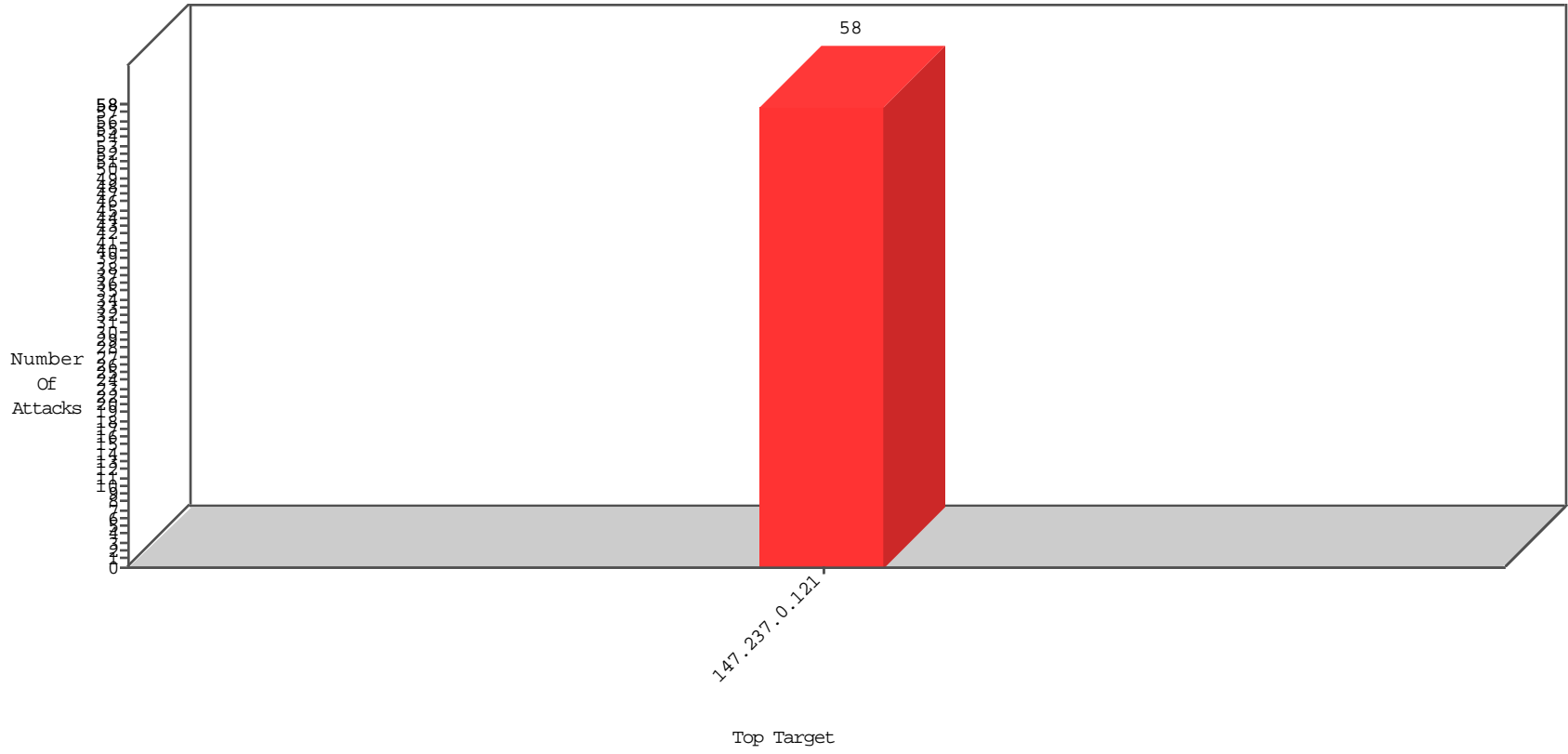


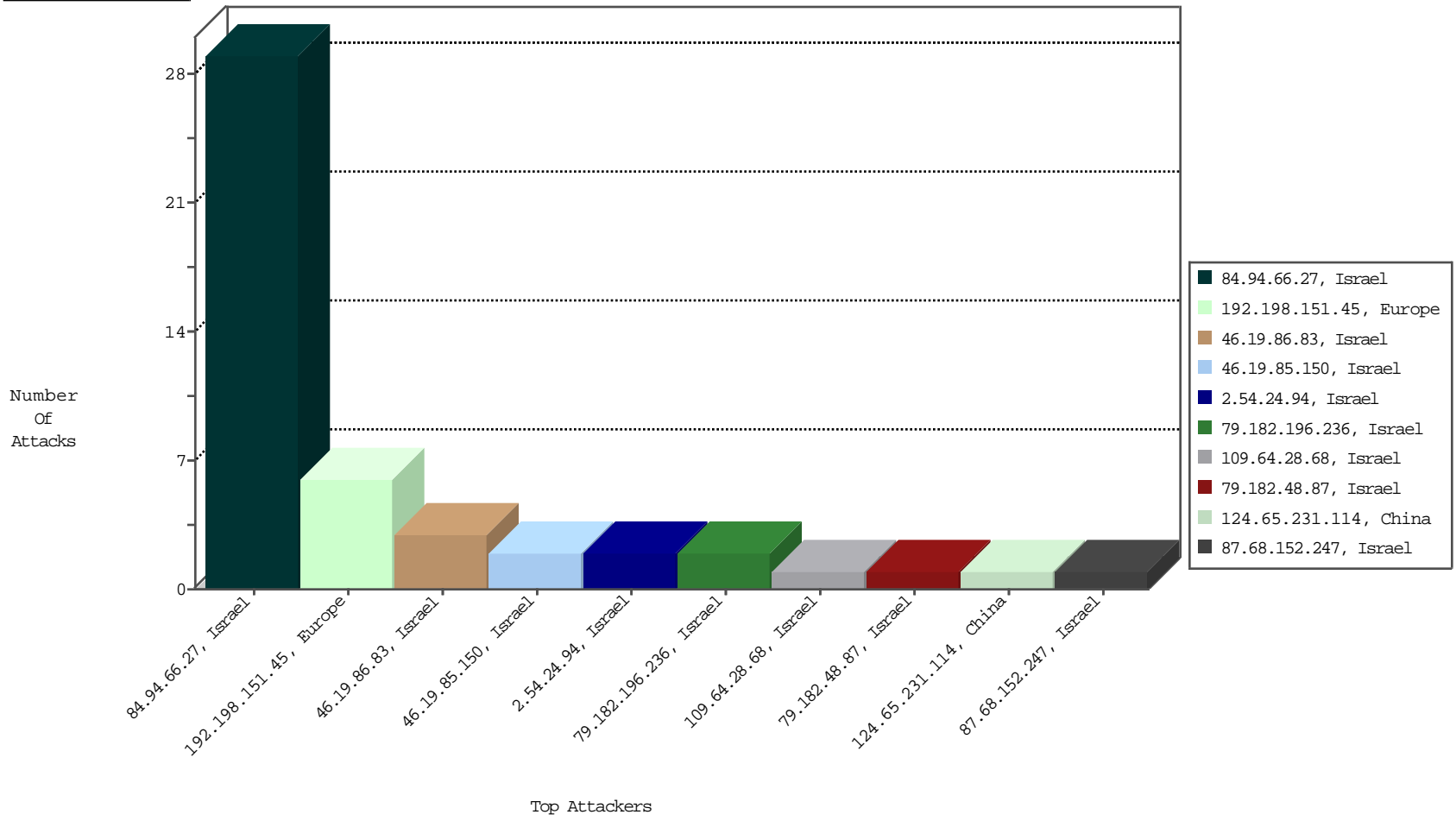
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



01-02-2016 to 01-03-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
------------------	--------------	----------------	------	-----------	---------------	----------------------	-------

01-02-2016 to 01-03-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
------------------	--------------	----------------	------	-----------	---------------	-------

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)	6
120.146.199.131	Australia	147.237.0.121		ET SCAN Potential SSH Scan	1
5.149.248.251	Netherlands	147.237.0.121		ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.0.121		ET SCAN Potential SSH Scan	1
124.65.231.114	China	147.237.0.121		ET SCAN Potential SSH Scan	1
209.105.232.241	United States	147.237.0.121		ET SCAN Potential SSH Scan	1
59.45.79.117	China	147.237.0.121		ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site Name	Signature	Device Action	Count
66.249.93.85	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	879
66.249.93.89	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	670
66.249.93.83	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	528
109.88.18.128	Belgium	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	323
217.132.13.104	Israel	147.237.0.121	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	252
66.102.9.87	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	149
66.102.9.74	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	127
185.27.105.65	Israel	147.237.0.121	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	126
66.249.93.85	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	115
66.102.9.97	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	98
66.249.93.83	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	95
149.88.13.33	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	90
66.249.93.89	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	82
149.78.24.21	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	65
149.78.230.148	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	63
66.249.69.175	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	63
66.249.69.165	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	54
217.69.133.251	Russian Federation	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	50
84.228.225.124	Israel	147.237.0.121	Bad TCP sequence	SYN retransmit with different window scale	monitor	49
54.243.190.43	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	46
149.88.102.19	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	40
217.69.133.248	Russian Federation	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	40
66.249.69.170	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	39
217.69.133.191	Russian Federation	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	38
149.88.116.181	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	38
93.172.42.33	Israel	147.237.0.121	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
109.65.183.152	Israel	147.237.0.121	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
217.69.133.252	Russian Federation	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	32
217.69.133.250	Russian Federation	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	29
207.46.13.164	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	26
66.102.9.50	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	26
66.249.93.211	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	25
66.249.69.175	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	25
217.69.133.21	Russian Federation	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	22
149.78.251.86	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	20
66.249.69.165	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	20
207.46.13.45	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	18
149.88.141.3	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	18
66.249.69.170	Israel	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	17
37.46.39.199	Israel	147.237.0.121	Bad TCP sequence	Invalid ACK number	monitor	16
157.55.39.76	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	13
207.46.13.59	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	13
66.102.9.39	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	11
217.69.133.249	Russian Federation	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	11
5.102.254.117	Israel	147.237.0.121	Bad TCP sequence	Invalid ACK number	monitor	10
31.210.188.100	Israel	147.237.0.121	Bad TCP sequence	Invalid ACK number	monitor	10
5.102.254.160	Israel	147.237.0.121	Bad TCP sequence	Invalid ACK number	monitor	10
209.126.117.15	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	10
66.249.93.208	United States	147.237.0.121	Geo-location enforcement	Geo-location inbound enforcement	drop	9
5.102.254.220	Israel	147.237.0.121	Bad TCP sequence	Invalid ACK number	monitor	9

01-02-2016 to 01-03-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
84.94.66.27	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceholder1_fuAddBoardExamsPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	9
84.94.66.27	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceholder1_fuAddStudyPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	9
84.94.66.27	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceholder1_fuAddTimetableDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	9
46.19.86.83	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 46.19.86.83 (sigalgs DoS Attack)	None	2
79.182.196.236	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceholder1\$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	2
84.94.66.27	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceholder1\$txtNimuk in www.miluim-ishi.aka.idf.il/valtamrequest	Block	2
87.68.45.189	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/loginhttps://www.miluim-ishi.aka.idf.il/login	Block	1
79.176.14.67	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.138.172	Israel	147.237.0.121		Double URL Encoding - parameter: returnUrl in www.miluim-ishi.aka.idf.il/login	Block	1
46.19.85.150	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
87.68.152.247	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https://www.miluim-ishi.aka.idf.il/	Block	1
79.182.48.87	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
2.54.24.94	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 2.54.24.94 (sigalgs DoS Attack)	None	1
176.13.1.188	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
109.64.28.68	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https://www.miluim-ishi.aka.idf.il/	Block	1
2.54.24.94	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
46.19.86.83	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
109.186.10.159	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
46.19.85.150	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 46.19.85.150 (sigalgs DoS Attack)	None	1

01-02-2016 to 01-03-2016