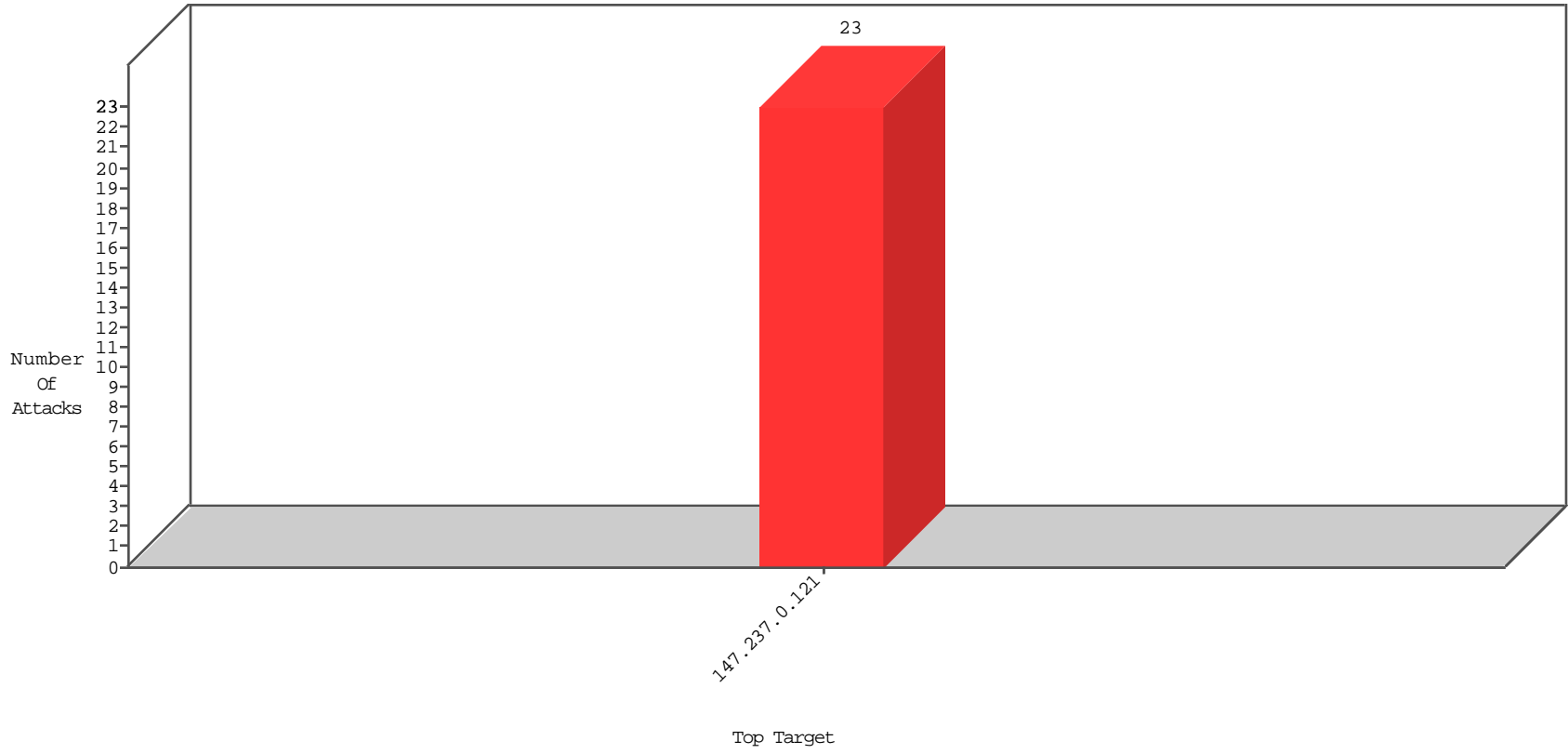


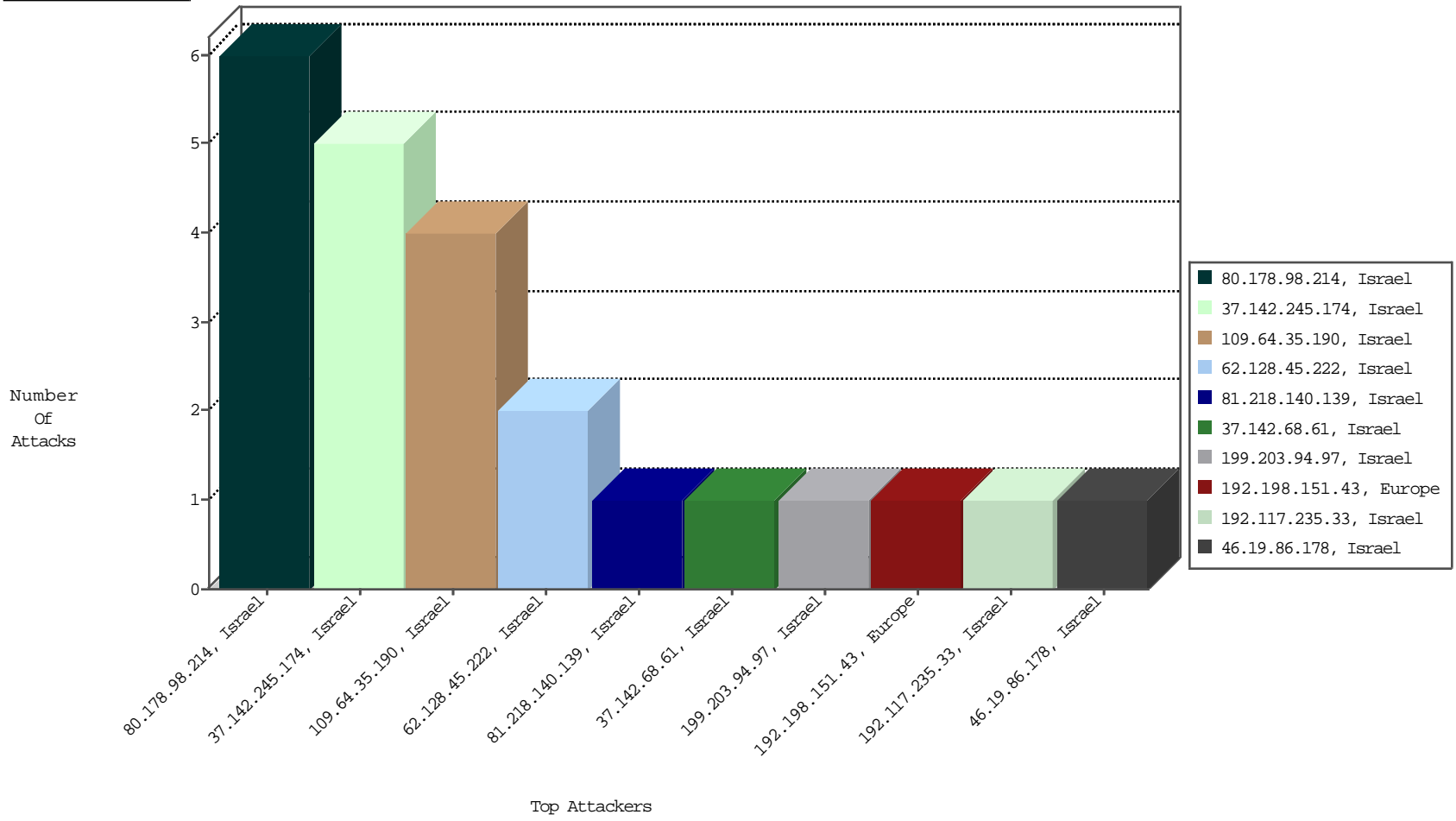
# Focused IP Under Attack Daily Report



## Top Targets



## Top Attackers



Top Attackers In DDoS-Defence

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

04-17-2016-10:06:00 to 04-17-2016-11:06:00

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
------------------	--------------	----------------	------	-----------	-------

## Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
194.9.252.237	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	598
82.80.26.75	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
46.16.142.100	Cyprus	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	149
149.88.60.169	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	143
149.88.53.163	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	93
149.88.166.35	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	88
17.78.105.88	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	83
192.115.177.203	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	61
149.88.253.59	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	46
199.203.93.50	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	40
149.88.138.66	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	40
149.88.44.191	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	40
193.109.196.137	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	40
17.78.122.217	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
192.116.176.221	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	28
199.203.93.50	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	24
81.218.241.26	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	17
79.181.230.241	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
217.68.8.59	Germany	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	14
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	12
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	11
37.46.39.132	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	11
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	9
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	8
94.230.86.201	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	4
62.219.154.108	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
62.219.154.108	Israel	147.237.0.121		Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
5.22.130.73	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	3
84.228.72.198	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
79.177.188.62	Israel	147.237.0.121		Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
5.22.129.236	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
212.150.71.177	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	1
46.19.86.113	Israel	147.237.0.121		Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
212.150.71.177	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
80.179.69.252	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
5.29.116.35	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	1
82.80.214.228	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
79.177.188.62	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
212.235.69.34	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.246.140.50	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.29.116.35	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
199.203.226.21	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	1

## Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
37.142.245.174	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/shamapchange parameter ct100\$ContentPlaceholder1\$txtPerutBakasha	Block	5
80.178.98.214	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceholder1\$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	5
109.64.35.190	Israel	147.237.0.121		Parameter Type Violation ct100_ContentPlaceholder1_fuAddStudyPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/uploadregister.axd	Block	3
62.128.45.222	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
109.64.35.190	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceholder1\$txtPermitFilesNames in www.miluim-ishi.aka.idf.il/valtamrequest	Block	1
199.203.94.97	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceholder1\$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
80.178.98.214	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected DBB40F2C2912C02679E426A846C19B99066CE247D2CE5C2E32695E9261D46F3FABD011DD443281FE20933E8926ADCDB7A0E9E5726117C5C0C5B55726EFF8DD7B52C191F63B890583AEF51913E0955E51C1192D02D6BF511E5B07DE46F3C23E1CA2B9DB62C95A9AD9615DE4EECC25BBCA6D08FAC1ACE2FB0E1DE16550D3086D, Observed 6E30FEAA8F4D8A474E70E5FF969F3FA03DDC71D3EDDA1F2A7CBAA84A9D57FD88E2B4F63D736481DC8A2D3BFFEF0B1661C084D494754BB6F30C5CE1A9BB31EBB1552B1B7284966E8BD30F4F82FCE7607360C3E69095607EF6B3F027CB438BE663F0A3A7	None	1
46.19.86.178	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceholder1\$ct100 in www.miluim-ishi.aka.idf.il/form3010	Block	1
192.117.235.33	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceholder1\$txtPerutBakasha	Block	1
62.128.45.222	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 62.128.45.222 (Open Mode)	None	1
81.218.140.139	Israel	147.237.0.121		Parameter Type Violation ct100_ContentPlaceholder1_fuAddAddressAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
37.142.68.61	Israel	147.237.0.121		Distributed Unauthorized URL Access on www.miluim-ishi.aka.idf.il/https://www.miluim-ishi.aka.idf.il/	Block	1
192.198.151.43	Europe	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceholder1\$ct100\$txtOldPass in www.miluim-ishi.aka.idf.il/personalsettings	Block	1