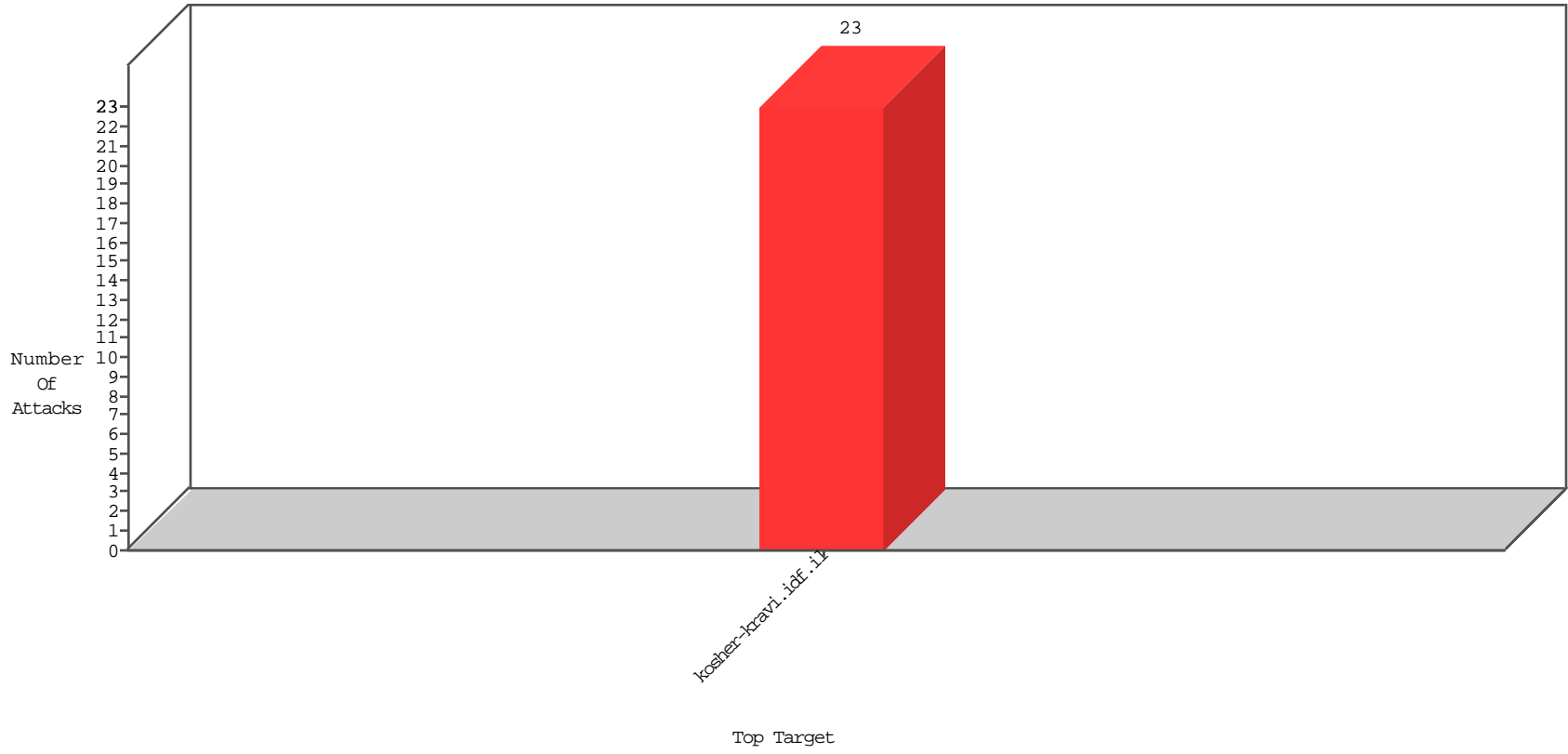


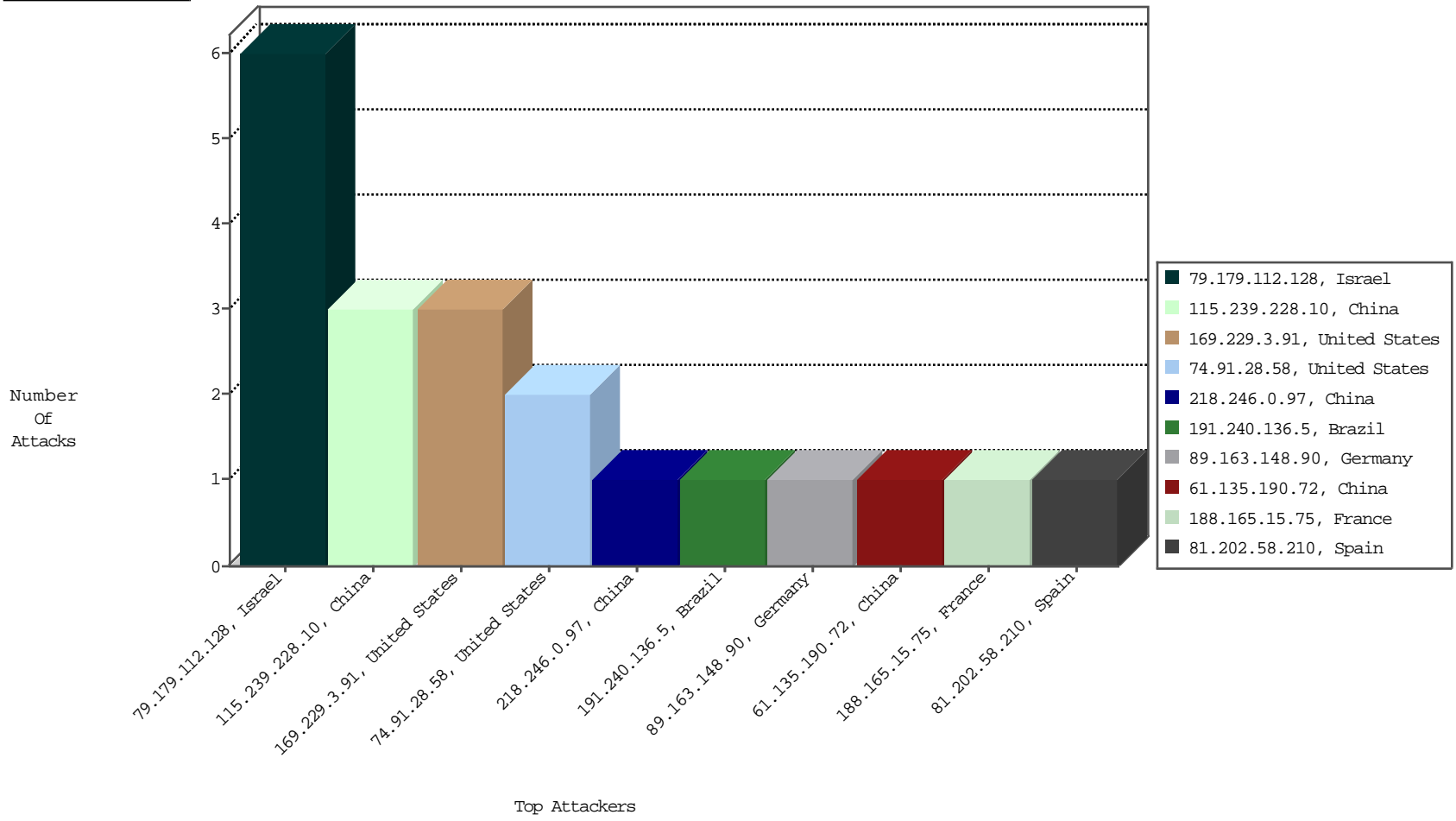
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
115.239.228.10	China	147.237.0.15	kosher-kravi.idf.il	Frk_Under_Attack_Con_Http	drop	BBL-Frankfurt	2
74.91.28.58	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-trafl	forward	DP-Tehila	1
115.239.228.10	China	147.237.0.15	kosher-kravi.idf.il	Frk_Purple_Con_Limit_Http	drop	BBL-Frankfurt	1

01-26-2016 to 01-27-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
188.165.15.75	France	147.237.0.15	kosher-kravi.idf.il	C228: HTTP: AhrefBot crawler	Block	1

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
59.45.79.117	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
89.163.148.90	Germany	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
191.240.136.5	Brazil	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
81.202.58.210	Spain	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
137.117.168.203	United States	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
80.82.64.68	Netherlands	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
216.243.31.2	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
191.240.136.5	Brazil	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
141.212.122.183	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.42	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.191	Israel	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
180.97.106.162	China	147.237.0.15	kosher-kravi.idf.i	drop	SAM rule	drop	1
80.246.133.114	Israel	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
66.249.65.224	Israel	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.120	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.208	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.82.64.68	Netherlands	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
52.28.32.164	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.130.5.207		147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.246.133.114	Israel	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
66.249.78.47	Israel	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
45.79.143.81		147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.223	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.82.64.68	Netherlands	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
54.67.38.74	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.182	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.39	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.247	Israel	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	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
64.125.239.109	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.86	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

01-26-2016 to 01-27-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
79.179.112.128	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/xmlrpc.php	Block	3
79.179.112.128	Israel	147.237.0.15	kosher-kravi.idf.i	Distributed PHP Attempt	Block	3
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.i	Unknown HTTP Request Method •mY[[#3]]ÃeÃ'Ã Ã¼ÃšÃ²[[#6]]Ã¼[[#20]]Ã,Ãe Ã°Ã-ÃfÃ¼Ãª#:#:Ã°9ÃžÃfÃ¶Ã•#Ã-]•xjÃ~[[#19]]Ã-gÃ?Ã% @Ã©YcÃ·E1Ã?Ã"bÃ²Ã¼ÃçÃ· in URL	Block	1
61.135.190.72	China	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	1
80.82.64.68	Netherlands	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to alqassam.ps/arabic/Ø§Ù,Ù?ÙŠØ`ÙŠÙ^	Block	1
74.91.28.58	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.366901.com/	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	Illegal Byte Code Character in Method •mY[[#3]]ÃeÃ'Ã Ã¼ÃšÃ²[[#6]]Ã¼[[#20]]Ã, ÃeÃ°Ã-ÃfÃ¼Ãª#:#:Ã°9ÃžÃfÃ¶Ã•#Ã-]•xjÃ~[[#19]]Ã-gÃ?Ã% @Ã©YcÃ·E1Ã?Ã"bÃ²Ã¼ÃçÃ·	Block	1

01-26-2016 to 01-27-2016