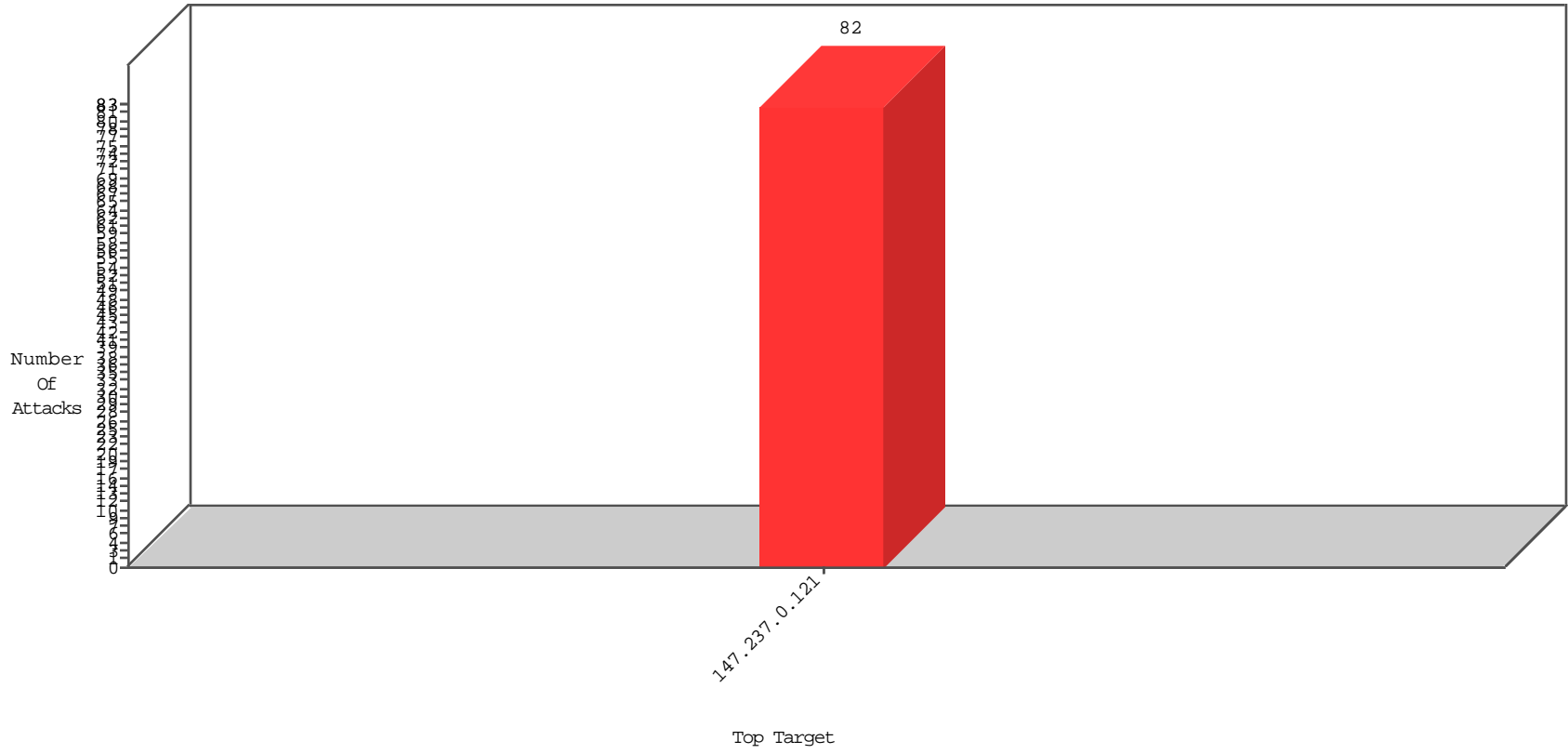


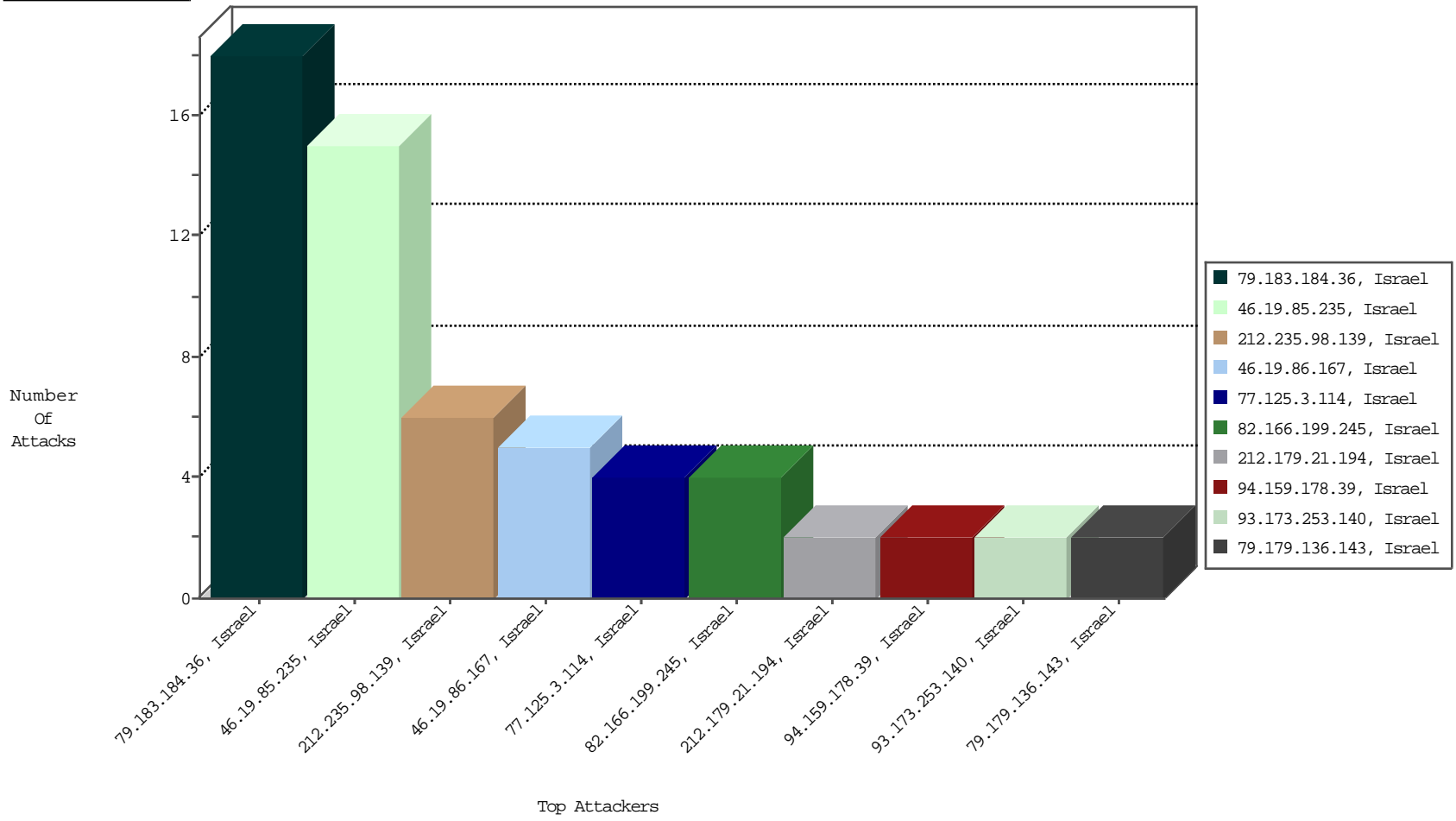
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
79.183.184.36	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BEL-Israel	18
46.19.86.167	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BEL-Israel	5
37.26.148.170	Israel	147.237.0.121		TCP handshake violation, first packet not syn	drop	BEL-Frankfurt	1

11-05-2015 to 11-06-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
------------------	--------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
46.19.85.235	Israel	147.237.0.121		POLICY-OTHER TCP packet with urgent flag attempt	12
41.140.253.9	Morocco	147.237.0.121		ET SCAN NMAP -sS window 1024	1
177.96.93.234	Brazil	147.237.0.121		ET SCAN NMAP -sS window 1024	1
41.140.253.9	Morocco	147.237.0.121		ET SCAN NMAP -sS window 4096	1
104.192.0.20	United States	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1
180.210.201.106	Singapore	147.237.0.121		ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.154	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	4328
66.249.93.146	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	4114
66.249.93.150	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2957
149.88.31.11	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1057
66.249.81.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	442
66.249.93.150	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	341
66.249.93.146	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	323
66.249.93.154	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	319
82.166.180.250	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	225
15.203.162.24	France	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	208
66.249.81.130	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	148
31.154.176.123	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.178.181.18	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
66.249.81.251	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	131
121.117.160.225	Japan	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	108
46.19.86.25	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
2.54.147.248	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
149.88.28.21	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	90
192.146.6.2	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	86
149.78.19.250	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	82
68.106.223.109	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	74
2.54.45.130	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
201.202.78.202	Costa Rica	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	68
66.249.93.247	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	60
149.78.221.136	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	57
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	56
149.78.41.177	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	48
66.249.81.238	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	46
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
66.249.83.212	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	42
66.249.81.251	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	41
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	40
66.102.9.39	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	39
66.249.93.241	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	38
66.249.81.130	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	38
66.249.82.147	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
46.19.85.235	Israel	147.237.0.121		Streaming Engine: TCP Urgent Data Enforcement	TCP segment with urgent pointer (no data). Urgent data indication was stripped. Please refer to sk36869.	drop	36
2.54.175.166	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
46.19.85.235	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	36
46.19.85.235	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	36
80.246.137.252	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
46.19.85.235	Israel	147.237.0.121		Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	36
66.249.81.254	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	35
208.184.112.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	34
66.249.93.220	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	33
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	32
46.19.85.198	Israel	147.237.0.121		Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	32
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	31
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	31
54.88.168.129	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	30

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
77.125.3.114	Israel	147.237.0.121		Unauthorized HTTP Method	Block	4
212.235.98.139	Israel	147.237.0.121		Parameter Type Violation ct100_ContentPlaceholder1_fuAddStudyPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/uploadregister.axd	Block	3
212.235.98.139	Israel	147.237.0.121		Parameter Type Violation ct100_ContentPlaceholder1_fuAddBoardExamsPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/uploadregister.axd	Block	2
93.173.253.140	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/changepassword/newpassword parameter ct100\$ContentPlaceholder1\$txtNewPass1	Block	2
212.179.21.194	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/ufi/reaction/	Block	2
82.166.199.245	Israel	147.237.0.121		PHP Attempt	Block	2
79.177.227.161	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/changepassword/newpassword parameter ct100\$ContentPlaceholder1\$txtNewPass1	Block	2
46.19.85.235	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/changepassword/newpassword parameter ct100\$ContentPlaceholder1\$txtNewPass1	Block	2
82.166.199.245	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/ajax/pages/fan_status.php	Block	2
84.108.63.42	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceholder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
79.179.136.143	Israel	147.237.0.121		PHP Attempt	Block	1
2.54.30.247	Israel	147.237.0.121		Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 2.54.30.247	Block	1
82.166.81.221	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https://www.miluim-ishi.aka.idf.il/	Block	1
87.68.36.62	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https://www.miluim-ishi.aka.idf.il/	Block	1
80.178.95.33	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceholder1\$txtCaptcha in www.miluim-ishi.aka.idf.il/login	Block	1
2.54.62.192	Israel	147.237.0.121		Unknown Parameter returnurl in www.miluim-ishi.aka.idf.il/login	Block	1
94.159.178.39	Israel	147.237.0.121		Multiple Unauthorized URL Access from 94.159.178.39	Block	1
212.199.69.1	Israel	147.237.0.121		Unknown Parameter ch in www.miluim-ishi.aka.idf.il/login	Block	1
89.138.27.15	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/changepassword/newpassword parameter ct100\$ContentPlaceholder1\$txtNewPass1	Block	1
82.81.26.223	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceholder1\$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	1
212.235.98.139	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceholder1_fuAddTimetableDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
94.159.178.39	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/1355-he/miluom.aspx	Block	1
79.179.136.143	Israel	147.237.0.121		Multiple Unauthorized URL Access from 79.179.136.143	Block	1
212.199.69.1	Israel	147.237.0.121		Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login	Block	1
93.173.166.22	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceholder1\$txtPerutBakasha in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
82.166.22.13	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
46.19.85.235	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	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
109.64.210.241	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceholder1\$txtFileNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1