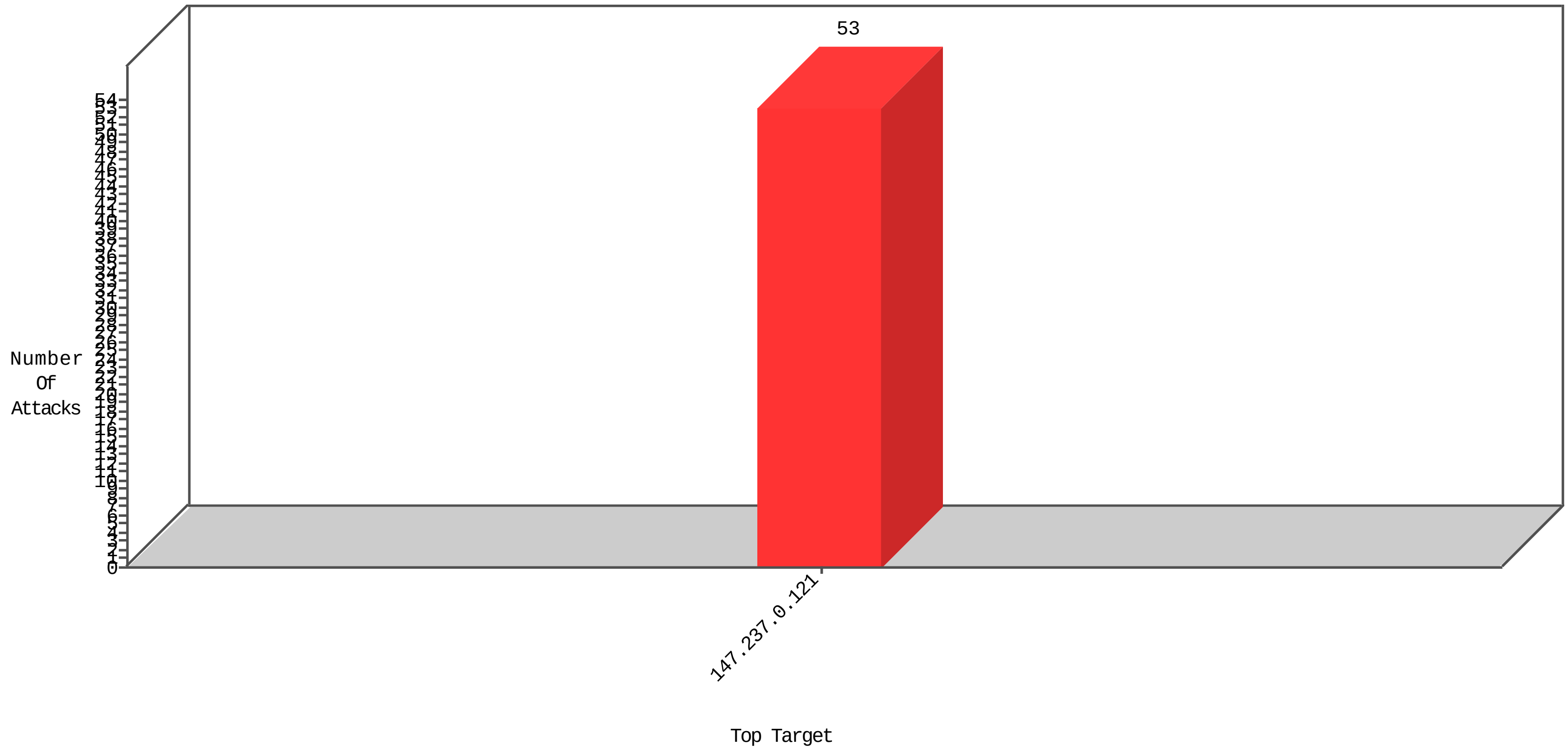
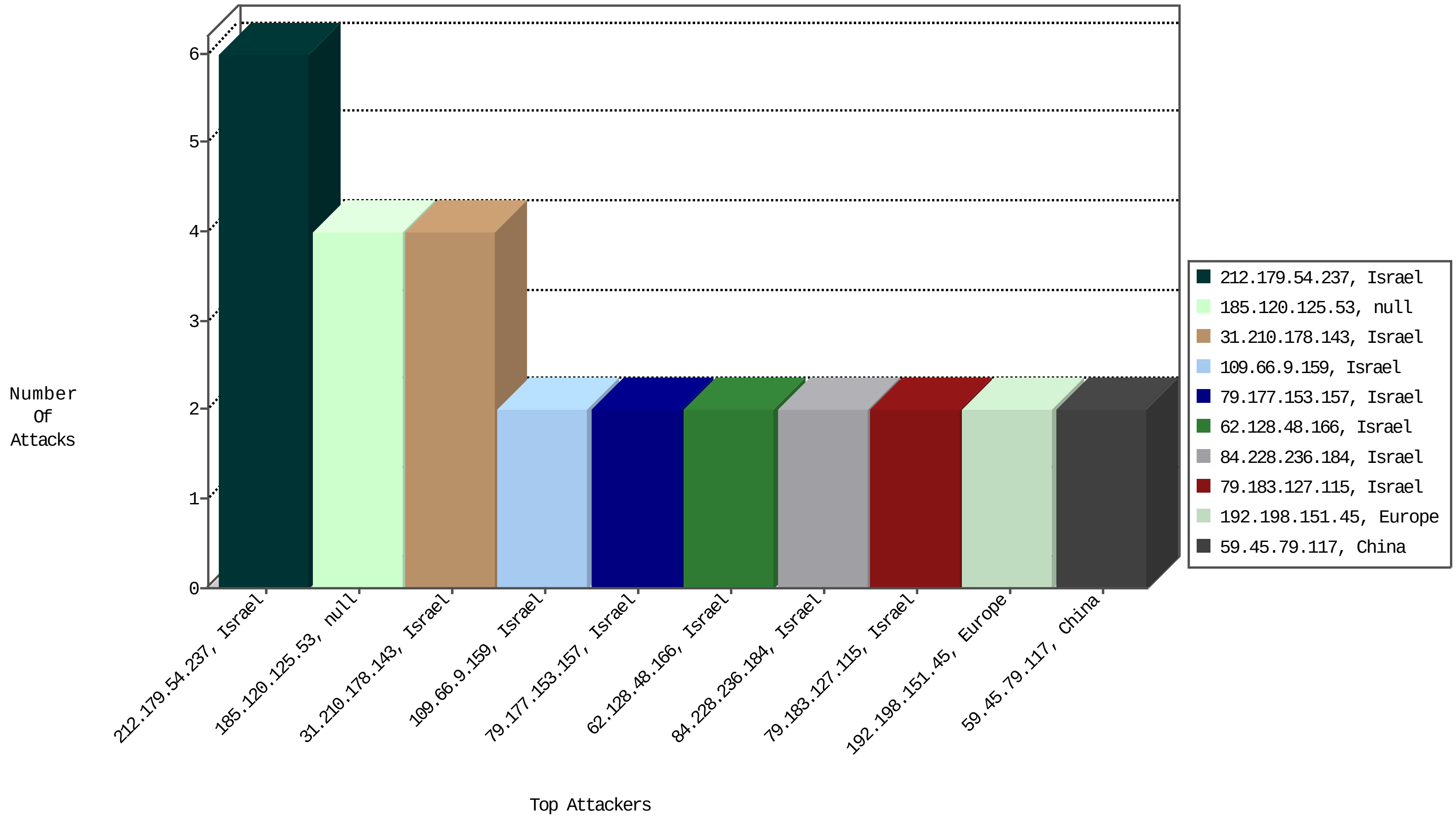
01-22-2016 to 01-23-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



01-22-2016 to 01-23-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
212.179.54.237	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	6
5.189.169.156	Germany	147.237.0.121		L4 Source or Dest Port Zero	drop	BBL-Frankfurt	1

01-22-2016 to 01-23-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

01-22-2016 to 01-23-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
218.246.0.97	China	147.237.0.121		ET SCAN NMAP -sS window 1024	2
59.45.79.117	China	147.237.0.121		ET SCAN Potential SSH Scan	2
192.198.151.45	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	2
223.4.174.30	China	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1
104.223.17.8	United States	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1
162.222.185.165	United States	147.237.0.121		ET SCAN Potential SSH Scan	1
199.203.9.99	Israel	147.237.0.121		ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
222.186.34.177	China	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1
119.146.221.68	China	147.237.0.121		ET SCAN Potential SSH Scan	1

01-22-2016 to 01-23-2016

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	1265
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1168
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1147
149.78.31.2	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	518
66.249.93.93	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	372
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	139
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	138
149.78.253.51	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	132
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	121
107.201.142.249	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	116
89.219.24.50	Estonia	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	108
149.78.37.10	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	93
149.78.105.139	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	70
81.180.66.34	Moldova, Republic of	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	46
54.174.56.131	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	46
66.249.93.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
149.78.254.125	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	41
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
192.115.177.203	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	37
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	33
66.249.81.251	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	32
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	31
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	29
66.249.66.107	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
195.195.81.215	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
31.210.187.198	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	25
66.249.93.208	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
149.50.124.156	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
149.88.53.241	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	24
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
52.91.218.126	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
149.78.180.56	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
66.249.93.97	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
149.78.124.81	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
130.193.50.201	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
64.120.47.67	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
66.249.88.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
93.158.152.203	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	14
178.154.189.201	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	14
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13
5.102.254.56	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	12
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	12
81.218.131.214	Israel	147.237.0.121		Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	11
31.210.177.45	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	11
66.249.66.107	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	11
52.90.227.202	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	10

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
185.120.125.53		147.237.0.121		Suspicious Response Code	Block	4
31.210.178.143	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	3
109.66.9.159	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	2
85.64.162.34	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	2
79.181.110.41	Israel	147.237.0.121		Parameter Type Violation virt in miluim-ishi.aka.idf.il/cellularreference	Block	2
62.128.48.166	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	2
84.228.236.184	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	2
185.120.125.51		147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
85.64.19.158	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected , Observed C7ED9C335FF5A20DAB45D3808FEB039D22667C7D0B18C01B095A82E7D5050ABCF483B86439A37164C06416E7AC052C7093348F8FCF07E1D250E1090186BF68ACADDF9463EBECF5185C33EC2CD7F96110F9997ACA9792BDCB117ECD216FB6B9F7C9521508E64B41470E74B9EF9D999786DD0EB0F9A082909F5A7A8C5AF0503FBA20B311290EB233A79D42DBFFE22783C5787C33837B3D2D24A6825053E4CB5A46	None	1
79.183.127.115	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 79.183.127.115 (sigalgs DoS Attack)	None	1
31.210.178.143	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 41933ABCA35EC7FB562FC9EE594D16CAE45BC0D49BF893F548F8B01D72771F8B68DDC569A467BDD182EFC82D177278D37351C4917BDCA7089CA6AE0F5D10C5AE4006077685876538A8E0D3E934B3D3EEE426C44CEB98BED38E0DC12FC37302C15E5B6939FEB2641BDBC4E2C6D4FB88F2745C3895383CF246DD9B61CD6B452A2F, Observed AD517229673FB59E410BD66A49031F5CB1C276E9F00294D834FDFC90D4BE447E1F43772E1C8446937FB0E45C78DC1303654072C2688C3DFB692AFC3AC3E3C385BECB2D4E8905C5A682D54904EE6594FF98305DF15B594D5E26EC58DD1A59993917C63E	None	1
82.166.240.200	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
79.177.153.157	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
79.183.127.115	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
109.253.134.51	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
84.108.164.86	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 609C94B976D3BC068AC81FE328EB13D4544F4FBA069D25838966DAFF046817B00F8B7B33F65414FDD7945FB38D83D9E1878704CAA7D9E35E37D32FD38FE4ABF04B95D1376EEB8F57847E3396A8E2A23107B27785B96CF82CDC653D84D6303EE652E546F39DD7E13A9F97FA58D80237211DE8CF7A6A159A75241557BA48E8EE7F, Observed EAB047E3809C6852BB351789D45E7086ACE94E50E0496994A8067DD1F6232E55C0A72CD1F1E6FB631134D0B2EE7AF66B5121948F5ABD5BE8F038A3F8CF39D74C44959AC09C9AC351018F0754159F7E894290940D918E9540BBD171861B56967C59D679	None	1
87.69.184.109	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
80.246.138.188	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
185.13.194.76	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
79.182.6.160	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
2.54.59.25	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
93.173.238.182	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
81.218.131.214	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
79.177.153.157	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 79.177.153.157 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1