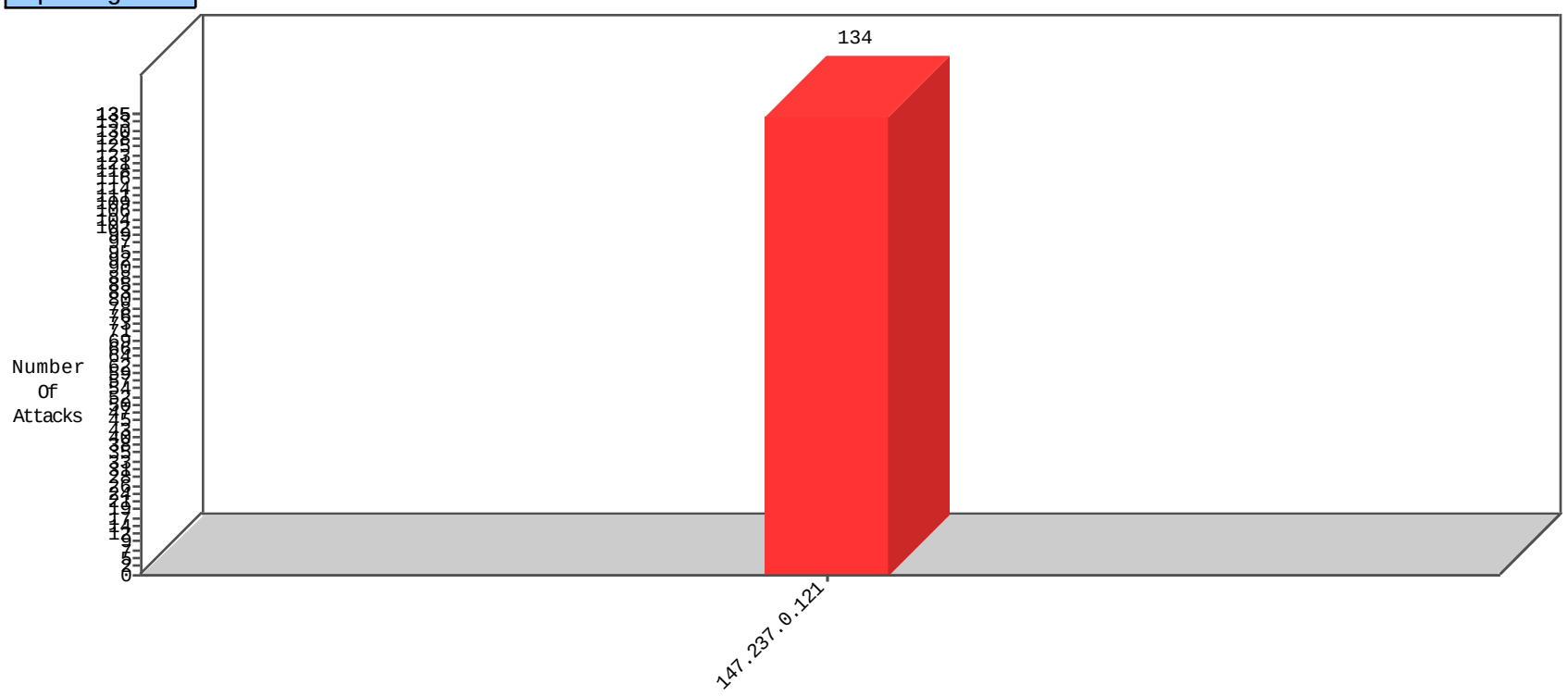
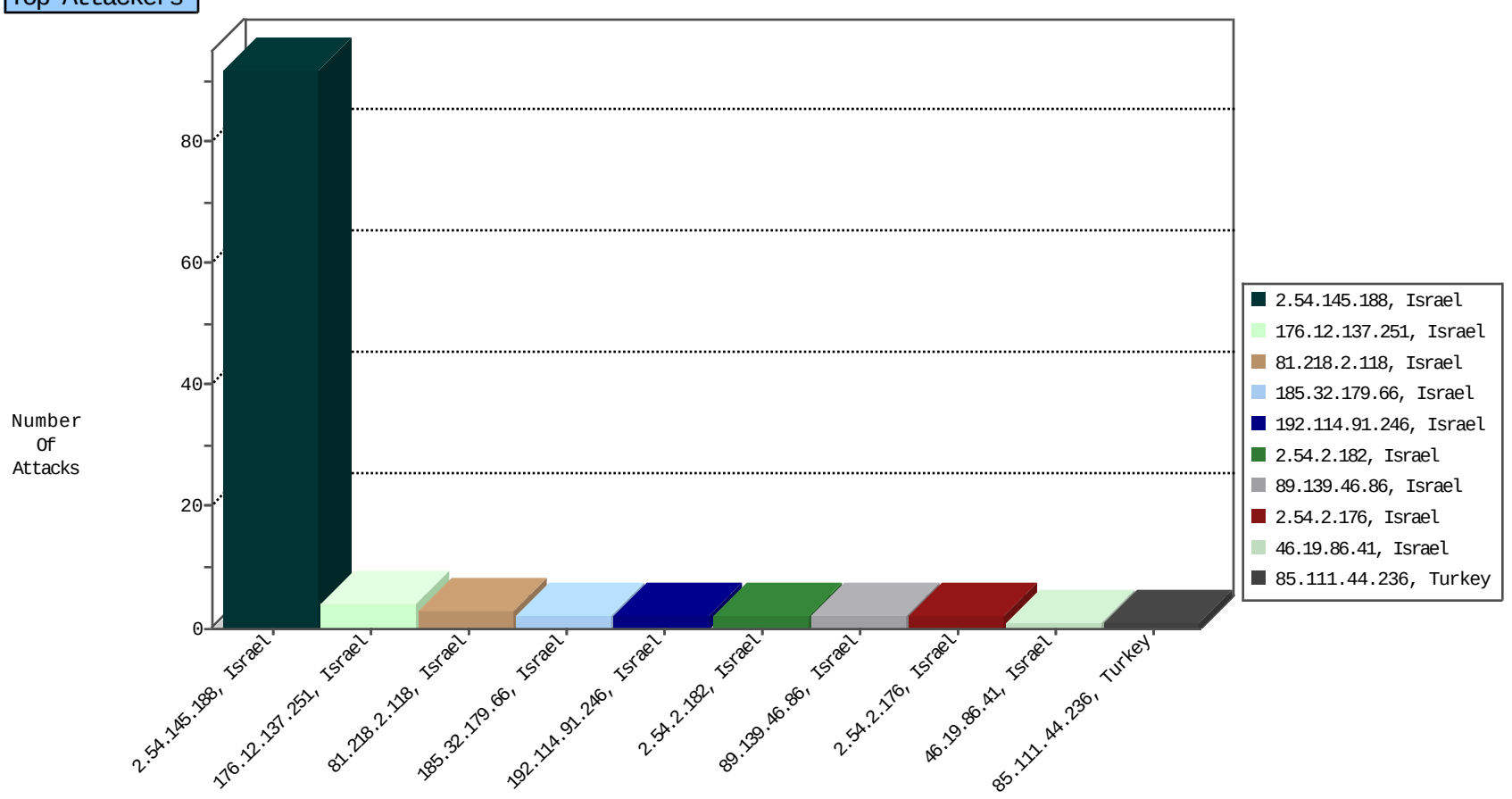
12-21-2015 to 12-22-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



12-21-2015 to 12-22-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
2.54.145.188	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	92
81.218.2.118	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3

12-21-2015 to 12-22-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

12-21-2015 to 12-22-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
191.237.42.242	United States	147.237.0.121		ET SCAN Potential SSH Scan	1
85.111.44.236	Turkey	147.237.0.121		ET SCAN Potential SSH Scan	1
187.120.82.122	Brazil	147.237.0.121		ET SCAN Potential SSH Scan	1
192.198.151.45	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	1
59.45.79.117	China	147.237.0.121		ET SCAN Potential SSH Scan	1
183.60.48.25	China	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1

12-21-2015 to 12-22-2015

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	2639
66.249.93.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2147
66.249.93.93	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1458
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1115
66.249.93.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1046
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	272
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	269
93.109.253.6	Cyprus	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	268
149.78.123.78	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	234
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	210
66.249.93.93	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	153
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	151
149.50.77.180	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	151
79.182.100.18	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
66.249.93.97	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	125
185.3.144.70	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	117
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	102
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	85
207.46.13.151	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	71
13.17.125.9	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	68
149.78.63.20	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	64
66.102.6.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	62
13.21.125.9	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	60
149.78.234.31	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	52
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	49
157.55.39.253	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	38
2.52.3.198	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	36
77.125.149.122	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
2.52.3.198	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	36
2.52.3.198	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	36
152.62.109.210	Europe	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	30
149.78.53.87	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	29
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	29
66.249.93.211	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
2.54.145.188	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
212.68.132.218	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	25
66.249.69.170	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
2.54.13.27	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	21
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
66.249.69.165	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
2.52.55.186	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	17
66.249.69.170	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
66.249.93.236	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
66.249.93.56	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
157.55.39.26	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	15
157.55.39.221	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	15
5.22.134.76	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	14

12-21-2015 to 12-22-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
176.12.137.251	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 176.12.137.251 (sigalgs DoS Attack)	None	3
185.32.179.66	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.2.182	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
192.114.91.246	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
132.64.26.112	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
77.125.74.179	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected , Observed 012E0D0F6702E8BAEAF6D5D97FFC2FAED992C4E6A4E121E6A85289F47EE83B1E4DEC64AB7EF998B30570F363AB9F69DB46C7F306ED526E66B251E44820C9663C0428F01A14F6E84BD589F7C85CB4ABC2DAE34F76674E494B0BE168FCE634DAC2E8C0C83183E57BA88726B731C0B49B35C70DEBCACF6C60920F23D7C79AD083C5D37610CAAF1A07DAB19EF60EC3C2CAC2E32A9A9F0E23A79E57D6F2E39A8097C0	None	1
5.102.214.250	Israel	147.237.0.121		Double URL Encoding - parameter: ReturnUrl in www.miluim-ishi.aka.idf.il/login	Block	1
2.54.2.176	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 2.54.2.176 (sigalgs DoS Attack)	None	1
176.13.23.163	Israel	147.237.0.121		Double URL Encoding - parameter: ReturnUrl in www.miluim-ishi.aka.idf.il/login	Block	1
89.139.46.86	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
46.19.86.239	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.5.77	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.179.188.234	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	1
46.19.85.6	Israel	147.237.0.121		Parameter Type Violation __EVENTVALIDATION in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
2.54.2.176	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
93.172.27.237	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
62.90.126.184	Israel	147.237.0.121		Suspicious Response Code	Block	1
2.54.144.189	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPass in www.miluim-ishi.aka.idf.il/login	Block	1
176.12.137.251	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
83.130.115.227	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
46.19.86.18	Israel	147.237.0.121		Double URL Encoding - parameter: ReturnUrl in www.miluim-ishi.aka.idf.il/login	Block	1
2.54.2.182	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 2.54.2.182 (sigalgs DoS Attack)	None	1
192.114.91.246	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 192.114.91.246 (Open Mode)	None	1
109.64.201.56	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/1399-he/miluim.aspx	Block	1
62.219.234.126	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
5.29.74.249	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
2.52.147.214	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
176.13.18.45	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
89.139.46.86	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 89.139.46.86 (sigalgs DoS Attack)	None	1
46.19.86.41	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1

12-21-2015 to 12-22-2015