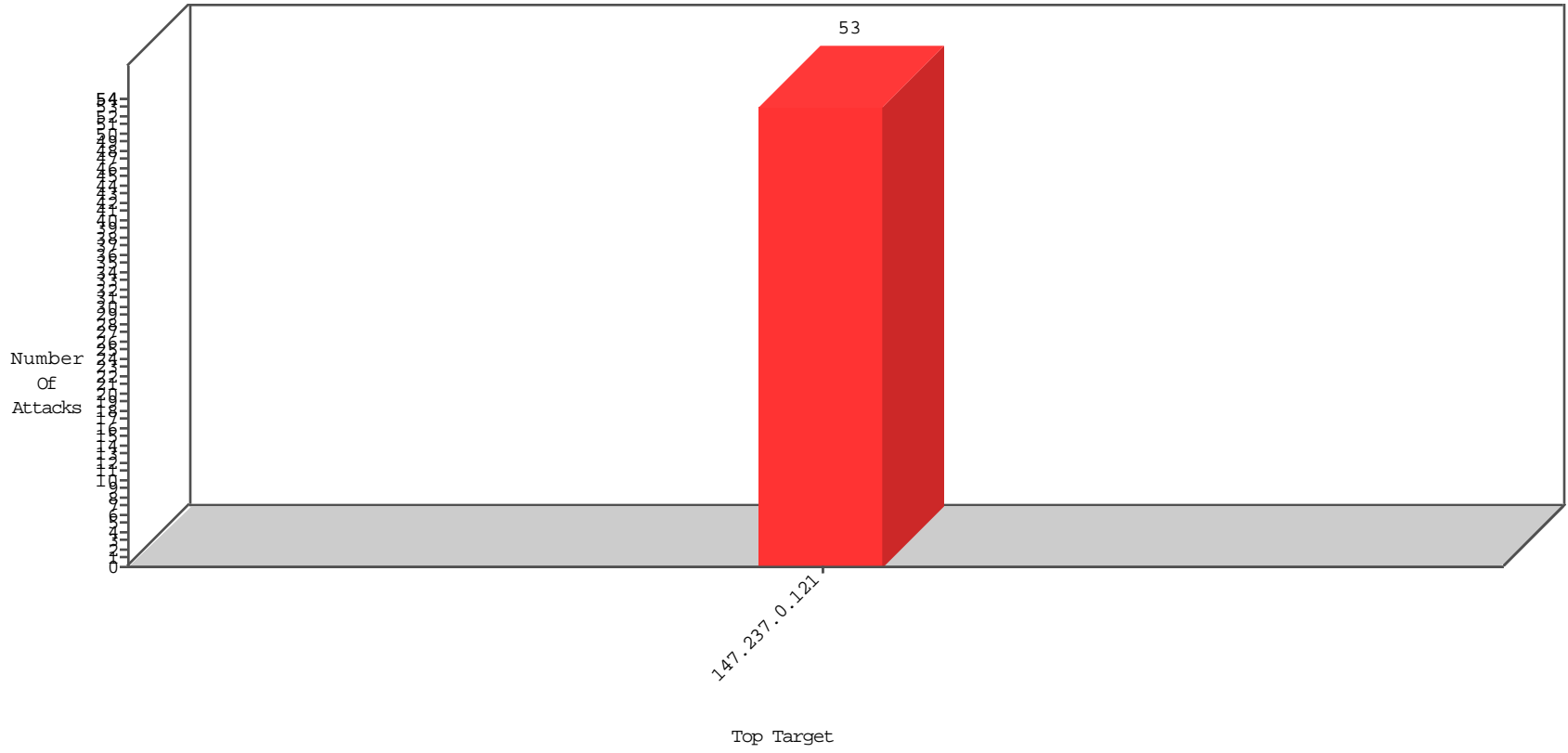


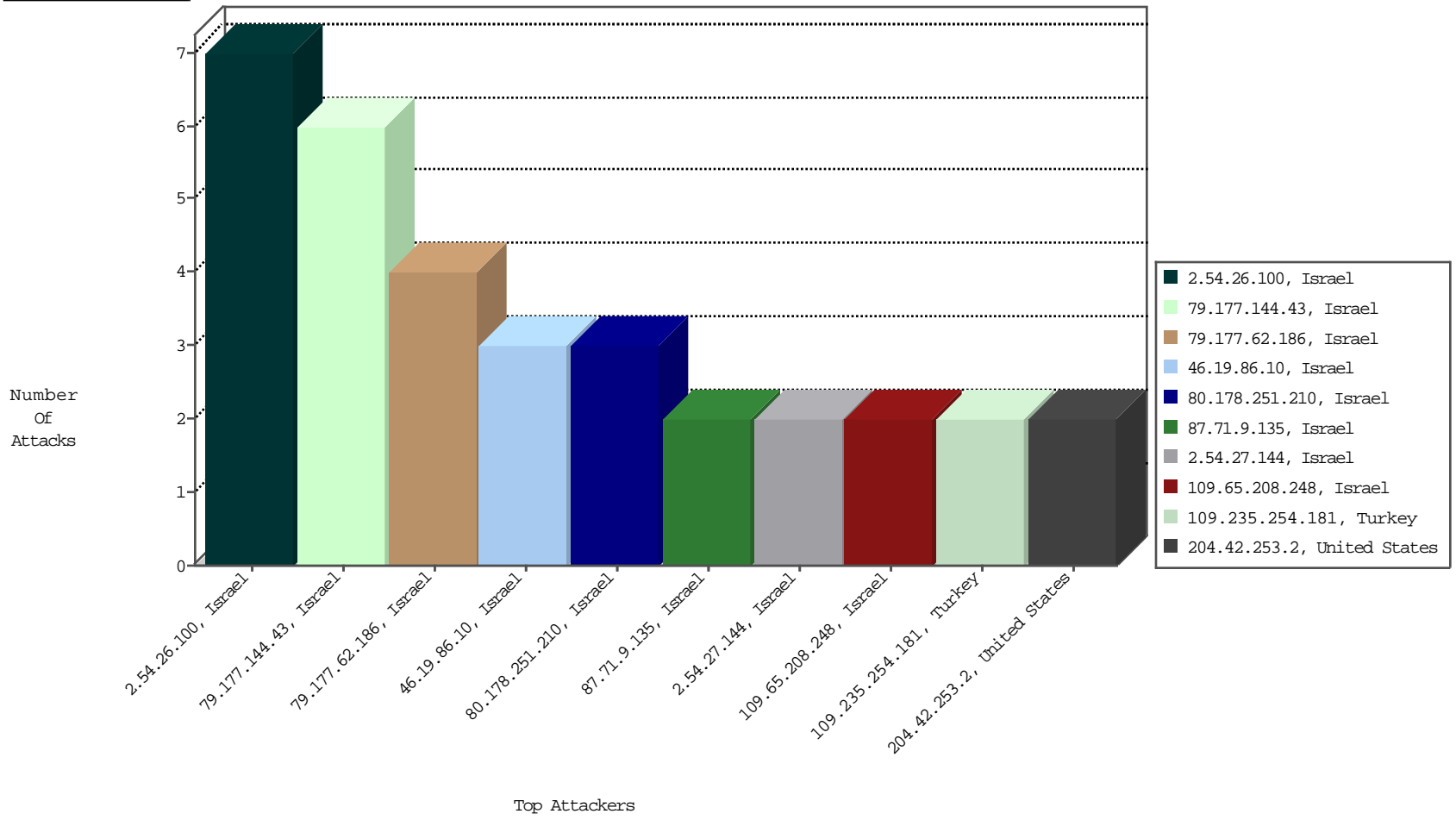
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
204.42.253.2	United States	147.237.0.121		Block_Ntp_All_Net	drop	NetV-London	2
198.23.165.141	United States	147.237.0.121		Block_Ntp_All_Net	drop	NetV-London	1

02-26-2016 to 02-27-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
------------------	--------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
109.235.254.181	Turkey	147.237.0.121		ET SCAN NMAP -sS window 2048	1
185.130.5.238		147.237.0.121		ET SCAN NMAP -sS window 1024	1
109.235.254.181	Turkey	147.237.0.121		ET SCAN NMAP -f -sS	1
162.248.141.24	Canada	147.237.0.121		ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
82.166.42.84	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1625
109.253.199.233	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	378
24.79.153.128	Canada	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	364
149.88.204.253	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	234
149.78.229.49	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	228
149.50.84.46	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	213
149.78.46.1	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	212
176.13.7.53	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	162
149.88.247.105	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	146
109.253.137.3	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
149.78.146.230	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	137
149.78.164.46	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	111
149.78.218.168	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	103
149.78.39.130	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	100
149.88.52.7	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	96
149.78.34.73	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	95
149.78.253.8	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	85
149.78.7.28	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	82
96.47.147.194	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	73
54.172.21.120	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	64
54.88.168.129	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	60
158.169.40.9	Belgium	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	59
149.78.98.21	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	56
149.78.232.87	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	54
84.108.3.7	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	54
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	48
149.78.247.58	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	48
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	48
40.77.167.37	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	47
12.21.46.2	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
2.52.170.148	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
79.181.96.54	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
149.78.103.29	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	31
141.0.14.197	Europe	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	31
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	29
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28
149.78.71.24	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
40.77.167.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	23
149.78.194.209	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	23
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
149.78.98.51	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	19
149.88.244.173	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
4.79.123.3	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
109.64.120.15	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	16
109.66.202.204	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	16
149.88.237.203	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13
46.19.86.96	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	11

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
2.54.26.100	Israel	147.237.0.121		Suspicious Response Code	Block	7
79.177.144.43	Israel	147.237.0.121		Multiple Unauthorized URL Access from 79.177.144.43	Block	4
80.178.251.210	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/changeunit	Block	3
79.177.62.186	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 79.177.62.186 (sigalgs DoS Attack)	None	3
87.71.9.135	Israel	147.237.0.121		Parameter Type Violation accept in www.miluum-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	2
46.19.86.10	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 46.19.86.10 (sigalgs DoS Attack)	None	2
79.177.144.43	Israel	147.237.0.121		PHP Attempt	Block	2
37.142.150.32	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 2C4C7ACE9A474CCC8AEE565030055BEE65A39D270B5CA59C0375D83B4396A48D338FF370055D7A792B3DD0022869FABEB04E6440B1179D13958B869480F7743316B61B1FE36533A300DF540910B09F405A4F83EA9E4E3E73E1AFBA9605123D2B31090F86EAFED3D3FF90830697333598E2348842C5EF32C651DF7FD61278C50, Observed AC3BE9712BC3CE7A82CFE07B2E352F8653E95D0E4426F61C86312675DD497730FCA96441B07F70C9C241499EB97B000E765FA28DF49D88BDE03DB757BCE6D971741CC9B503BC29B2A47AA8A24F940E2FFFFD9C5C42943192BBE5AEAC5255A9E86782AF	None	1
213.57.233.55	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/changeunit	Block	1
109.65.28.91	Israel	147.237.0.121		Parameter Type Violation accept in www.miluum-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
46.117.39.222	Israel	147.237.0.121		Parameter Type Violation accept in www.miluum-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
2.54.27.144	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluum-ishi.aka.idf.il/login	Block	1
109.186.185.57	Israel	147.237.0.121		Unauthorized HTTP Method	Block	1
79.177.62.186	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
37.142.202.225	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected NA, Observed BDD946E9B1112C7706CBF8B847184A03DC04663F323FE13767E7D86E019AD5E3AA229FFF8387A8CF482EEEC7C8DF8AEEA831455B3742FDF466EA8022D4593CB41D03C0439F7DB428DA0C3D2E3E8200ABEE40510ADC856D41667D5B852FD59D977E40078E654CC4137597E703110F73CA5FD02852E16041396D42696E64C55E9E5690600B0026FD81C5D833BD164882187CBCF76804C6E6AFC6F6E22DF2FDF22D	None	1
109.65.208.248	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 109.65.208.248 (sigalgs DoS Attack)	None	1
84.108.69.180	Israel	147.237.0.121		Suspicious Response Code	Block	1
46.120.190.244	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
2.54.27.144	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluum-ishi.aka.idf.il/login	Block	1
212.179.34.170	Israel	147.237.0.121		Suspicious Response Code	Block	1
93.172.0.41	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluum-ishi.aka.idf.il/generalpetition	Block	1
109.65.208.248	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
85.65.170.38	Israel	147.237.0.121		Unauthorized URL Access to www.miluum-ishi.aka.idf.il/https://www.miluum-ishi.aka.idf.il/	Block	1
79.177.52.97	Israel	147.237.0.121		Parameter Type Violation accept in www.miluum-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
5.29.95.197	Israel	147.237.0.121		Unauthorized URL Access to www.miluum-ishi.aka.idf.il/https://www.miluum-ishi.aka.idf.il/	Block	1
213.57.41.157	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	1
109.64.91.135	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
46.19.86.10	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
109.66.144.65	Israel	147.237.0.121		Parameter Type Violation accept in www.miluum-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
85.250.158.59	Israel	147.237.0.121		Unauthorized URL Access to www.miluum-ishi.aka.idf.il/	Block	1