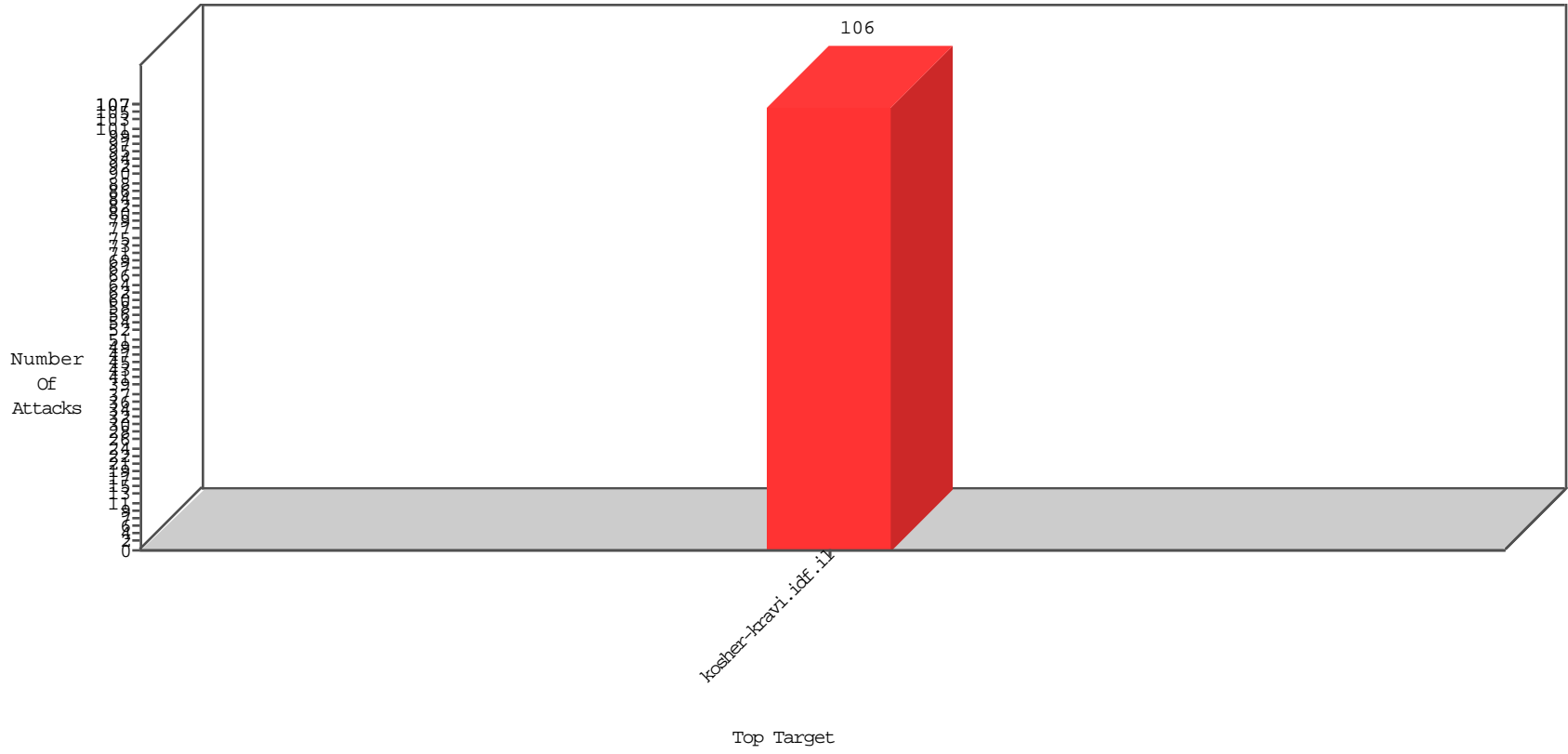


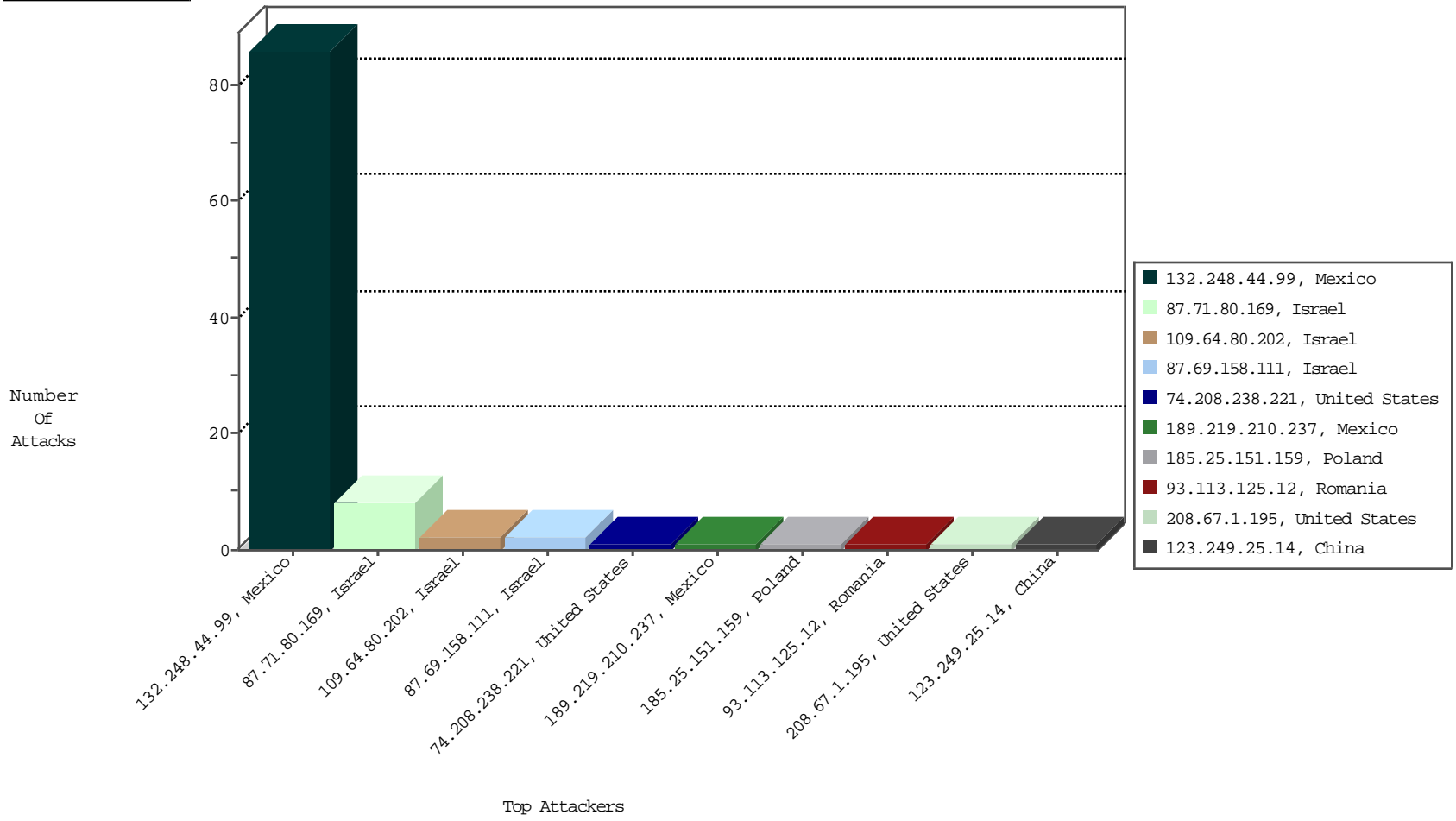
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
199.58.80.184	Canada	147.237.0.15	kosher-kravi.idf.il	L4 Source or Dest Port Zero	drop	DP-Tehila	1
118.144.72.177	China	147.237.0.15	kosher-kravi.idf.il	L4 Source or Dest Port Zero	drop	BBL-Frankfurt	1

03-14-2016 to 03-15-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
132.248.44.99	Mexico	147.237.0.15	kosher-kravi.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	82
132.248.44.99	Mexico	147.237.0.15	kosher-kravi.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	2

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
132.248.44.99	Mexico	147.237.0.15	kosher-kravi.idf.i	ET WEB_SERVER Muieblackcat scanner	2
123.249.25.14	China	147.237.0.15	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
189.219.210.237	Mexico	147.237.0.15	kosher-kravi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
74.208.238.221	United States	147.237.0.15	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
208.67.1.195	United States	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
52.27.210.67	United States	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	29
93.113.125.12	Romania	147.237.0.15	kosher-kravi.idf.i	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	9
52.27.210.67	United States	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	Invalid ACK number	alert	5
93.113.125.12	Romania	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
184.105.247.248	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.74	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.52	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.71	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.i	drop	SAM rule	drop	1
132.248.44.99	Mexico	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
193.105.134.220	Sweden	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.219	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
93.113.125.12	Romania	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
216.243.31.2	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
174.129.246.193	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
139.196.14.152	China	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
64.125.239.167	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
199.30.25.157	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.220	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
38.229.1.15	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.100	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.73	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
71.6.216.56	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
199.30.25.157	United States	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
159.226.95.66	China	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

03-14-2016 to 03-15-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
87.71.80.169	Israel	147.237.0.15	kosher-kravi.idf.il	Distributed PHP Attempt	Block	4
87.71.80.169	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/xmlrpc.php	Block	4
109.64.80.202	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/xmlrpc.php	Block	1
185.25.151.159	Poland	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to testp3.pospr.waw.pl/testproxy.php	Block	1
87.69.158.111	Israel	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	1
93.113.125.12	Romania	147.237.0.15	kosher-kravi.idf.il	Abnormally Long Request URL	Block	1
87.69.158.111	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/xmlrpc.php	Block	1
109.64.80.202	Israel	147.237.0.15	kosher-kravi.idf.il	Distributed PHP Attempt	Block	1

03-14-2016 to 03-15-2016