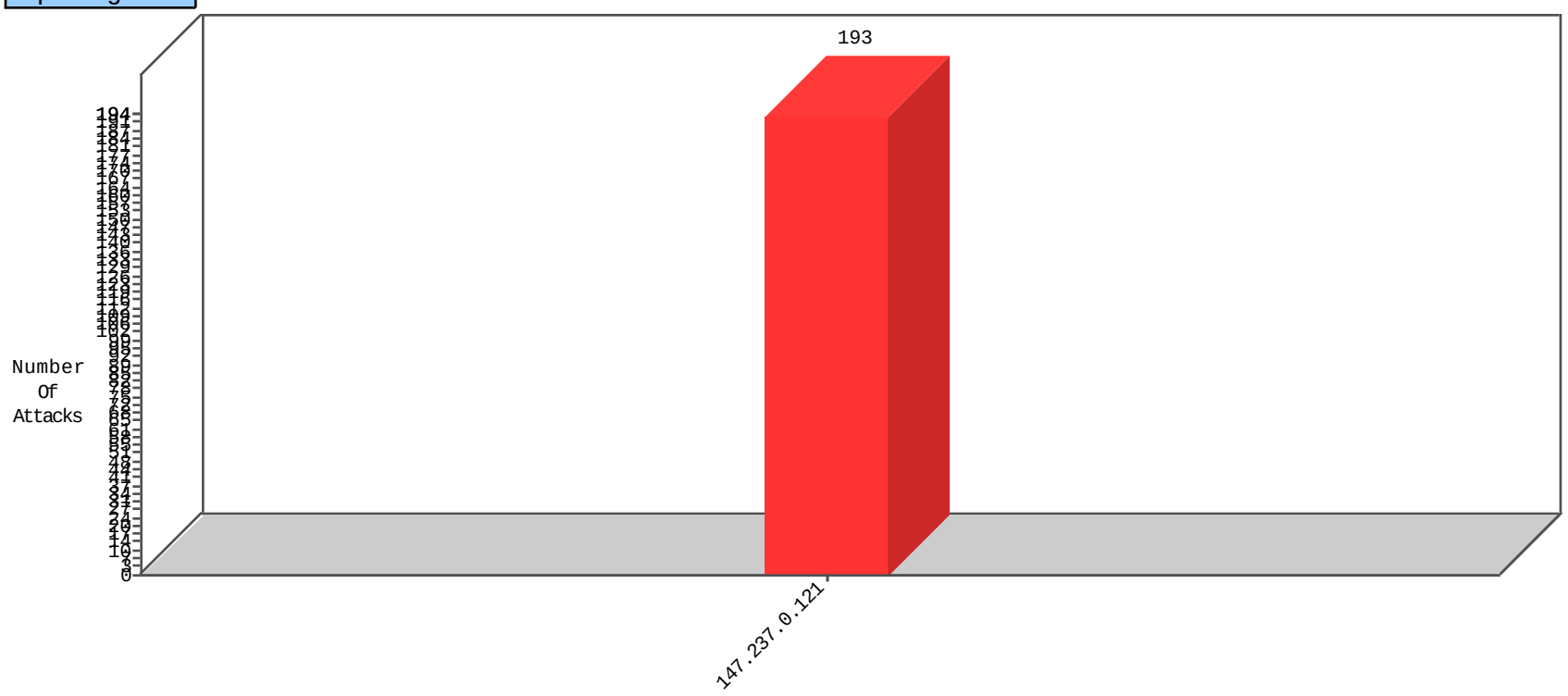
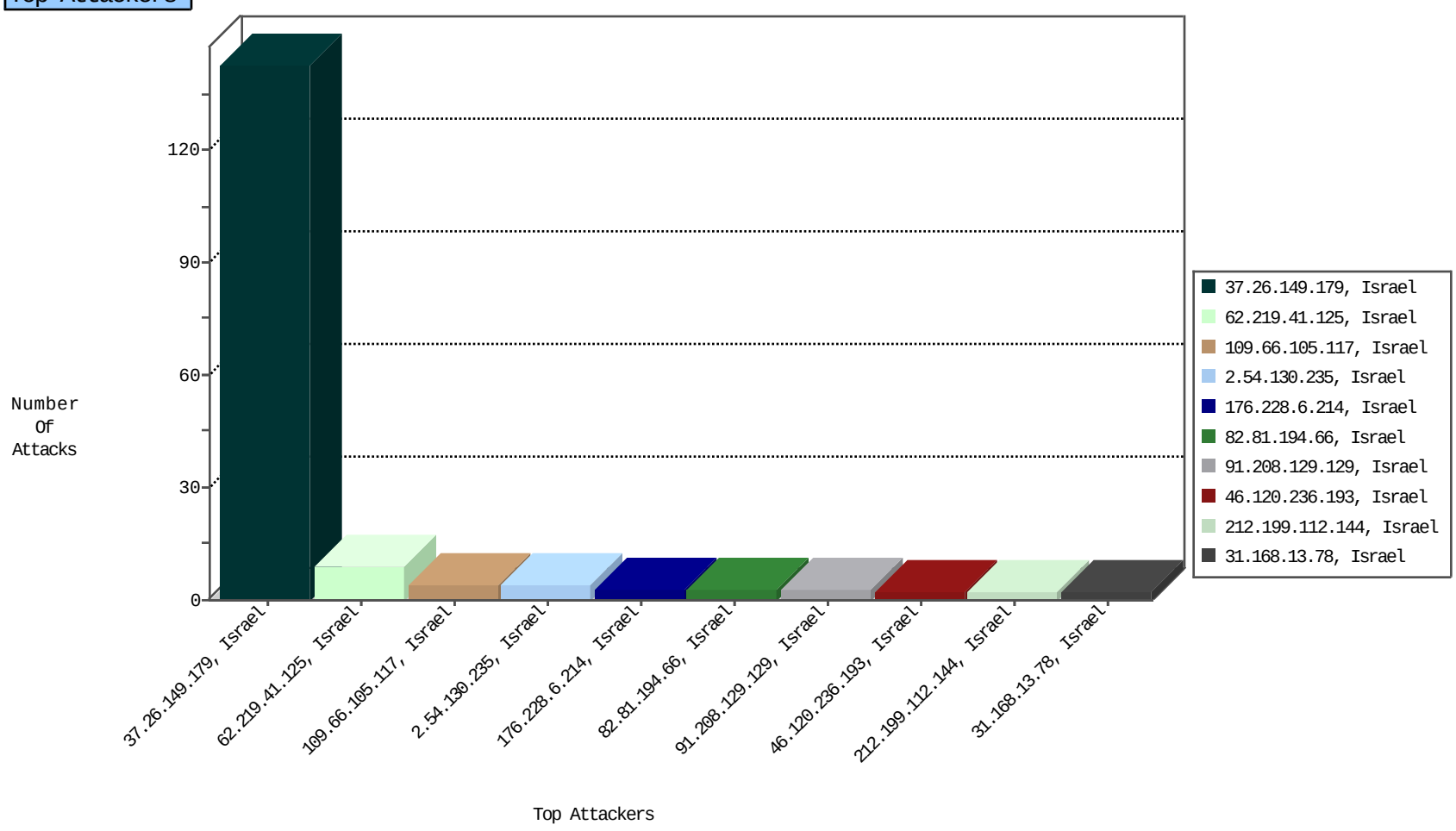
11-23-2015 to 11-24-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



11-23-2015 to 11-24-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
37.26.149.179	Israel	147.237.0.121		Anomaly-TLS-renegotiation-Cli	dest-reset	BBL-Israel	140
91.208.129.129	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3
178.62.126.13	United States	147.237.0.121		Frk_Under_Attack_Con_Tcp	drop	BBL-Frankfurt	2

11-23-2015 to 11-24-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

11-23-2015 to 11-24-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
59.45.79.117	China	147.237.0.121		ET SCAN Potential SSH Scan	1
74.117.209.135	United States	147.237.0.121		ET SCAN NMAP -sS window 1024	1

11-23-2015 to 11-24-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.146	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	4180
66.249.93.150	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	3558
66.249.93.154	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	3331
64.79.85.205	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	536
46.19.85.48	Israel	147.237.0.121		Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	363
66.249.93.150	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	306
46.19.85.48	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	298
66.249.93.146	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	286
66.249.93.154	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	279
92.69.247.242	Netherlands	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	270
149.88.189.227	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	260
149.78.228.38	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	201
40.129.98.162	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	146
2.54.159.165	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.54.135.111	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
149.88.219.42	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	108
149.78.235.159	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	103
46.19.86.62	Israel	147.237.0.121		Bad TCP sequence		monitor	100
149.88.202.196	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	100
46.164.156.174	Ukraine	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	90
149.88.186.52	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	90
66.249.66.109	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	82
46.19.85.48	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	alert	81
15.203.233.78	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	79
201.85.85.123	Brazil	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	74
149.88.109.230	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	64
201.31.215.129	Brazil	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	62
66.249.81.130	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	62
149.78.22.6	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	62
85.250.81.228	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	58
66.249.81.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	56
149.78.248.164	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	51
149.78.27.42	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	50
66.102.9.61	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	49
66.249.66.107	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	48
149.78.231.61	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
149.78.42.7	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
66.102.7.179	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	44
94.223.148.170	Germany	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	41
88.3.78.146	Spain	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	40
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	40
66.249.93.224	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	40
173.234.233.203	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
149.78.157.242	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
2.52.3.235	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	37
46.19.86.42	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	37
66.249.81.251	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	35
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	33

11-23-2015 to 11-24-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
62.219.41.125	Israel	147.237.0.121		Multiple Unauthorized URL Access from 62.219.41.125	Block	9
109.66.105.117	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/ufi/reaction/	Block	4
2.54.130.235	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	4
176.228.6.214	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$ctl00$txtNewPass1 in www.miluim-ishi.aka.idf.il/personalsettings	Block	3
82.81.194.66	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	3
37.26.149.179	Israel	147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	3
46.120.236.193	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNimuk in www.miluim-ishi.aka.idf.il/valtamrequest	Block	2
132.64.217.110	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$ctl00$txtOldPass in www.miluim-ishi.aka.idf.il/personalsettings	Block	1
31.154.5.181	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/medicalcommitteerequest parameter ctl00$ContentPlaceHolder1$txtFilesNames	Block	1
212.179.62.20	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
85.65.80.198	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
212.199.112.144	Israel	147.237.0.121		Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login	Block	1
81.218.55.253	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
31.168.13.78	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 31.168.13.78 (Unknown SSL Session)	None	1
212.199.34.114	Israel	147.237.0.121		Distributed Unknown Parameter on www.miluim-ishi.aka.idf.il/login parameter ch	Block	1
93.172.171.169	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
46.121.113.242	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
2.54.32.164	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected , Observed 9E9069DE1B2D1294D3B573151AB70845DF48540995B4C15C2AD078B8731D98B3196995C011D1E056948FE9C359C44B93430A42BF2C0E5F807989B594D4B4785DB693DFA829A98F3487EEB1BE1800865B13DE6884A363F56AA933B764F5B3FC12E7DFE05132F0F11A08A261FC4D451F8CFC0CAB600BE57E634DEDED3DCF8151480A182E01224534C23FB783F2A0843BB68D849AE90F51AA3EB7B83862B3EA8BFC	None	1
192.118.10.10	Israel	147.237.0.121		Parameter Type Violation ReturnUrl in www.miluim-ishi.aka.idf.il/login	Block	1
31.168.13.78	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
212.199.57.205	Israel	147.237.0.121		Unknown Parameter ch in www.miluim-ishi.aka.idf.il/login	Block	1
62.128.45.222	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
212.117.136.6	Israel	147.237.0.121		Distributed Unknown Parameter on www.miluim-ishi.aka.idf.il/login parameter prm	Block	1
83.130.100.207	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
212.199.112.144	Israel	147.237.0.121		Unknown Parameter ch in www.miluim-ishi.aka.idf.il/login	Block	1

11-23-2015 to 11-24-2015