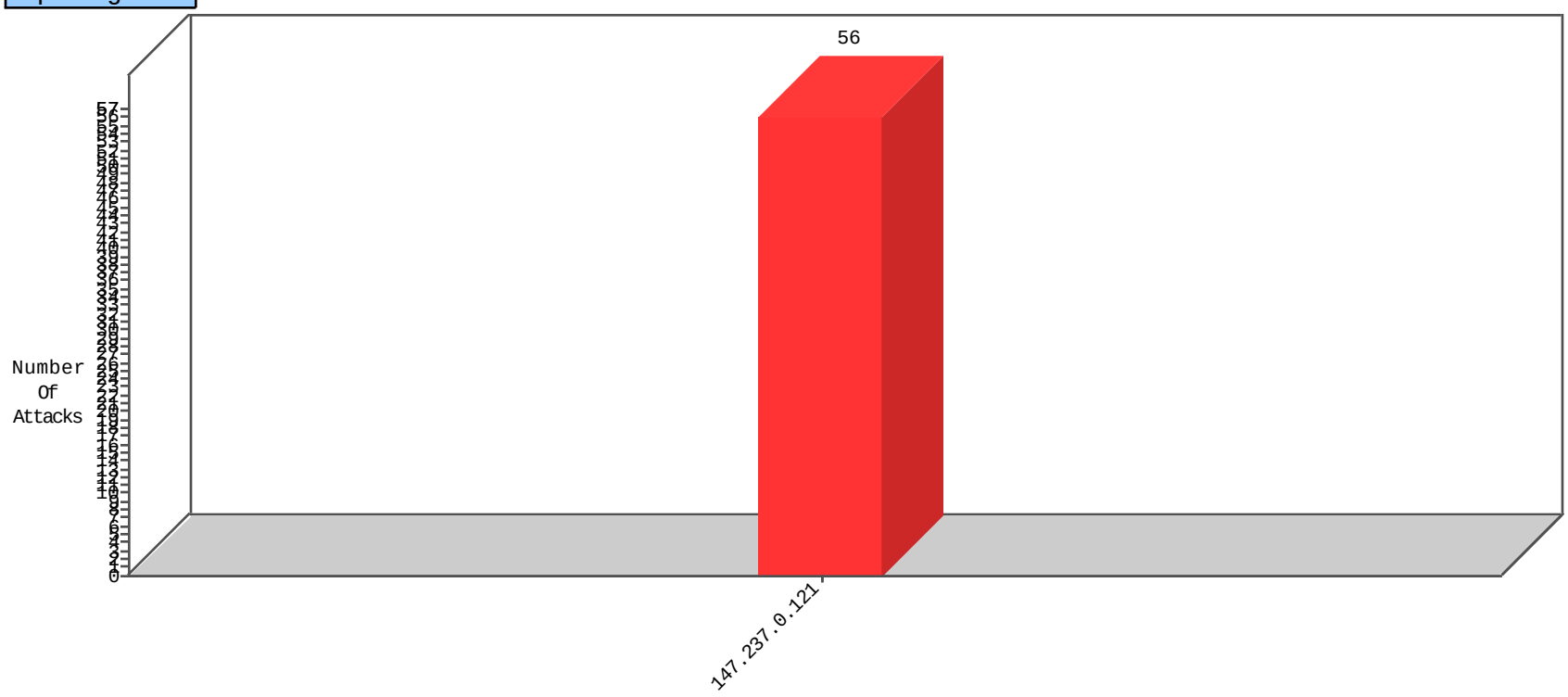
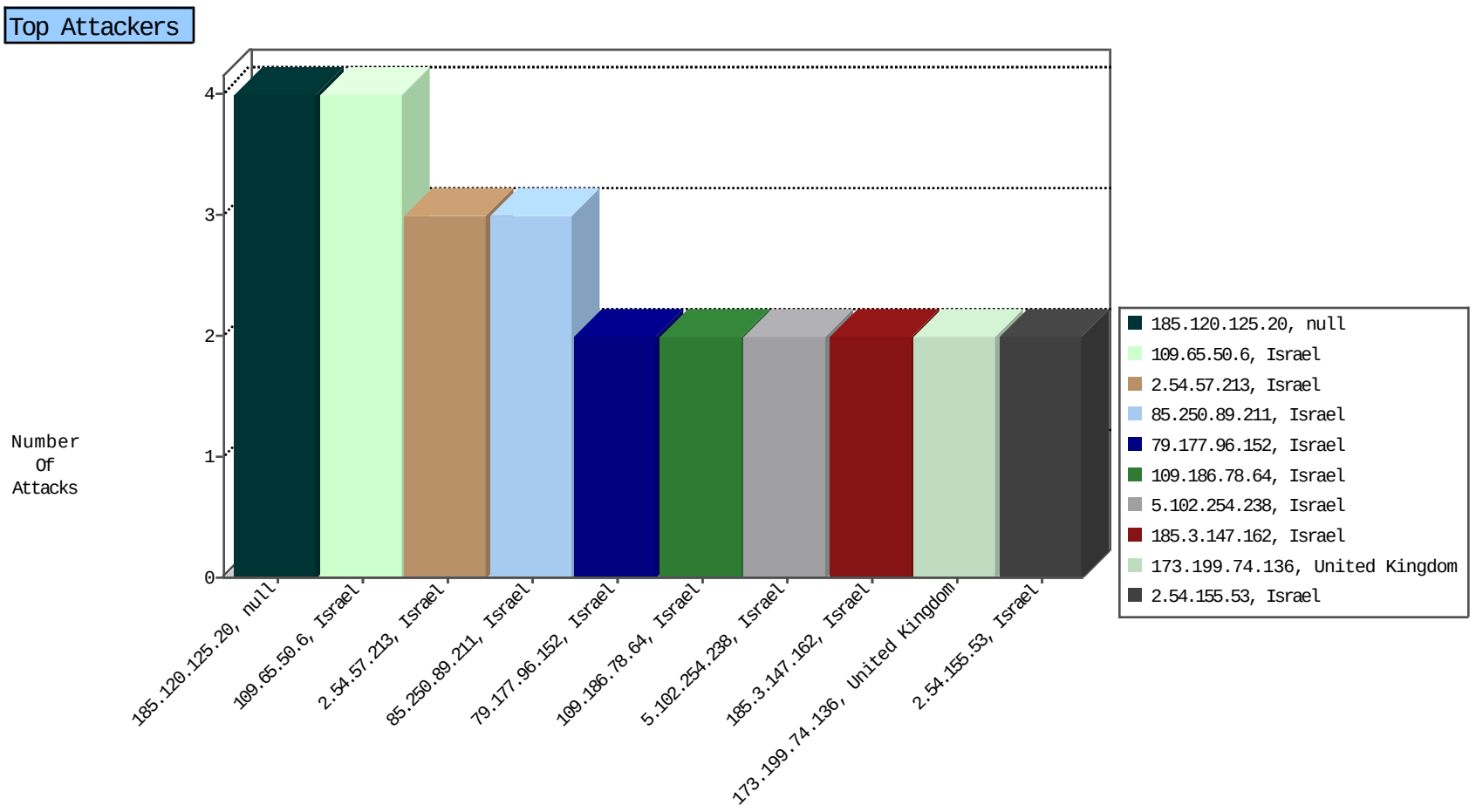
01-08-2016 to 01-09-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



01-08-2016 to 01-09-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
85.250.89.211	Israel	147.237.0.121		Block_Udp_All_Nets	drop	DP-Tehila	3
5.22.129.227	Israel	147.237.0.121		network flood IPv4 TCP-RST	drop	BBL-Israel	1
109.65.29.32	Israel	147.237.0.121		network flood IPv4 TCP-RST	drop	BBL-Israel	1

01-08-2016 to 01-09-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

01-08-2016 to 01-09-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
79.177.107.122	Israel	147.237.0.121		ET SCAN NMAP -sA (2)	2
173.199.74.136	United Kingdom	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	2
168.63.206.180	United States	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	2
80.248.146.42	Russian Federation	147.237.0.121		ET SCAN NMAP -sS window 1024	1
62.210.203.114	France	147.237.0.121		ET SCAN Potential SSH Scan	1
80.82.69.146	Netherlands	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

01-08-2016 to 01-09-2016

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	861
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	837
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	695
149.78.81.31	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	316
149.88.158.222	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	297
149.88.13.144	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	250
2.52.160.120	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
84.228.91.226	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
149.78.255.165	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	136
38.127.167.44	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	122
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	121
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	112
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	97
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	81
149.88.128.46	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	78
157.55.39.2	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	77
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	77
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	61
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	56
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	50
138.134.102.16	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	50
66.102.7.179	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	44
149.88.132.190	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	40
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	38
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
80.246.136.68	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	36
176.13.11.34	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	36
149.78.31.17	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	31
66.249.69.175	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	30
31.210.188.118	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	29
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
109.65.173.149	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
79.181.6.140	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
176.13.15.56	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	25
66.249.69.165	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	24
66.249.81.251	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	24
40.77.167.95	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	23
77.125.111.46	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	21
157.55.39.75	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
66.85.131.68	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	19
84.108.224.168	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	19
80.246.136.68	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	18
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
84.108.224.168	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	17
74.216.18.141	Canada	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
176.13.14.224	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	16
66.249.69.175	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
37.26.149.238	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	16

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
185.120.125.20		147.237.0.121		Suspicious Response Code	Block	4
109.65.50.6	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	4
2.54.57.213	Israel	147.237.0.121		Multiple Unauthorized URL Access from 2.54.57.213	Block	3
109.186.78.64	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNimuk in www.miluim-ishi.aka.idf.il/valtamrequest	Block	2
46.116.167.43	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
185.3.147.162	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	2
5.102.254.238	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	2
192.198.151.36	Europe	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	1
109.64.3.40	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
79.180.9.164	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
46.116.87.199	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
85.250.27.203	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected CA547C1FC4A2844F3DDCD1367B6206FF34A1054DC44CE520A49A7C1F0384880034A3CDA773A1A694EA7C4835C1CA453BCC23552EE40F48B6804B46E312CD19BDF7D3549343431621695A5B63530C0D5842B00D0F441094422BBBCA6D5DF4C7B2C1635FA74D4CD09868EC4E48389F083683ACAB3AD6DDB14DC9A3D87F6B970405, Observed 1B806BACC24BFF18EFA33060A422BDA73CA2050605CB094250B1D005EFF5DD9180E17439F17940CDCE56F227B66B0E1988B234FF30E5F227194F8003CF444CD58EB624E4C5998153C3A2A4F3B5DCE96EF68796B80F17514BF400325A7D6DA0AE6E6CF4	None	1
79.177.96.152	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 79.177.96.152 (sigalgs DoS Attack)	None	1
2.54.155.53	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 2.54.155.53 (sigalgs DoS Attack)	None	1
212.150.245.250	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
109.64.110.159	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/1325-he/miluim.aspx	Block	1
80.246.136.117	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 2E168099F5DD6AD6963C3B033FD4008690F68688F44C2DCBC5C969348FA20BE85323BA7110ED04D153D82921886E07FAFF16B9F081FD67197F207E2A4BAA46D97896392AD7789BF74DB8A77AA5CA3A36A2F6A64B01949AE8C5976C497942F8EFBA92D1474198819B0197A75448BB9C3C99CEE85448399B5BEFC23BCF6463F09A, Observed C4BB3E18A3F044473EC06A687F5ED5C1528116C0A3C4E78FEFB34A05BC58A060EB1C96338C454F6473A3387BBF8AD1CB2DBE73D81294B0379428C267D0ECEDFD0DAE4DBB9700B32DEAC9E6E2085D832B72B67FA4937572A77F9BDB9D3FC647CA142BF4	None	1
89.138.177.93	Israel	147.237.0.121		Double URL Encoding - parameter: ReturnUrl in www.miluim-ishi.aka.idf.il/login	Block	1
79.177.96.152	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
2.54.155.53	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
213.8.204.33	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
109.64.117.184	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
84.108.104.225	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
46.117.135.106	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
93.172.87.60	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	1
79.179.12.137	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
85.64.181.132	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
79.176.15.239	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected , Observed 99174267B5BD1319A24158ADED450533CB3EA1CDF358AAED7034AC689C6DB020E509795C0414E1CDEEC2DCE74EC941E261989E4B2B2F0CF6D92E697F1FCC7E3CDD8A77278A04DCB746A6B2A566FB26D201400114865F78FD54000DCCDF1D82CEC5297EFDF6A8846AC2A26312769038F38E1978B8E4E968CC6F3AEC6C9254FF223A2A7BA3B2F15BEF2B8E80E3CFDF872A8E63D01F37D34DB886C4244314410D80	None	1
2.54.136.144	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1