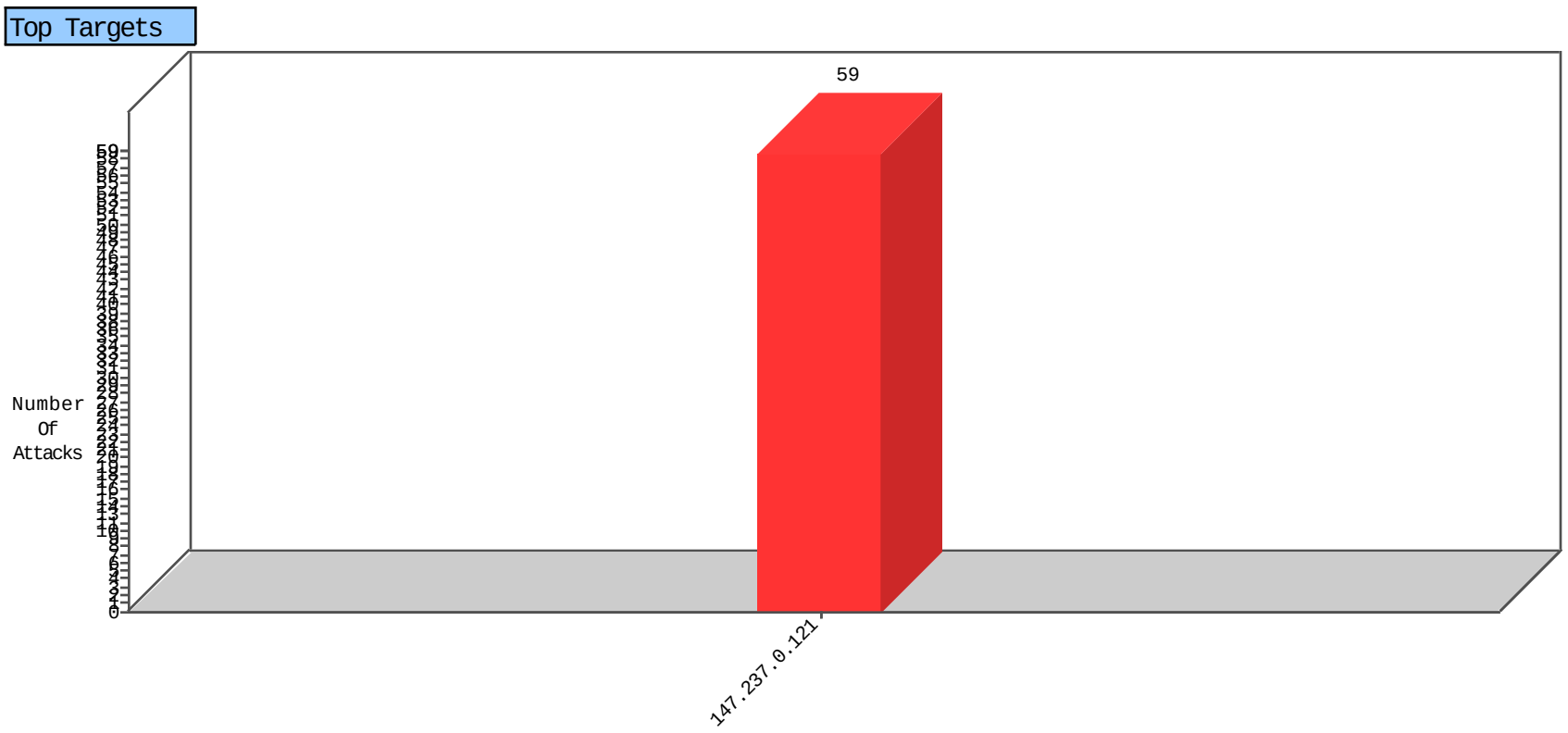
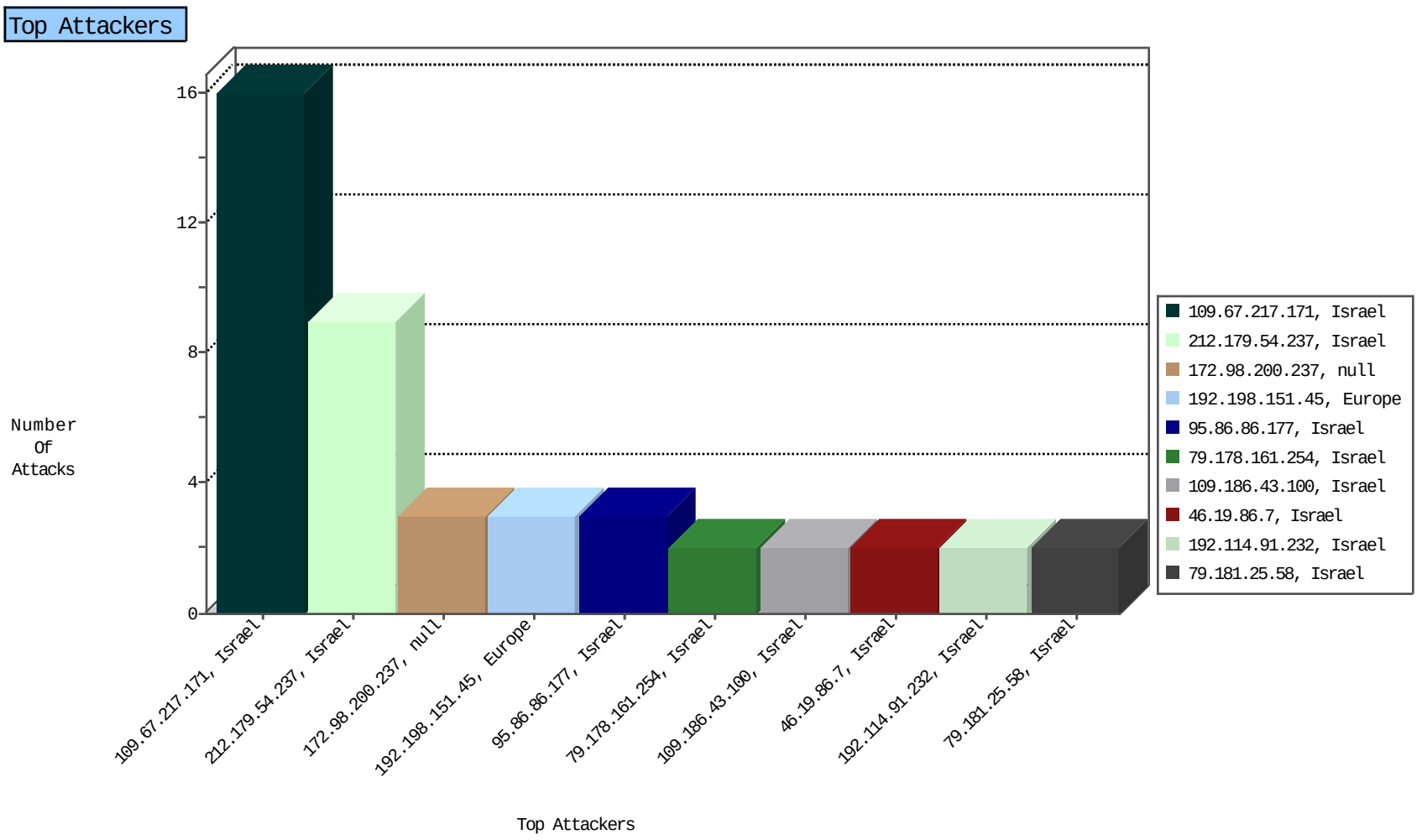
01-23-2016 to 01-24-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



01-23-2016 to 01-24-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
212.179.54.237	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	9

01-23-2016 to 01-24-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

01-23-2016 to 01-24-2016

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)	3
172.98.200.237		147.237.0.121		ET SCAN NMAP -f -sS	1
172.98.200.237		147.237.0.121		ET SCAN NMAP -sS window 3072	1
93.174.93.181	Netherlands	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1
159.122.111.166	Netherlands	147.237.0.121		ET SCAN NMAP -sS window 1024	1
172.98.200.237		147.237.0.121		ET SCAN NMAP -sS window 2048	1
184.173.48.221	United States	147.237.0.121		ET SCAN NMAP -sS window 1024	1
218.246.0.97	China	147.237.0.121		ET SCAN NMAP -sS window 1024	1
114.112.90.54	China	147.237.0.121		ET SCAN NMAP -sS window 1024	1

01-23-2016 to 01-24-2016

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	1100
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1049
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	830
62.194.173.206	Netherlands	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	486
149.78.75.203	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	176
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	151
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	149
149.78.254.125	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	135
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	131
188.201.183.105	Netherlands	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	88
149.88.189.227	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	80
149.78.230.122	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	74
149.78.42.29	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	68
66.249.82.149	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	52
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	47
84.80.116.238	Netherlands	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	44
149.78.222.223	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	41
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	35
66.249.81.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	33
217.69.133.191	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
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
66.249.93.214	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
79.180.143.133	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	23
37.142.203.3	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	22
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
37.142.203.3	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	22
77.125.150.68	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	21
64.120.47.235	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	21
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
24.99.67.57	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
66.249.93.208	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
109.160.175.133	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
77.127.61.51	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
109.160.175.133	Israel	147.237.0.121		Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
82.81.48.142	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	16
54.84.111.66	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
149.78.176.91	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	11
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	11
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	11
66.249.81.254	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	10
209.126.117.15	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	10
173.245.115.77	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	9
37.26.146.183	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	9
188.120.148.200	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	9
66.249.93.211	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	9
66.249.93.238	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

01-23-2016 to 01-24-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
109.67.217.171	Israel	147.237.0.121		Unauthorized HTTP Method	Block	16
95.86.86.177	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	3
192.114.91.232	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	2
46.19.86.7	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	2
46.19.85.158	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.181.25.58	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 79.181.25.58 (sigalgs DoS Attack)	None	1
109.186.43.100	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 109.186.43.100 (Open Mode)	None	1
79.181.25.58	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
37.46.39.208	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1
212.179.8.162	Israel	147.237.0.121		Unknown Parameter ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/smsverify	Block	1
109.64.169.59	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected AEBBA3598646C87D6C896195F99675AC5533833228310585514E2A9B95498A42A9B1CDFACAE29FCE7BEDE3D166706844FC694438E06D484591CAC9F27C07730E7B3FB391932A2A13D77C0A8A1E6F215DDFC874DB2B9E2758D58E9EECE25B07867F8313BC49D772B104BFF03FEF1D919313D0FFCCDE9951F87EE5003BAA02FB76, Observed A0D43D7C44C989AC665CCE27079BCF68B89FFC4D3294D9A77CF87839D5879D590122575C9CEDC86240A73185D5354E51A9A17C25A55DCE454700BA03F82803F1F643936565DA1D13BE7642F1C3234AB18BC59A9805ADF891A17342B6DE0F64EC27B944	None	1
79.178.161.254	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 79.178.161.254 (sigalgs DoS Attack)	None	1
109.186.43.100	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
79.182.61.51	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
37.142.68.32	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
213.8.204.23	Israel	147.237.0.121		Unknown Parameter zi in www.miluim-ishi.aka.idf.il/login	Block	1
109.66.119.74	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
79.178.161.254	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
109.253.157.82	Israel	147.237.0.121		Parameter Type Violation virt in www.miluim-ishi.aka.idf.il/cellularreference	Block	1
79.182.126.198	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/cellularreference parameter virt	Block	1

01-23-2016 to 01-24-2016