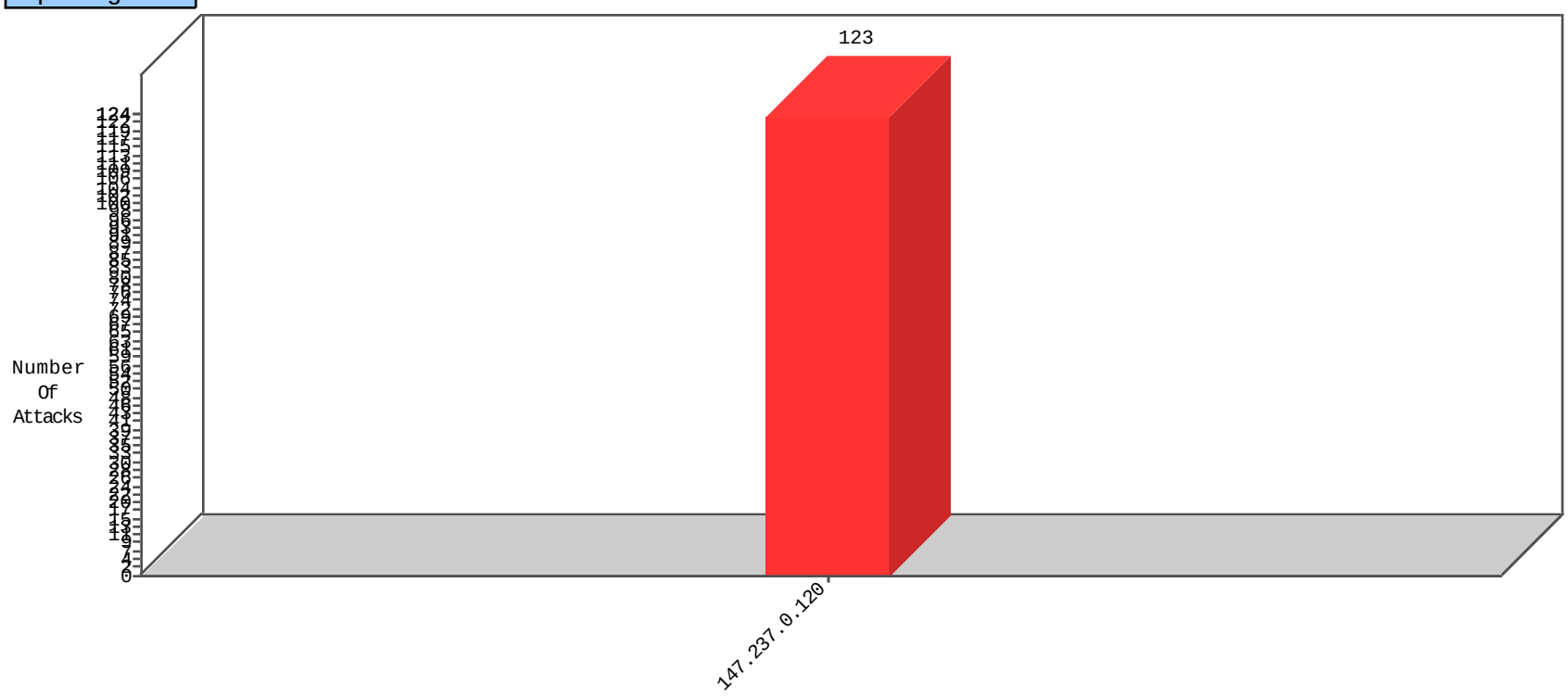
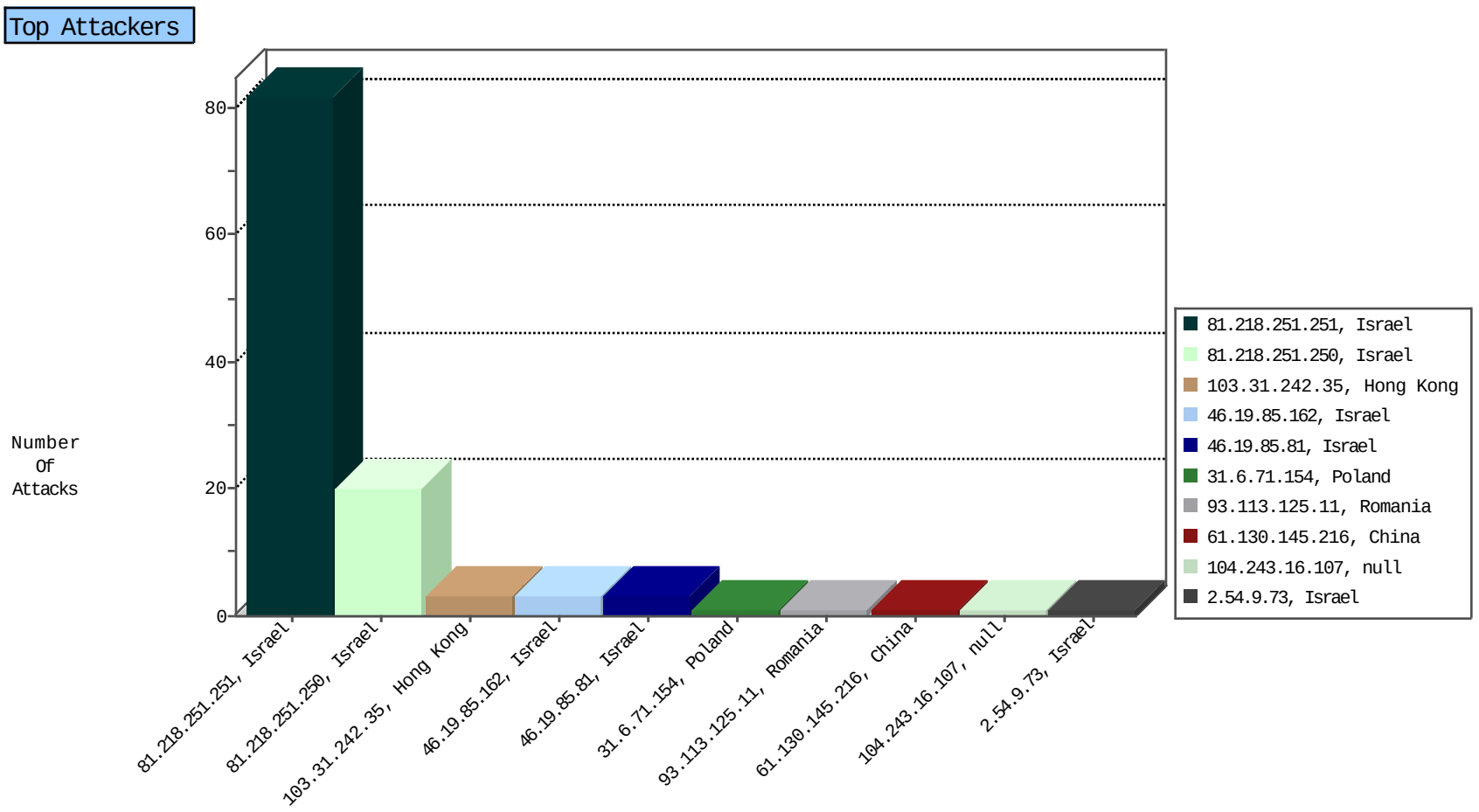
11-25-2015 to 11-26-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



11-25-2015 to 11-26-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
103.31.242.35	Hong Kong	147.237.0.120		Frk_Under_Attack_Con_Http	drop	BBL-Frankfurt	2
103.31.242.35	Hong Kong	147.237.0.120		Frk_Purple_Con_Limit_Http	drop	BBL-Frankfurt	1

11-25-2015 to 11-26-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
81.218.251.251	Israel	147.237.0.120		C1000004: HTTP: options method (Microsoft)	Block	82
81.218.251.250	Israel	147.237.0.120		C1000004: HTTP: options method (Microsoft)	Block	20

11-25-2015 to 11-26-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
31.6.71.154	Poland	147.237.0.120		ET SCAN NMAP -sS window 1024	1
61.130.145.216	China	147.237.0.120		ET SCAN NMAP -sS window 1024	1
93.174.93.68	Netherlands	147.237.0.120		ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	China	147.237.0.120		ET SCAN Potential SSH Scan	1
61.216.2.14	Taiwan	147.237.0.120		ET SCAN NMAP -sS window 1024	1
104.243.16.107		147.237.0.120		ET SCAN NMAP -sS window 1024	1

11-25-2015 to 11-26-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.81.224	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	61128
66.249.81.230	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	29575
66.249.81.227	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	23536
109.67.165.250	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4608
149.88.105.220	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	3308
2.54.11.3	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
2.54.17.55	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1521
149.78.2.63	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1446
79.176.151.221	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1224
149.78.237.83	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1196
149.88.214.23	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	876
149.78.253.15	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	723
149.78.22.6	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	622
68.180.229.121	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	441
69.158.26.196	Canada	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	429
2.54.9.235	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	405
157.55.39.112	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	377
207.59.14.130	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	254
157.55.39.55	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	229
149.78.20.112	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	219
49.244.86.141	Nepal	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	204
66.249.81.227	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	176
46.19.86.101	Israel	147.237.0.120		SYN Attack	SYN -> SYN-ACK -> RST	reject	169
149.78.36.205	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	160
66.249.93.203	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	158
66.249.93.207	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	153
66.102.9.100	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	151
109.65.163.147	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
77.126.104.144	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
109.64.34.120	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.177.151.151	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.182.30.242	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
149.78.47.62	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	141
66.249.93.199	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	131
66.249.81.230	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	131
149.78.229.75	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	127
66.102.9.80	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	126
199.207.253.101	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	124
66.249.81.224	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	122
79.183.205.30	Israel	147.237.0.120		drop	SAM rule	drop	116
66.102.9.90	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	116
66.249.73.228	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	113
66.249.73.212	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	111
149.78.166.10	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	106
51.175.93.165	United Kingdom	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	106
149.78.27.28	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	106
149.78.78.243	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	106
157.55.39.244	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	105
157.55.39.243	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	101
66.249.93.172	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	99

11-25-2015 to 11-26-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
93.113.125.11	Romania	147.237.0.120		Unauthorized URL Access to /readme_for_decrypt.txt	Block	1
46.19.85.81	Israel	147.237.0.120		Illegal HTTP Version	Block	1
46.19.85.162	Israel	147.237.0.120		Malformed URL _pk_ses.104.b624=*	Block	1
95.86.89.17	Israel	147.237.0.120		Unknown Parameter ctl00$ContentPlaceHolder1$ucNewsControl$txtSearch in www.miluim.aka.idf.il/994-he/miluim.aspx	Block	1
46.19.85.81	Israel	147.237.0.120		Malformed URL _pk_ses.104.b624=*	Block	1
46.19.85.162	Israel	147.237.0.120		Unknown HTTP Request Method 9.1448434819.; in URL _pk_ses.104.b624=*	Block	1
168.235.200.121	United States	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/×²Ö³Ö´	Block	1
46.19.85.81	Israel	147.237.0.120		Unknown HTTP Request Method 7.; in URL _pk_ses.104.b624=*	Block	1
85.64.90.68	Israel	147.237.0.120		Unauthorized URL Access to miluim.aka.idf.il/ufi/reaction/	Block	1
2.54.9.73	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
176.12.145.174	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1359-he/miluim.aspxâ€?â€Ž	Block	1
46.19.85.162	Israel	147.237.0.120		Illegal HTTP Version	Block	1

11-25-2015 to 11-26-2015