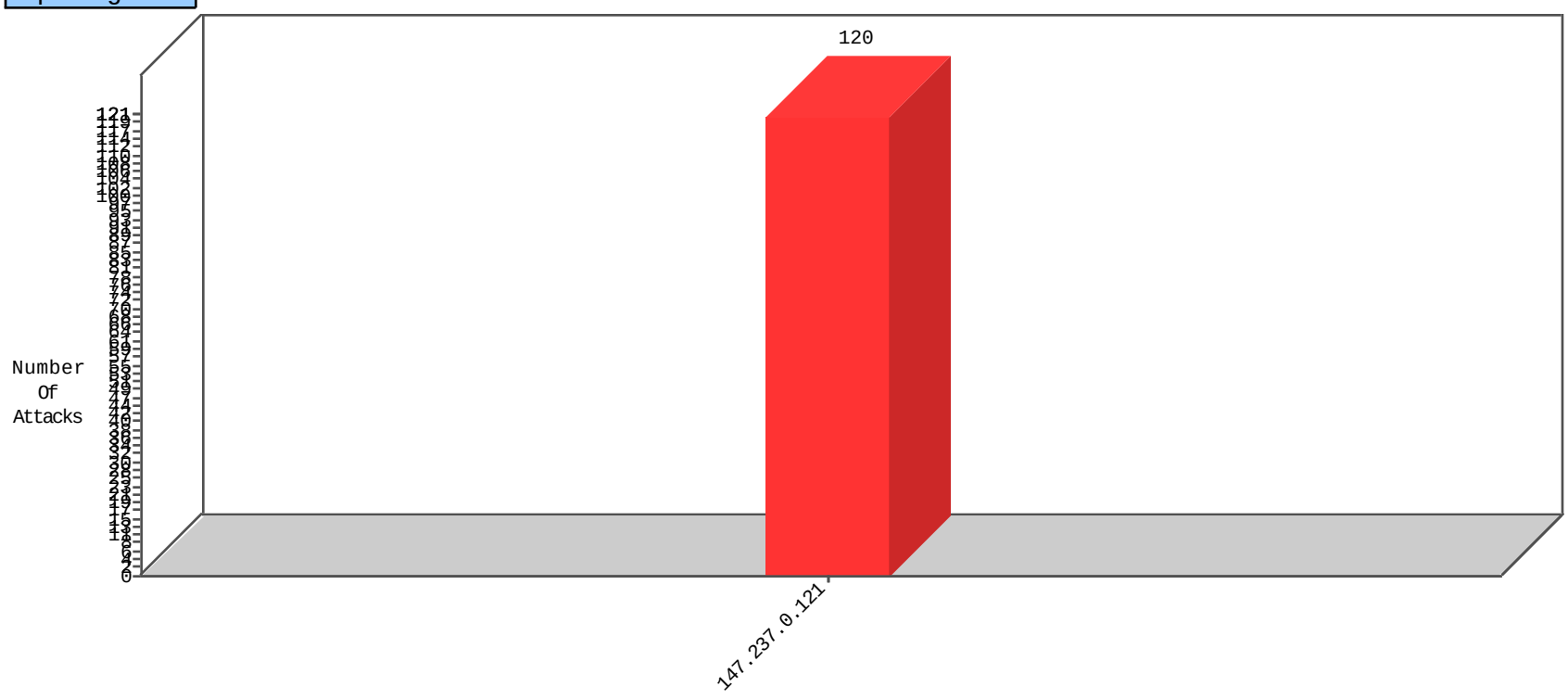
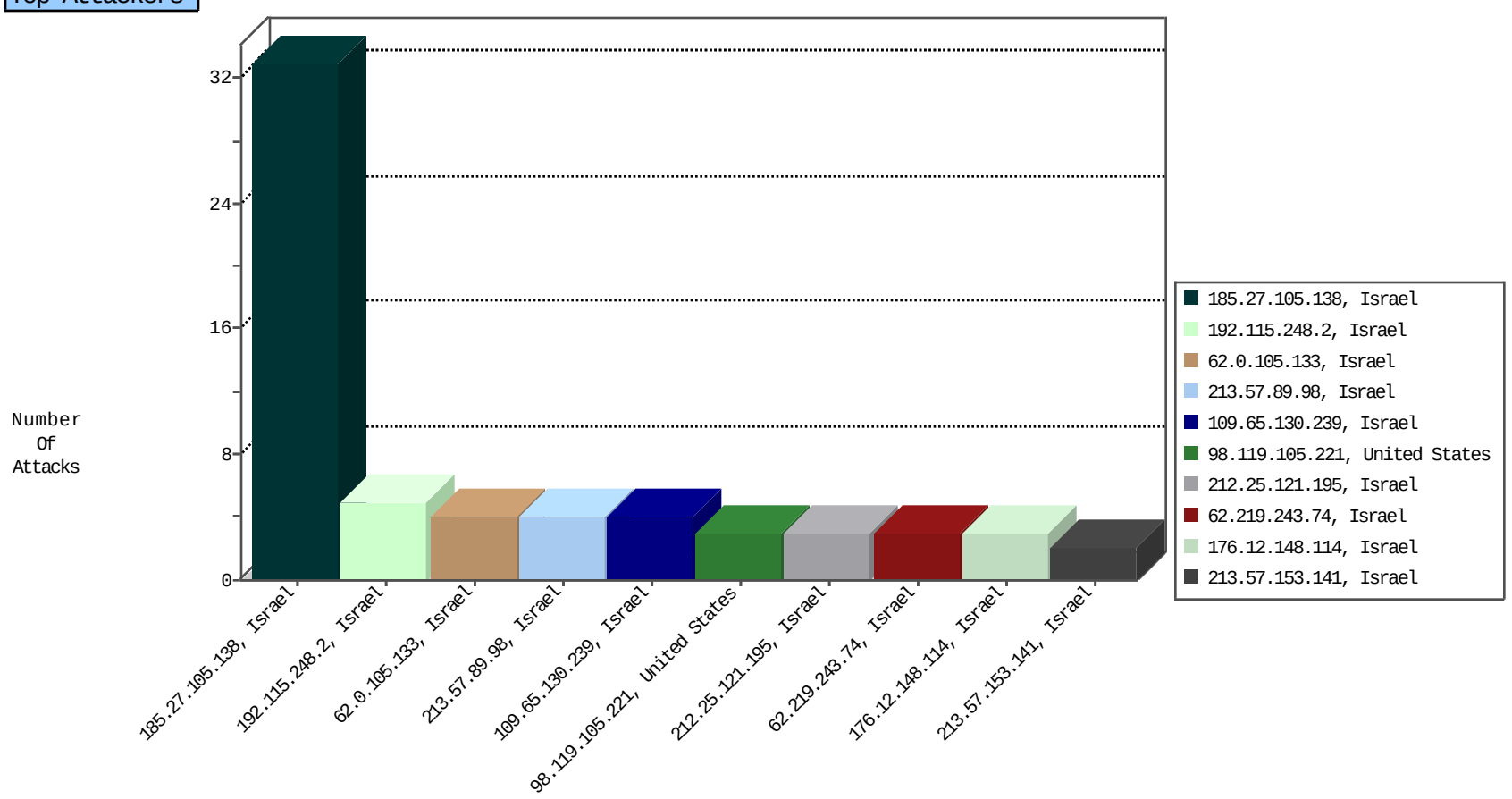
12-01-2015 to 12-02-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



12-01-2015 to 12-02-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
185.27.105.138	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	33
212.25.121.195	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3
62.219.243.74	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3
110.188.1.30	China	147.237.0.121		Invalid TCP Flags	drop	BBL-Frankfurt	2

12-01-2015 to 12-02-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

12-01-2015 to 12-02-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
192.198.151.45	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	2
98.119.105.221	United States	147.237.0.121		ET SCAN NMAP -f -sS	1
98.119.105.221	United States	147.237.0.121		ET SCAN NMAP -sS window 2048	1
61.240.144.64	China	147.237.0.121		ET SCAN Potential SSH Scan	1
98.119.105.221	United States	147.237.0.121		ET SCAN NMAP -sS window 1024	1
192.198.151.37	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	1
209.126.116.147	United States	147.237.0.121		ET SCAN NMAP -sS window 1024	1

12-01-2015 to 12-02-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.145	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	3396
66.249.93.153	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	3167
66.249.93.149	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2931
140.101.20.1	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1314
66.249.93.153	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	294
66.249.93.149	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	293
66.249.93.145	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	276
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	242
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	216
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	183
190.172.1.216	Argentina	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	173
149.78.41.56	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	140
185.27.105.138	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	126
13.21.125.9	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	117
149.78.30.195	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	85
149.88.89.180	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	84
138.134.102.15	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	65
138.134.192.10	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	62
66.249.80.51	Australia	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	61
192.115.177.203	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	61
149.78.231.185	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	50
194.90.119.123	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	49
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	47
149.78.98.21	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
149.78.35.188	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
66.249.81.251	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	42
5.102.254.104	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	40
79.153.149.215	Spain	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	38
66.249.81.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	38
149.88.246.26	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	36
77.125.149.122	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
80.246.130.34	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	33
149.78.157.246	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	33
199.203.93.50	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	32
149.78.253.32	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	29
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28
194.50.175.183	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	28
66.102.9.50	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28
70.32.45.67	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
66.249.81.129	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
82.81.81.218	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	25
149.78.92.198	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
89.139.11.205	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	25
46.19.86.56	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	24
66.249.93.215	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	24
66.102.9.39	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
66.249.81.251	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	21
149.88.226.62	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
82.81.81.218	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	20

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
192.115.248.2	Israel	147.237.0.121		Unauthorized HTTP Method	Block	5
62.0.105.133	Israel	147.237.0.121		Suspicious Response Code	Block	4
109.65.130.239	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected B5EA31B867824E5490810416AC0E2D1836ABD6AE54AFD739698517054CECA51591DE630095129A7CD588AD235A5B29FF8B5B70A042950ED51C8C18A51883B93668B2F035261EF8033F9EA8D438FACCE200306F3984E3146F0C2F374F3936BEF21B5310A5F6E5A5800066E99B1F592E6C975DC60B9F45B04DC2C71E0E67A4E01C, Observed FE4FCF2B09B5EE58C8B543656CD5CEFE70678BF9A63806AF37C935B3EF81CAF5F43E0B23232F29AA6D37B9AF18C2A0556CAF920BA906B756399B58341F92EDEB790E3B9C58830B16E7412B062A549C73AEA69DD01EB0912E74A2A872362C57F3084DE4	None	4
213.57.89.98	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	4
176.12.148.114	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	3
213.57.153.141	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.17	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
84.109.153.92	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
198.20.69.74	United States	147.237.0.121		Unauthorized URL Access to 147.237.0.121/	Block	2
132.64.26.228	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
212.179.44.34	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/changepassword/newpassword parameter ctl00$ContentPlaceHolder1$txtNewPass1	Block	2
185.32.179.42	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
37.26.148.147	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	2
79.180.203.10	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtId in www.miluim-ishi.aka.idf.il/login	Block	2
46.19.85.126	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
192.114.23.210	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
138.134.192.10	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/changepassword/newpassword parameter ctl00$ContentPlaceHolder1$txtNewPass1	Block	1
109.64.63.232	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
81.218.101.66	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/ufi/reaction/	Block	1
77.126.196.171	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 77.126.196.171 (Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST))	None	1
195.110.40.7	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
176.13.16.209	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
31.168.123.130	Israel	147.237.0.121		Unknown Parameter ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/smsverify	Block	1
109.160.160.242	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
85.65.16.122	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
80.246.138.226	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 80.246.138.226 (sigalgs DoS Attack)	None	1
192.114.91.249	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
2.52.141.255	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
109.65.35.7	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
77.126.196.171	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
176.13.20.31	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/changeunit parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	1
37.26.146.157	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
91.195.163.17	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddIDCardDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
80.246.138.226	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
176.13.11.136	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 176.13.11.136 (sigalgs DoS Attack)	None	1
2.54.29.65	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.111.1.128	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
79.178.134.245	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
132.66.50.14	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	1
91.195.163.17	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
81.218.55.253	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	1
62.90.117.133	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.118.10.10	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
176.13.11.136	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
31.154.91.53	Israel	147.237.0.121		Unknown Parameter returnurl in www.miluim-ishi.aka.idf.il/login	Block	1
109.66.196.73	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	1
84.228.60.193	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1

12-01-2015 to 12-02-2015