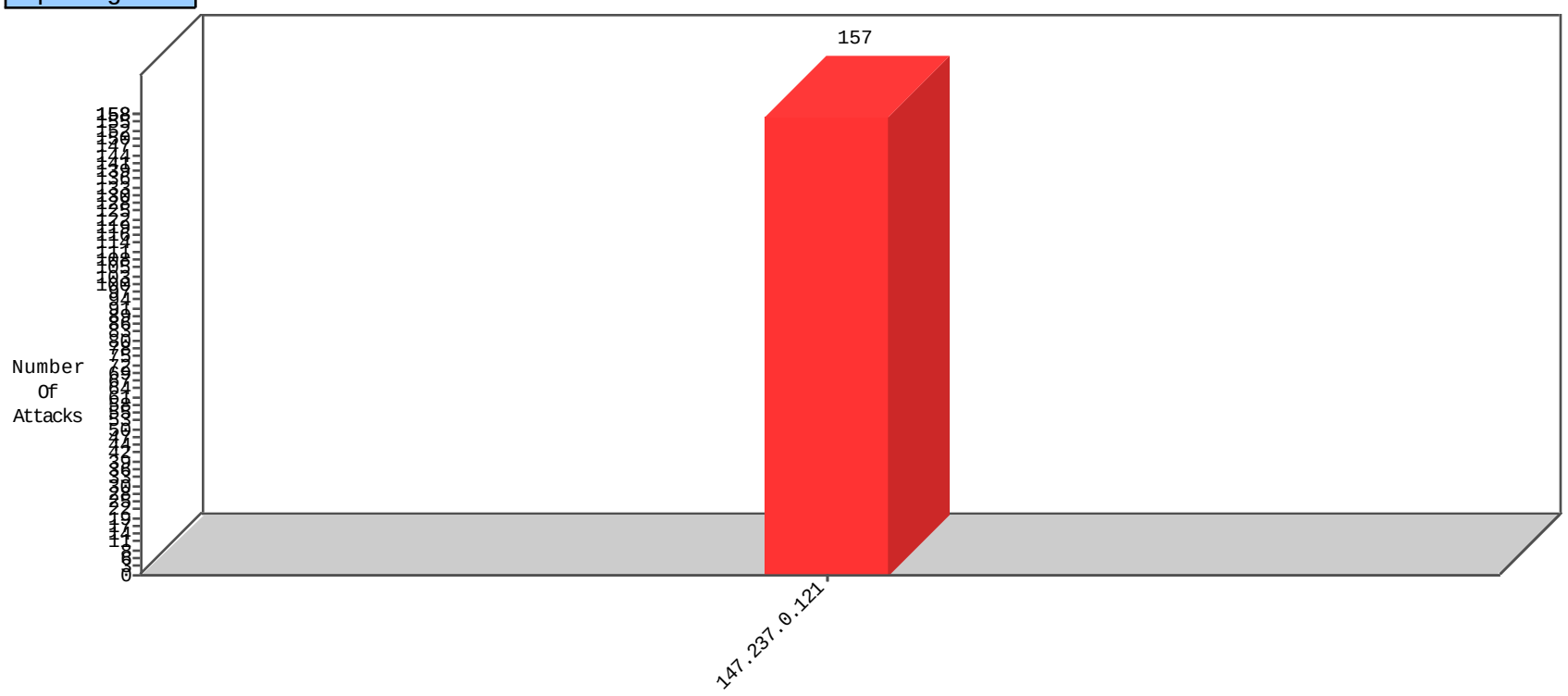
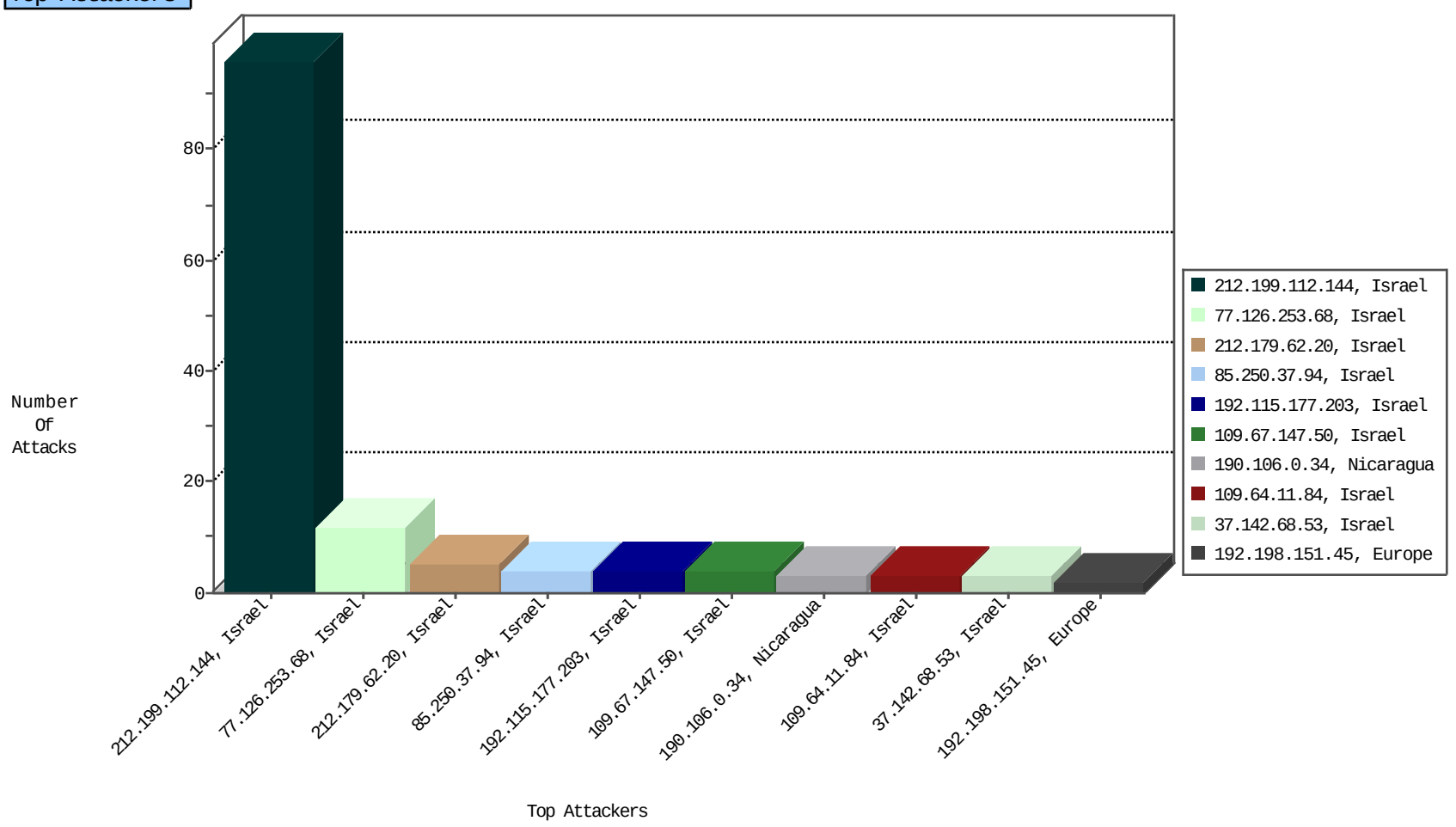
11-18-2015 to 11-19-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



11-18-2015 to 11-19-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
212.199.112.144	Israel	147.237.0.121		Anomaly-TLS-renegotiation-Cli	dest-reset	BBL-Israel	96
77.126.253.68	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	12
31.168.133.226	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	2

11-18-2015 to 11-19-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
85.64.119.24	Israel	147.237.0.121		13840: TLS: OpenSSL Heartbeat Packet	Block	1

11-18-2015 to 11-19-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
192.198.151.45	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	2
68.168.137.2	Canada	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1
74.117.209.136	United States	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1
131.109.15.2	United States	147.237.0.121		ET SCAN NMAP -sS window 4096	1
190.106.0.34	Nicaragua	147.237.0.121		ET SCAN NMAP -sS window 2048	1
74.117.209.135	United States	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1
131.109.15.2	United States	147.237.0.121		ET SCAN NMAP -sS window 3072	1
190.106.0.34	Nicaragua	147.237.0.121		ET SCAN NMAP -f -sS	1
190.106.0.34	Nicaragua	147.237.0.121		ET SCAN NMAP -sS window 3072	1

11-18-2015 to 11-19-2015

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	2581
66.249.93.150	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2264
66.249.93.146	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1961
207.232.41.2	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	347
81.218.174.57	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
143.112.144.129	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	284
66.249.93.150	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	249
66.249.93.154	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	231
66.249.93.146	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	210
192.146.6.2	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	200
176.13.14.187	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	193
212.199.112.144	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	185
207.232.41.2	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	175
192.115.177.203	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	169
2.54.169.33	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
109.67.16.112	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.54.9.113	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
80.246.136.64	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.54.157.6	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.52.170.21	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.54.49.128	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
54.243.190.43	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	136
72.37.140.41	Italy	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	125
46.116.124.93	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	125
149.78.148.43	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	125
176.13.11.153	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	123
46.19.86.1	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	119
46.19.85.155	Israel	147.237.0.121		drop	SAM rule	drop	109
149.88.10.13	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	108
46.19.86.1	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	108
46.19.86.1	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
46.19.86.1	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	106
2.52.177.251	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	100
46.120.32.218	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	100
46.120.32.218	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	100
149.88.30.56	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	98
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	95
84.95.131.192	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	94
46.19.85.6	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
46.19.85.109	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
2.54.63.222	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
46.19.85.42	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
89.139.164.207	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	89
185.32.179.117	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	87
176.13.9.207	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	87
5.102.254.197	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	86
176.13.7.146	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	86
2.52.177.251	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	84
212.150.245.250	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	81
176.12.148.152	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	79

11-18-2015 to 11-19-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
212.179.62.20	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	5
192.115.177.203	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	4
109.67.147.50	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/ufi/reaction/	Block	4
109.64.11.84	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	3
2.54.156.53	Israel	147.237.0.121		Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login	Block	2
85.250.37.94	Israel	147.237.0.121		PHP Attempt	Block	2
85.250.37.94	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/ajax/pages/fan_status.php	Block	2
77.127.94.48	Israel	147.237.0.121		PHP Attempt	Block	1
46.19.85.220	Israel	147.237.0.121		Parameter Type Violation ReturnUrl in www.miluim-ishi.aka.idf.il/login	Block	1
109.65.114.77	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
77.127.94.48	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/ajax/pages/fan_status.php	Block	1
37.142.68.53	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddIDCardDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
212.76.102.16	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/newpassword/forgotpassword	Block	1
46.19.86.164	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
109.65.205.253	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
80.178.147.60	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
37.142.68.53	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
87.69.243.168	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected , Observed 11732F2A6552022320571BEC87C338CDA49A1F7C64E9FC7A33D3FE22E2B6D59074683F223EEB6B4E77867DE381B600DBF72C5603C68B7A7CB545BF6D80FF177B33DED58DBC553C04ACD62E2D0A427332F28128A39776D1EF2E0C8B0A9EDA30707C509EBC51F92C0AD8A5637730E8FD3C7165EA91AABD48CFB037F41CE1F9773E6F949DC84D749B957AD8DB563F57F992D2E96FE25E561D612DE0A5ABDE2167D3	None	1
77.126.215.108	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
84.108.77.143	Israel	147.237.0.121		Unknown Parameter taf in www.miluim-ishi.aka.idf.il/login	Block	1
37.142.68.53	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1

11-18-2015 to 11-19-2015