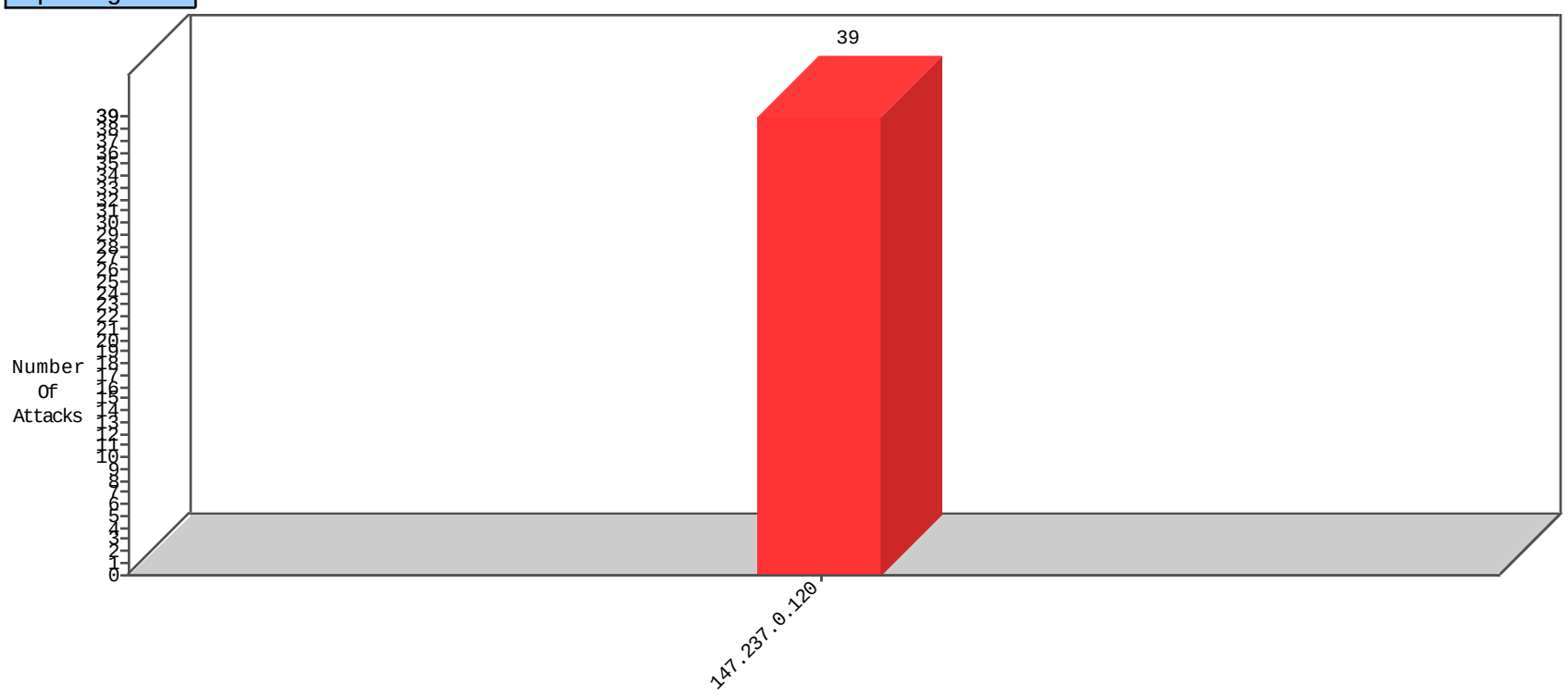
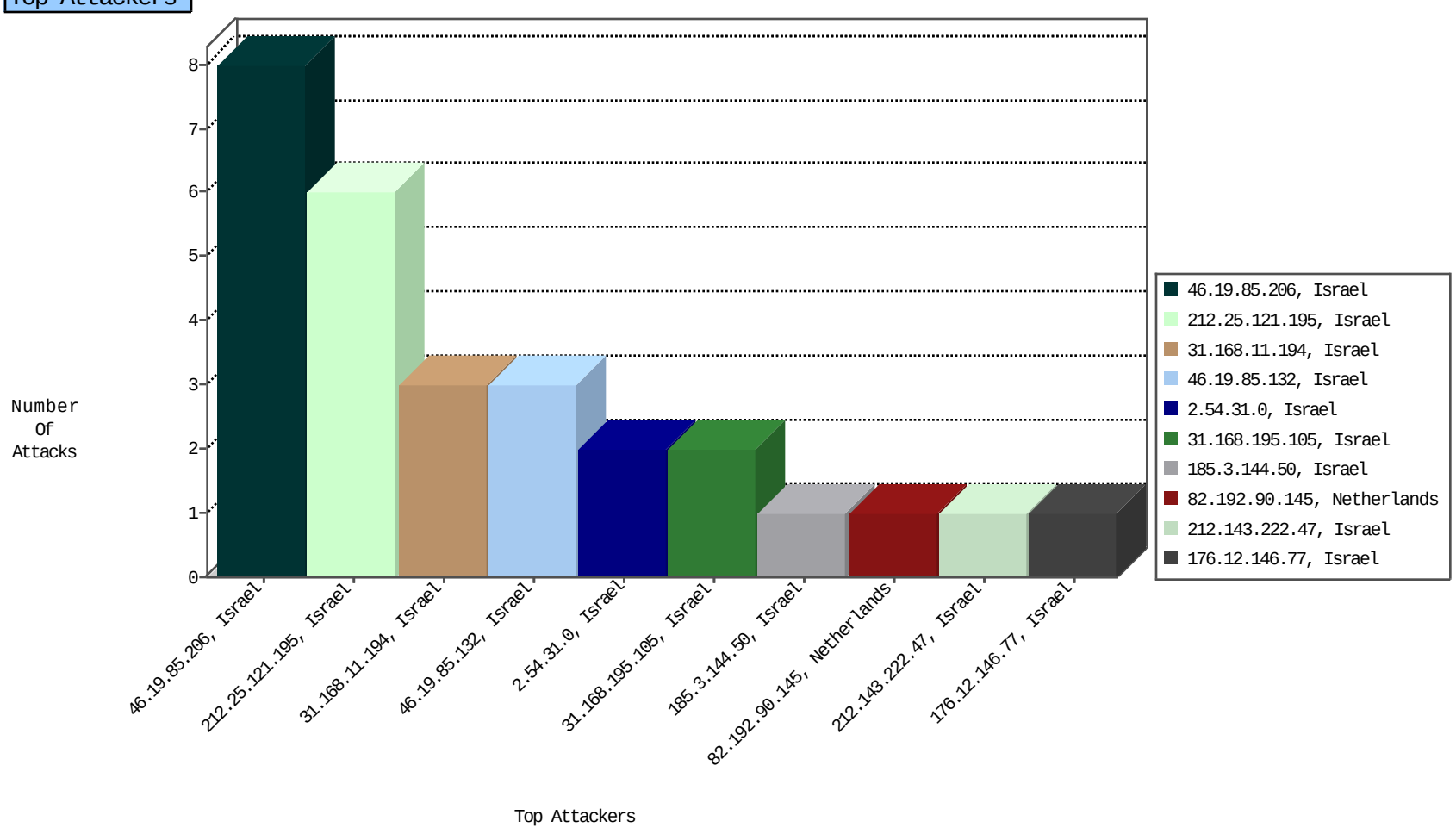
12-01-2015 to 12-02-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



12-01-2015 to 12-02-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
212.25.121.195	Israel	147.237.0.120		Block_Udp_All_Nets	drop	BBL-Israel	6

12-01-2015 to 12-02-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

12-01-2015 to 12-02-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
46.151.55.35	Ukraine	147.237.0.120		ET SCAN NMAP -sS window 1024	1
82.192.90.145	Netherlands	147.237.0.120		ET SCAN Potential SSH Scan	1
209.126.116.147	United States	147.237.0.120		ET SCAN NMAP -sS window 1024	1
79.174.70.237	Russian Federation	147.237.0.120		ET SCAN Potential SSH Scan	1
132.70.66.14	Israel	147.237.0.120		ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1

12-01-2015 to 12-02-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.198	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	108429
66.249.93.206	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	58932
66.249.93.202	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	46154
66.249.81.224	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	38157
66.249.81.227	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	18388
66.249.81.230	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	16624
79.180.136.1	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2430
82.81.193.202	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
5.22.134.105	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
194.90.7.25	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
157.55.39.122	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1809
2.54.129.7	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1602
207.46.13.91	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1392
207.46.13.4	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1123
178.94.5.58	Ukraine	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1112
2.52.52.96	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1053
2.52.173.29	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	936
40.77.167.14	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	693
68.180.229.121	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	682
168.63.137.102	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	588
66.249.93.206	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	509
149.78.23.220	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	480
66.249.93.202	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	450
66.249.93.198	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	427
134.191.232.71	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	338
194.69.103.164	United Kingdom	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	232
24.12.74.89	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	232
149.88.127.48	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	231
149.78.241.104	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	214
2.52.163.193	Israel	147.237.0.120		SYN Attack	SYN -> SYN-ACK -> RST	reject	212
66.249.66.49	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	208
140.247.218.52	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	203
207.46.13.81	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	203
149.78.236.41	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	198
149.78.232.218	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	190
74.73.86.132	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	190
149.88.127.10	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	186
146.127.253.14	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	174
134.191.232.69	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	168
66.249.66.52	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	155
149.88.77.45	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	152
79.182.115.100	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.54.182.119	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.178.127.243	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
149.78.21.75	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	134
66.102.9.90	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	134
134.191.232.68	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	132
66.249.66.55	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	129
46.19.85.142	Israel	147.237.0.120		SYN Attack	SYN -> SYN-ACK -> RST	reject	122
149.78.226.190	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	108

12-01-2015 to 12-02-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
31.168.11.194	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1377-he/milu	Block	2
2.54.31.0	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1377-he/milu	Block	2
31.168.195.105	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/894-he/miluim.asp	Block	2
46.19.85.206	Israel	147.237.0.120		Abnormally Long Request method	Block	1
176.12.146.77	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
46.19.85.206	Israel	147.237.0.120		Multiple Illegal HTTP Version from 46.19.85.206	Block	1
46.19.85.132	Israel	147.237.0.120		Illegal HTTP Version	Block	1
46.19.86.20	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1376-he/miluim.aspxâ€?â€Ž	Block	1
46.19.85.206	Israel	147.237.0.120		Illegal HTTP Version _pk_ses.104.b624=*	Block	1
31.168.67.176	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1377-he/miluim.aspxâ€?â€Ž	Block	1
185.3.144.50	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1337-he/	Block	1
46.19.85.206	Israel	147.237.0.120		Multiple Malformed URL from 46.19.85.206	Block	1
46.19.85.132	Israel	147.237.0.120		Malformed URL sdch	Block	1
2.54.149.161	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1377-he/miluim.aspxâ€?â€Ž	Block	1
85.64.247.215	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/templates/general/www.ishurim.aka.idf.il/1044-he/ishurim.aspx	Block	1
46.19.85.206	Israel	147.237.0.120		Malformed URL _pk_id.104.b624=0d26d95a488bc08c.1449003556.1.1449003556.1449003556.;	Block	1
212.117.143.250	Israel	147.237.0.120		Unauthorized URL Access to miluim.aka.idf.il/main/home/default.aspx	Block	1
46.19.85.206	Israel	147.237.0.120		Multiple Unknown HTTP Request Method from 46.19.85.206	Block	1
46.19.85.132	Israel	147.237.0.120		Unknown HTTP Request Method ate, in URL sdch	Block	1
31.168.11.194	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1377-he/milu	Block	1
89.138.232.230	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
46.19.85.206	Israel	147.237.0.120		Multiple Abnormally Long Request from 46.19.85.206	Block	1
37.26.148.183	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1377-he/miluim.aspxâ€?â€Ž	Block	1
212.143.222.47	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1377-he/miluim.aspxâ€?â€Ž	Block	1
46.19.85.206	Israel	147.237.0.120		Unknown HTTP Request Method b624=%5B%22%22%2C%22%22%2C1449003556%2C%22https%3A%2F%2Fwww.google.co.il%2F%22%5D; in URL _pk_id.104.b624=0d26d95a488bc08c.1449003556.1.1449003556.1449003556.	Block	1

12-01-2015 to 12-02-2015