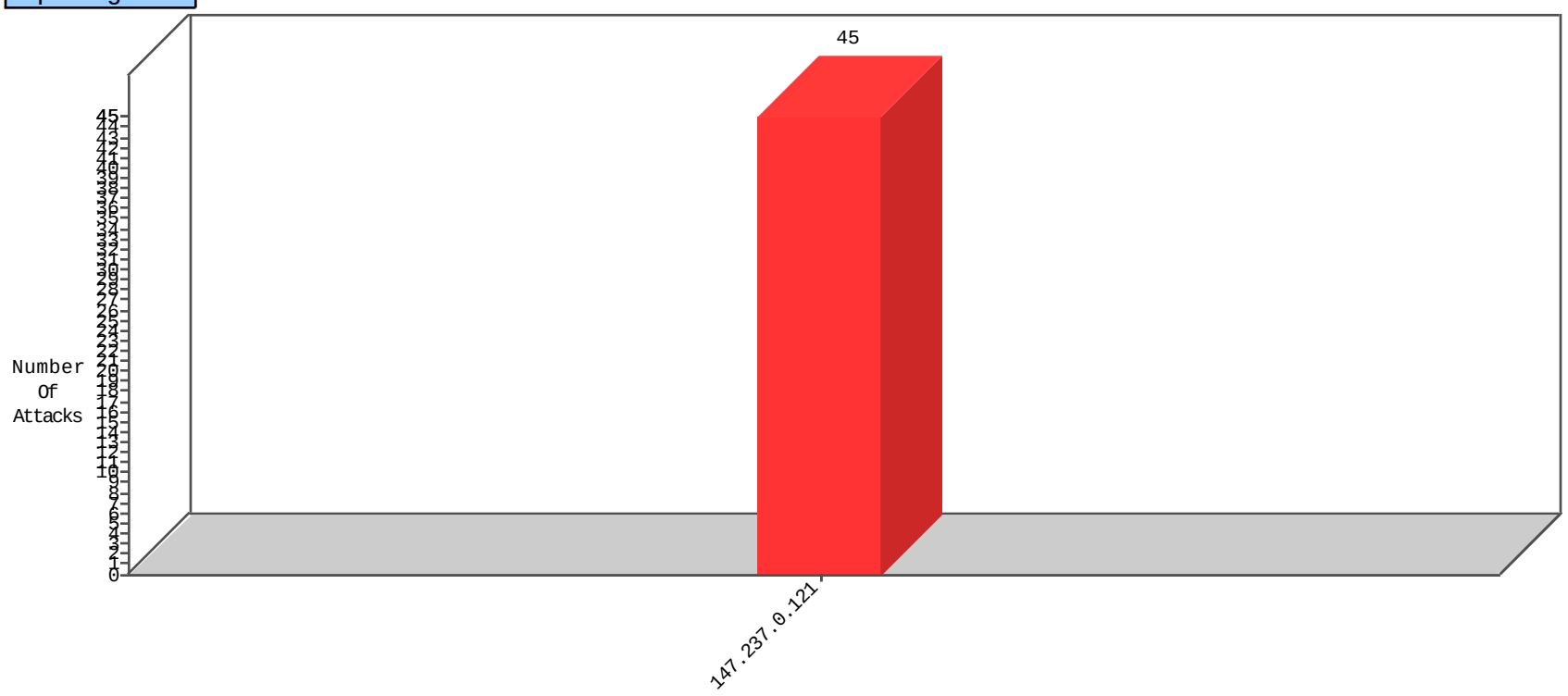
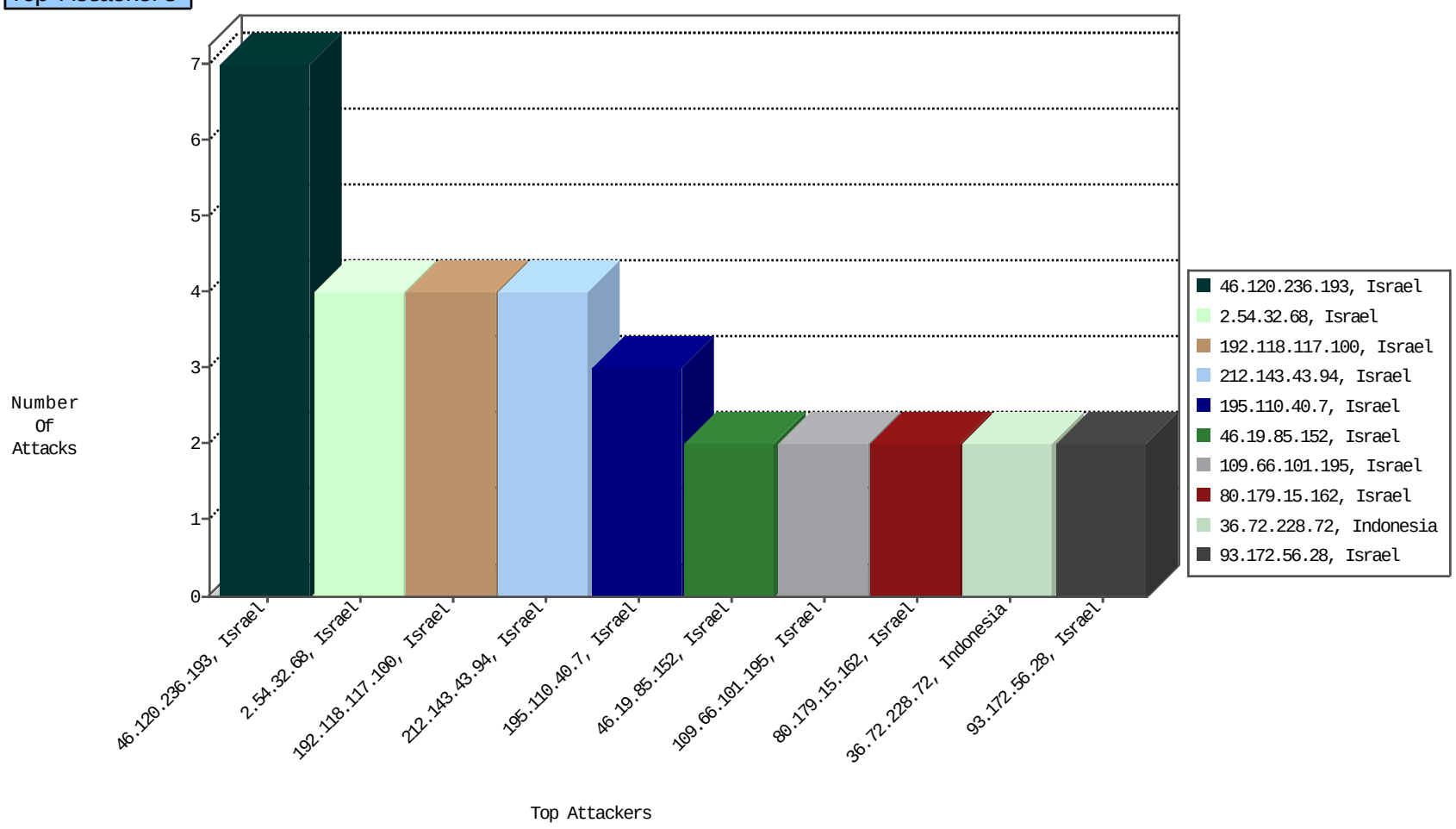
11-22-2015 to 11-23-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



11-22-2015 to 11-23-2015

Top Attackers In DDoS-Defence

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

11-22-2015 to 11-23-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

11-22-2015 to 11-23-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
36.72.228.72	Indonesia	147.237.0.121		ET SCAN NMAP -sS window 3072	1
42.159.26.35	China	147.237.0.121		ET SCAN Potential SSH Scan	1
104.219.238.10		147.237.0.121		ET SCAN Potential SSH Scan	1
113.108.21.16	China	147.237.0.121		ET SCAN Potential SSH Scan	1
222.21.43.56	China	147.237.0.121		ET SCAN Potential SSH Scan	1
36.72.228.72	Indonesia	147.237.0.121		ET SCAN NMAP -sS window 4096	1
43.229.53.89	Japan	147.237.0.121		ET SCAN Potential SSH Scan	1
109.251.56.171	Ukraine	147.237.0.121		ET SCAN NMAP -sS window 1024	1
192.198.151.44	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	1

11-22-2015 to 11-23-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.154	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	4245
66.249.93.146	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	4226
66.249.93.150	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	3723
92.69.247.242	Netherlands	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	776
149.78.147.185	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	747
64.79.85.205	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	500
199.201.66.0	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	473
66.249.93.150	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	364
66.249.93.154	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	344
66.249.93.146	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	287
77.248.233.109	Netherlands	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	172
13.17.125.9	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	113
81.218.174.57	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	80
149.78.30.195	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	75
54.243.190.43	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	74
149.88.7.101	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	72
177.32.211.92	Brazil	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	66
13.21.125.9	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	66
149.78.232.189	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	65
66.249.82.147	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	52
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	51
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	50
66.102.9.50	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	50
192.115.177.203	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	49
149.78.164.41	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	48
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	48
200.46.160.83	Panama	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
149.78.231.61	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
66.249.81.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	42
149.88.86.121	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	41
138.134.102.16	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	37
84.228.233.27	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
192.115.177.202	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	36
149.88.149.123	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	35
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	33
66.102.7.172	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	32
66.102.9.39	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28
66.102.9.44	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28
66.249.93.224	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
66.249.93.244	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
192.114.105.254	Israel	147.237.0.121		Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	26
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
149.78.38.162	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
149.88.216.249	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	24
66.249.93.241	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
66.102.9.22	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
209.135.211.201	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22

11-22-2015 to 11-23-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
46.120.236.193	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/valtamrequest parameter ctl00$ContentPlaceHolder1$txtNimuk	Block	4
212.143.43.94	Israel	147.237.0.121		Unauthorized HTTP Method	Block	4
192.118.117.100	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	4
195.110.40.7	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	3
2.54.32.68	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/valtamrequest parameter ctl00$ContentPlaceHolder1$txtNimuk	Block	3
93.172.56.28	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtId in www.miluim-ishi.aka.idf.il/login	Block	2
80.179.15.162	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	2
46.19.85.152	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected FF2F9C0BC2BB3AF09B1E8AB2CA313DC896308CD7987D9B6FC4879522B85763AFB53CCBEC578EF4820E9D65D9C399AA6DC743F87DE1CE4849C72160E7059EE37CCFB2B8467A746613AD0D106B6AE1B78F4737E659640E921C81375324F4E5D999DA48F3004F21BAD478A24F5F357EB0988FFA0C7AE07EE392C168E171563D2601, Observed 4CA8DF67B05A64D9E749E386AC14FE7BA0CA9A78D71C50A61B35A94FFC8874A9614BD4125606BDB7A452100AF534D08A66FF400F6BE7CE0690621C2488FA7857D0A82B8FF97D99036DF53CB708951C25152B8293232A9A6870E6E0FDABD28AC7E04182	None	2
109.66.101.195	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
46.120.236.193	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddTimetableDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
2.54.32.68	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected , Observed 7A0112D0F6FBA991E1A276739E376026AE26EBFEBF3AB3179B5CD348E04A55BEC170CAB97E4D7418D7FC62F98EA95FD050AFDE7C5F127453994F61CCBFCA82505D2193B8555218C2F15E31BD5AC63573CF17E421E558283ED467CC4FDFC03D6F4B73148291A6490C9289D9467A86A63E5B667977561E5B833E5383DB2A0B1902698981E002CD3F30CC873DB61575705AF2A6072392321EE7A64C4BEF7C9582F4	None	1
85.64.159.154	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected , Observed 39900DE553498A7BCF56CBF896CAE2CCC5362C9F34B8520F9735A23198B06FDA68EABAB75548644E7751B76B0822448CFC67FEB5A3ACF8336CC4EC91AAFB9C85933751F0ABDCFA2B7A68CAB420B5F7930852C0F377499A2892B62BFC4C47414CEB5D71CC99DEC658EA737FC3EBAC8DF7B8246F76E8EADCB0E38E6F73ADCE9725DBB8296F777986F8C32A80ADEE7BDE1545FB016626CA5B02411F1DC58DE2AFDF	None	1
109.186.167.99	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
79.183.21.232	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
46.120.236.193	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNimuk in www.miluim-ishi.aka.idf.il/valtamrequest	Block	1
176.13.2.174	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 023DBB759E4799AC319ADC328DC3C0FE5392C9FEC401256E781D59D2C2B782A6AB879D9426AB0EA6343BD2CDDDA644B218C4BA1060480C8CD21DE083A7D5C6251D8BFB6D7CFE7CA2ACB8DE8337B7904C396DA0FEFA82C4C23D2551B94CD10C830410807AF5A11C72F625753191E7885C4D8F432E2D601D7588C31677B732FF51, Observed 18289FC5E3043D4B5A7395B8BFC67B7508C10DD92050ADB197D68329E7A703CE613928068C8EFA092238E8356325214441F438CD80FB2B026FB7606A7D3C4154165A3538D76DB67FED93D3FECA46F66275817EE89F9B67D93B4EB366762747D8464486	None	1
31.210.186.225	Israel	147.237.0.121		Unknown Parameter tzav in www.miluim-ishi.aka.idf.il/login	Block	1
109.66.101.195	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddIDCardDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
46.120.236.193	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddStudyPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
80.179.37.165	Israel	147.237.0.121		Unknown Parameter tzav in www.miluim-ishi.aka.idf.il/login	Block	1

11-22-2015 to 11-23-2015