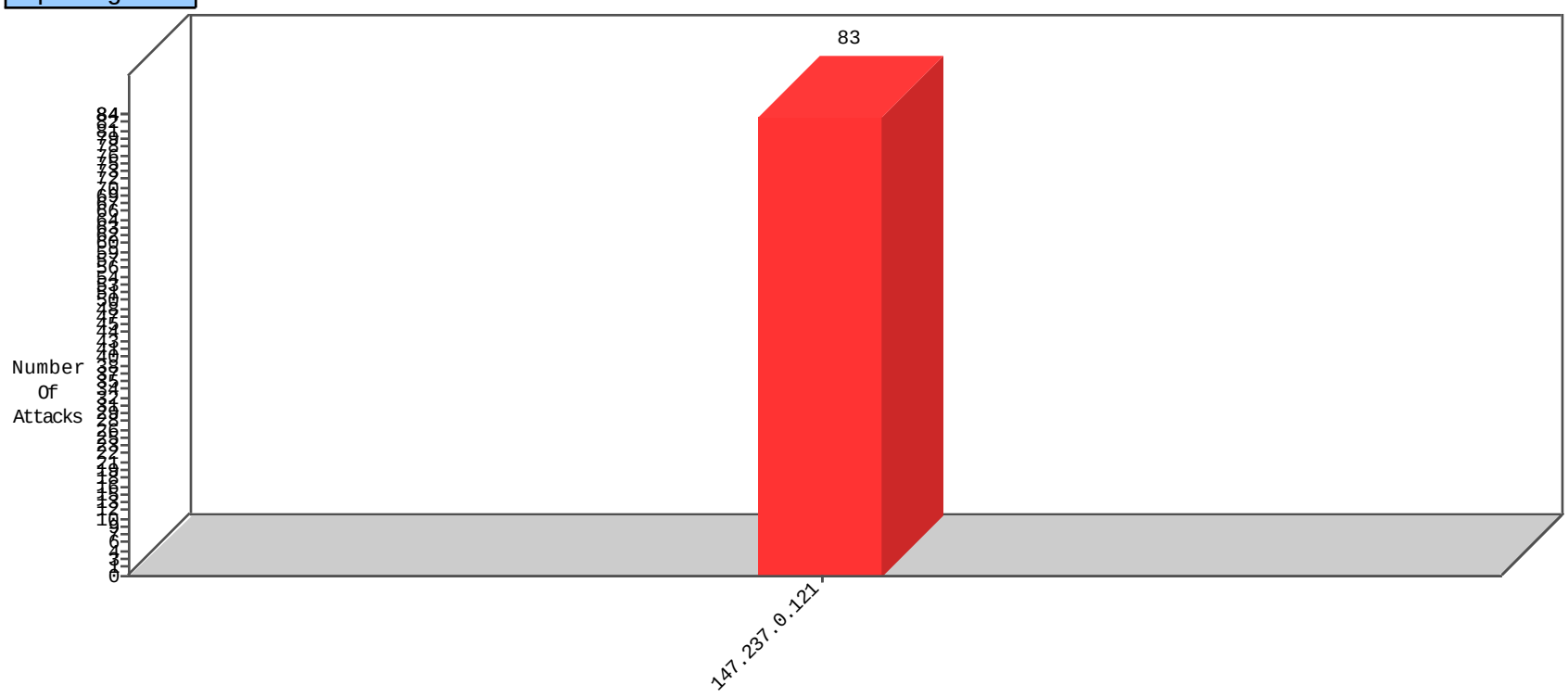
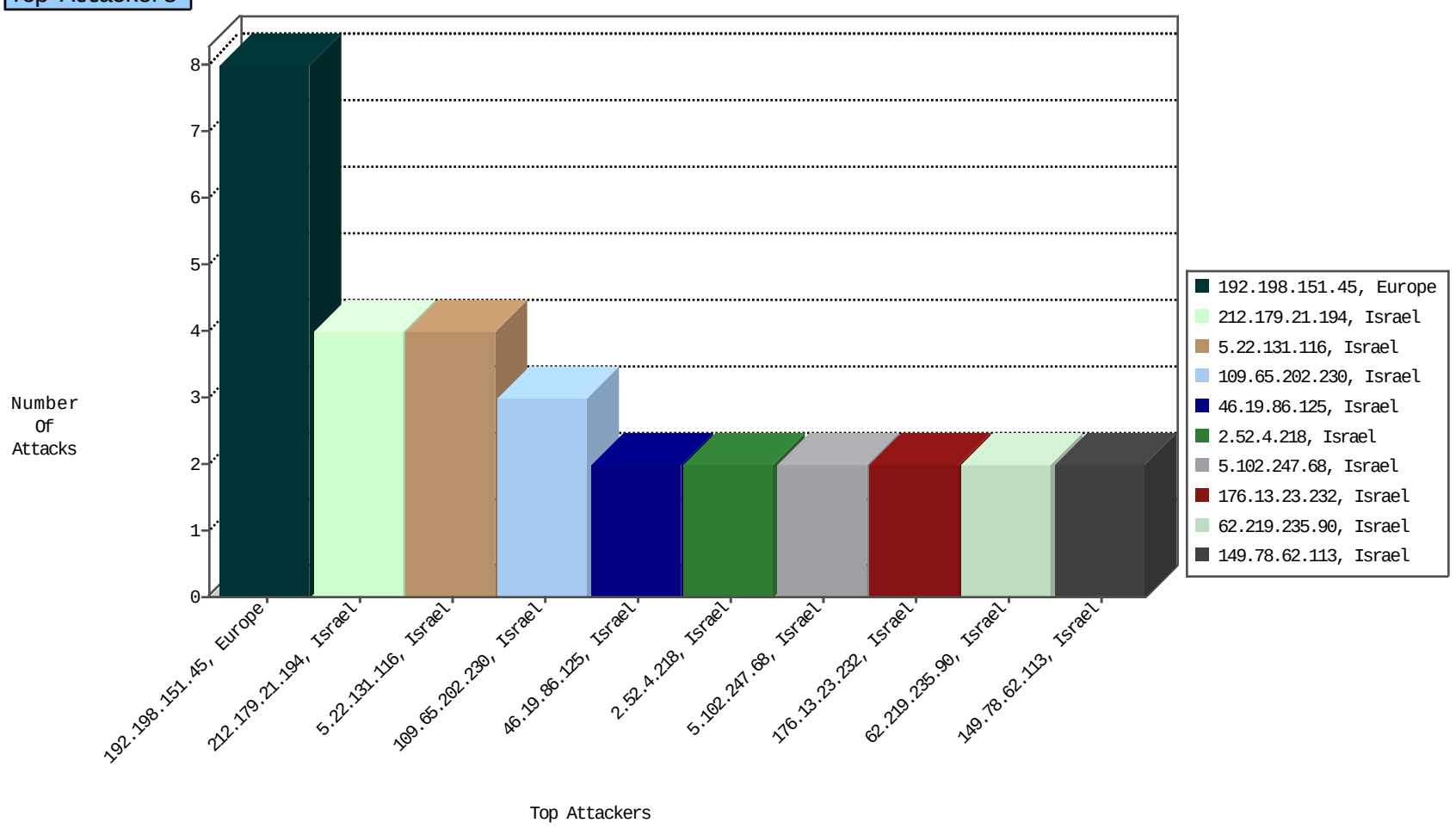
12-09-2015 to 12-10-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



12-09-2015 to 12-10-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
149.78.62.113	Israel	147.237.0.121		Invalid TCP Flags	drop	BBL-Israel	2

12-09-2015 to 12-10-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

12-09-2015 to 12-10-2015

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)	8
5.22.131.116	Israel	147.237.0.121		INDICATOR-SCAN myscan	2
5.22.131.116	Israel	147.237.0.121		GPL SCAN myscan	2
92.43.70.181	United Kingdom	147.237.0.121		ET SCAN NMAP -sS window 1024	1
177.185.208.71	Brazil	147.237.0.121		ET SCAN Potential SSH Scan	1
222.186.56.32	China	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1
87.66.80.152	Belgium	147.237.0.121		ET SCAN Potential SSH Scan	1
177.74.89.101	Brazil	147.237.0.121		ET SCAN Potential SSH Scan	1
187.111.59.158	Brazil	147.237.0.121		ET SCAN Potential SSH Scan	1
197.157.244.243	Somalia	147.237.0.121		ET SCAN Potential SSH Scan	1

12-09-2015 to 12-10-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.153	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2569
66.249.93.149	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2402
66.249.93.145	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1985
149.78.62.113	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1204
149.78.76.61	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	691
2.54.131.111	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	450
149.78.134.165	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	277
66.249.93.149	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	255
66.249.93.145	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	241
77.125.155.150	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	225
66.249.93.153	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	212
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	194
37.54.66.100	Ukraine	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	192
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	188
112.185.130.163	Korea, Republic of	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	183
2.54.43.220	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	180
192.114.23.211	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
149.88.5.166	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	141
213.57.118.110	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	92
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	80
149.88.206.3	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	76
149.88.188.166	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	61
167.220.196.29	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	56
85.64.27.161	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	53
66.249.74.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	50
149.88.59.58	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
149.88.8.14	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
37.157.143.2	Bulgaria	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	44
66.249.81.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	43
2.54.20.39	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	39
149.78.32.190	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	38
213.57.118.110	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	37
2.52.29.66	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	37
66.249.75.36	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
77.125.149.122	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
66.249.74.81	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	34
87.69.153.198	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	32
149.78.204.73	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	30
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	29
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	29
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
192.115.177.203	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	25
84.228.225.204	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	25
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	23
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
209.135.211.151	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	21
84.228.225.204	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	20
2.52.151.142	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	20
213.91.213.66	Bulgaria	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	19

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
212.179.21.194	Israel	147.237.0.121		Suspicious Response Code	Block	4
109.65.202.230	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	3
62.219.235.90	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.215	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
185.32.179.78	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.48	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
77.126.101.158	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.168.124	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.52.4.218	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.125	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
80.246.136.84	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.41	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
212.143.3.44	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.10.89	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.38.220	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPass in www.miluim-ishi.aka.idf.il/login	Block	1
85.64.194.223	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
79.176.72.178	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
217.132.50.203	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
5.102.247.68	Israel	147.237.0.121		Parameter Type Violation ctl00_ContentPlaceHolder1_fuAddBoardExamsPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/uploadregister.axd	Block	1
2.52.38.208	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
132.72.79.155	Israel	147.237.0.121		Suspicious Response Code	Block	1
80.246.136.156	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.126.7.56	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
176.13.16.170	Israel	147.237.0.121		Unknown Parameter ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/smsverify	Block	1
2.54.164.224	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
93.173.247.163	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.178.57.220	Israel	147.237.0.121		Distributed Unknown Parameter on www.miluim-ishi.aka.idf.il/smsverify parameter ctl00$ContentPlaceHolder1$txtCaptcha	Block	1
46.116.244.80	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.32.179.212	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected , Observed 897012DB4266291E51A38560CD8CC0C197E0F007DE9514814A05161DC9B0CEE3D01F7ED6C14D2B2D63D181F4B00140008F61BDF09BB4AD17C50AA4EB9295797F14CB601CD41ED02B3558275BD07CB381D9F2BAD1CA9C4ACE91F8C77309D38C27EE71E3E58EDC4D6322CAD2F859599805CC426D9CAE5BEB3668AC4D1651B3571610B4B805CE1EDEB5609334A068853D54ECABA01D6283C08A87BE1F7629733A97	None	1
5.102.247.68	Israel	147.237.0.121		Parameter Type Violation ctl00_ContentPlaceHolder1_fuAddStudyPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/uploadregister.axd	Block	1
2.52.152.112	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 2.52.152.112 (sigalgs DoS Attack)	None	1
176.13.1.26	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
83.130.115.175	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
46.19.85.60	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.8.204.67	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.23.232	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 176.13.23.232 (sigalgs DoS Attack)	None	1
109.64.35.136	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
79.180.229.122	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/1384-he/miluim.aspx	Block	1
62.219.99.154	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
45.55.176.8		147.237.0.121		Unauthorized URL Access to 147.237.0.121/	Block	1
192.116.146.145	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
2.52.152.112	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
176.13.6.249	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.109.113.192	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.126.225.207	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
213.57.54.114	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
176.13.23.232	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
5.29.77.180	Israel	147.237.0.121		Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 5.29.77.180	Block	1
2.52.30.254	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1