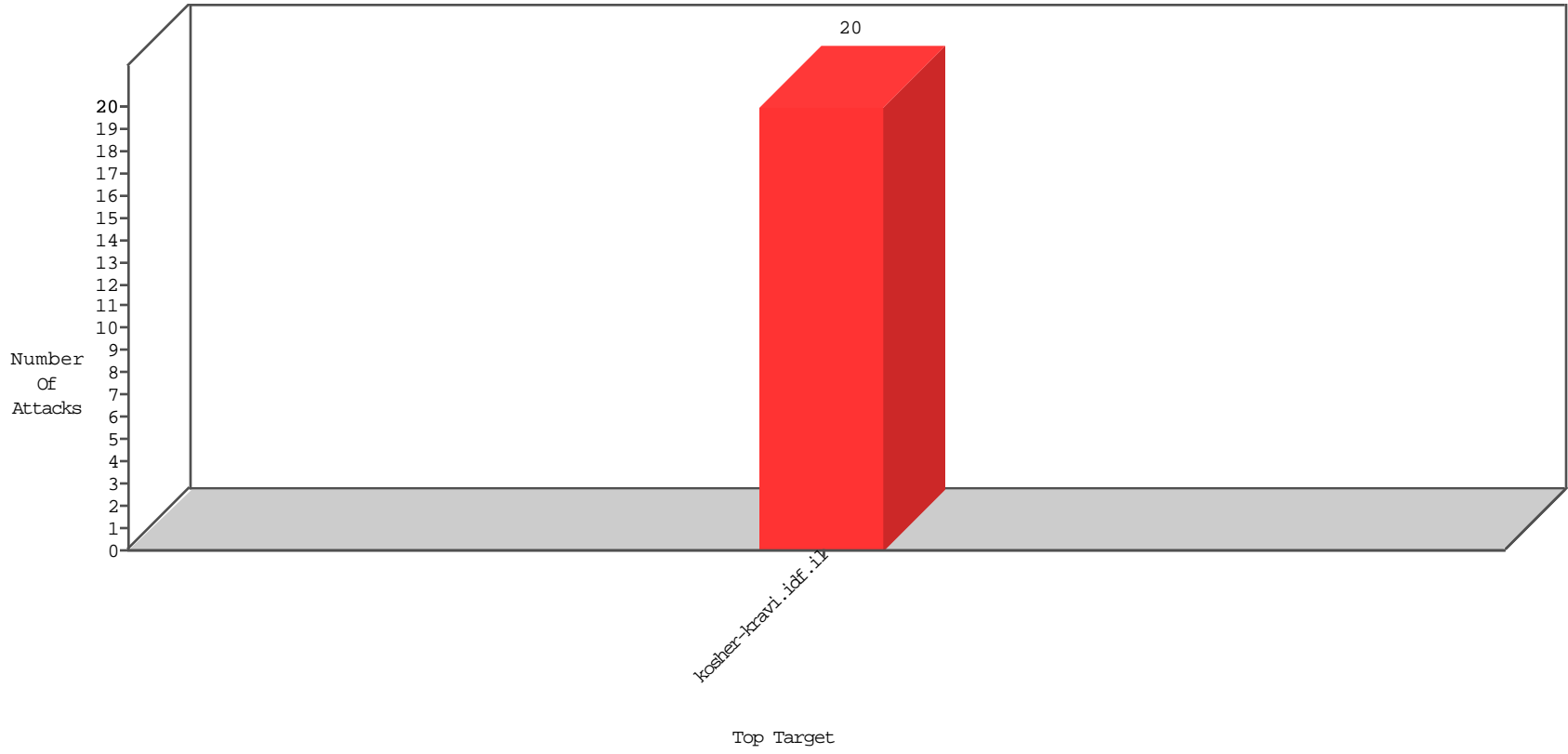


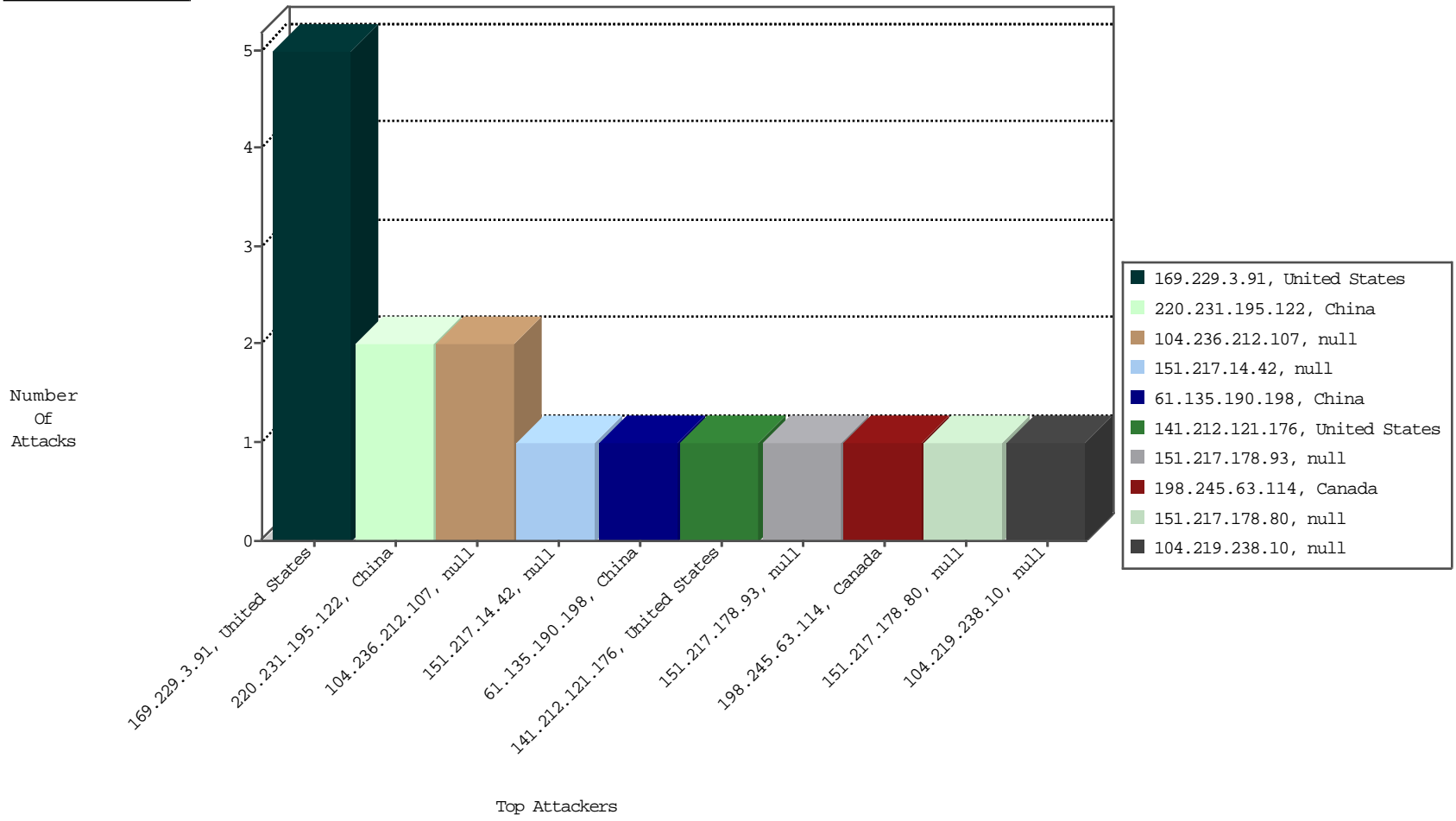
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



12-30-2015 to 12-31-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
194.72.112.130	United Kingdom	147.237.0.15	kosher-kravi.idf.il	Frk_Purple_Con_Limit_Http	drop	BBL-Frankfurt	1

12-30-2015 to 12-31-2015

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
104.219.238.10		147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.178.55		147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.93		147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
220.231.195.122	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
98.119.105.221	United States	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.14.42		147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.80		147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.106.94.126		147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
220.231.195.122	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
198.245.63.114	Canada	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
104.217.216.173	United States	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	22
85.170.253.62	France	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
85.170.253.62	France	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
157.55.39.142	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
216.243.31.2	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
176.13.0.21	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.192	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
101.198.159.31	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
198.245.63.114	Canada	147.237.0.15	kosher-kravi.idf.il	Directory Traversal	directory traversal overflow	monitor	1
184.105.247.211	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	reject	1
109.253.222.152	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.38	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
193.105.134.220	Sweden	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.13.0.21	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.207	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.92	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.35.62.37	Switzerland	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1
141.212.121.176	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
194.72.112.130	United Kingdom	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	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.253.158.147	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.35.62.50	Switzerland	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.177	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.204	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
109.253.222.152	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
64.125.239.126	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.35.62.184	Switzerland	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

12-30-2015 to 12-31-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.i	Illegal Byte Code Character in Method (Ã;8Ã¥Ã-[[#30]]Ã±ZÃ,qJQt^Ã¢Ã->nxÃ (Block	1
198.245.63.114	Canada	147.237.0.15	kosher-kravi.idf.i	URL is Above Root Directory www.kosher-kravi.idf.il/./shared/usercontrols/headerupper/	Block	1
104.236.212.107		147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.i	Illegal Byte Code Character in URL x²^x²[[#15]]xªÃ-p•Ö`â, ªkxx±Ã?[[#11]]Ã·Ã x[[#20]]x,[[#3]]8mÖ±Ã»x«x"[[#24]]do&x³Ö,Ã§^ Ö%â€žÖµÖ´	Block	1
141.212.121.176	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.i	Malformed URL x²^x²[[#15]]xªÃ-p•Ö`â,ªkxx±Ã?[[#11]]Ã·Ã x[[#20]]x, [[#3]]8mÖ±Ã»x«x"[[#24]]do&x³Ö,Ã§^ Ö%â€žÖµÖ´	Block	1
61.135.190.198	China	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.i	Abnormally Long Request method	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.i	Unknown HTTP Request Method (Ã;8Ã¥Ã-[[#30]]Ã±ZÃ,qJQt^Ã¢Ã->nxÃ (in URL x²^x²[[#15]]xªÃ-p•Ö`â,ªkxx±Ã?[[#11]]Ã·Ã x[[#20]]x,[[#3]]8mÖ±Ã»x«x" [[#24]]do&x³Ö,Ã§^ Ö%â€žÖµÖ´	Block	1
104.236.212.107		147.237.0.15	kosher-kravi.idf.i	Multiple Unauthorized URL Access from 104.236.212.107	Block	1

12-30-2015 to 12-31-2015