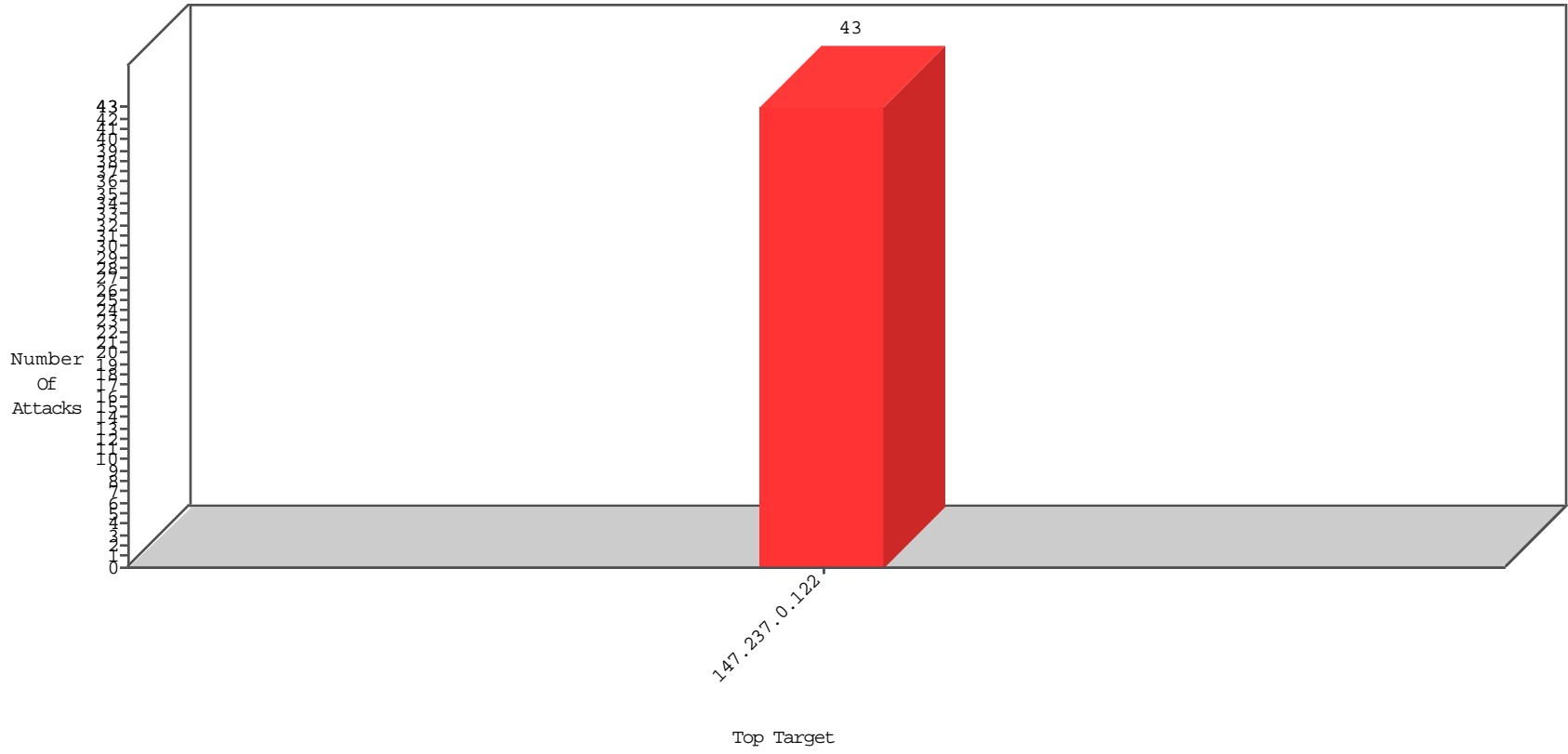


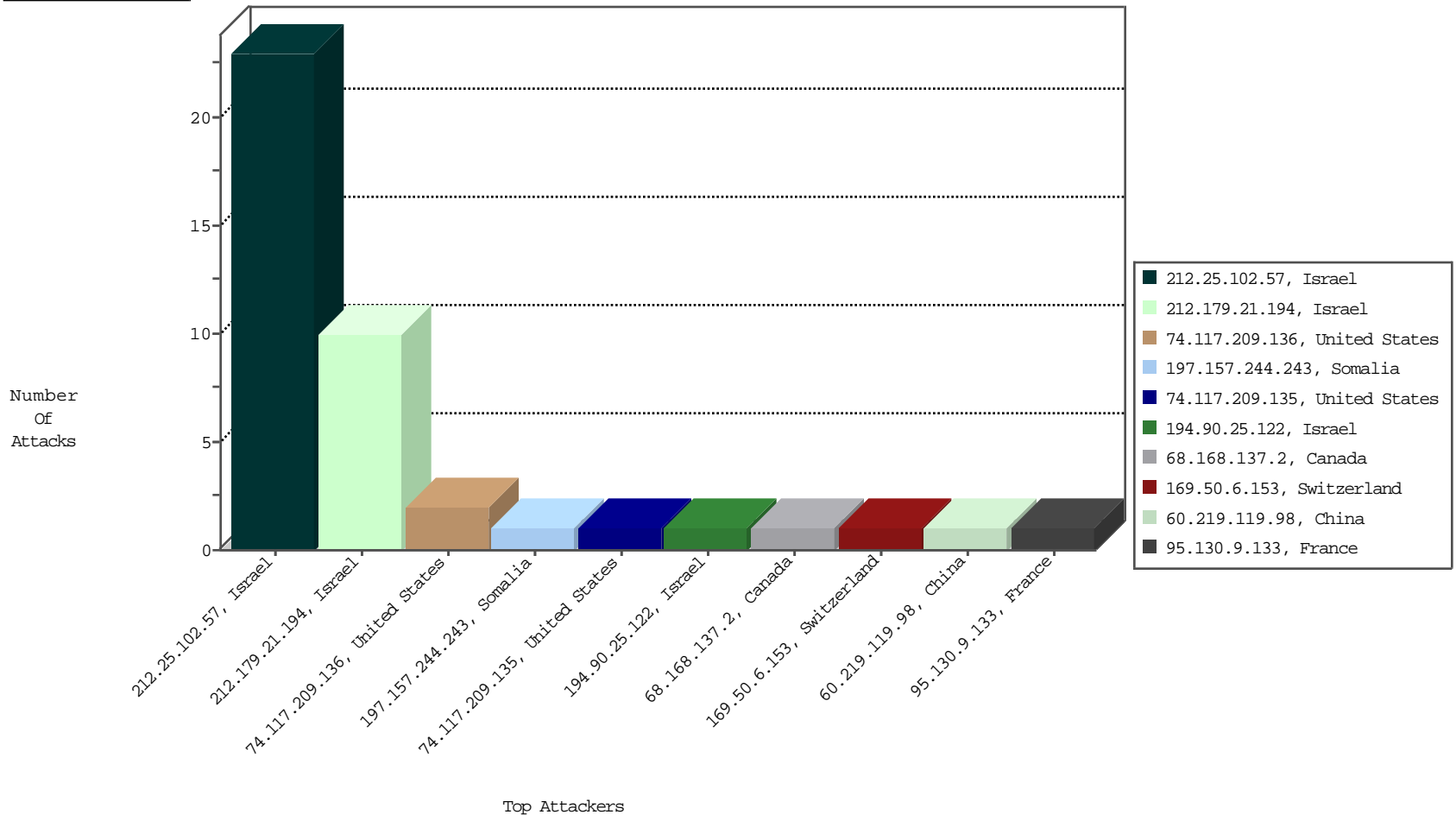
# Focused IP Under Attack Daily Report



## Top Targets



## Top Attackers



11-17-2015 to 11-18-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
------------------	--------------	----------------	------	-----------	---------------	----------------------	-------

11-17-2015 to 11-18-2015

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
74.117.209.136	United States	147.237.0.122		ET SCAN Potential VNC Scan 5900-5920	2
95.130.9.133	France	147.237.0.122		ET SCAN Potential SSH Scan	1
197.157.244.243	Somalia	147.237.0.122		ET SCAN Potential SSH Scan	1
59.45.79.117	China	147.237.0.122		ET SCAN Potential SSH Scan	1
68.168.137.2	Canada	147.237.0.122		ET SCAN Potential VNC Scan 5900-5920	1
169.50.6.153	Switzerland	147.237.0.122		ET SCAN Potential SSH Scan	1
60.219.119.98	China	147.237.0.122		ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
74.117.209.135	United States	147.237.0.122		ET SCAN Potential VNC Scan 5900-5920	1

## Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
212.25.102.57	Israel	147.237.0.122		Bad TCP sequence	Invalid ACK number	monitor	104
212.179.21.194	Israel	147.237.0.122		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
212.179.21.194	Israel	147.237.0.122		SYN Attack	SYN -> SYN-ACK -> RST	reject	29
212.25.102.57	Israel	147.237.0.122		Bad TCP sequence	Invalid ACK number	alert	29
212.25.102.57	Israel	147.237.0.122		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
194.90.25.122	Israel	147.237.0.122		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
61.135.190.69	China	147.237.0.122		Geo-location enforcement	Geo-location inbound enforcement	drop	4
74.82.47.34	United States	147.237.0.122		Geo-location enforcement	Geo-location inbound enforcement	drop	2
62.210.209.237	France	147.237.0.122		Geo-location enforcement	Geo-location inbound enforcement	drop	2
128.232.110.28	United Kingdom	147.237.0.122		Geo-location enforcement	Geo-location inbound enforcement	drop	2
141.212.121.192	United States	147.237.0.122		Geo-location enforcement	Geo-location inbound enforcement	drop	2
216.243.31.2	United States	147.237.0.122		Geo-location enforcement	Geo-location inbound enforcement	drop	2
169.229.3.90	United States	147.237.0.122		Geo-location enforcement	Geo-location inbound enforcement	drop	2
62.210.132.11	France	147.237.0.122		Geo-location enforcement	Geo-location inbound enforcement	drop	2
194.90.25.122	Israel	147.237.0.122		Bad TCP sequence	Invalid ACK number	monitor	1
141.212.121.184	United States	147.237.0.122		Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.8	United States	147.237.0.122		Geo-location enforcement	Geo-location inbound enforcement	drop	1
198.20.69.74	United States	147.237.0.122		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
137.116.71.170	United States	147.237.0.122		Geo-location enforcement	Geo-location inbound enforcement	drop	1
212.179.21.194	Israel	147.237.0.122		Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.19	United States	147.237.0.122		Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.121.183	United States	147.237.0.122		Geo-location enforcement	Geo-location inbound enforcement	drop	1

11-17-2015 to 11-18-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
212.25.102.57	Israel	147.237.0.122		Multiple Double URL Encoding from 212.25.102.57	Block	16
212.25.102.57	Israel	147.237.0.122		Untraceable SSL Sessions: Unknown Server Certificate	None	2
212.179.21.194	Israel	147.237.0.122		Untraceable SSL Sessions: Unknown Server Certificate	None	2
212.179.21.194	Israel	147.237.0.122		SSL Untraceable Connection - Unknown Server Certificate	None	2
212.25.102.57	Israel	147.237.0.122		Unauthorized URL Access to owa.miluim-mefakdim.aka.idf.il/x/_vti_bin/ewainternalwebservice.json/undo	Block	2
212.179.21.194	Israel	147.237.0.122		Unknown Parameter Paged in sp.miluim-mefakdim.aka.idf.il/u5405/_layouts/15/inplview.aspx	None	1
212.179.21.194	Israel	147.237.0.122		Parameter Read Only Violation in www.miluim-mefakdim.aka.idf.il/templates/login/login.aspx	None	1
212.25.102.57	Israel	147.237.0.122		SSL Untraceable Connection - Unknown Server Certificate	None	1
212.179.21.194	Israel	147.237.0.122		Double URL Encoding - parameter: TARGET in www.miluim-mefakdim.aka.idf.il/templates/login/otp.aspx	Block	1
194.90.25.122	Israel	147.237.0.122		SSL Untraceable Connection - Unknown Server Certificate	None	1
212.179.21.194	Israel	147.237.0.122		Multiple Double URL Encoding from 212.179.21.194	Block	1
212.25.102.57	Israel	147.237.0.122		Double URL Encoding - parameter: context in owa.miluim-mefakdim.aka.idf.il/x/_vti_bin/ewainternalwebservice.json/findrange	Block	1
212.179.21.194	Israel	147.237.0.122		Too Many Headers per Response - 25 Headers	Block	1
212.25.102.57	Israel	147.237.0.122		Unknown Parameter SortField in sp.miluim-mefakdim.aka.idf.il/u5405/_layouts/15/inplview.aspx	None	1
212.179.21.194	Israel	147.237.0.122		Multiple Untraceable SSL Sessions from 212.179.21.194 (Unknown Server Certificate)	None	1

11-17-2015 to 11-18-2015