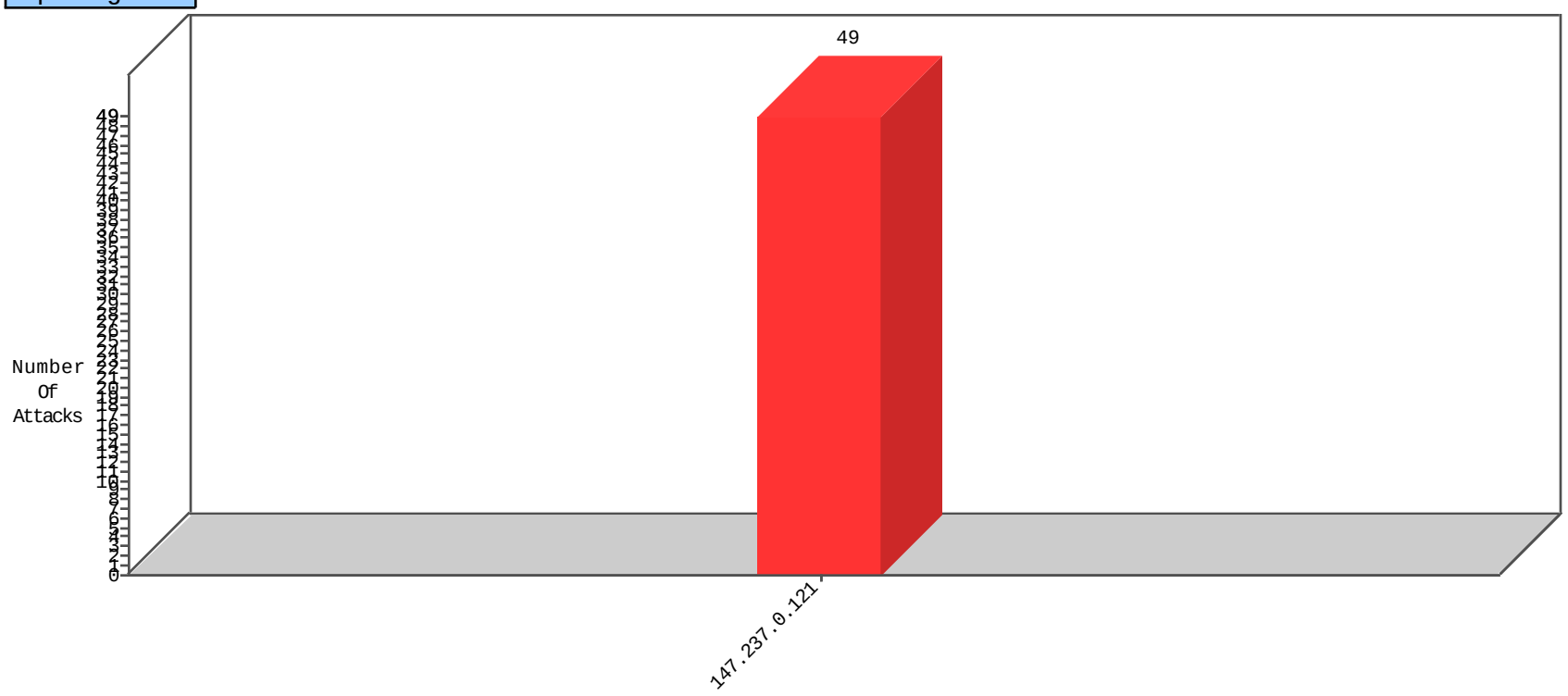
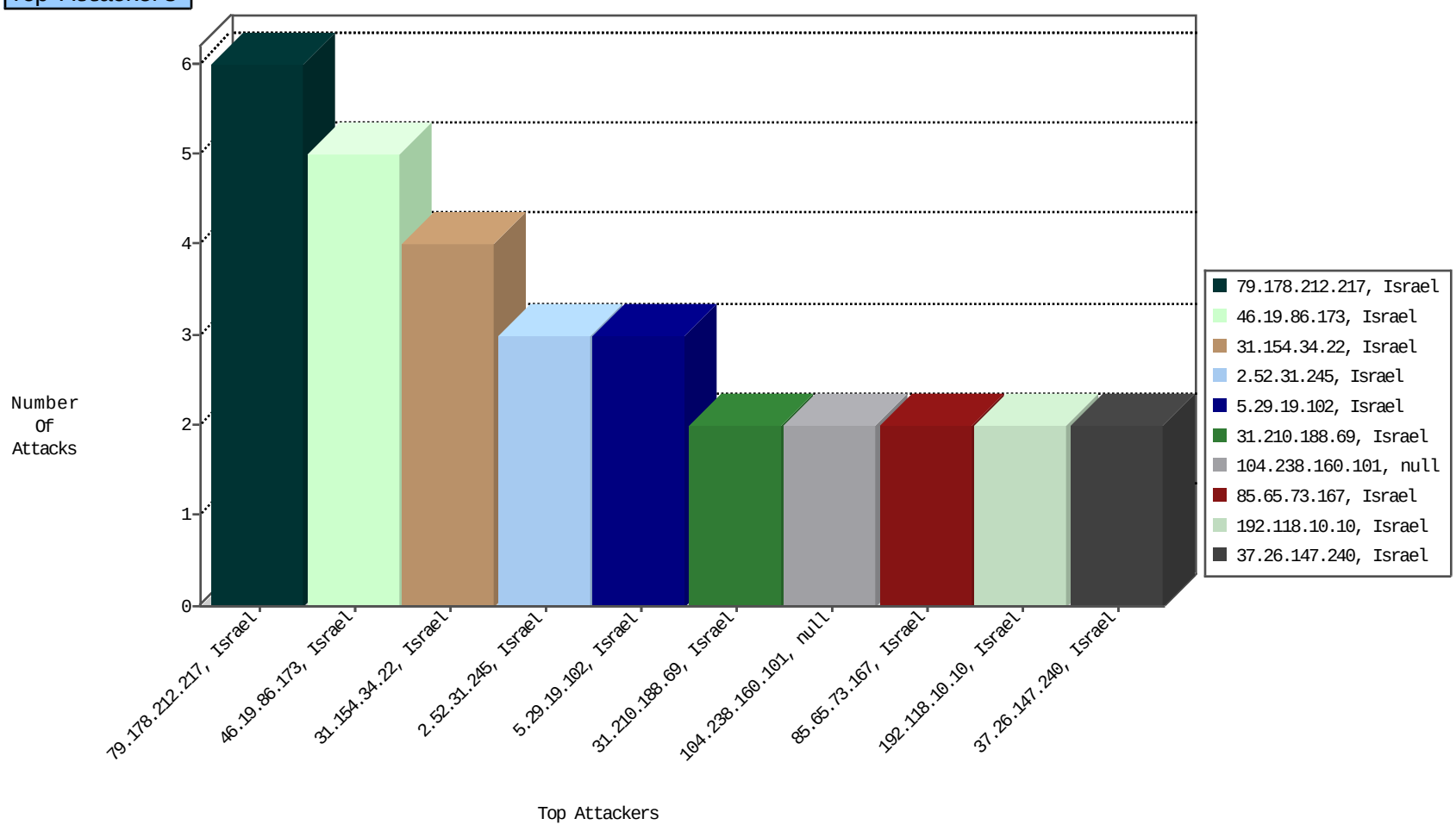
12-31-2015 to 01-01-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



12-31-2015 to 01-01-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
79.178.212.217	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	6

12-31-2015 to 01-01-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

12-31-2015 to 01-01-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
31.154.34.22	Israel	147.237.0.121		ET SCAN NMAP -sA (2)	4
59.45.79.117	China	147.237.0.121		ET SCAN Potential SSH Scan	1
104.238.160.101		147.237.0.121		ET SCAN NMAP -sS window 4096	1
208.67.1.121	United States	147.237.0.121		ET SCAN Potential SSH Scan	1
59.39.213.43	China	147.237.0.121		ET SCAN Potential SSH Scan	1
104.238.160.101		147.237.0.121		ET SCAN NMAP -sS window 1024	1
185.130.5.231		147.237.0.121		ET SCAN Potential SSH Scan	1

12-31-2015 to 01-01-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2489
66.249.93.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2021
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1422
134.191.232.68	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	628
149.88.26.61	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	337
40.77.167.14	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	264
149.78.40.110	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	232
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	200
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	196
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	177
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	139
134.191.232.72	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	128
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	104
149.50.77.180	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	95
80.15.43.13	France	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	92
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	90
207.46.13.113	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	88
149.78.242.138	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	76
149.50.105.154	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	62
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	55
149.88.40.122	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	49
66.249.93.214	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	48
207.46.13.91	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
149.78.230.148	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	41
213.57.178.125	Israel	147.237.0.121		Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	40
149.78.50.201	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	40
213.57.178.125	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	40
209.135.211.161	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	36
2.52.177.61	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
207.46.13.164	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	35
157.55.39.178	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	30
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	29
87.68.250.56	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	28
66.102.6.90	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
84.94.161.247	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	25
46.19.85.165	Israel	147.237.0.121		Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	25
66.249.73.174	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
149.78.62.113	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
149.50.97.200	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
66.102.9.61	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	19
66.249.93.211	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
66.249.73.165	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
62.0.34.177	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	17
149.88.89.180	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
66.249.81.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
37.26.146.192	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	16

12-31-2015 to 01-01-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
2.52.31.245	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	3
46.19.86.173	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	3
31.210.188.69	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
5.29.19.102	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	2
132.73.197.106	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
46.121.119.197	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/volunteeringbyage	Block	1
212.179.129.6	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
84.94.61.202	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddStudyEmploymentPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
46.19.86.173	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 46.19.86.173 (sigalgs DoS Attack)	None	1
192.118.10.10	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 192.118.10.10 (Unknown SSL Session)	None	1
79.177.116.13	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/changeunit	Block	1
37.26.147.240	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 37.26.147.240 (sigalgs DoS Attack)	None	1
2.54.145.153	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
213.8.39.241	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
85.65.73.167	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 85.65.73.167 (sigalgs DoS Attack)	None	1
46.19.86.173	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
31.154.33.190	Israel	147.237.0.121		Unknown Parameter tzav in www.miluim-ishi.aka.idf.il/login	Block	1
192.118.10.10	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
80.179.125.162	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
37.26.147.240	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
2.54.169.69	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
85.65.73.167	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
31.154.160.9	Israel	147.237.0.121		Suspicious Response Code	Block	1
212.25.91.30	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
82.166.183.151	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	1
46.19.85.214	Israel	147.237.0.121		Double URL Encoding - parameter: ReturnUrl in www.miluim-ishi.aka.idf.il/login	Block	1
5.29.19.102	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$Submit1 in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	1

12-31-2015 to 01-01-2016