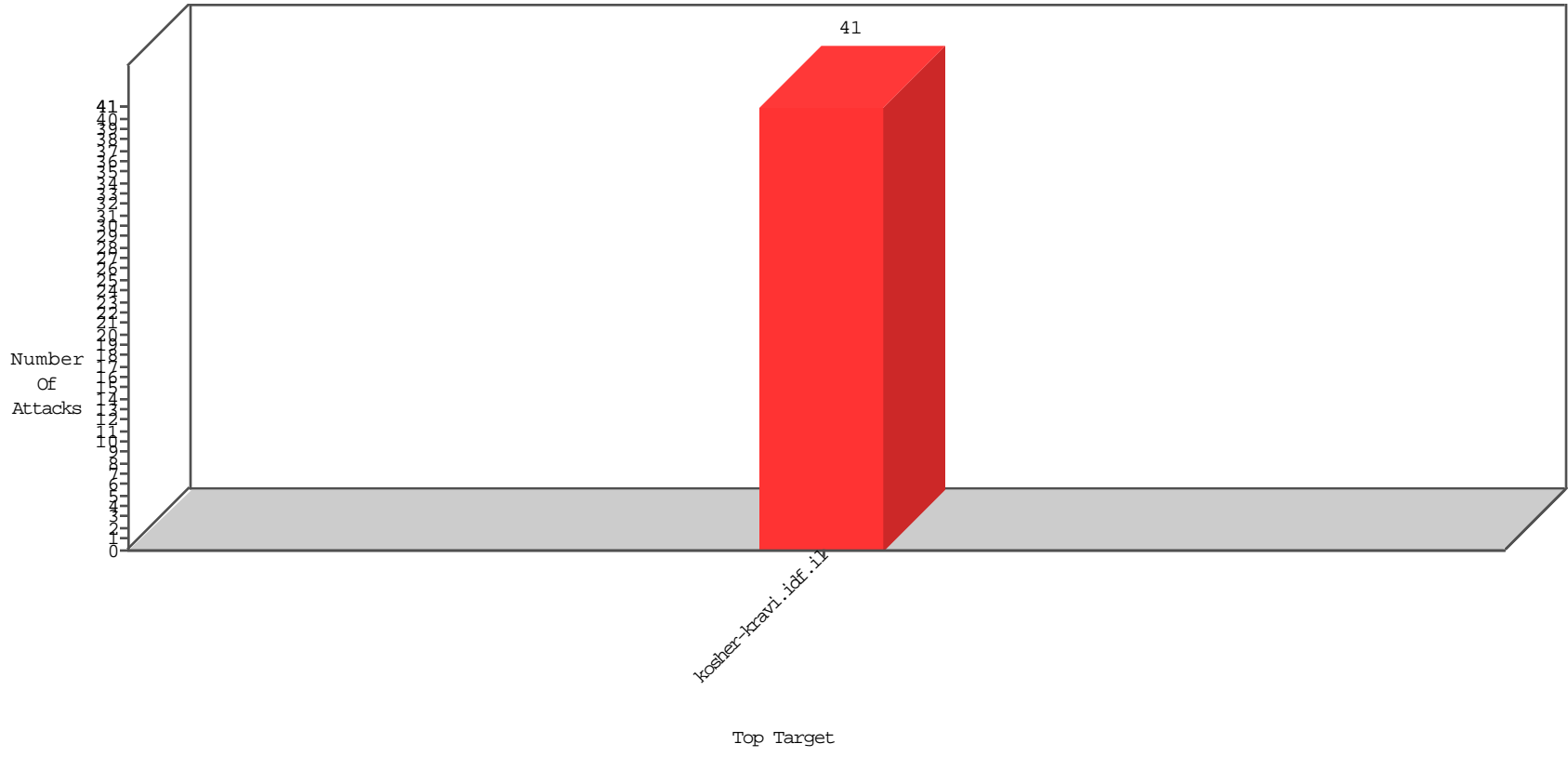


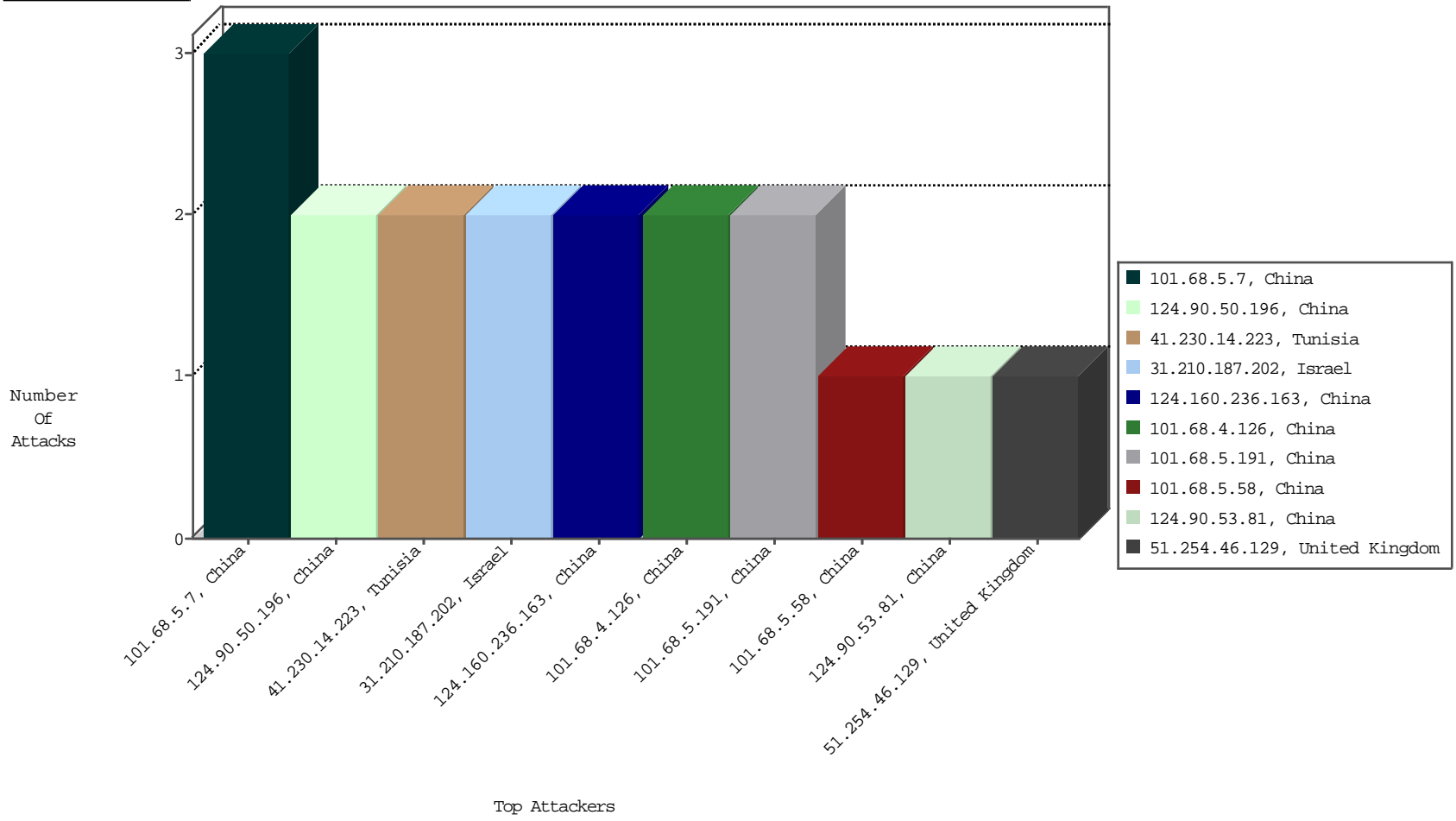
# Focused IP Under Attack Daily Report



Top Targets



Top Attackers



12-02-2015 to 12-03-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
202.112.51.96	China	147.237.0.15	kosher-kravi.idf.il	block-sp-trafl	drop	EBL-Frankfurt	1

12-02-2015 to 12-03-2015

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
51.254.46.129	United Kingdom	147.237.0.15	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
59.45.79.117	China	147.237.0.15	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
85.165.60.202	Norway	147.237.0.15	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
101.68.5.7	China	147.237.0.15	kosher-kravi.idf.i	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
182.72.242.152	India	147.237.0.15	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
54.224.149.230	United States	147.237.0.15	kosher-kravi.idf.i	Tehila - Perl LWP with fake user agent	1
82.192.90.145	Netherlands	147.237.0.15	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
89.248.172.140	Netherlands	147.237.0.15	kosher-kravi.idf.i	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
125.65.165.215	China	147.237.0.15	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
185.106.94.46		147.237.0.15	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
84.228.166.68	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
37.58.75.46	Netherlands	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	14
85.250.237.187	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
46.19.85.182	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
216.243.31.2	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
128.232.110.28	United Kingdom	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.85.3	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
169.229.3.90	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
123.101.0.90	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
80.246.133.130	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.19.85.18	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
199.115.117.117	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.192	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
101.68.4.126	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
64.125.239.183	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
2.54.23.28	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.90	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
123.182.243.196	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
80.246.133.130	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.49	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
202.112.51.96	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.205	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
104.40.190.105	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.10	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.12.137.15	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.182	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
216.218.206.75	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.206	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
123.57.57.11	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.58	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
180.97.106.162	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.192	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
216.218.206.94	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

12-02-2015 to 12-03-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
101.68.5.7	China	147.237.0.15	kosher-kravi.idf.i	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
101.68.4.126	China	147.237.0.15	kosher-kravi.idf.i	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
101.68.5.191	China	147.237.0.15	kosher-kravi.idf.i	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
124.160.236.163	China	147.237.0.15	kosher-kravi.idf.i	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
101.68.4.153	China	147.237.0.15	kosher-kravi.idf.i	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
41.230.14.223	Tunisia	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.kosher-kravi.idf.il/templ@es/homepage/homepage.aspx	Block	1
124.90.50.196	China	147.237.0.15	kosher-kravi.idf.i	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
123.157.192.122	China	147.237.0.15	kosher-kravi.idf.i	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.93.167	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/1134-he	Block	1
31.210.187.202	Israel	147.237.0.15	kosher-kravi.idf.i	Distributed PHP Attempt	Block	1
128.232.110.29	United Kingdom	147.237.0.15	kosher-kravi.idf.i	Distributed Unauthorized URL Access on 147.237.0.15/	Block	1
124.90.48.188	China	147.237.0.15	kosher-kravi.idf.i	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
54.153.33.152	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	1
124.90.53.81	China	147.237.0.15	kosher-kravi.idf.i	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
123.158.49.63	China	147.237.0.15	kosher-kravi.idf.i	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
101.68.4.70	China	147.237.0.15	kosher-kravi.idf.i	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
31.210.187.202	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/xmlrpc.php	Block	1
124.90.49.253	China	147.237.0.15	kosher-kravi.idf.i	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
101.68.5.58	China	147.237.0.15	kosher-kravi.idf.i	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
61.135.190.69	China	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	1
124.90.53.236	China	147.237.0.15	kosher-kravi.idf.i	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
123.158.61.34	China	147.237.0.15	kosher-kravi.idf.i	Untraceable SSL Sessions: Protocol violation (SSL_CONN_SERVER_HELLO)	None	1
41.230.14.223	Tunisia	147.237.0.15	kosher-kravi.idf.i	Multiple Unauthorized URL Access from 41.230.14.223	Block	1
124.90.50.196	China	147.237.0.15	kosher-kravi.idf.i	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.81.155	Israel	147.237.0.15	kosher-kravi.idf.i	Distributed Unauthorized URL Access on kosher-kravi.idf.il/1134-he	Block	1
124.90.48.183	China	147.237.0.15	kosher-kravi.idf.i	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1

12-02-2015 to 12-03-2015