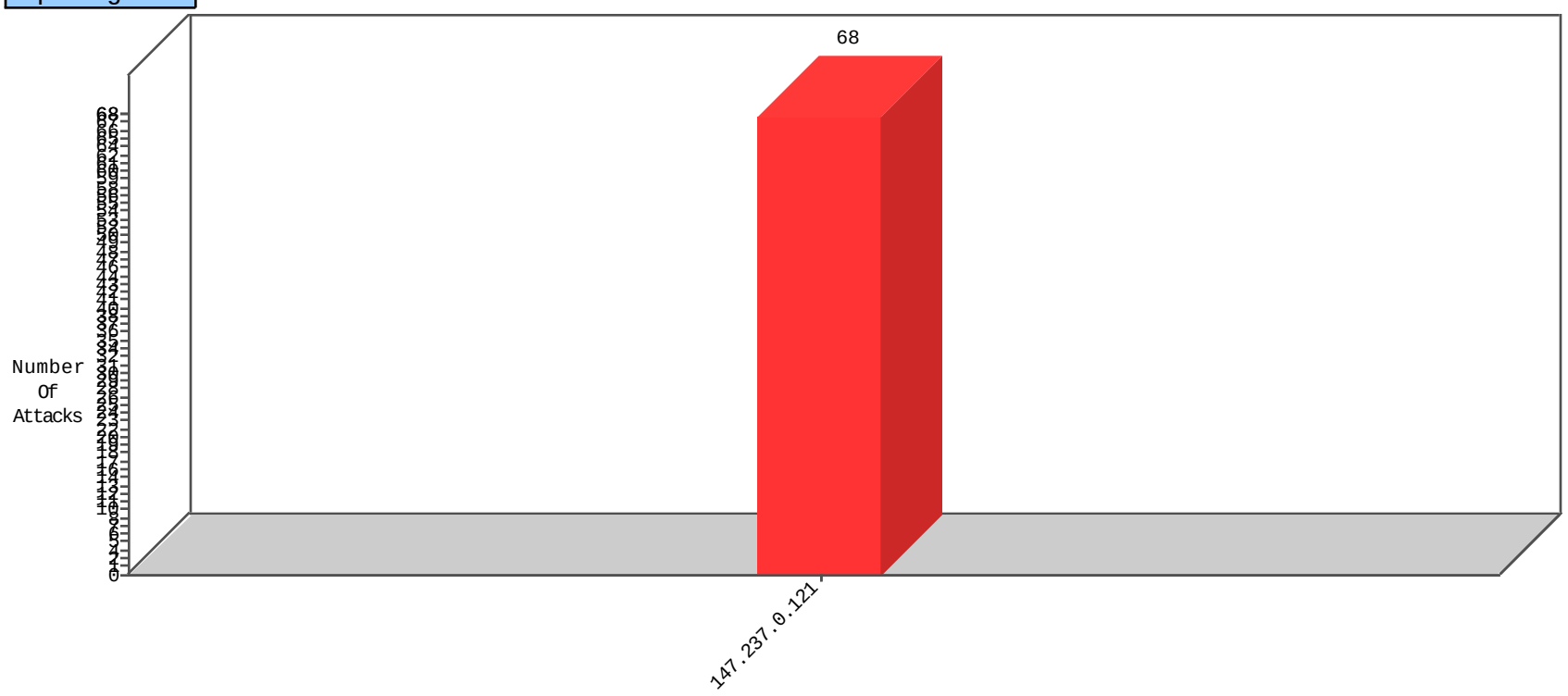
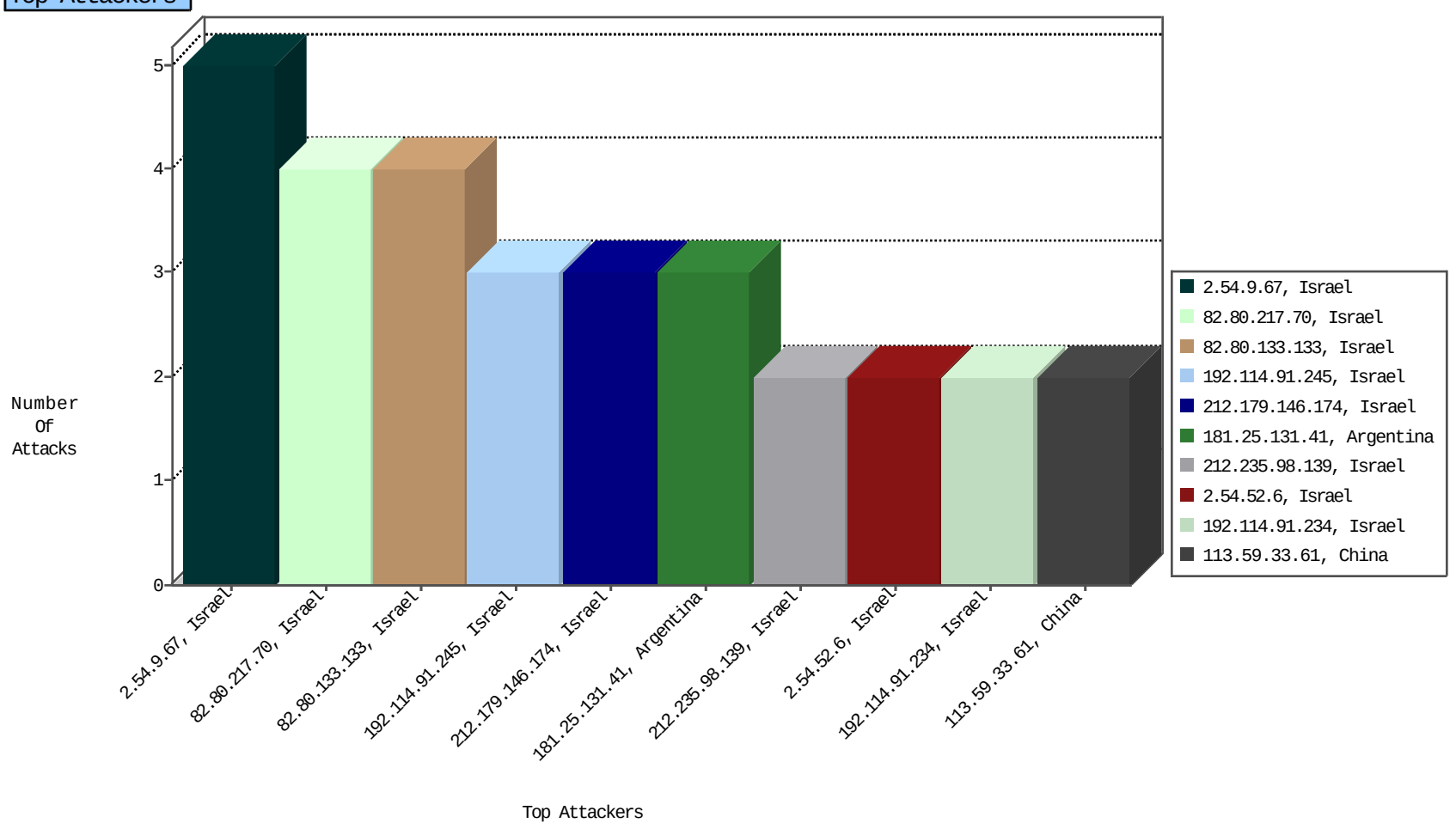
12-15-2015 to 12-16-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



12-15-2015 to 12-16-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
82.80.217.70	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3
212.179.146.174	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3
192.118.132.185	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	2

12-15-2015 to 12-16-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

12-15-2015 to 12-16-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
192.198.151.37	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	2
59.45.79.117	China	147.237.0.121		ET SCAN Potential SSH Scan	1
113.59.33.61	China	147.237.0.121		ET SCAN NMAP -f -sS	1
137.117.34.247	United States	147.237.0.121		ET SCAN Potential SSH Scan	1
109.186.1.100	Israel	147.237.0.121		ET SCAN NMAP -sA (2)	1
113.59.33.61	China	147.237.0.121		ET SCAN NMAP -sS window 2048	1
178.169.143.78	Bulgaria	147.237.0.121		ET SCAN NMAP -sS window 4096	1
192.198.151.45	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	1

12-15-2015 to 12-16-2015

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	3111
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2624
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2573
149.78.6.241	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	920
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	327
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	275
149.78.62.113	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	268
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	246
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	244
77.180.44.128	Germany	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	217
2.52.154.88	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	216
66.249.93.93	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	186
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	154
27.55.174.121	Thailand	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	152
79.182.29.192	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	142
149.78.241.12	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	124
66.249.93.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	114
217.149.241.2	Poland	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	113
46.19.85.181	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
149.78.251.113	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	78
84.94.109.16	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
149.78.242.29	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	70
149.88.24.88	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	64
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	64
24.23.174.144	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	59
149.88.89.180	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	54
66.102.9.22	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	48
217.69.133.169	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	44
149.88.241.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	44
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	40
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	33
66.102.9.33	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	32
149.88.185.109	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	29
169.253.194.1	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
149.78.63.20	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	24
212.150.66.161	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	20
66.102.6.147	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	19
66.102.6.149	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	19
66.102.9.61	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	19
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
178.62.85.75	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
149.78.225.234	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
66.249.93.17	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
66.249.93.53	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
132.72.176.144	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
62.128.45.222	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	16
5.102.254.154	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	16
83.223.122.22	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	12
66.102.6.153	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	11

12-15-2015 to 12-16-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
82.80.133.133	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$Submit1 in www.miluim-ishi.aka.idf.il/changeunit	Block	4
192.114.91.245	Israel	147.237.0.121		Suspicious Response Code	Block	3
31.168.225.146	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	2
2.54.9.67	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.52.6	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.136.204	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.9.67	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	2
217.132.57.254	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.4.23	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
212.235.98.139	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 212.235.98.139 (Open Mode)	None	1
192.114.91.234	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 192.114.91.234 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
93.173.53.126	Israel	147.237.0.121		Unknown Parameter ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/smsverify	Block	1
79.181.196.73	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 672D484E4582424CC7BFB4EF7A49BD65E893D5882E8BF5CBE77E18BF51EF4C71DA444100AE7F8C30360590319FCB1B4104BA1A81ABA6F0817CC404795ABB6D5125235E85BDDA4A2CA549E37CD8653267824346C69DDFD79CB29112F731FD775D918774A1D118D09EAEB441D7D3B8C2C4996DE36CF9ACE288A08CF0EBCA3A7D91, Observed FED98605D32D5BEC4DE16D6AD85B4398F56FD09FBE3AAAF9B8C358510A08DB6F0D3096FC65196010EF782682EF88722A9E790DCFBD58EC286897FA97E4ED933AB9D81F6735D4473512F3336622EDFB139465E0C10EFE7BB707097FA1F6A829212FE577	None	1
2.54.168.10	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.20.64	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.179.21.194	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	1
181.25.131.41	Argentina	147.237.0.121		Multiple Untraceable SSL Sessions from 181.25.131.41 (sigalgs DoS Attack)	None	1
84.229.49.40	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
31.210.186.215	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
212.235.98.139	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
192.114.91.234	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
93.173.242.212	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
2.54.190.66	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
2.54.9.67	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 2.54.9.67 (sigalgs DoS Attack)	None	1
212.179.62.20	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
181.25.131.41	Argentina	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
85.64.244.63	Israel	147.237.0.121		Suspicious Response Code	Block	1
37.142.68.117	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
213.8.39.241	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
147.236.38.69	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
82.80.217.70	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/rules.abe	Block	1
31.44.128.151	Israel	147.237.0.121		Unknown Parameter ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/smsverify	Block	1
212.179.129.6	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
181.25.131.41	Argentina	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
87.68.244.93	Israel	147.237.0.121		Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login	Block	1
77.126.21.40	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
2.54.160.132	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
212.25.84.200	Israel	147.237.0.121		Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login	Block	1
83.130.113.213	Israel	147.237.0.121		Distributed Unauthorized URL Access on www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1

12-15-2015 to 12-16-2015