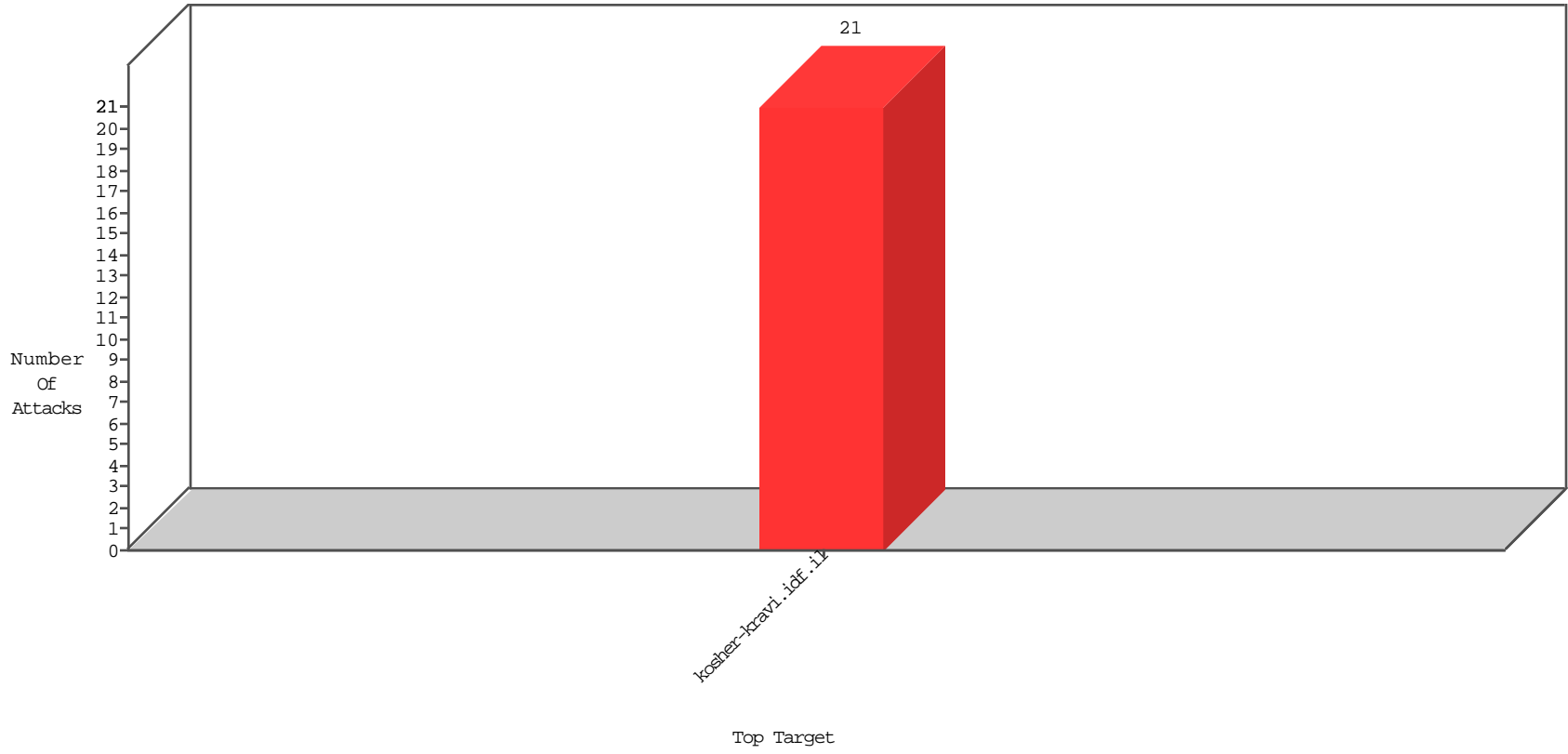


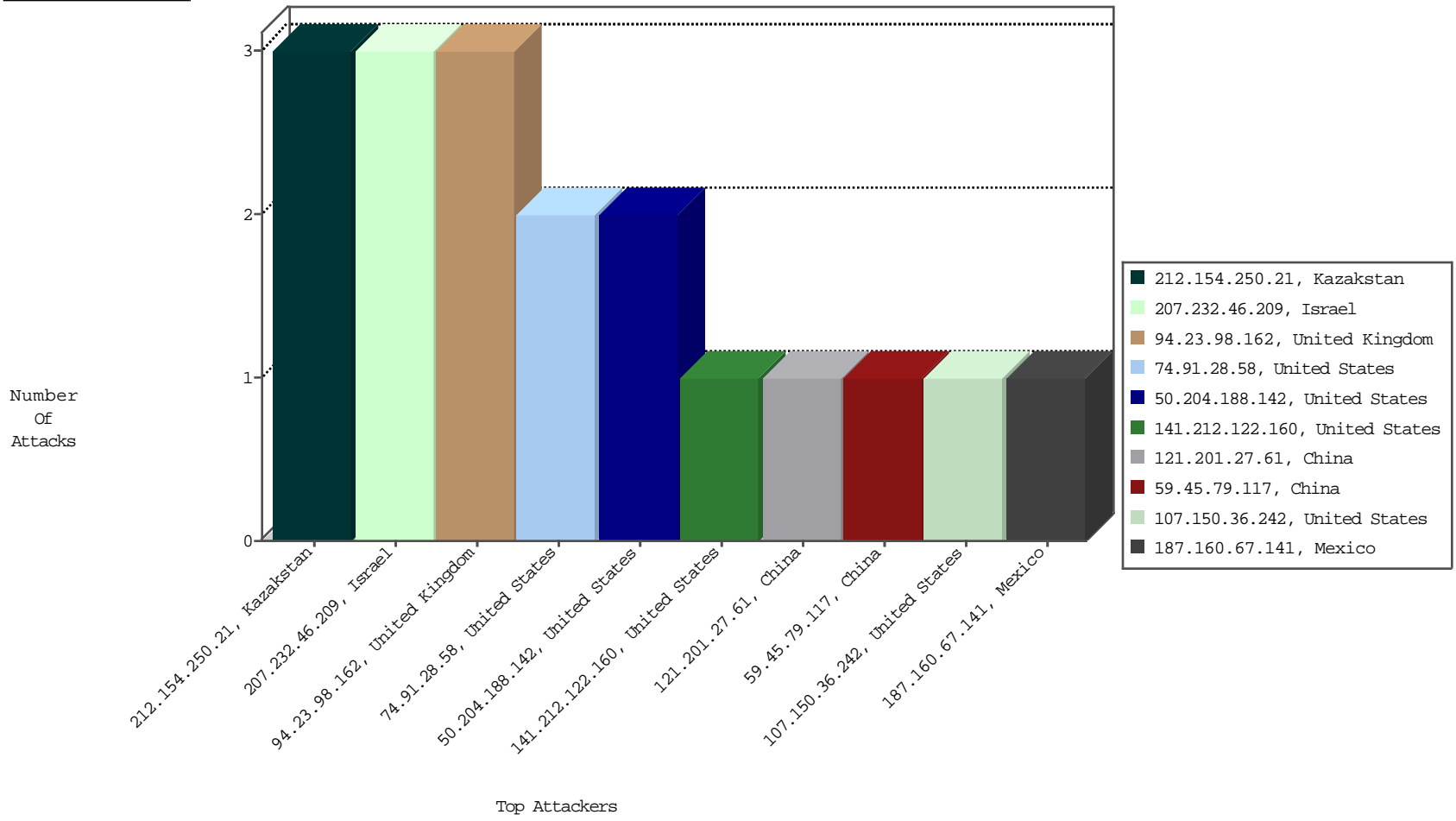
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
94.23.98.162	United Kingdom	147.237.0.15	kosher-kravi.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	BBL-Frankfurt	1
74.91.28.58	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-trafl	forward	DP-Tehila	1

01-27-2016 to 01-28-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
212.154.250.21	Kazakstan	147.237.0.15	kosher-kravi.idf.il	C003: HTTP: phpMyAdmin access	Block	1

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
50.204.188.142	United States	147.237.0.15	kosher-kravi.idf.i	ET SCAN NMAP -f -sS	1
59.45.79.117	China	147.237.0.15	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
107.150.36.242	United States	147.237.0.15	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
187.160.67.141	Mexico	147.237.0.15	kosher-kravi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
50.204.188.142	United States	147.237.0.15	kosher-kravi.idf.i	ET SCAN NMAP -sS window 2048	1
94.76.14.140	Bahrain	147.237.0.15	kosher-kravi.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
121.201.27.61	China	147.237.0.15	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
222.186.34.171	China	147.237.0.15	kosher-kravi.idf.i	ET SCAN Potential VNC Scan 5900-5920	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
92.253.64.93	Jordan	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence		monitor	121
92.253.64.93	Jordan	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	64
80.179.22.139	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	37
92.253.64.93	Jordan	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	alert	25
92.253.64.93	Jordan	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
46.19.86.224	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.86.224	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
94.23.98.162	United Kingdom	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
216.243.31.2	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
212.154.250.21	Kazakstan	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.167	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.251	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.253.131.190	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
74.82.47.46	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.79	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1
185.35.62.86	Switzerland	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
109.253.131.190	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.98	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.13.20.49	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
185.130.5.247		147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.166	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.13.20.49	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
64.125.239.197	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

01-27-2016 to 01-28-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
207.232.46.209	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 207.232.46.209	Block	2
212.154.250.21	Kazakstan	147.237.0.15	kosher-kravi.idf.il	Malformed URL <title>phpmyadmin	Block	1
74.91.28.58	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.x99moyu.net/	Block	1
185.35.62.11	Switzerland	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
212.154.250.21	Kazakstan	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/phpmyadmin/	Block	1
94.23.98.162	United Kingdom	147.237.0.15	kosher-kravi.idf.il	Distributed Malformed URL	Block	1
94.23.98.162	United Kingdom	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
207.232.46.209	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/sip_storage/files/3/1773.jpg	Block	1
141.212.122.160	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1

01-27-2016 to 01-28-2016