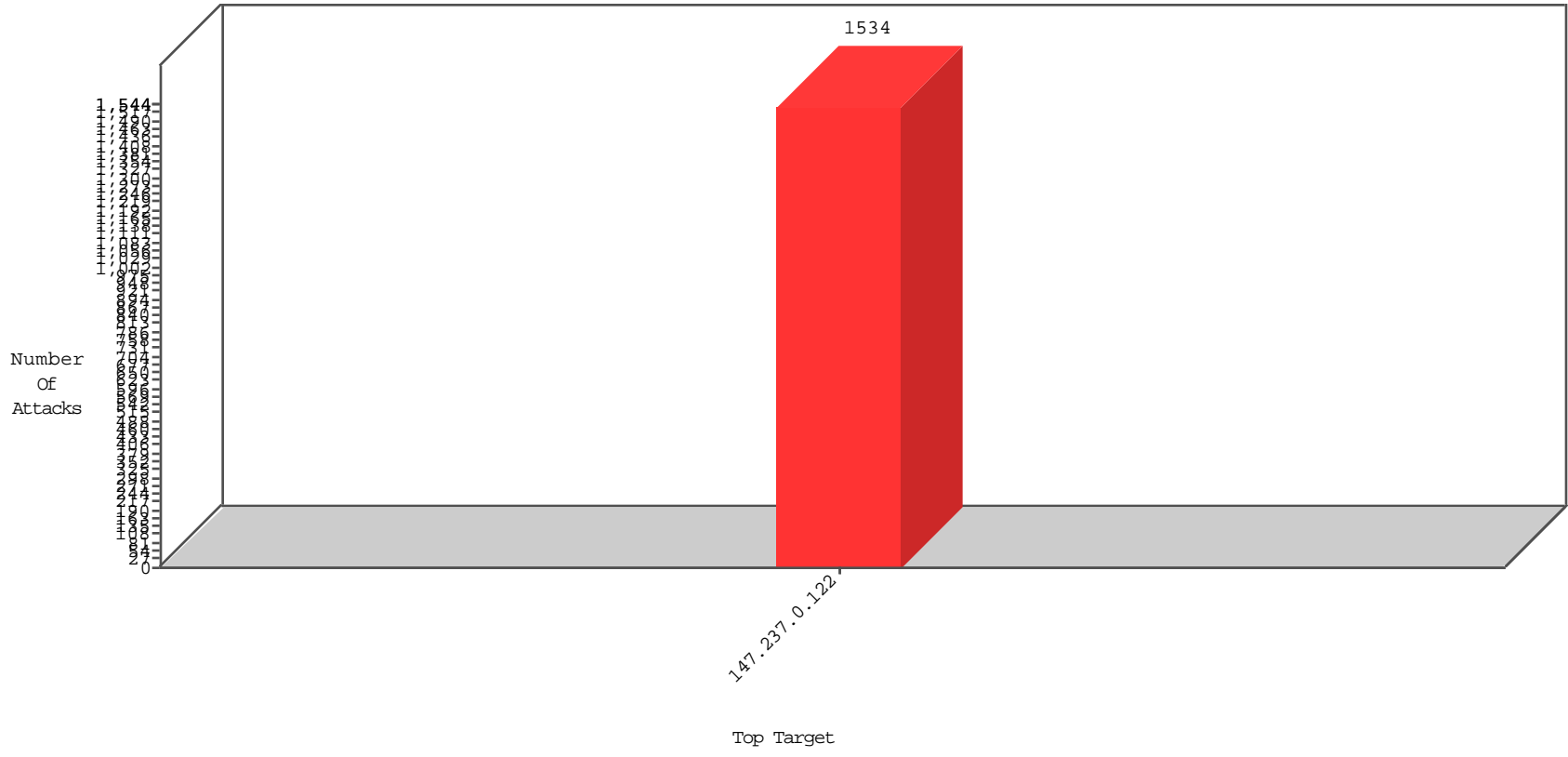


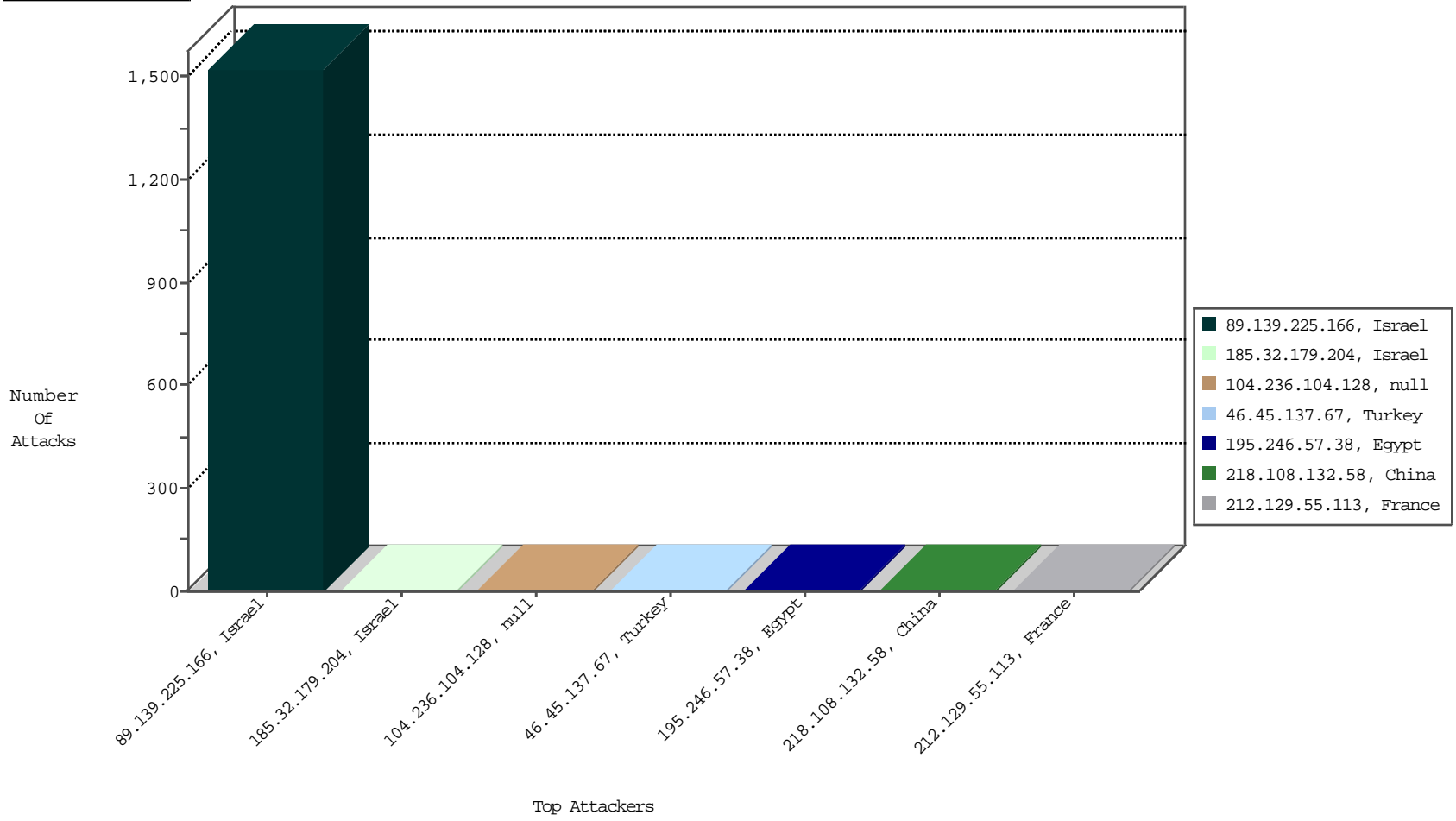
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



02-05-2016 to 02-06-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
195.246.57.38	Egypt	147.237.0.122		I4 Source or Dest Port Zero	drop	BEL-Israel	1

02-05-2016 to 02-06-2016

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
218.108.132.58	China	147.237.0.122		ET SCAN Potential VNC Scan 5900-5920	1
212.129.55.113	France	147.237.0.122		ET SCAN Potential SSH Scan	1
46.45.137.67	Turkey	147.237.0.122		ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site Name	Signature	Device Action	Count
89.139.225.166	Israel	147.237.0.122	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	37591
185.32.179.204	Israel	147.237.0.122	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.32.179.231	Israel	147.237.0.122	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
89.139.225.166	Israel	147.237.0.122	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
61.135.190.197	China	147.237.0.122	Geo-location enforcement	Geo-location inbound enforcement	drop	4
216.243.31.2	United States	147.237.0.122	Geo-location enforcement	Geo-location inbound enforcement	drop	2
74.82.47.39	United States	147.237.0.122	Geo-location enforcement	Geo-location inbound enforcement	drop	1
169.229.3.91	United States	147.237.0.122	Geo-location enforcement	Geo-location inbound enforcement	drop	1
54.251.144.191	Singapore	147.237.0.122	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.115	United States	147.237.0.122	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.35.62.250	Switzerland	147.237.0.122	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.124	United States	147.237.0.122	Geo-location enforcement	Geo-location inbound enforcement	drop	1
64.125.239.10	United States	147.237.0.122	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.115	United States	147.237.0.122	Geo-location enforcement	Geo-location inbound enforcement	drop	1
128.232.110.28	United Kingdom	147.237.0.122	Geo-location enforcement	Geo-location inbound enforcement	drop	1

02-05-2016 to 02-06-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
89.139.225.166	Israel	147.237.0.122		Unauthorized URL Access to owa.miluim-mefakdim.aka.idf.il/x/_vti_bin/ewainternalwebservice.json/findrange	Block	1136
89.139.225.166	Israel	147.237.0.122		Multiple Unauthorized URL Access from 89.139.225.166	Block	384
185.32.179.204	Israel	147.237.0.122		Distributed Double URL Encoding	Block	3
89.139.225.166	Israel	147.237.0.122		SSL Untraceable Connection - Unknown SSL Session	None	1
104.236.104.128		147.237.0.122		Unauthorized URL Access to fedssso.miluim-mefakdim.aka.idf.il/index.htm	Block	1
89.139.225.166	Israel	147.237.0.122		SSL Untraceable Connection - Unknown Server Certificate	None	1
89.139.225.166	Israel	147.237.0.122		Multiple Untraceable SSL Sessions from 89.139.225.166 (Unknown Server Certificate)	None	1
89.139.225.166	Israel	147.237.0.122		Parameter Read Only Violation in www.miluim-mefakdim.aka.idf.il/templates/login/login.aspx	None	1
104.236.104.128		147.237.0.122		Unauthorized URL Access to fedssso.miluim-mefakdim.aka.idf.il/	Block	1
89.139.225.166	Israel	147.237.0.122		Double URL Encoding - parameter: TARGET in www.miluim-mefakdim.aka.idf.il/templates/login/otp.aspx	Block	1

02-05-2016 to 02-06-2016