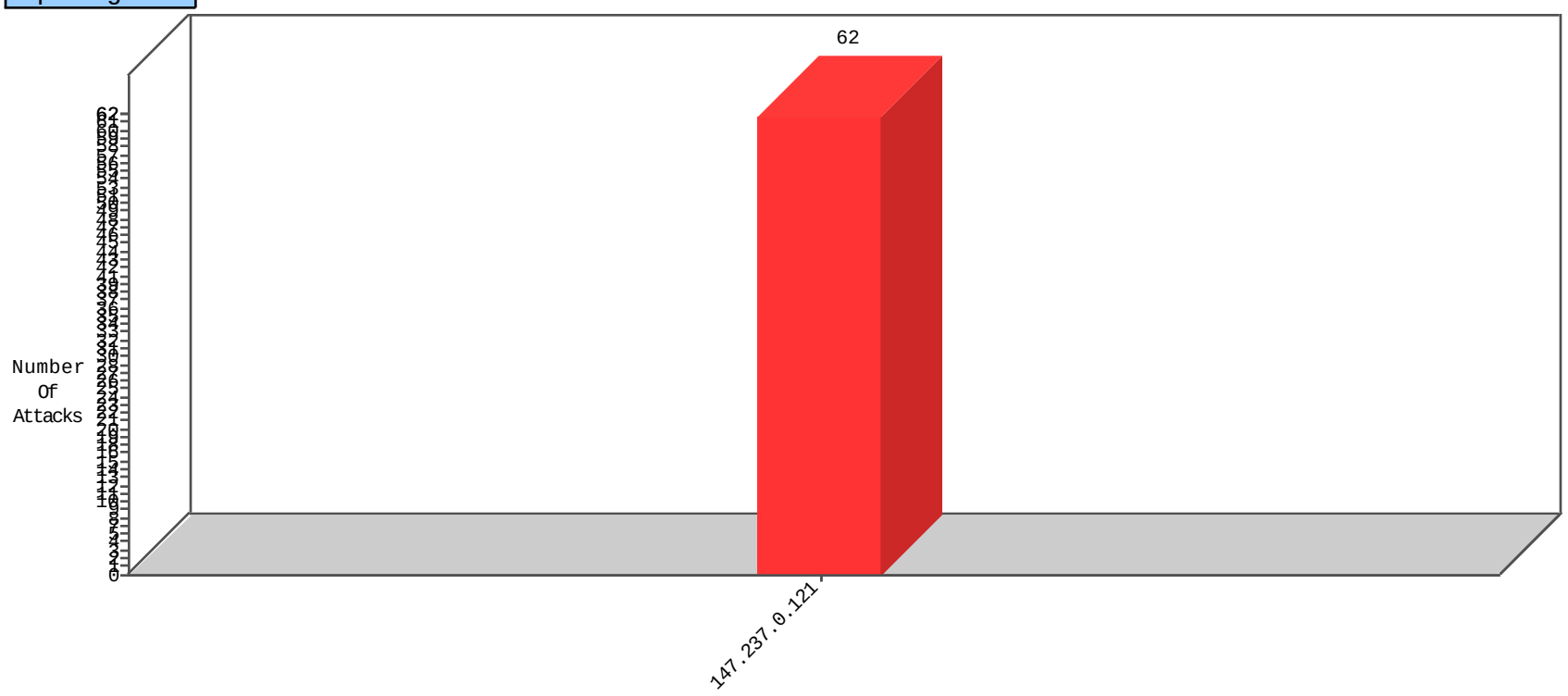
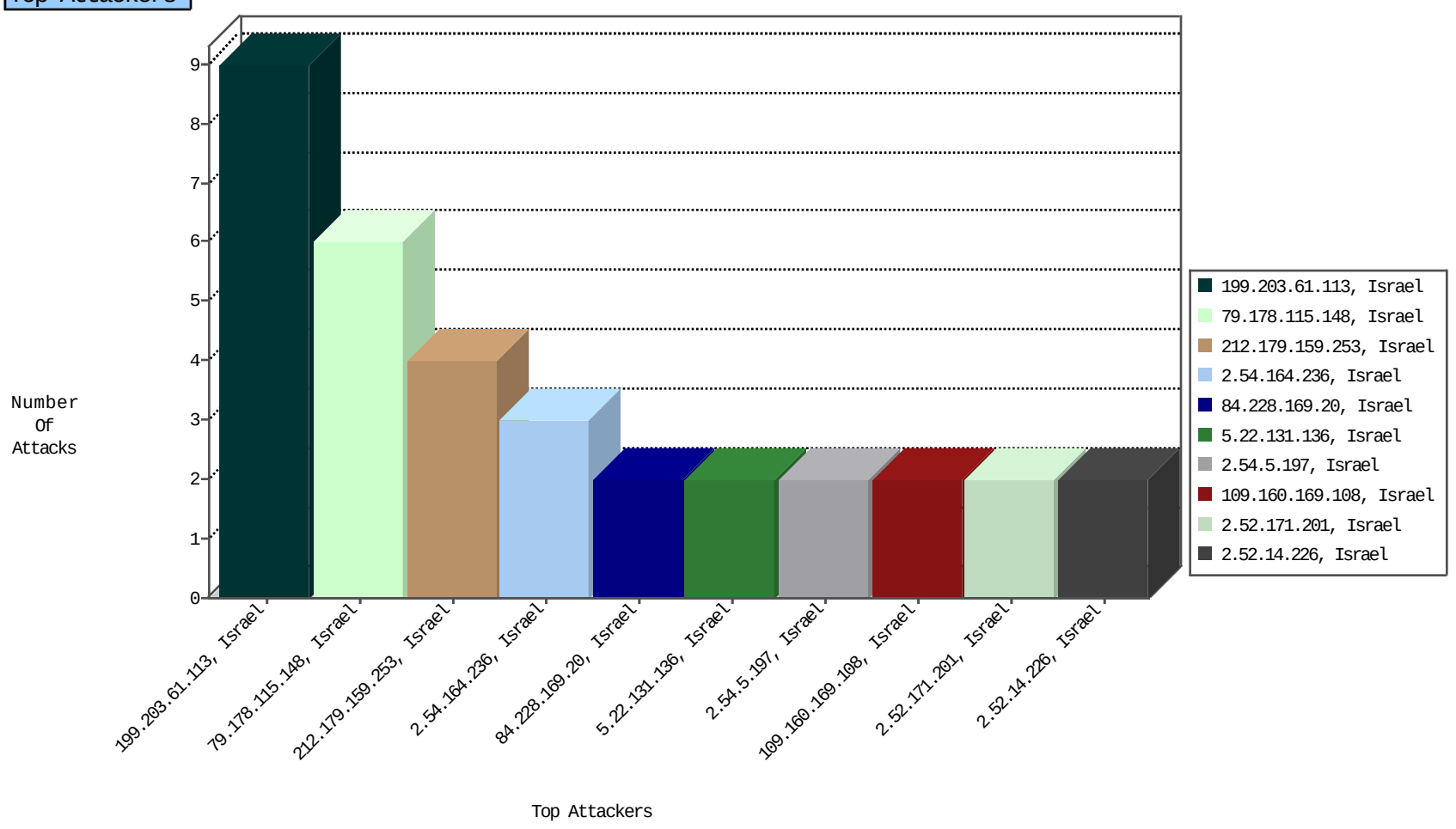
12-07-2015 to 12-08-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



12-07-2015 to 12-08-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
79.178.115.148	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	6
132.66.97.233	Israel	147.237.0.121		IIS-SSL-CSL-DoS	dest-reset	BBL-Israel	1

12-07-2015 to 12-08-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

12-07-2015 to 12-08-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
132.248.94.130	Mexico	147.237.0.121		ET SCAN Potential SSH Scan	1
59.45.79.117	China	147.237.0.121		ET SCAN Potential SSH Scan	1
192.198.151.45	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	1

12-07-2015 to 12-08-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.153	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2879
66.249.93.145	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2696
66.249.93.149	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2357
64.79.85.205	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	517
149.78.254.244	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	289
66.249.93.145	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	266
66.249.93.153	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	248
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	213
149.88.116.181	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	212
66.249.93.149	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	202
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	196
194.42.67.50	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	172
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	151
2.52.44.115	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
17.78.162.212	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	106
149.88.212.86	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	97
149.78.63.20	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	94
149.78.221.136	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	87
149.78.18.80	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	59
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	55
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	51
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	50
66.249.81.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
149.88.198.132	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	43
17.78.161.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	42
149.78.176.38	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	41
46.19.86.102	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
46.19.85.151	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
5.28.156.96	Israel	147.237.0.121		Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	34
5.28.156.96	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	34
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	32
79.179.134.146	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	31
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
147.235.8.72	Israel	147.237.0.121		Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	27
80.246.136.96	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	27
66.249.81.129	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
84.110.32.90	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	25
194.90.119.124	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	25
66.249.81.251	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
37.157.143.2	Bulgaria	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	23
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	21
209.135.211.206	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	21
147.235.8.72	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	21
80.246.136.96	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	19
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
66.249.93.223	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
149.88.150.186	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
149.78.233.91	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
31.168.13.78	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	16
190.212.67.118	Nicaragua	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16

12-07-2015 to 12-08-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
199.203.61.113	Israel	147.237.0.121		Suspicious Response Code	Block	9
212.179.159.253	Israel	147.237.0.121		Unauthorized HTTP Method	Block	4
2.54.164.236	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	3
109.160.169.108	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
212.199.34.114	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	2
2.52.14.226	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
5.22.131.136	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.52.171.201	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
199.203.56.230	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
84.228.169.20	Israel	147.237.0.121		Parameter Type Violation ctl00_ContentPlaceHolder1_fuAddStudyPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/uploadregister.axd	Block	1
79.179.127.200	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
79.183.62.245	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/changepassword/resetpasswor	Block	1
5.28.176.61	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/1377-he/miluim.aspx	Block	1
2.54.5.197	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
84.228.169.20	Israel	147.237.0.121		Parameter Type Violation ctl00_ContentPlaceHolder1_fuAddTimetableDocs&FilesToSend in www.miluim-ishi.aka.idf.il/uploadregister.axd	Block	1
79.179.134.146	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/1381-he/miluim.aspx	Block	1
2.54.164.244	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/â€?â€Ž	Block	1
212.179.230.141	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
176.13.8.205	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.216	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
37.26.147.230	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
2.54.5.197	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.150.190.98	Israel	147.237.0.121		Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login	Block	1
87.68.62.161	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
79.181.55.225	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.168.43	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	1
192.118.10.10	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
81.218.40.59	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
46.19.85.66	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.133.141	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	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
87.68.71.76	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/login	Block	1
79.182.25.122	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1

12-07-2015 to 12-08-2015