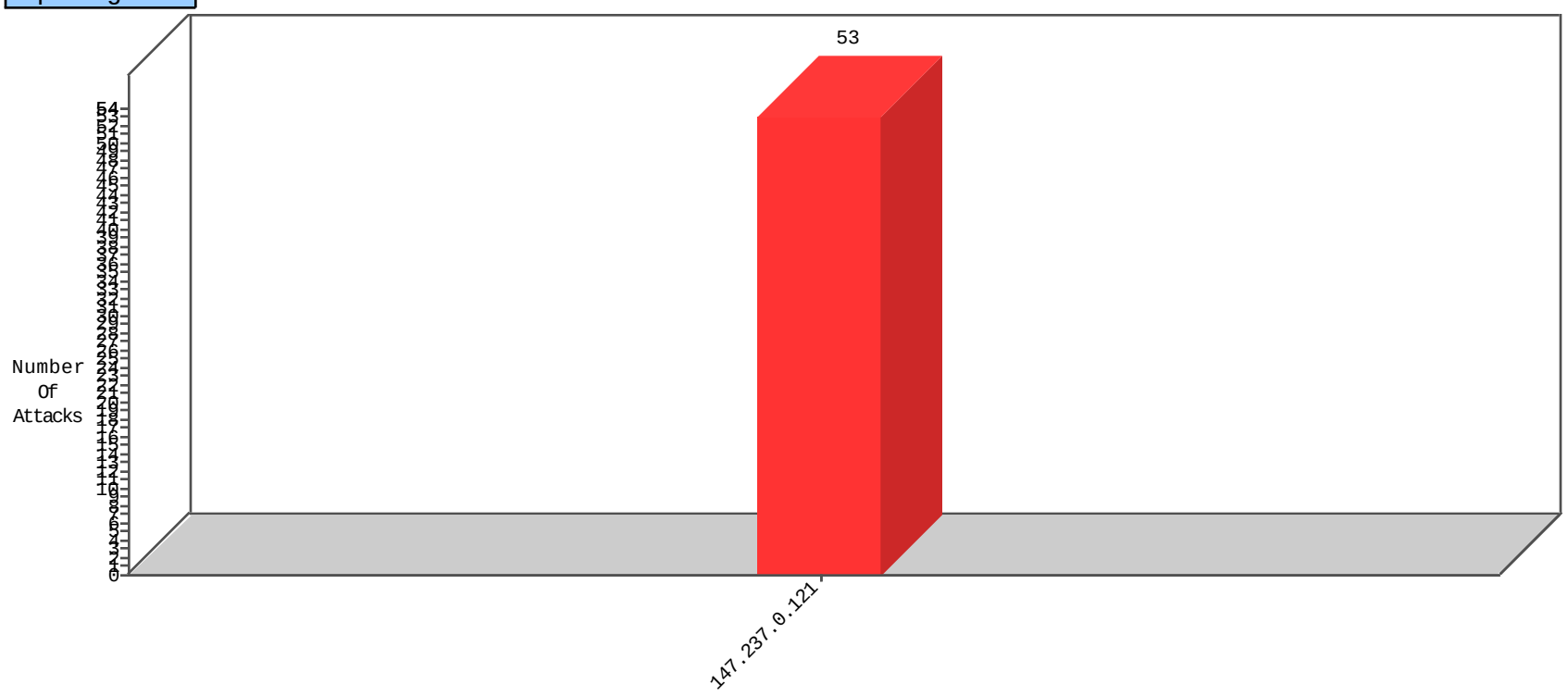
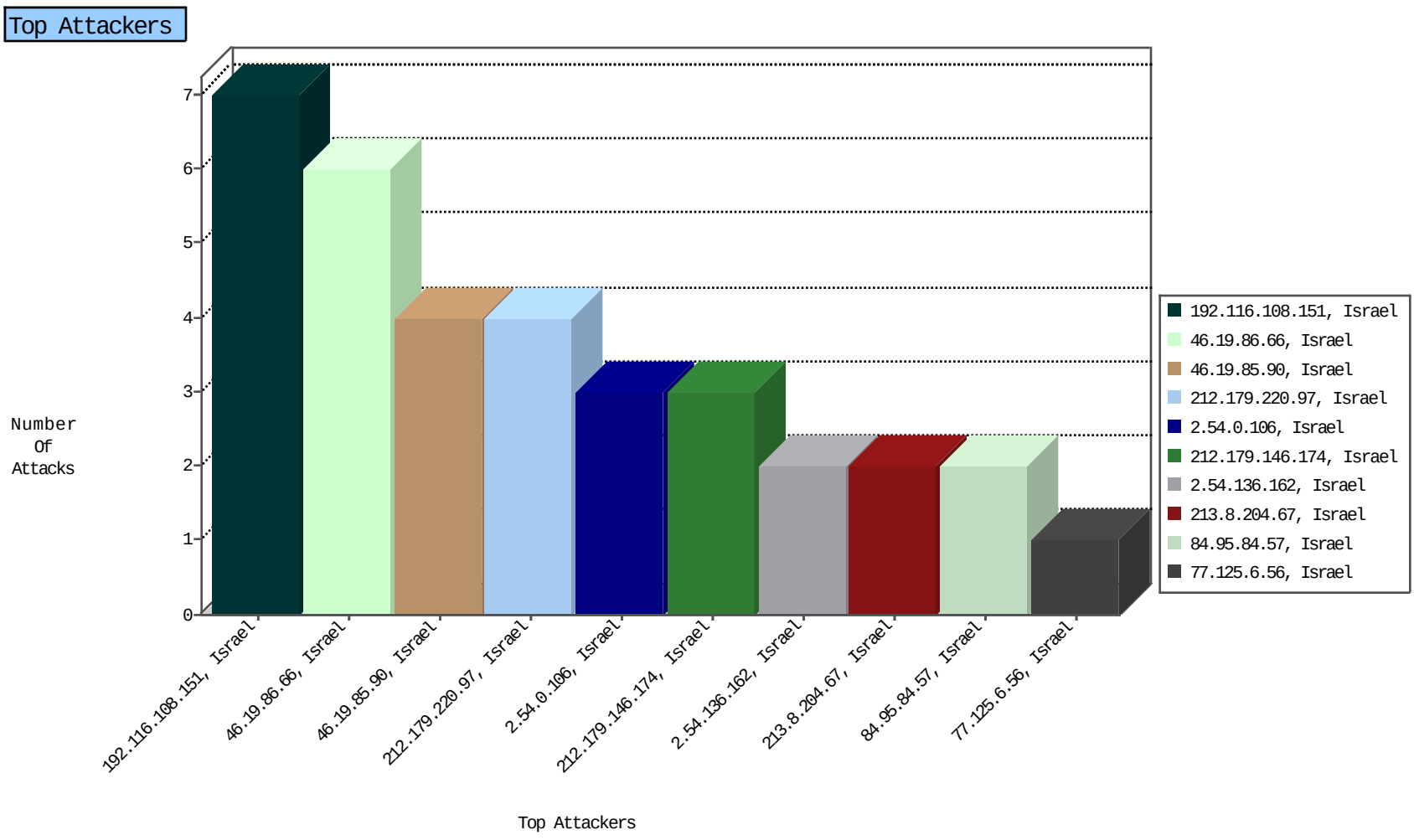
12-16-2015 to 12-17-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



12-16-2015 to 12-17-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
46.19.86.66	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	6
212.179.146.174	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3

12-16-2015 to 12-17-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

12-16-2015 to 12-17-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
120.150.29.211	Australia	147.237.0.121		ET SCAN NMAP -sS window 1024	1
59.45.79.117	China	147.237.0.121		ET SCAN Potential SSH Scan	1
196.47.173.21	Cote D'Ivoire	147.237.0.121		ET SCAN NMAP -sS window 1024	1

12-16-2015 to 12-17-2015

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	3552
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2791
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2410
88.12.10.182	Spain	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	361
202.182.0.200	Thailand	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	314
199.207.253.96	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	304
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	294
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	265
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	229
149.78.105.4	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	228
149.78.62.113	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	223
46.19.86.30	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	196
72.37.140.47	Italy	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	192
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	182
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	158
140.101.20.1	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	153
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	153
149.78.50.201	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	148
149.88.236.241	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	130
149.78.27.168	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	107
66.102.6.149	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	103
149.78.109.90	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	102
149.78.255.48	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	101
13.17.125.9	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	99
212.235.98.139	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	88
13.21.125.9	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	81
149.88.7.255	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	65
40.77.167.1	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	59
37.230.221.40	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	50
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	48
149.78.41.170	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	42
84.228.244.72	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
46.19.86.66	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
138.134.102.16	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	36
46.19.86.84	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
217.69.133.169	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	36
128.139.23.196	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	35
66.249.66.109	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	34
66.102.9.33	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	32
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28
209.135.211.191	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28
149.78.241.12	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
173.208.58.155	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
149.88.89.180	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
37.26.147.138	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	27
217.132.4.52	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	26
46.19.86.13	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	25
84.110.211.6	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	25

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
212.179.220.97	Israel	147.237.0.121		Unauthorized HTTP Method	Block	4
192.116.108.151	Israel	147.237.0.121		Parameter Type Violation __EVENTVALIDATION in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	3
2.54.0.106	Israel	147.237.0.121		Unauthorized HTTP Method	Block	3
46.19.85.90	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 46.19.85.90 (sigalgs DoS Attack)	None	2
213.8.204.67	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.90	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	2
192.116.108.151	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddDocs&FileToActivate in www.miluim-ishi.aka.idf.il/login	Block	2
192.116.108.151	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddDocs&FilesToCheck in www.miluim-ishi.aka.idf.il/login	Block	2
84.95.84.57	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
46.19.86.95	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
2.54.136.162	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
109.67.2.135	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
82.80.142.209	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
89.138.113.182	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
77.125.6.56	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
2.54.141.217	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
128.139.23.196	Israel	147.237.0.121		Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 128.139.23.196	Block	1
83.130.113.213	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
93.173.148.161	Israel	147.237.0.121		Untraceable SSL Sessions: Unknown SSL Session	None	1
81.218.50.26	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 0E892005EA70D2EDA52299A22A98CE60DC85ED7DD33BC4880D849C02FC70CAB147752EFC25FE6766C175F49FFF460318D1C00044259982306CF1A5C47EF1FACC2AE91A84FE57541AE4436B71ACFE51440A2DAFF036913EB9CE751CE262F231CFF55536ADD70506463B2BAEE566DD302F91828DE19C3C0B422AC4251092E96402, Observed 91520A3409CD704D92FB09AF6CD949579F1C2E1BA0242F512B00BD19D2350A6DF010F1749F7A275672EF58975D6CF5DFFB170E3029F775E074D569048B2DE4CA84C57E6B6A11DB3FE64D0B0225ED684A3008CB5EC6F4B9DA903980A15202B785BE9D25	None	1
31.154.5.181	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 82D32CBC515B84F044333113D97B476016A77475BF3D9EA743FD16C161360305EC05DA83B80EFF82B2032D08752A4004BF1E7A094B96303A07E32C9DB13126C62DF0C803CDFE39E4F26789324972C156D7C811F4195142297187862743DD48791B0C7008B7B75F32A6D253E9873CE1F6AFDFBC15F20CE0F42BED3B41F920D7AB, Observed E13CADD7F9AED0CFB014A81AFA70C9E095F477AFD9484897530E575821348DD584049C08DA3C95B6A125D993D66A42CEAE1F6FA28A6305DF181200838813EF3844D06B4717DCB93F8A3A95E16925BEE283FA8AF866EFE910F6C682324B66A23579D01C	None	1
132.73.203.238	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
84.95.84.57	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 84.95.84.57 (Unknown SSL Session)	None	1
46.19.86.71	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.136.162	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 2.54.136.162 (sigalgs DoS Attack)	None	1
95.86.90.222	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
81.218.159.27	Israel	147.237.0.121		Unauthorized HTTP Method	Block	1
31.154.155.182	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.114.91.244	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1