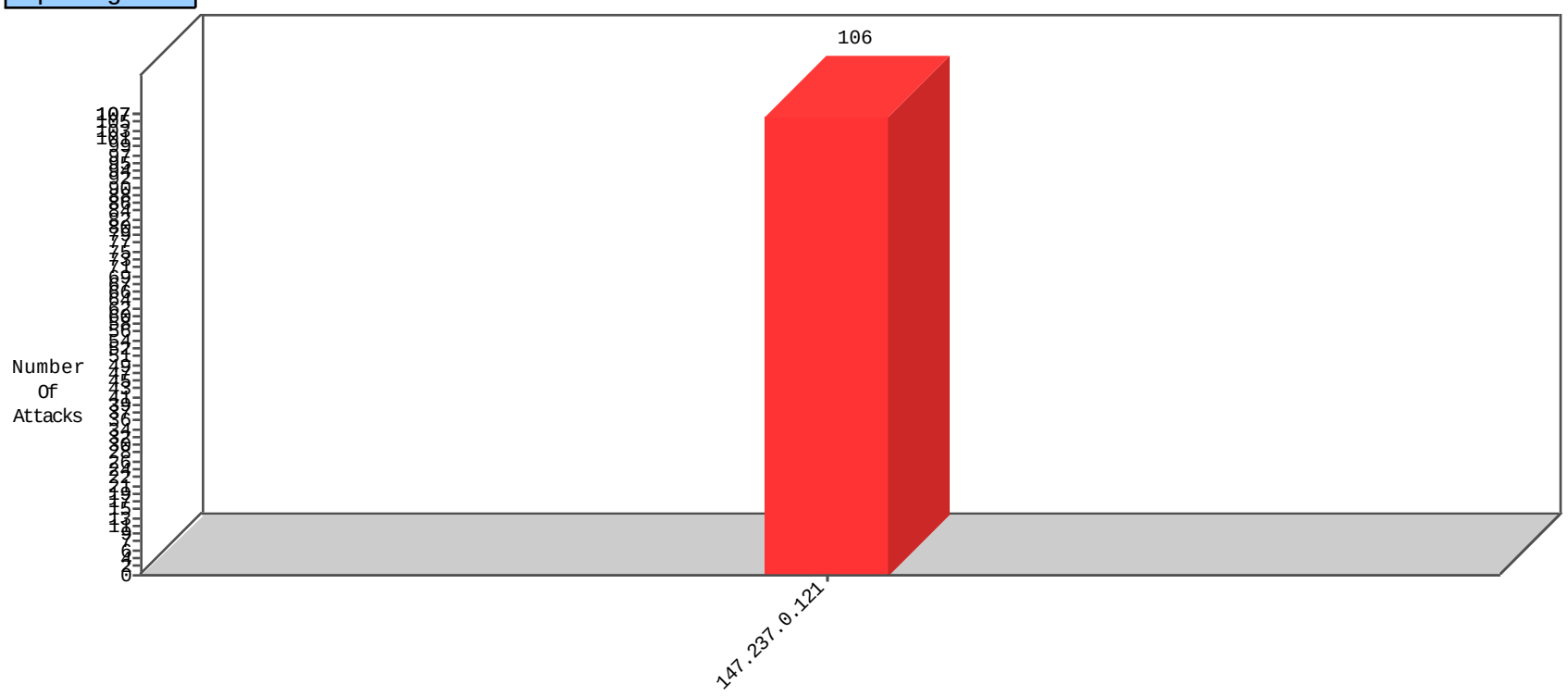
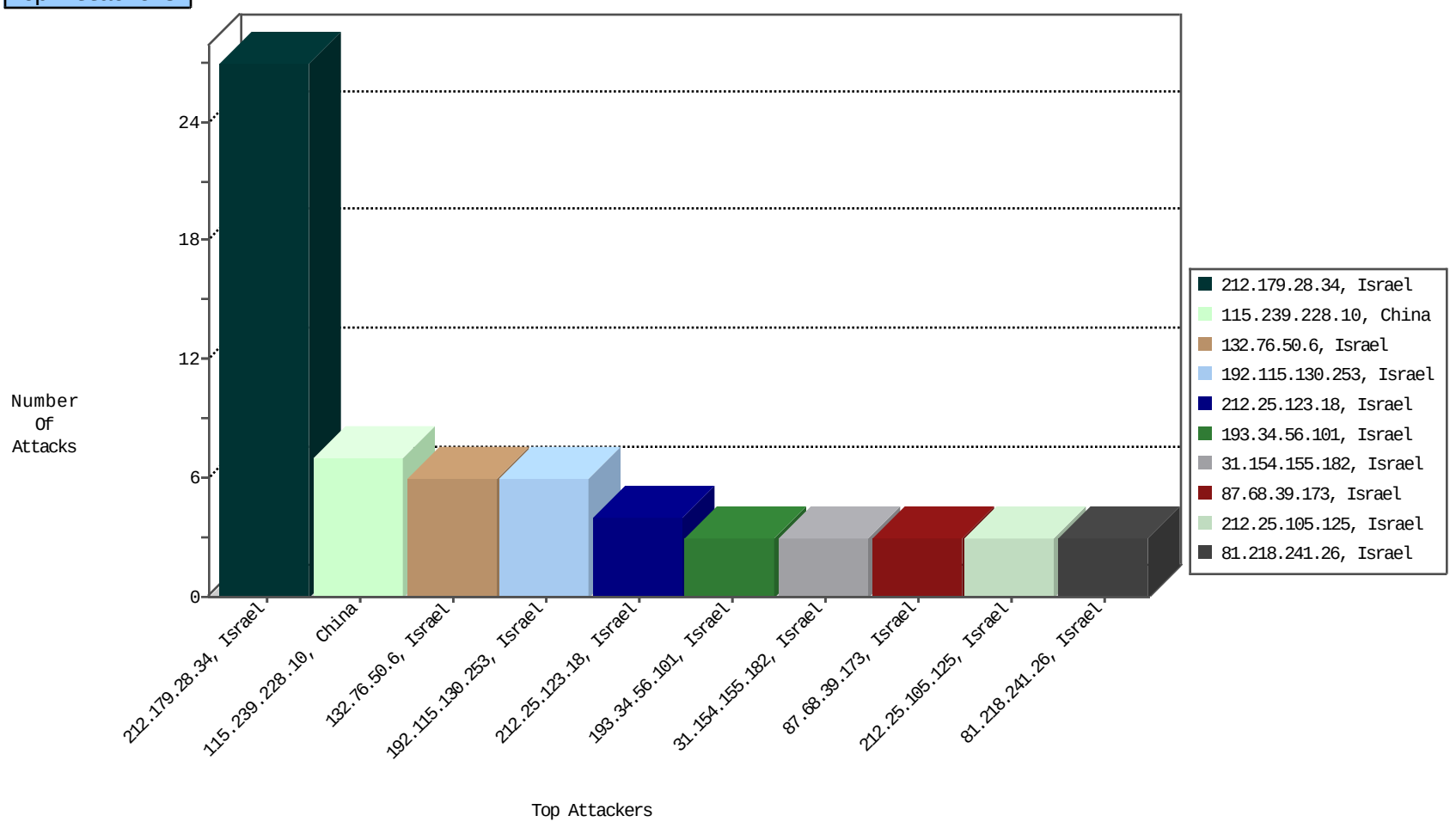
12-22-2015 to 12-23-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



12-22-2015 to 12-23-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
212.179.28.34	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	27
115.239.228.10	China	147.237.0.121		Frk_Under_Attack_Con_Http	drop	BBL-Frankfurt	4
115.239.228.10	China	147.237.0.121		Frk_Purple_Con_Limit_Http	drop	BBL-Frankfurt	3

12-22-2015 to 12-23-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

12-22-2015 to 12-23-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
45.63.8.95		147.237.0.121		ET SCAN NMAP -sS window 1024	1
125.211.216.68	China	147.237.0.121		ET SCAN Potential SSH Scan	1
212.25.105.125	Israel	147.237.0.121		SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
51.254.44.137	United Kingdom	147.237.0.121		ET SCAN Potential SSH Scan	1
183.60.48.25	China	147.237.0.121		ET SCAN Potential SSH Scan	1

12-22-2015 to 12-23-2015

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	2989
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2841
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2509
108.171.128.172	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	490
159.203.134.134	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	432
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	291
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	291
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	268
149.78.229.16	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	259
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	248
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	247
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	221
149.78.43.88	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	206
149.78.174.246	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	165
84.228.144.175	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
207.46.13.151	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	133
149.88.186.52	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	122
149.88.233.73	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	116
85.115.52.201	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	114
79.179.4.1	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
207.46.13.162	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	74
62.90.193.162	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	64
157.55.39.79	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	59
203.79.120.21	New Zealand	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	44
93.172.27.237	Israel	147.237.0.121		drop	SAM rule	drop	36
82.81.23.71	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
109.66.52.82	Israel	147.237.0.121		Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	36
149.78.230.148	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	35
40.77.167.7	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	33
93.109.253.6	Cyprus	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	32
149.78.170.141	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	29
66.102.6.147	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
66.249.74.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
79.181.8.147	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	25
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	24
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
70.32.45.67	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	21
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
64.120.46.187	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	19
149.88.119.205	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	19
79.178.188.35	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	18
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
2.54.137.138	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	17
2.54.137.138	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	17
2.54.137.138	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	17
84.108.206.76	Israel	147.237.0.121		Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13
66.102.6.153	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	11

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
132.76.50.6	Israel	147.237.0.121		Suspicious Response Code	Block	6
192.115.130.253	Israel	147.237.0.121		Suspicious Response Code	Block	6
212.25.123.18	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 44DC1CEB2389AD9966E7188120275E331606405207BE6B374C085705058DA0F617140B93B306C43740F1F5D7C2D676ABDD75F68789E4F398EAAF10A701D23BCFE1DA29B89BC75D8797A7E1DF276A6873DB0BF3881009EFD925644040D257B7B7FF537ABEB4CB2EF7335E940FAAB44B5C94EF81839298EF63D2DA63C100DB9F38, Observed 529D39144C51315E790B739D448EBFB4459EA494C4B06A3232ABC074490CE772557AED2F79E864C6778EC0055240C35395AA757E8E78C7871CCBE1EF1B5B99874FDD1FD973A250207BF37E6E5EDCC38DAE91FBBC53883E2E4C8404A8B4C3EACB9015BF	None	3
87.68.39.173	Israel	147.237.0.121		Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login	Block	3
31.154.155.182	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	3
193.34.56.101	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	3
81.218.241.26	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/$$$&?&?$$$	Block	3
46.19.86.167	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
185.32.179.216	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
192.114.87.2	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/1399-he/miluim.aspx	Block	2
46.19.85.114	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
37.26.147.246	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.253.222.220	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
213.8.84.204	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	2
31.168.13.78	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
132.64.160.121	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddStudyEmploymentPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
80.246.136.216	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 80.246.136.216 (sigalgs DoS Attack)	None	1
213.57.222.239	Israel	147.237.0.121		Unknown Parameter onepasswdfill in www.miluim-ishi.aka.idf.il/login	Block	1
46.19.85.71	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected A9630F3C8A0282BC49CEF2CFC01F97B4BBF48E970452CEE33DED4F56C2DD86F43F4ACF60F77C94E0B32B26FD98476931283C2C425B749DD06237D4591B02F7724A6022A307F8DE8DBC406CEDCF9A85E83D1FE65F5926D0922F6B1653809548D81BA51553ABA1C7F65C51938DAC9FAF3C883D6EF8CB60D85F5FAD67FD3A44F5A9, Observed 464F6C3C955A218FCB2120424EF7EAE7AD1D04BE20E10E8D95FD36DDDB63C8D9F53FE2E5A888258ED44F22CD2C5B175F515DE21EF0388EB15AD22A304CECC039F8682E6D546188BA6ADD92F89748F2B9859E0C9B1C3161D172613CE545D81FA603566E	None	1
2.54.0.10	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
194.90.186.65	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
176.12.142.29	Israel	147.237.0.121		Double URL Encoding - parameter: ReturnUrl in www.miluim-ishi.aka.idf.il/login	Block	1
85.64.88.58	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
46.19.86.185	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.168.201.223	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
212.25.123.18	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
80.246.136.216	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
2.54.11.118	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	1
212.25.105.125	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 212.25.105.125 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
176.13.3.205	Israel	147.237.0.121		Double URL Encoding - parameter: ReturnUrl in www.miluim-ishi.aka.idf.il/login	Block	1
79.181.31.112	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 79.181.31.112 (Open Mode)	None	1
212.117.136.6	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	1
176.12.136.102	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
80.246.137.53	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
46.19.86.149	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.25.105.125	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
185.32.179.90	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
79.181.31.112	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
37.26.148.143	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
176.12.138.59	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1