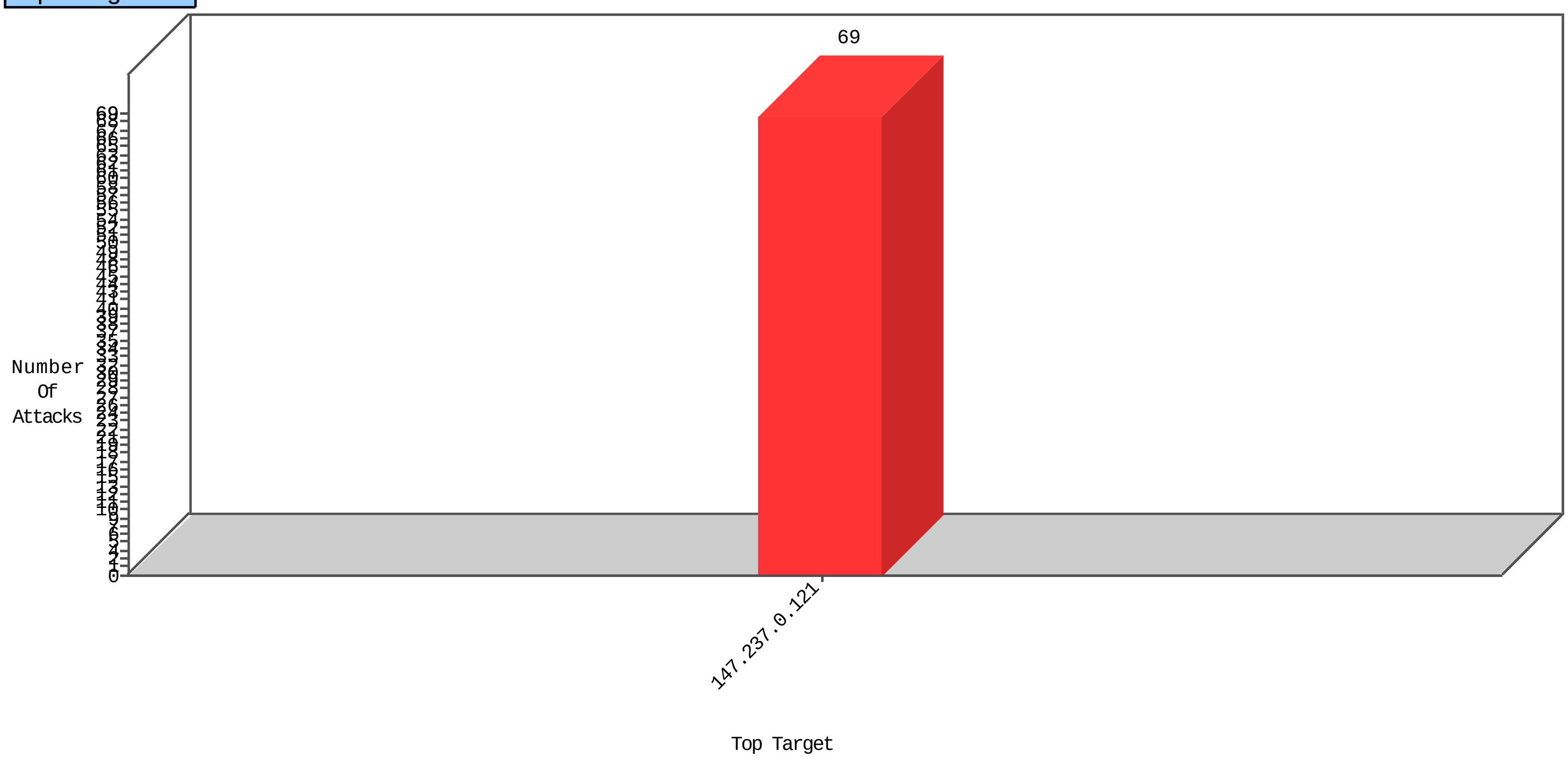
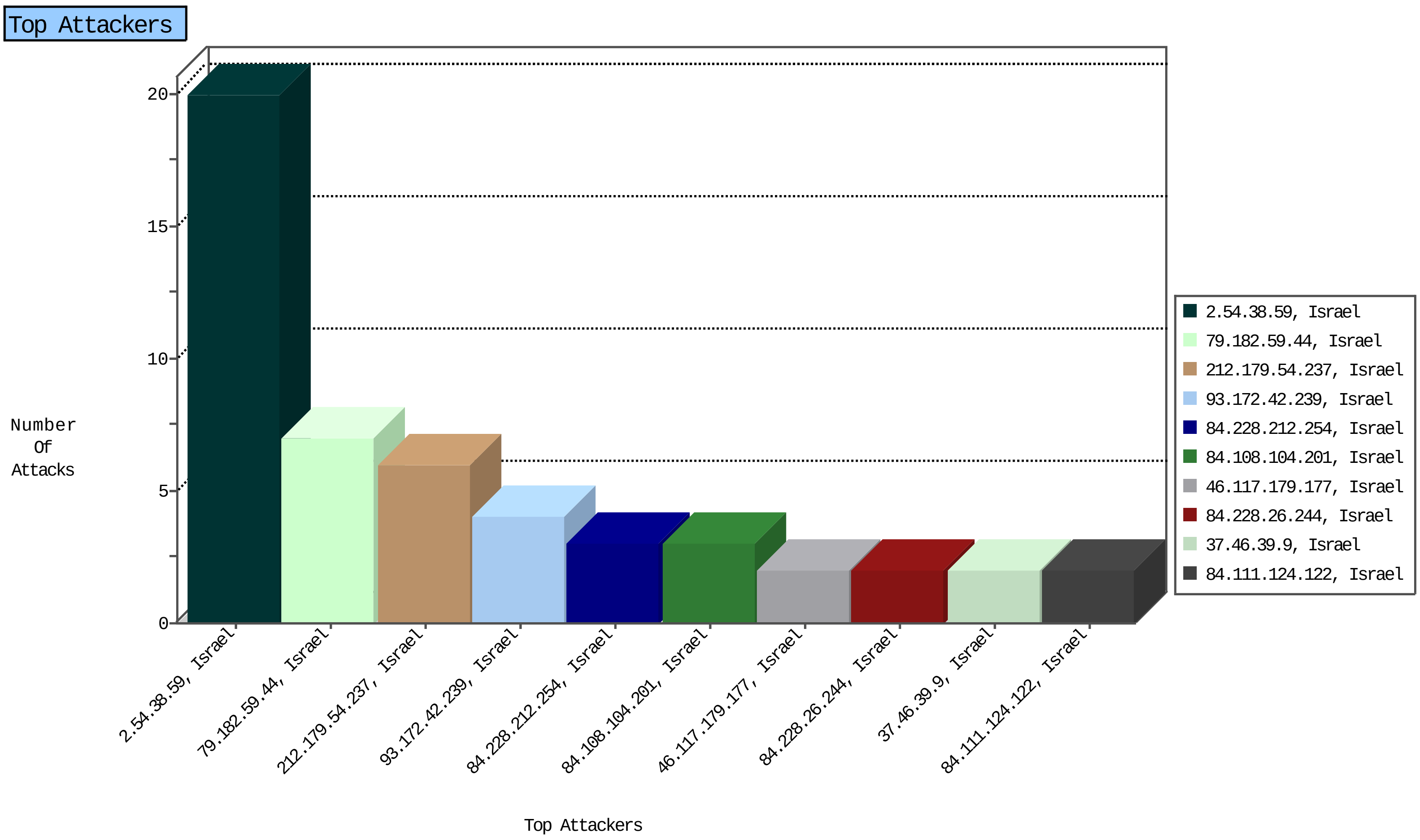
02-13-2016 to 02-14-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



02-13-2016 to 02-14-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
2.54.38.59	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	20
212.179.54.237	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	6

02-13-2016 to 02-14-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

02-13-2016 to 02-14-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
61.244.111.77	Hong Kong	147.237.0.121		ET SCAN Potential SSH Scan	1
183.82.106.200	India	147.237.0.121		ET SCAN NMAP -sS window 1024	1
46.45.137.67	Turkey	147.237.0.121		ET SCAN NMAP -sS window 1024	1
79.182.59.44	Israel	147.237.0.121		ET DOS SSL Bomb DoS Attempt	1
218.200.188.213	China	147.237.0.121		ET SCAN Potential SSH Scan	1

02-13-2016 to 02-14-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
149.78.151.84	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1295
149.88.142.117	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1009
139.181.48.2	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	870
149.78.253.154	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	756
149.78.221.220	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	629
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	550
149.78.23.38	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	516
85.115.52.201	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	504
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	456
149.78.234.95	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	333
149.78.1.229	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	331
149.78.218.168	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	314
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	270
149.88.149.123	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	262
149.88.21.171	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	245
149.78.27.221	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	191
149.88.198.241	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	179
149.78.245.131	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	173
149.50.97.37	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	150
149.78.196.122	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	105
149.78.34.82	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	94
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	92
5.29.183.191	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	90
149.78.48.204	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	89
149.88.225.203	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	87
149.78.250.79	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	79
149.88.71.71	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	71
149.78.30.244	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	67
149.88.77.45	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	62
108.171.135.165	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	60
40.114.210.53	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	58
79.181.136.215	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
190.242.47.19	Colombia	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	50
149.78.128.23	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	48
149.88.196.104	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	42
149.78.43.80	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	41
2.54.38.59	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	41
109.67.185.169	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
82.81.23.71	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	33
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	33
212.99.116.110	France	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28
66.102.9.44	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
199.255.138.45	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
149.88.109.74	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	19
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
79.182.59.44	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
84.228.26.244	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
149.50.95.40	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
149.88.165.95	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
79.182.59.44	Israel	147.237.0.121		Suspicious Response Code	Block	6
46.117.179.177	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	2
93.172.42.239	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	2
84.228.212.254	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 84.228.212.254 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	2
84.108.104.201	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	2
37.46.39.9	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	2
93.172.42.239	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 93.172.42.239 (sigalgs DoS Attack)	None	2
84.229.42.182	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPass in www.miluim-ishi.aka.idf.il/login	Block	1
84.111.124.122	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 84.111.124.122 (sigalgs DoS Attack)	None	1
83.130.109.77	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
198.20.69.74	United States	147.237.0.121		Unauthorized URL Access to 147.237.0.121/	Block	1
85.65.36.7	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
84.111.124.122	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
77.125.140.209	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
93.173.3.222	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/sms	Block	1
84.228.212.254	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
84.108.104.201	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 84.108.104.201 (sigalgs DoS Attack)	None	1
5.102.195.157	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
213.57.7.4	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/smsverify+	Block	1
93.172.40.253	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
84.228.26.244	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 84.228.26.244 (Open Mode)	None	1
79.181.136.215	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
109.67.190.238	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 6C378EE46E75FB0395B5F0B558761BB0CD036C4DC758544B5958D4D89F74E4B78462326A5753916133C5DC7833B2759603C95A6B163211948685FED268301906DA567AD7ACFCFCF2689448CF79FBEBE5C4A5E5B57D65490015FF9CCBFFFAD8590FD5C153F48A6BEA97A026A4CF2F090FF039BF449E4EF356571F959033629CE3, Observed 271274B503397CD03F09A361E41694B87C8B43C748BE14FE613FBD7005FE57449EAA55969DAB4F9D38A9F61D969265990107701ABA64FBEFF95EFC0D23559C6263D28543B421D349F590E6D1E7F2FD8D82B132BDCAC9880BE7048167AC7D88EF16D076	None	1
84.228.236.233	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/s	Block	1
217.132.130.249	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
84.228.26.244	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
176.13.15.166	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1