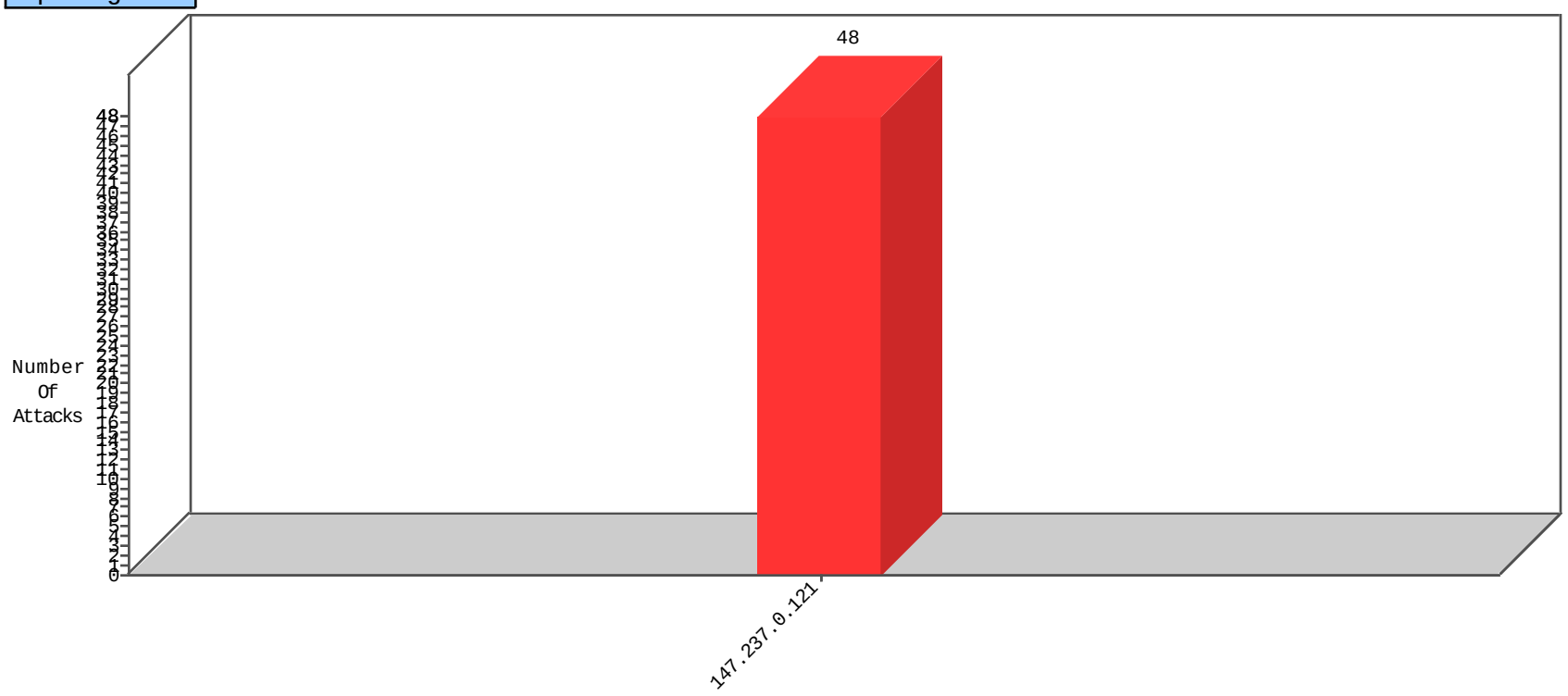
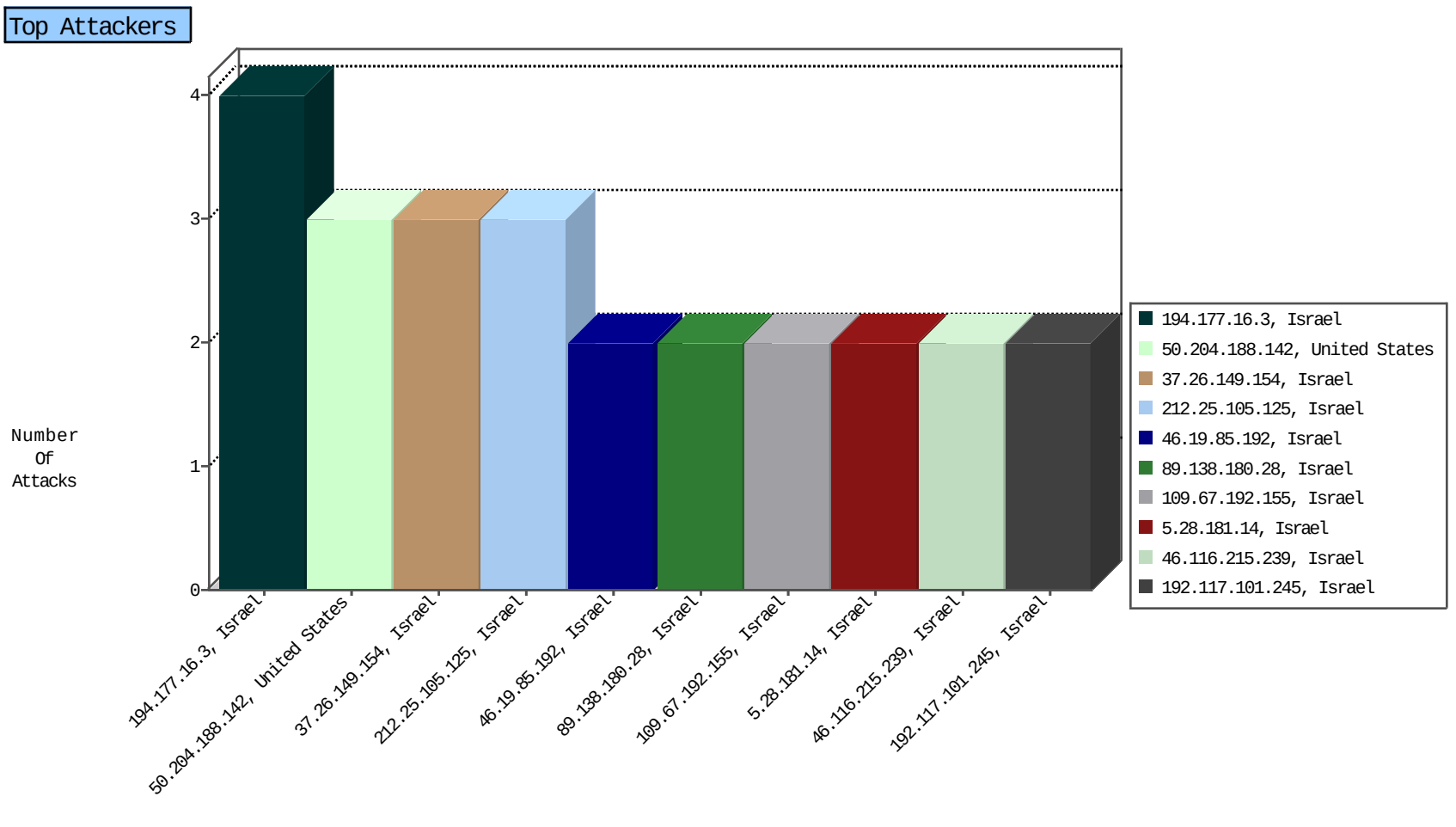
12-29-2015 to 12-30-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



12-29-2015 to 12-30-2015

Top Attackers In DDoS-Defence

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

12-29-2015 to 12-30-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

12-29-2015 to 12-30-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
212.25.105.125	Israel	147.237.0.121		SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
50.204.188.142	United States	147.237.0.121		ET SCAN NMAP -sS window 2048	1
59.45.79.117	China	147.237.0.121		ET SCAN Potential SSH Scan	1
177.55.154.39	Brazil	147.237.0.121		ET SCAN Potential SSH Scan	1
50.204.188.142	United States	147.237.0.121		ET SCAN NMAP -f -sS	1
50.204.188.142	United States	147.237.0.121		ET SCAN NMAP -sS window 4096	1
104.219.238.10		147.237.0.121		ET SCAN NMAP -sS window 1024	1
192.198.151.45	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	1
23.234.5.107	United States	147.237.0.121		ET SCAN Potential SSH Scan	1

12-29-2015 to 12-30-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2491
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2418
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2315
2.54.55.62	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	837
187.237.14.195	Mexico	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	531
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	260
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	245
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	233
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	215
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	152
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	144
207.46.13.164	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	127
66.102.6.90	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	113
187.189.9.193	Mexico	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	107
82.80.173.170	Israel	147.237.0.121		Bad TCP sequence		monitor	100
94.16.11.27	Germany	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	75
2.52.27.73	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	65
149.50.77.180	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	63
79.180.203.164	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	58
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	56
157.55.39.179	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	53
37.26.149.176	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	50
157.55.39.178	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	49
149.78.230.148	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
207.46.13.46	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
207.46.13.6	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	44
178.90.105.6	Kazakstan	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	43
188.98.104.57	Germany	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	42
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	41
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
40.77.167.25	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
79.182.229.1	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	35
66.249.93.211	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	34
149.88.73.50	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	30
2.54.54.53	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	28
2.52.27.73	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	27
2.52.27.73	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	27
66.249.66.105	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
2.52.27.73	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	27
194.177.16.3	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	25
82.80.173.170	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	25
37.26.149.176	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
82.80.173.170	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	25
37.26.149.176	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	25
2.52.27.73	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	24
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	24
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
87.68.250.56	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	22
15.90.162.11	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	19

12-29-2015 to 12-30-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
194.177.16.3	Israel	147.237.0.121		Unauthorized HTTP Method	Block	4
37.26.149.154	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.67.192.155	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	2
46.116.215.239	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	2
89.138.180.28	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	2
46.19.85.192	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.177.152.12	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
5.28.181.14	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/volunteeringbyage	Block	2
192.117.101.245	Israel	147.237.0.121		Unauthorized HTTP Method	Block	2
109.67.108.250	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
46.19.86.245	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
5.29.107.15	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
194.90.89.245	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
89.138.161.168	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
2.54.165.133	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
212.179.231.229	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
31.154.19.5	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/ajax/order/displayorderprint	Block	1
5.28.178.94	Israel	147.237.0.121		Unknown Parameter tzav in www.miluim-ishi.aka.idf.il/login	Block	1
176.13.3.66	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.210.188.6	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
199.203.159.137	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
93.157.86.33	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
46.19.86.179	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected C1F5CAD76BA4C1669E451E0C2932381DE51BFB153033458029DBFF8D5043E4C63FA2919047C29EEC3CCE3ACDD7313BA252C7398CC74061C64C20FF327F51441CFB62F6F7166A52317782808F657492A2F5B33DCC9E302132EEA1172155F59B547A683A2DEF65C2CBEF7AEE95246A2841038521C8D46CED3B90FCD112DABFAFA5, Observed 0A5F68D15D5A994E6D64E8A6C199309C7BC8F951927FD5FD51C9847977546DF72B5CD57275C8BEC6FA0C941BE11293419326C95440F30500C0A673F0109E60805E2F85E78B72FAC16D5D05EE8E5E9DA412077D6B1AD38A8BFE93F46E8E1CB0E8C92AAB	None	1
87.69.211.179	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
37.26.149.154	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected B3356A55C25EE4556A691B537392201A7DD52A5668B2907A249107B6642FA5DAAAD2B8B6DC5EBF6BB4F1A39C052720EA515E7E8CE595EA1E178BC463ECA374FC16F95A9F7F3DFE55422AD6AF0E46B373C08FB0E94A855E81CFC5F014FE30A2FBD617CD093032D83ECFD28E0E374C8145633890A071B3308F4D6130CB313F7885, Observed D79955B92F20032FA5BC817EE8C82A1082D732DFD96C34923BDE6C35B86CF756F2A20DAC643D86707D946A2D74487325C3D4FD87D95009F85DF4DB48BD2392B9EC8A12650DEDC0E7911F244CA2FA3F5FC9382368D805FB539C1C1AC64CA915D8D57D0B	None	1
2.54.41.131	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
212.25.105.125	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1

12-29-2015 to 12-30-2015