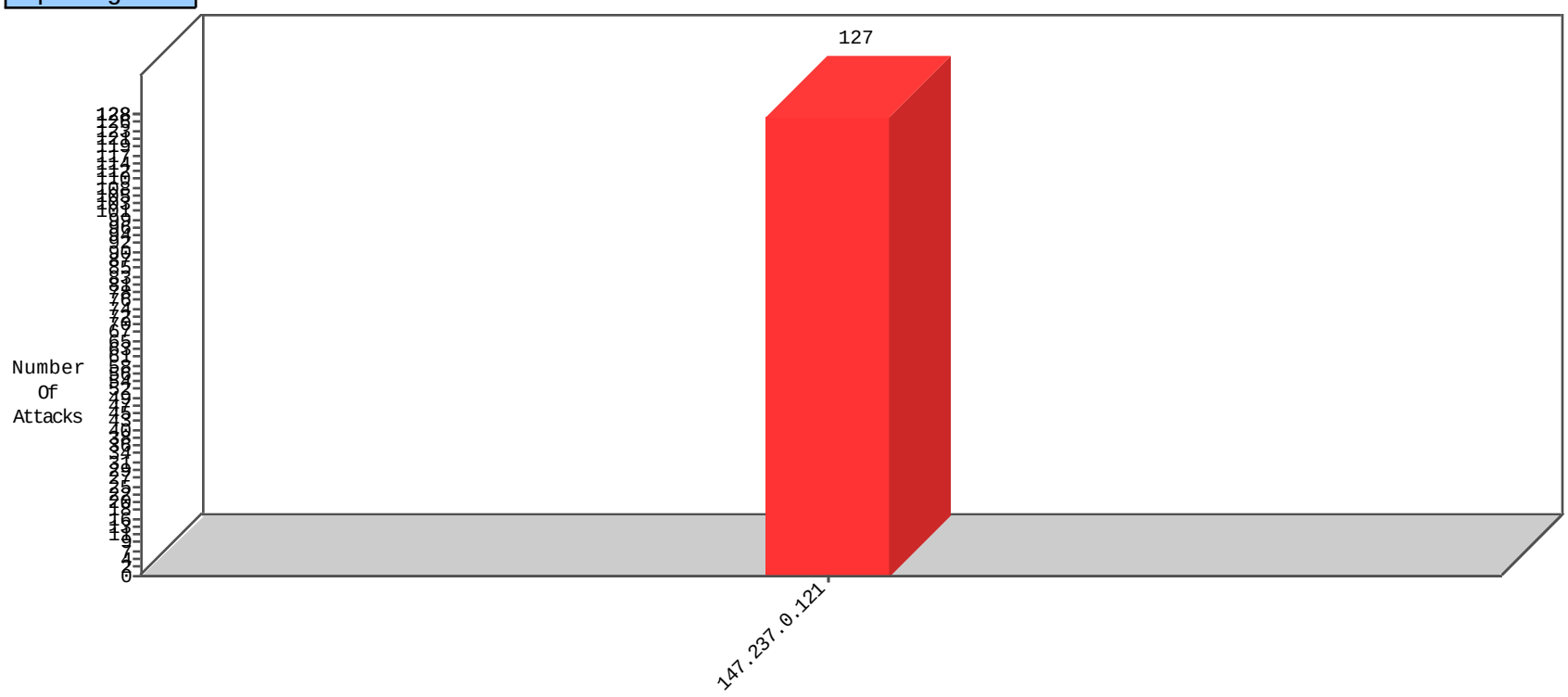
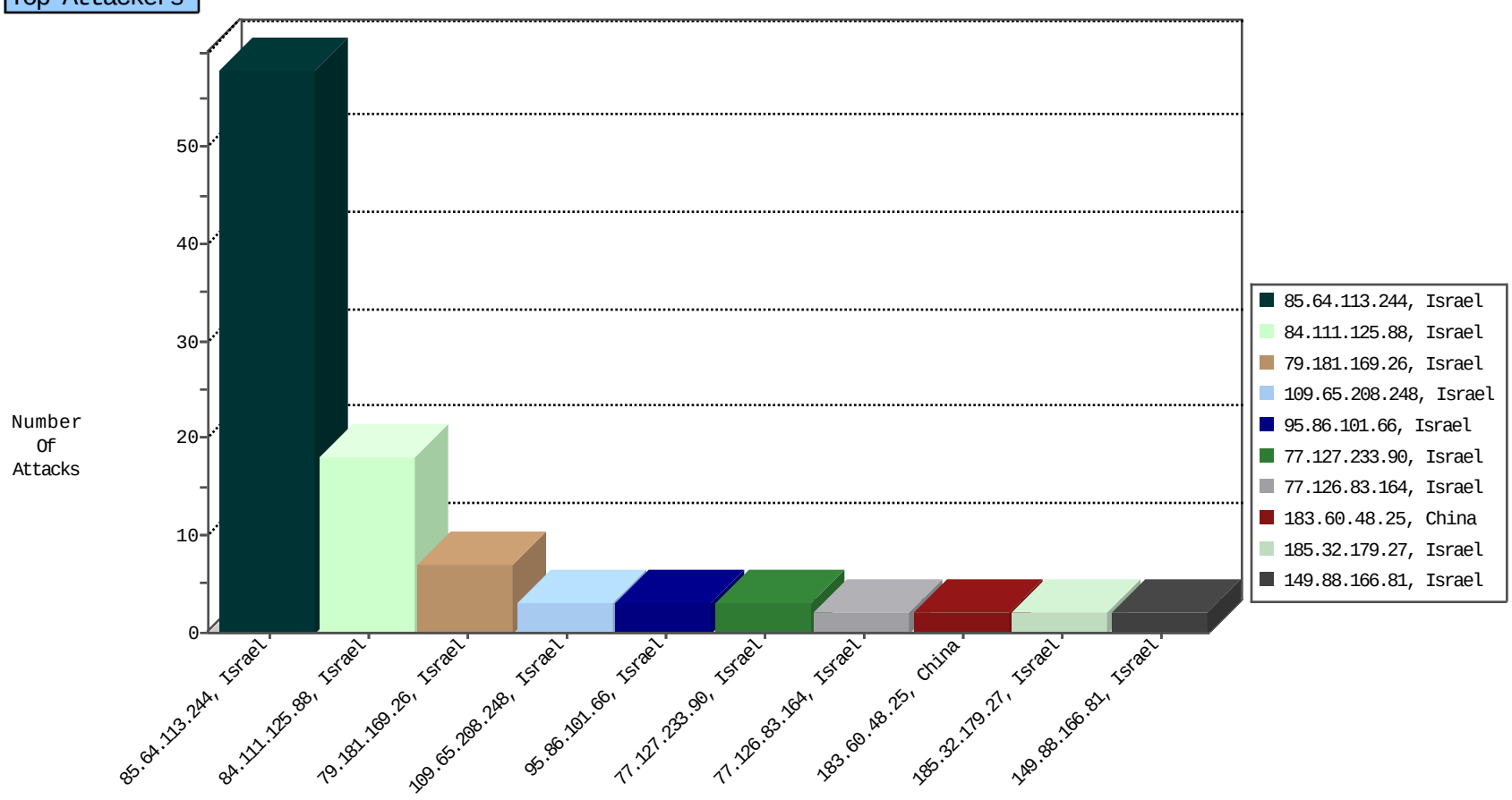
02-27-2016 to 02-28-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



02-27-2016 to 02-28-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
84.111.125.88	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	18
185.130.5.173		147.237.0.121		JLM_Under_Attack_Con_Tcp	drop	NetV-London	2
149.88.166.81	Israel	147.237.0.121		Invalid TCP Flags	drop	BBL-Israel	2
205.209.185.11	United States	147.237.0.121		Block_Ntp_All_Net	drop	NetV-London	1
184.105.139.82	United States	147.237.0.121		Block_Ntp_All_Net	drop	NetV-London	1
184.105.139.116	United States	147.237.0.121		Block_Ntp_All_Net	drop	NetV-London	1
185.40.4.98		147.237.0.121		Block_Udp_All_Nets	drop	NetV-London	1
185.94.111.1		147.237.0.121		Block_Udp_All_Nets	drop	NetV-London	1

02-27-2016 to 02-28-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

02-27-2016 to 02-28-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
183.60.48.25	China	147.237.0.121		ET SCAN Potential SSH Scan	1
194.63.140.74	Russian Federation	147.237.0.121		ET SCAN Potential SSH Scan	1
180.191.105.107	Philippines	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
202.170.80.40	Mongolia	147.237.0.121		ET SCAN Potential SSH Scan	1

02-27-2016 to 02-28-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
80.81.125.58	Spain	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1170
97.84.247.179	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	761
149.78.86.160	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	491
208.81.64.248	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	408
176.13.12.168	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	324
149.88.56.171	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	229
149.78.28.152	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	214
98.139.248.67	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	212
149.78.23.162	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	202
178.248.90.71	Italy	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	158
149.78.181.169	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	150
40.77.167.37	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	150
2.54.180.162	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
149.88.49.199	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	138
149.78.230.199	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	118
149.78.229.49	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	105
149.88.24.27	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	96
149.78.180.56	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	89
149.88.31.164	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	86
149.88.24.5	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	83
149.78.67.66	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	56
149.50.80.156	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	50
149.50.84.46	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	46
84.108.249.169	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	45
149.88.166.81	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	44
149.78.146.230	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	42
149.88.201.72	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
149.78.46.1	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	38
149.88.127.190	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	33
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	31
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	29
149.88.55.192	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28
12.21.46.2	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
84.108.3.7	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	25
149.78.207.76	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
217.69.133.248	Russian Federation	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
77.127.192.217	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	22
149.88.128.169	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	19
149.78.103.29	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
212.214.229.27	Sweden	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
37.142.136.98	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
149.78.157.205	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13
149.78.69.60	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13
149.78.32.152	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13
66.102.9.22	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13
149.78.128.23	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	12
66.102.9.44	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	11

02-27-2016 to 02-28-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
85.64.113.244	Israel	147.237.0.121		Unauthorized HTTP Method	Block	32
85.64.113.244	Israel	147.237.0.121		Multiple Unauthorized URL Access from 85.64.113.244	Block	25
79.181.169.26	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 79.181.169.26 (sigalgs DoS Attack)	None	6
95.86.101.66	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	3
77.127.233.90	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	3
89.138.239.148	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	2
109.65.208.248	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 109.65.208.248 (sigalgs DoS Attack)	None	2
84.109.16.188	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	2
77.126.83.164	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	2
2.54.28.15	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	2
185.32.179.27	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	2
79.182.102.90	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
5.29.168.89	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	1
109.66.60.111	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
79.176.229.76	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
193.43.245.250	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
84.108.224.86	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
46.120.166.156	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
109.67.33.17	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
85.64.113.244	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/img/	Block	1
2.52.175.254	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
138.36.0.3		147.237.0.121		Unauthorized URL Access to 147.237.0.121/index.php	Block	1
89.138.163.102	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
79.181.169.26	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
109.65.208.248	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1

02-27-2016 to 02-28-2016