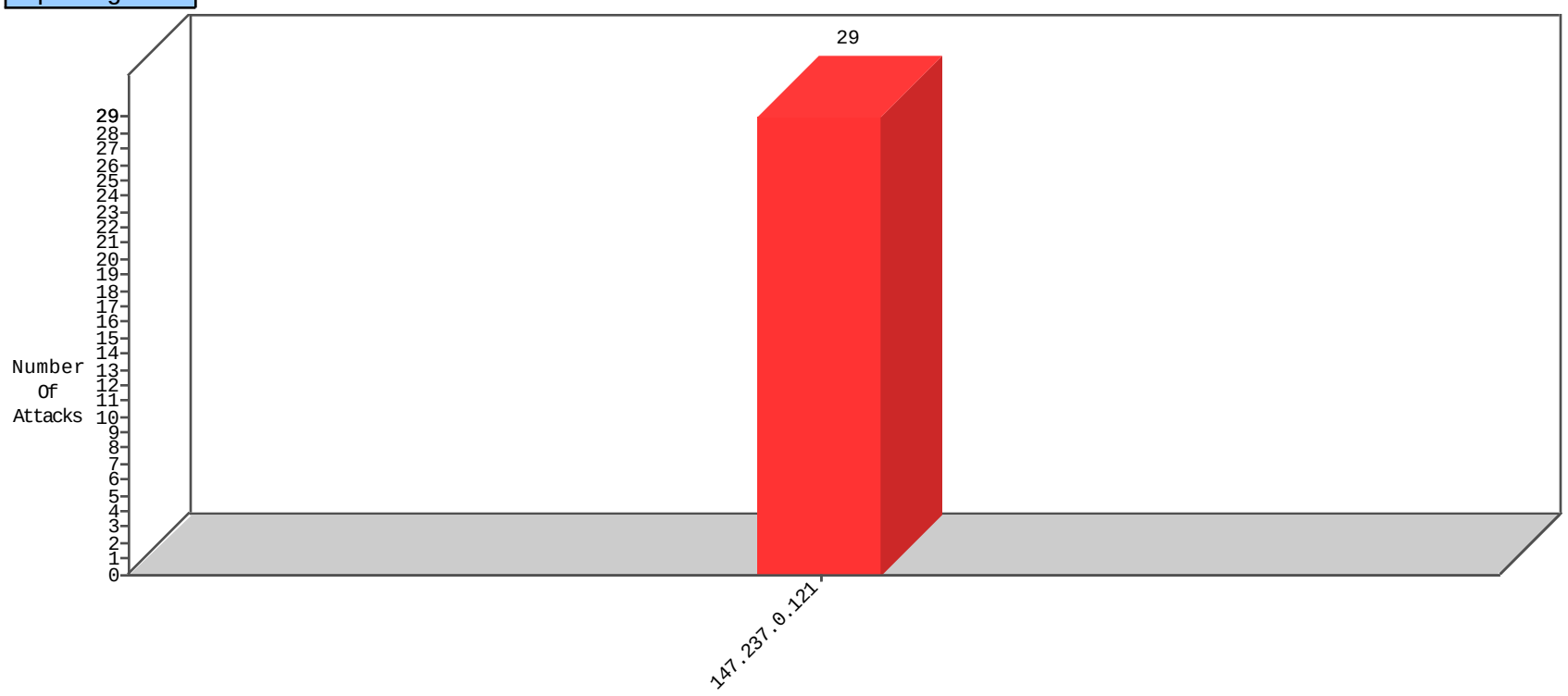
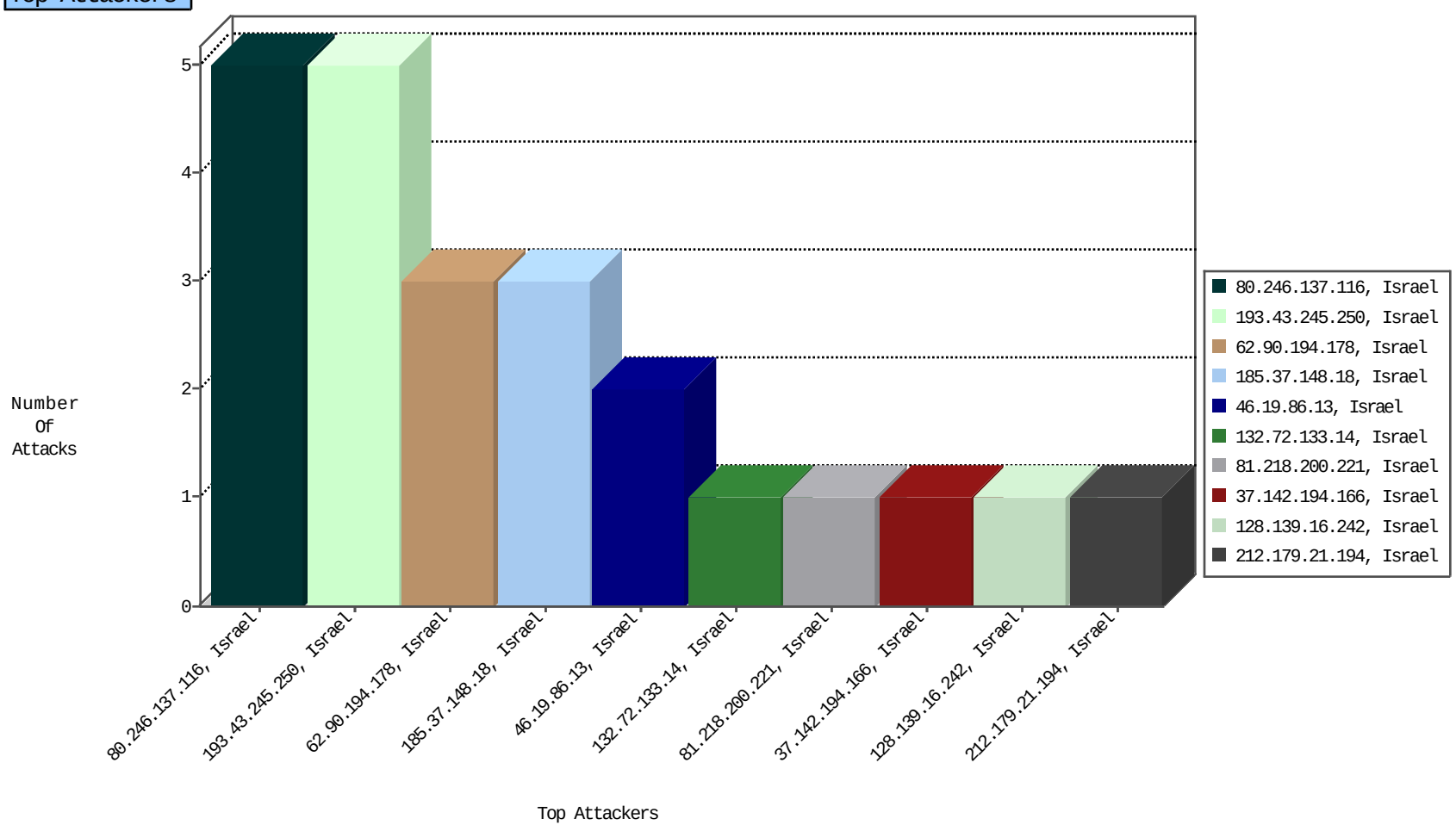
04-20-2016-11:06:00 to 04-20-2016-12:06:00

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



04-20-2016-11:06:00 to 04-20-2016-12:06:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
80.246.137.116	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	5

04-20-2016-11:06:00 to 04-20-2016-12:06:00

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

04-20-2016-11:06:00 to 04-20-2016-12:06:00

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
185.37.148.18	Israel	147.237.0.121		ET SCAN NMAP -sA (2)	1

04-20-2016-11:06:00 to 04-20-2016-12:06:00

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
194.9.253.237	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	253
167.220.196.227	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	165
80.246.137.116	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
74.125.122.49	Europe	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	74
46.16.142.100	Cyprus	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	73
74.91.23.166	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	71
192.146.6.2	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	68
195.110.137.138	Italy	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	54
81.218.198.64	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	32
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
66.102.9.50	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
54.240.197.226	Ireland	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13
108.171.133.166	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	12
108.171.128.166	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	12
209.126.117.15	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	10
46.19.85.150	Israel	147.237.0.121		Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
212.199.69.1	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	9
149.50.81.224	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
54.240.197.227	Ireland	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	9
37.26.149.128	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	9
37.46.41.42	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	4
2.53.170.100	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	4
185.3.147.3	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	2
91.197.61.250	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	2
5.29.185.31	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	2
5.29.185.31	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	2
31.168.13.78	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	1
5.22.131.61	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.234	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1
91.197.61.250	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	1
5.29.155.53	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.90	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
31.168.13.78	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
5.29.101.25	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	1
31.210.186.59	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
5.29.101.25	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
106.184.3.122	Japan	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.150	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
212.179.21.194	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.22.130.99	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
84.111.225.218	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
5.29.155.53	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	1

04-20-2016-11:06:00 to 04-20-2016-12:06:00

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
193.43.245.250	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	5
46.19.86.13	Israel	147.237.0.121		Distributed Unauthorized URL Access on www.miluim-ishi.aka.idf.il/usercontrols/header/	Block	2
62.90.194.178	Israel	147.237.0.121		Multiple Unauthorized URL Access from 62.90.194.178	Block	2
109.66.32.11	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
185.37.148.18	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/newpassword/	Block	1
81.218.200.221	Israel	147.237.0.121		Distributed Unauthorized URL Access on www.miluim-ishi.aka.idf.il/usercontrols/header/	Block	1
31.168.175.226	Israel	147.237.0.121		Distributed Unauthorized URL Access on www.miluim-ishi.aka.idf.il/usercontrols/header/	Block	1
128.139.16.242	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNimuk in www.miluim-ishi.aka.idf.il/valtamrequest	Block	1
46.19.86.185	Israel	147.237.0.121		Distributed Unauthorized URL Access on www.miluim-ishi.aka.idf.il/usercontrols/header/	Block	1
82.166.227.17	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddStudyEmploymentPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
31.210.186.59	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/shamapchange	Block	1
132.72.133.14	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
212.179.21.194	Israel	147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	1
109.64.195.92	Israel	147.237.0.121		Distributed Unauthorized URL Access on www.miluim-ishi.aka.idf.il/usercontrols/header/	Block	1
37.142.194.166	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 0821277D5612C1C242E996282AD5C4CB170DA7254ACCC053E4916AB78D5A4AF82F061FC30641444710169A5B59EF12B9EEAB097D4C95226647F793983FBED2EC95638F459E5448DAAF498EA34F283D8BC1302BD2F75840A618B327C00EA1D13A06CDBC715C17C6DC487FF1C9EDDB2DF37A939C4AA3DF23460BA6313DAA2768C3, Observed EC1A44D4D44ABEADC54E833CE1CCAE0BC11BAFBD8314D2A0DD2A495965257259D32A6BB21A7456941EE7F501D2979889347BE0303B20904D720586A18D7D87A925FBC81A69E506BBCB06C430558B1270A1FF98C1E6C4F858AE2D6F6B1F445E91B3AEDC	None	1
185.37.148.18	Israel	147.237.0.121		Multiple Unauthorized URL Access from 185.37.148.18	Block	1
62.90.194.178	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/newpassword/	Block	1

04-20-2016-11:06:00 to 04-20-2016-12:06:00