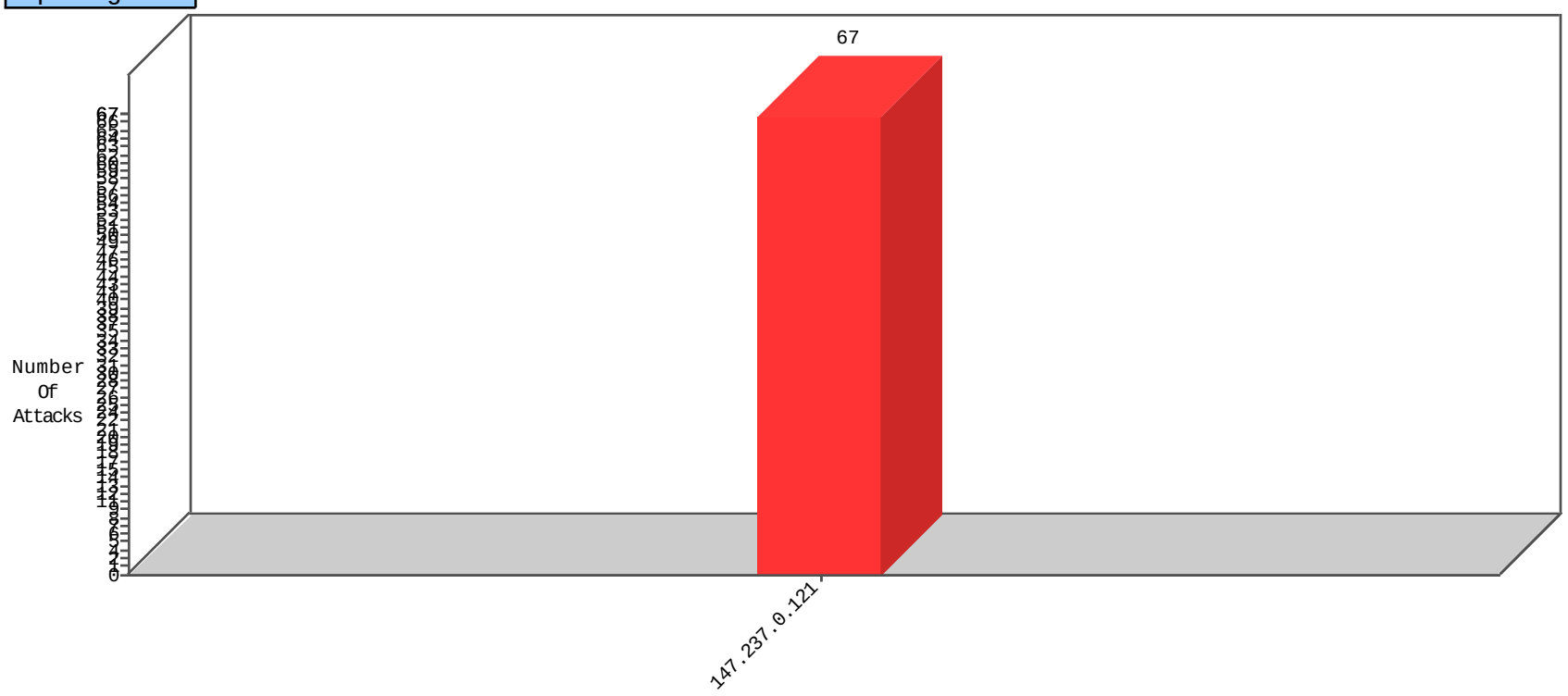
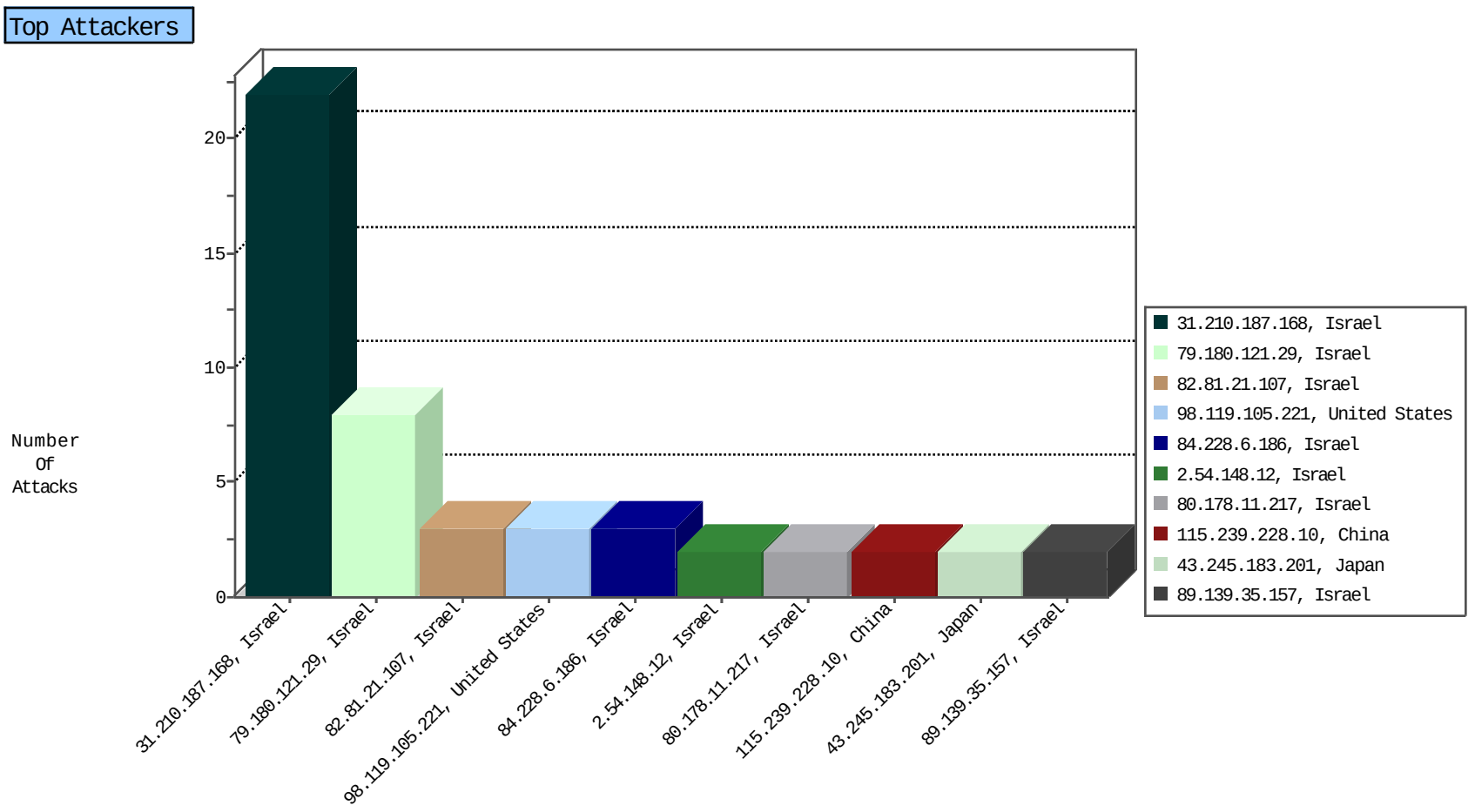
12-25-2015 to 12-26-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



12-25-2015 to 12-26-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
115.239.228.10	China	147.237.0.121		Frk_Purple_Con_Limit_Http	drop	BBL-Frankfurt	2

12-25-2015 to 12-26-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

12-25-2015 to 12-26-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
218.104.49.211	China	147.237.0.121		ET SCAN Potential SSH Scan	1
43.245.183.201	Japan	147.237.0.121		ET SCAN NMAP -f -sS	1
59.45.79.117	China	147.237.0.121		ET SCAN Potential SSH Scan	1
93.174.93.181	Netherlands	147.237.0.121		ET SCAN Potential SSH Scan	1
98.119.105.221	United States	147.237.0.121		ET SCAN NMAP -f -sS	1
98.119.105.221	United States	147.237.0.121		ET SCAN NMAP -sS window 4096	1
185.130.5.231		147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1
43.245.183.201	Japan	147.237.0.121		ET SCAN NMAP -sS window 2048	1
62.232.207.210	United Kingdom	147.237.0.121		ET SCAN Potential SSH Scan	1
94.102.48.195	Netherlands	147.237.0.121		ET SCAN NMAP -sS window 1024	1
98.119.105.221	United States	147.237.0.121		ET SCAN NMAP -sS window 2048	1
172.98.200.238		147.237.0.121		ET SCAN NMAP -sS window 4096	1

12-25-2015 to 12-26-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1251
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1182
66.249.93.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	857
149.88.8.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	541
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	173
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	164
149.88.176.226	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	135
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	131
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	128
80.113.194.205	Netherlands	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	117
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	109
27.55.25.104	Thailand	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	99
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	87
27.55.135.233	Thailand	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	80
2.52.55.198	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	71
149.88.176.16	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	56
157.55.39.178	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	48
149.78.230.148	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	41
216.53.143.123	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	41
176.221.173.226	Georgia	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	40
149.78.8.188	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	31
157.55.39.54	United States	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	28
52.91.82.13	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
88.167.249.103	France	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
149.78.103.175	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
85.228.29.249	Sweden	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
209.135.211.206	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	21
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
66.249.64.170	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
66.249.93.236	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
66.249.81.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13
5.22.134.18	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	11
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	11
209.126.117.15	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	10
130.193.51.95	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	9
66.249.64.165	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	9
213.57.134.53	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
66.249.69.175	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	8
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	7
207.46.13.2	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	6
5.102.254.51	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	6
5.102.254.91	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	5
31.210.187.149	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	5
157.55.39.179	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	5
149.78.202.185	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	5
46.121.229.142	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	5

12-25-2015 to 12-26-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
31.210.187.168	Israel	147.237.0.121		Multiple Unauthorized URL Access from 31.210.187.168	Block	14
31.210.187.168	Israel	147.237.0.121		Parameter Type Violation v in www.miluim-ishi.aka.idf.il/logincss	Block	8
79.180.121.29	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesIDs in www.miluim-ishi.aka.idf.il/changeunit	Block	4
80.178.11.217	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
84.228.6.186	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 84.228.6.186 (sigalgs DoS Attack)	None	2
79.180.121.29	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddDocs&FileToActivate in www.miluim-ishi.aka.idf.il/login	Block	2
79.180.121.29	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddDocs&FilesToCheck in www.miluim-ishi.aka.idf.il/login	Block	2
37.26.149.184	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
85.64.168.12	Israel	147.237.0.121		Unknown Parameter ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/smsverify	Block	2
79.183.108.124	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
2.54.185.215	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
151.229.82.216	United Kingdom	147.237.0.121		Parameter Type Violation ctl00_ContentPlaceHolder1_fuAddAddressAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
82.81.21.107	Israel	147.237.0.121		Parameter Type Violation ctl00_ContentPlaceHolder1_fuAddTimetableDocs&FilesToSend in www.miluim-ishi.aka.idf.il/uploadregister.axd	Block	1
2.54.139.101	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/â€?â€Ž	Block	1
89.139.35.157	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
185.3.144.46	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 185.3.144.46 (sigalgs DoS Attack)	None	1
2.54.148.12	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 2.54.148.12 (sigalgs DoS Attack)	None	1
89.139.35.157	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.81.21.107	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTimetableFilesNames in www.miluim-ishi.aka.idf.il/valtamrequest	Block	1
185.3.144.46	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
84.228.6.186	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
2.54.148.12	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
109.253.201.79	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.81.21.107	Israel	147.237.0.121		Parameter Type Violation ctl00_ContentPlaceHolder1_fuAddBoardExamsPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/uploadregister.axd	Block	1

12-25-2015 to 12-26-2015