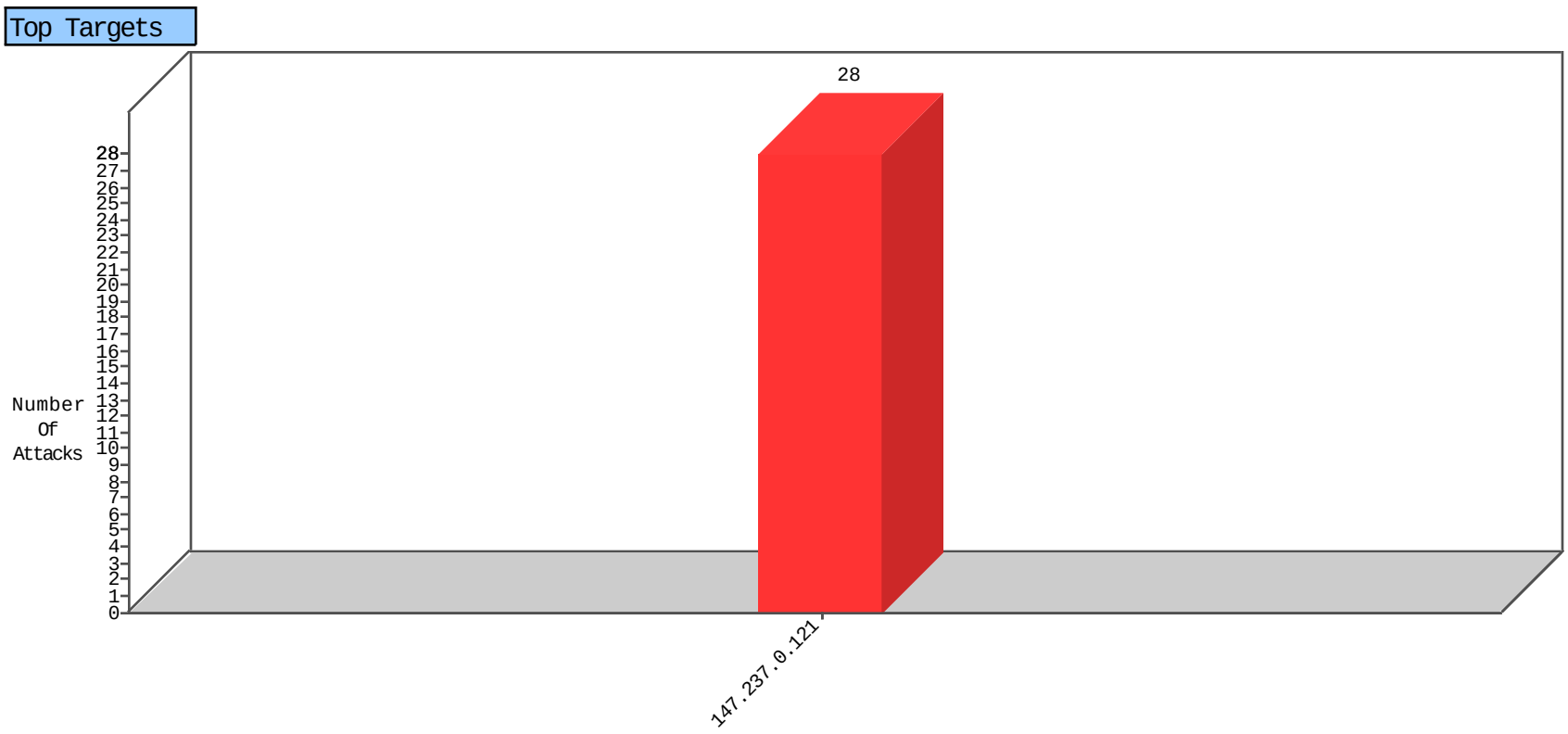
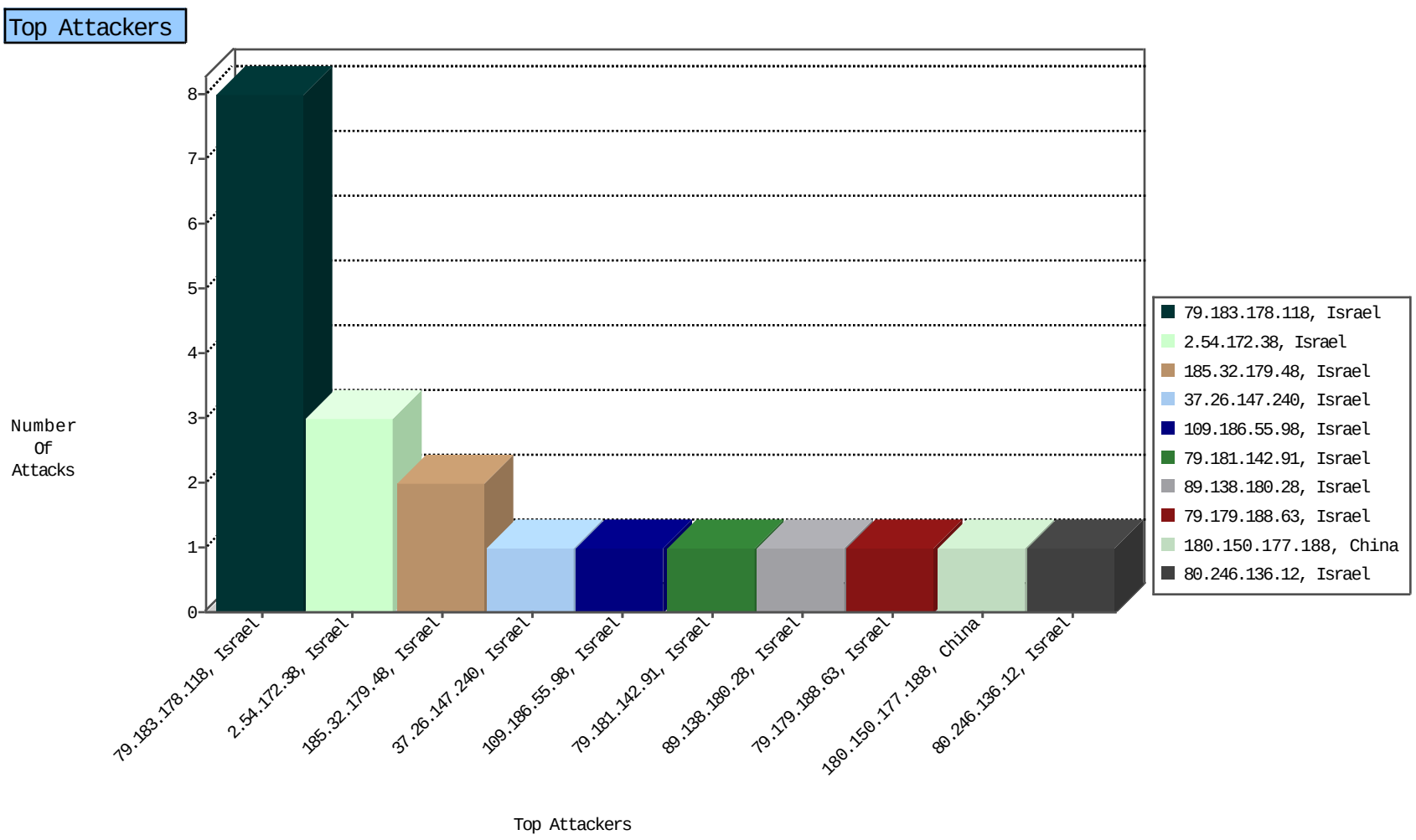
01-01-2016 to 01-02-2016

Focused IP Under Attack Daily Report





01-01-2016 to 01-02-2016

Top Attackers In DDoS-Defence

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

01-01-2016 to 01-02-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

01-01-2016 to 01-02-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
189.50.11.43	Brazil	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
121.183.175.167	Korea, Republic of	147.237.0.121		ET SCAN Potential SSH Scan	1
185.130.5.235		147.237.0.121		ET SCAN Potential SSH Scan	1
120.194.193.15	China	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1
180.150.177.188	China	147.237.0.121		ET SCAN NMAP -sS window 1024	1

01-01-2016 to 01-02-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	692
66.249.93.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	673
64.79.85.205	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	548
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	502
149.78.30.109	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	240
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	175
207.46.13.164	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	169
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	119
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	118
79.176.9.221	Israel	147.237.0.121		Bad TCP sequence		monitor	113
221.116.11.243	Japan	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	104
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	101
73.201.116.151	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	85
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	80
207.46.13.59	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	66
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	63
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	62
149.78.140.193	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	49
79.176.9.221	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	41
149.78.62.113	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	38
2.54.43.194	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
66.249.69.165	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	36
149.88.110.162	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	36
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	33
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
109.64.102.139	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	25
66.249.81.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
2.54.171.207	Israel	147.237.0.121		SYN Attack		reject	25
149.88.7.140	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
79.176.9.221	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	19
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
79.176.9.221	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	18
109.64.102.139	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	17
84.228.225.124	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	16
37.46.39.173	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	16
66.249.69.165	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
2.54.171.207	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	13
217.69.133.249	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
2.54.171.207	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	9
66.249.81.129	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	9
66.249.82.153	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	9
2.54.171.207	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	9
84.229.173.227	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.93.211	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	9
66.249.69.175	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	9
2.54.171.207	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	9
79.180.218.82	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	9
94.230.86.168	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	9

01-01-2016 to 01-02-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
79.183.178.118	Israel	147.237.0.121		Suspicious Response Code	Block	8
2.54.172.38	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	3
185.32.179.48	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 185.32.179.48 (sigalgs DoS Attack)	None	1
79.179.188.63	Israel	147.237.0.121		Unauthorized HTTP Method	Block	1
80.246.136.12	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
185.32.179.48	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
79.181.142.91	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/login	Block	1
89.138.180.28	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
37.26.147.240	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
194.90.15.61	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
79.182.112.97	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
109.186.55.98	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
37.142.252.55	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1

01-01-2016 to 01-02-2016