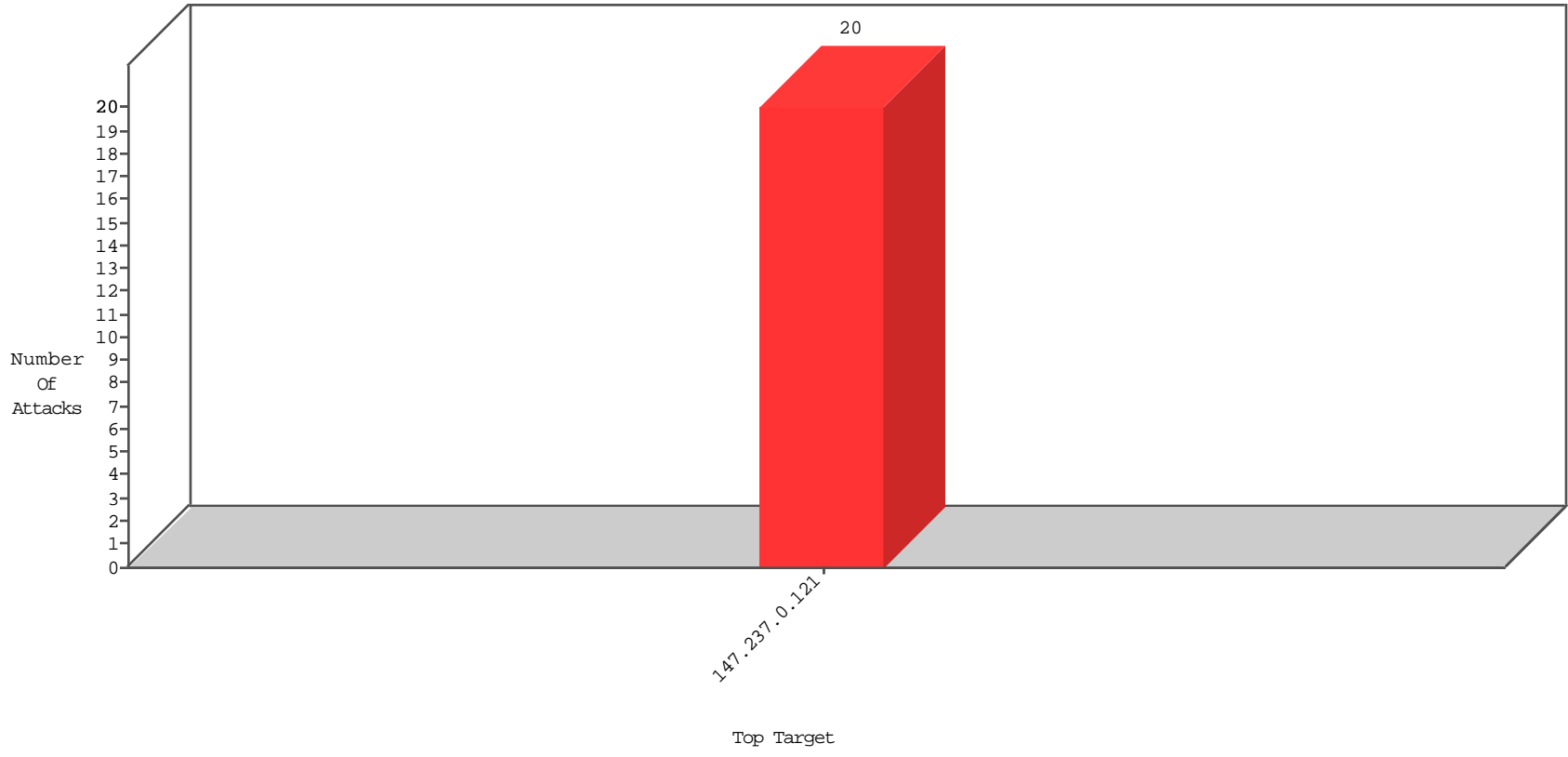


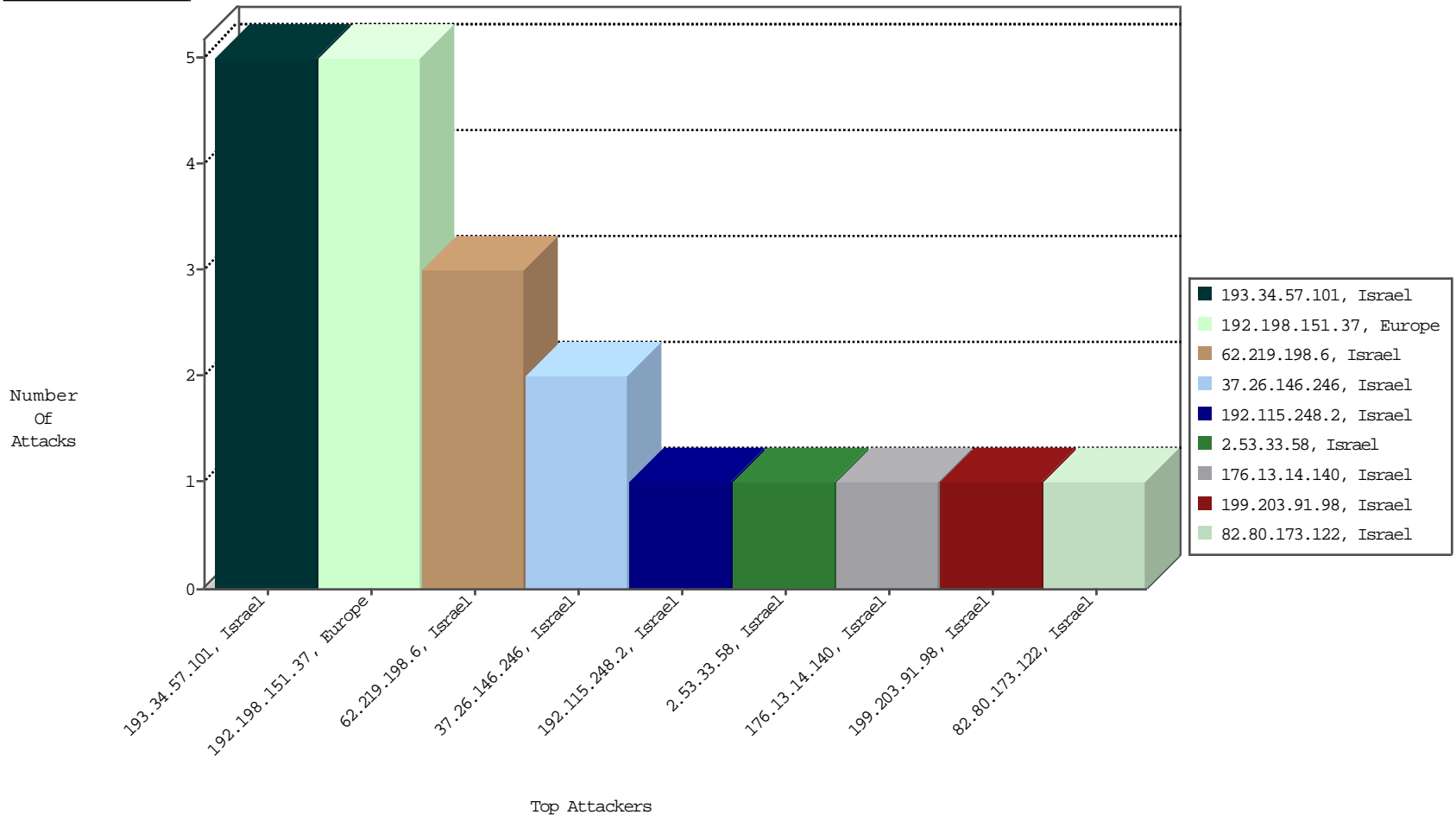
# Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
------------------	--------------	----------------	------	-----------	---------------	----------------------	-------

04-10-2016-14:06:02 to 04-10-2016-15:06:02

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
192.198.151.37	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	1

## Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site Name	Signature	Device Action	Count
62.90.66.8	Israel	147.237.0.121	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	738
167.220.196.142	United Kingdom	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	201
74.91.23.166	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	136
46.19.86.22	Israel	147.237.0.121	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	126
149.88.154.189	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	79
149.88.235.47	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	53
192.115.177.203	Israel	147.237.0.121	SYN Attack	SYN -> SYN-ACK -> RST	reject	50
130.119.13.66	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	47
23.81.90.154	United States	147.237.0.121	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
79.178.207.3	Israel	147.237.0.121	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
199.207.253.96	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	32
138.134.102.15	Israel	147.237.0.121	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
17.78.107.174	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	16
107.23.104.115	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	13
46.19.86.186	Israel	147.237.0.121	drop	SAM rule	drop	8
192.114.105.254	Israel	147.237.0.121	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
37.26.147.162	Israel	147.237.0.121	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.46.39.44	Israel	147.237.0.121	Bad TCP sequence	Invalid ACK number	monitor	3
66.102.6.90	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	2
85.130.173.109	Israel	147.237.0.121	Bad TCP sequence	Invalid ACK number	monitor	2
31.210.186.11	Israel	147.237.0.121	Bad TCP sequence	Invalid ACK number	monitor	1
212.143.186.38	Israel	147.237.0.121	Bad TCP sequence	Invalid ACK number	monitor	1
199.203.215.1	Israel	147.237.0.121	Bad TCP sequence	Invalid ACK number	alert	1
37.26.147.162	Israel	147.237.0.121	Bad TCP sequence	Invalid ACK number	monitor	1
5.22.135.144	Israel	147.237.0.121	Bad TCP sequence	Invalid ACK number	monitor	1
212.179.28.34	Israel	147.237.0.121	Bad TCP sequence	Invalid ACK number	monitor	1
192.114.105.254	Israel	147.237.0.121	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
91.135.102.184	Israel	147.237.0.121	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
199.203.215.1	Israel	147.237.0.121	Bad TCP sequence	Invalid ACK number	monitor	1
5.22.135.178	Israel	147.237.0.121	Bad TCP sequence	Invalid ACK number	monitor	1
218.22.211.69	China	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	1
31.154.5.110	Israel	147.237.0.121	Bad TCP sequence	Invalid ACK number	monitor	1
85.130.173.109	Israel	147.237.0.121	Bad TCP sequence	Invalid ACK number	alert	1
5.102.254.115	Israel	147.237.0.121	Bad TCP sequence	Invalid ACK number	monitor	1

## Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
192.198.151.37	Europe	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtNimuk in www.miluim-ishi.aka.idf.il/valtamrequest	Block	4
193.34.57.101	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	3
62.219.198.6	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	2
193.34.57.101	Israel	147.237.0.121		Cookie Injection on cookie .ASPXAUTH with value 6634499D9245918DBCA0C4E12A2ED6603511AACFC906FF3A98ECFE0BA069AD379CF5C2D84A03EDBB8459D9A6D13553C5AC8E1EA6B76EB39430A752F76C8C25D2C5C23309441A6401D858B06207C925052A01F79D6B7EAEFDB77F6ECE36DF810143186D814B407323C650999B19217576B2AAE46481252C5F53168FFF7E530B10ABAE2BB6E5434343CD52B68D45AF60AB68B97AED5749D8CB3BD4386F3FE8EC38	None	2
192.115.248.2	Israel	147.237.0.121		Unauthorized HTTP Method	Block	1
2.53.33.58	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/usercontrols/header/	Block	1
199.203.91.98	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
37.26.146.246	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 37.26.146.246 (sigalgs DoS Attack)	None	1
82.80.173.122	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
37.26.146.246	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
176.13.14.140	Israel	147.237.0.121		Double URL Encoding - parameter: returnUrl in www.miluim-ishi.aka.idf.il/login	Block	1
62.219.198.6	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected D26D2DB60FE45154CF53E1EE742C444F22A14CA58C3494A7E082A74C52FF071555172248A9005D49E823CD8D28A10FC4678B068B699C710A3F49F6838A38A2A74ECC41320B0ED877B137064A972A1670FE95C6652FF091A33058943BCF0E8FB70C55DFFAB7BC1BEC76F2BB54E4E3936BD33B5C205326160684545E970EC69493, Observed 48580DA06B3BF385F5DEB3C1FAF35B25287A6A06127E59A70BA612BACAEF272DBACBD9ECDE4AA7EF01D011085CB46C82FBE71ACC8614BA89358186F071504173720A9B4B19F8FCAFCF749EE560329CC5E24D93714AA0801F8E1BDBC71118F21718332D	None	1