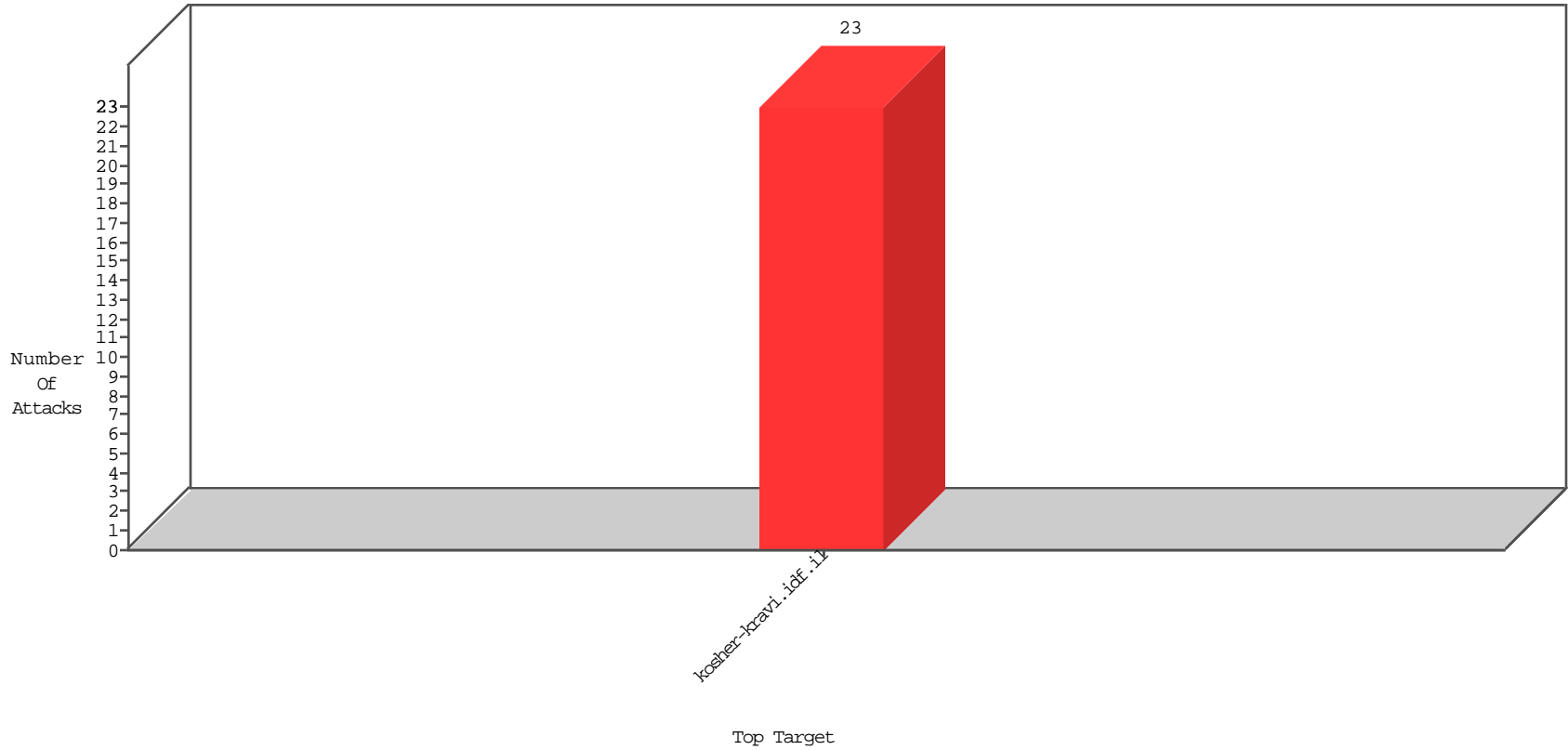


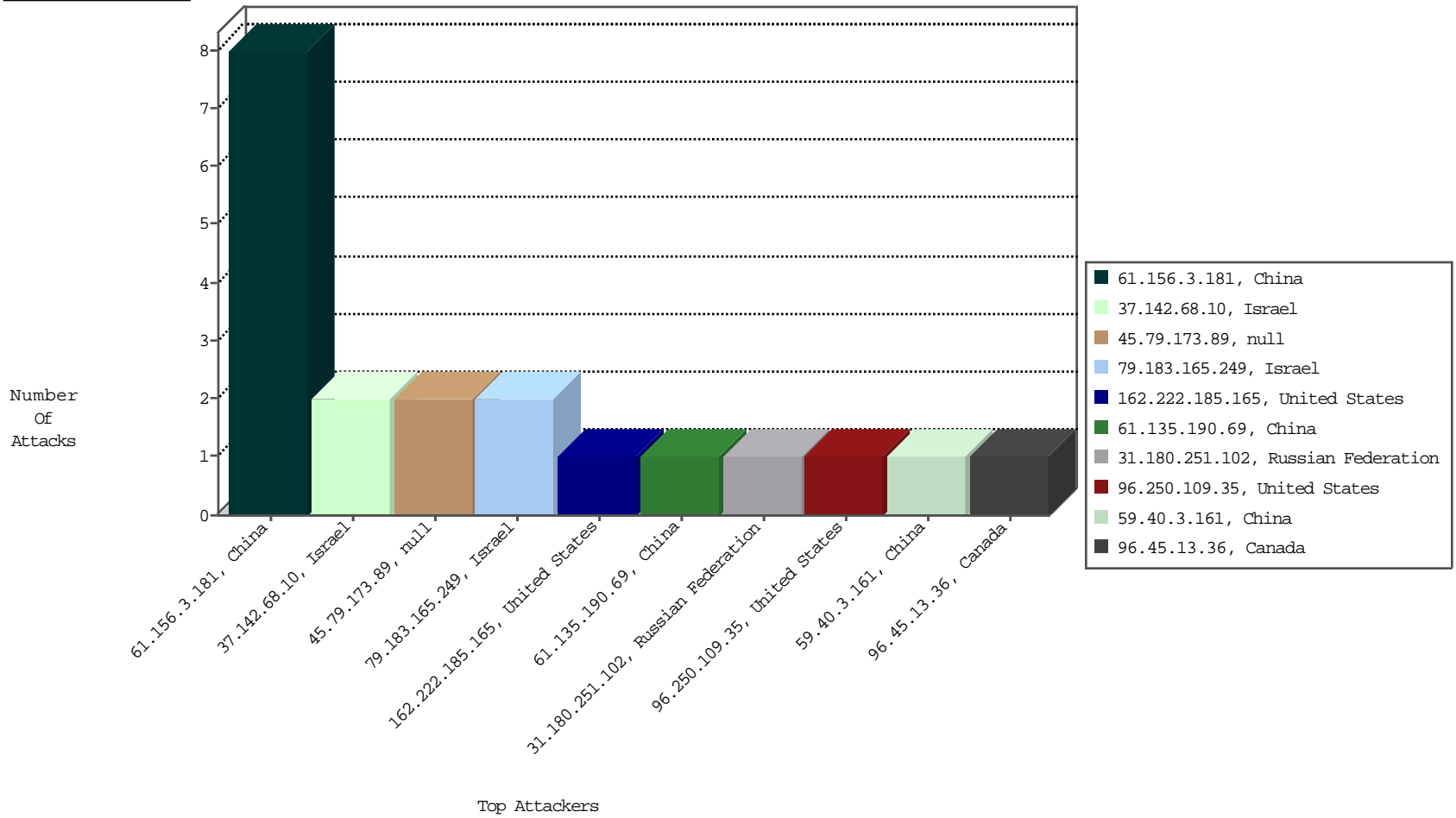
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



12-18-2015 to 12-19-2015

Top Attackers In DDoS-Defence

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

12-18-2015 to 12-19-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
61.156.3.181	China	147.237.0.15	kosher-kravi.idf.il	20085: HTTP: Mueblackcat Security Scanner Initial Request	Block	5

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
61.156.3.181	China	147.237.0.15	kosher-kravi.idf.i	ET WEB_SERVER Muieblackcat scanner	3
189.218.109.225	Mexico	147.237.0.15	kosher-kravi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
31.180.251.102	Russian Federation	147.237.0.15	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
45.79.173.89		147.237.0.15	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
162.222.185.165	United States	147.237.0.15	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
190.83.191.141	Trinidad and Tobago	147.237.0.15	kosher-kravi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
40.115.58.160	United States	147.237.0.15	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
59.40.3.161	China	147.237.0.15	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
96.45.13.36	Canada	147.237.0.15	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
45.79.173.89		147.237.0.15	kosher-kravi.idf.il	drop		drop	62
45.79.173.89		147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
45.79.173.89		147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
68.65.120.48		147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
216.243.31.2	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
74.82.47.36	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
45.79.173.89		147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
213.57.57.113	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
120.237.118.132	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
61.156.3.181	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
180.97.106.36	China	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1
74.82.47.59	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.97	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.71	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
120.237.118.132	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
64.125.239.115	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
198.20.69.74	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
82.173.165.123	Netherlands	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1
59.46.158.24	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.108	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.90	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
213.57.57.113	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
96.250.109.35	United States	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
61.156.3.181	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.90	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

12-18-2015 to 12-19-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
96.250.109.35	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.kosher-kravi.idf.il/sip_storage/files/3/1773.jpg	Block	1
61.135.190.69	China	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	1
37.142.68.10	Israel	147.237.0.15	kosher-kravi.idf.i	PHP Attempt	Block	1
79.183.165.249	Israel	147.237.0.15	kosher-kravi.idf.i	Distributed PHP Attempt	Block	1
37.142.68.10	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/xmlrpc.php	Block	1
79.183.165.249	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/xmlrpc.php	Block	1
45.79.173.89		147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to /	Block	1

12-18-2015 to 12-19-2015