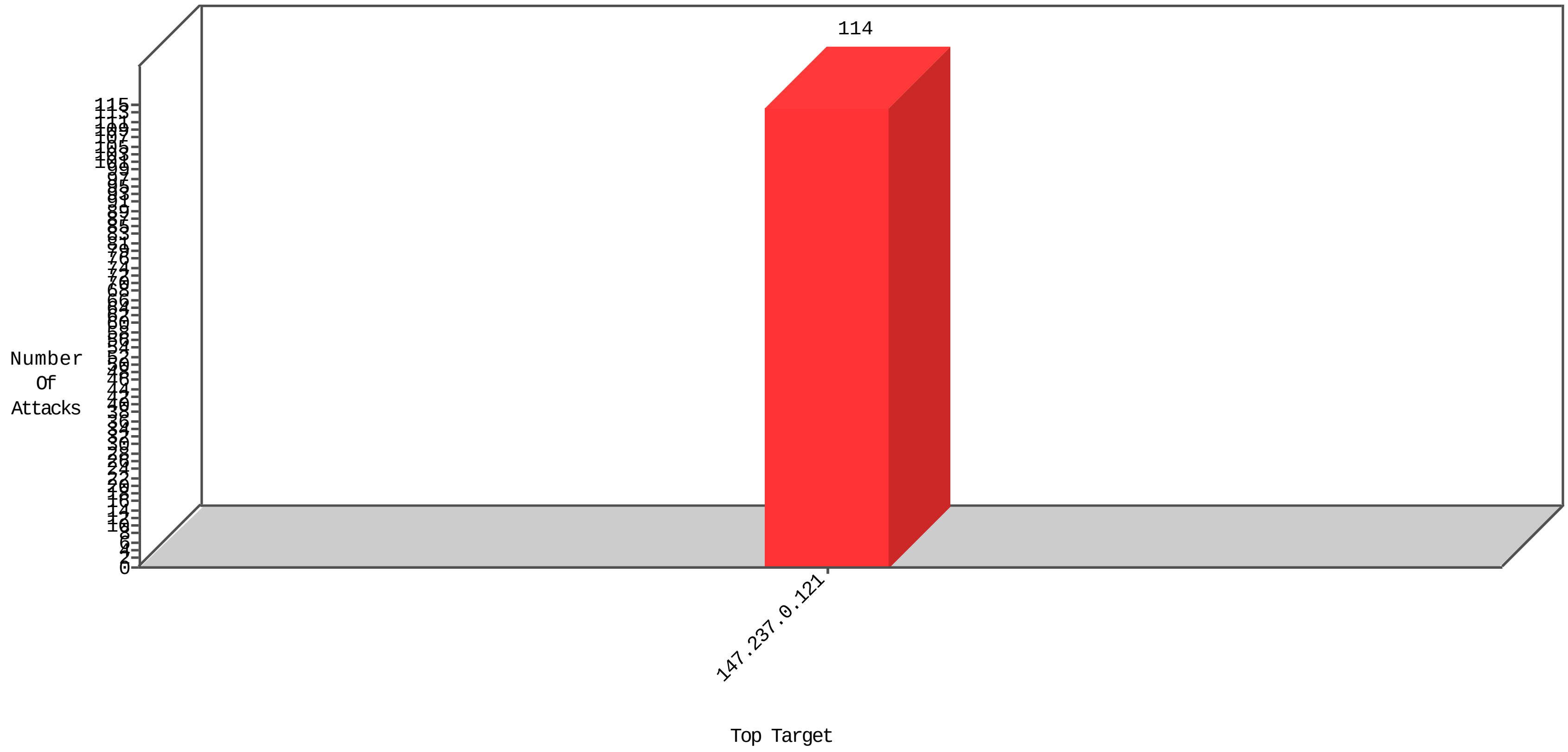
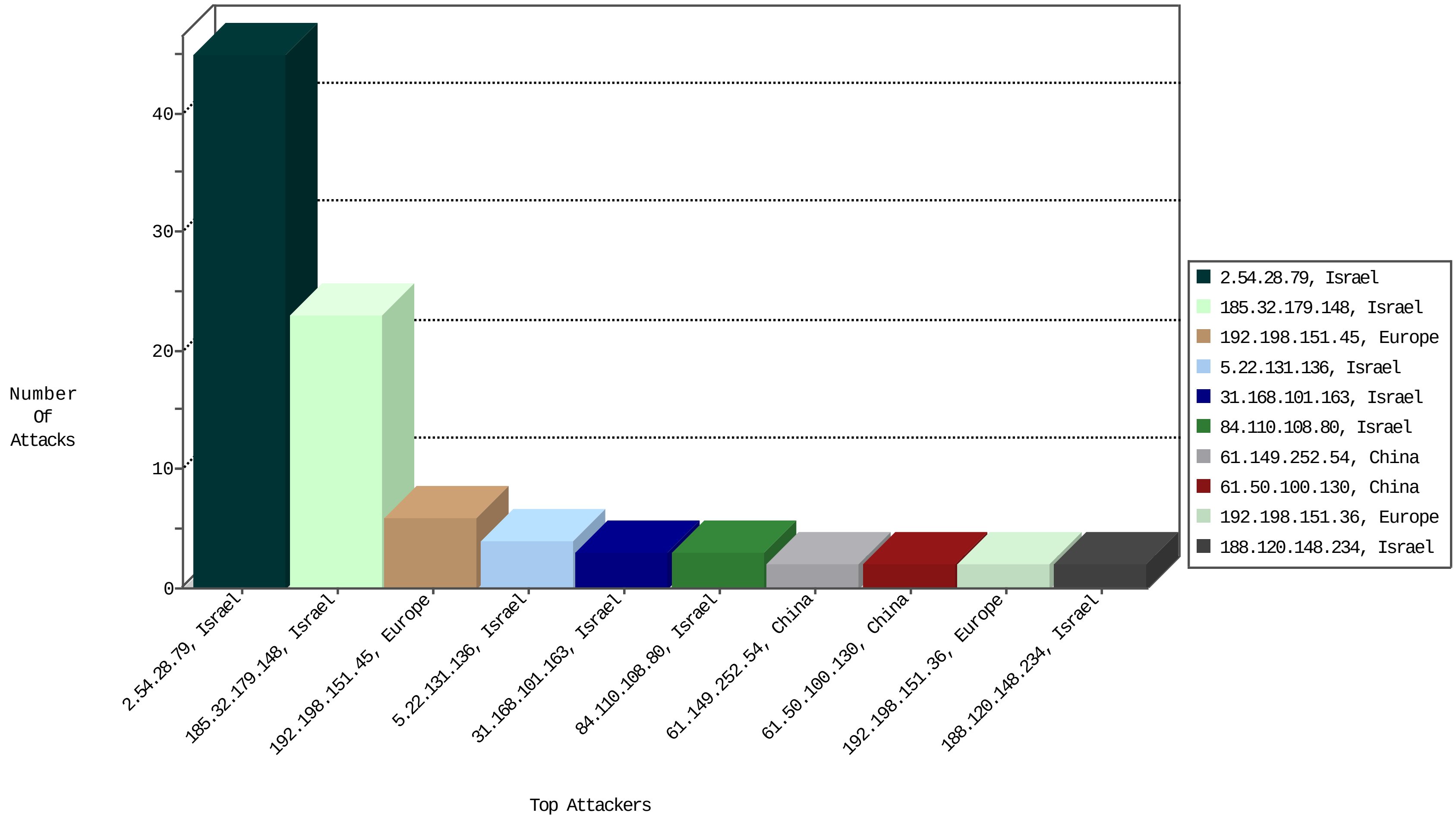
12-04-2015 to 12-05-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



12-04-2015 to 12-05-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
2.54.28.79	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	45
185.32.179.148	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	23

12-04-2015 to 12-05-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

12-04-2015 to 12-05-2015

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
192.198.151.36	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	2
36.110.44.178	China	147.237.0.121		ET SCAN NMAP -f -sS	1
61.50.100.130	China	147.237.0.121		ET SCAN NMAP -f -sS	1
61.149.252.54	China	147.237.0.121		ET SCAN NMAP -f -sS	1
61.149.252.58	China	147.237.0.121		ET SCAN NMAP -f -sS	1
61.182.170.38	China	147.237.0.121		ET SCAN Potential SSH Scan	1
213.168.248.217	Ireland	147.237.0.121		ET SCAN Potential SSH Scan	1
218.205.129.146	China	147.237.0.121		ET SCAN NMAP -sS window 2048	1
36.110.44.178	China	147.237.0.121		ET SCAN NMAP -sS window 2048	1
61.50.100.130	China	147.237.0.121		ET SCAN NMAP -sS window 2048	1
61.149.252.54	China	147.237.0.121		ET SCAN NMAP -sS window 2048	1
61.149.252.58	China	147.237.0.121		ET SCAN NMAP -sS window 2048	1
109.105.211.204	Bosnia and Herzegovina	147.237.0.121		ET SCAN Potential SSH Scan	1
218.205.129.146	China	147.237.0.121		ET SCAN NMAP -f -sS	1

12-04-2015 to 12-05-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.153	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1609
66.249.93.145	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1549
149.78.109.90	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1278
66.249.93.149	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1107
64.79.85.205	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	548
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	169
149.88.180.188	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	157
66.249.93.149	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	151
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	149
66.249.93.145	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	138
66.249.93.153	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	138
149.78.254.244	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	136
149.78.41.56	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	121
66.249.93.223	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	114
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	100
149.78.20.236	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	98
2.52.15.202	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	83
149.88.237.77	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	79
90.194.115.102	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	66
149.78.234.91	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	65
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	55
79.183.183.75	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	54
149.78.22.68	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	49
66.102.9.22	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
138.134.192.10	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	36
37.142.64.54	Israel	147.237.0.121		Bad TCP sequence		monitor	36
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	31
173.162.34.45	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	29
194.12.254.131	Bulgaria	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
209.135.211.206	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
66.249.81.251	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
66.249.93.247	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
149.88.226.62	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	24
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
66.249.81.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	21
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
66.249.93.215	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
46.19.86.89	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	18
66.249.81.129	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
66.249.81.167	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
188.120.148.148	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	17
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
66.249.93.241	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
66.249.80.42	Australia	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
5.102.254.205	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	16
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	14
149.78.176.158	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	14
66.249.93.241	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	14
66.102.9.39	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
84.110.108.80	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	3
31.168.101.163	Israel	147.237.0.121		Unknown Parameter ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/smsverify	Block	3
5.22.131.136	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 5.22.131.136 (sigalgs DoS Attack)	None	2
188.120.148.234	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	2
5.22.131.136	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	2
2.54.5.197	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
5.102.254.3	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
109.67.190.8	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
37.142.247.252	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
2.54.42.4	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.154.113	Israel	147.237.0.121		Parameter Type Violation __EVENTVALIDATION in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
5.102.254.163	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
176.12.144.220	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
46.19.86.65	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.160.25	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 109.65.160.25 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
79.177.63.143	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
109.65.160.25	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
37.142.247.252	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 37.142.247.252 (sigalgs DoS Attack)	None	1