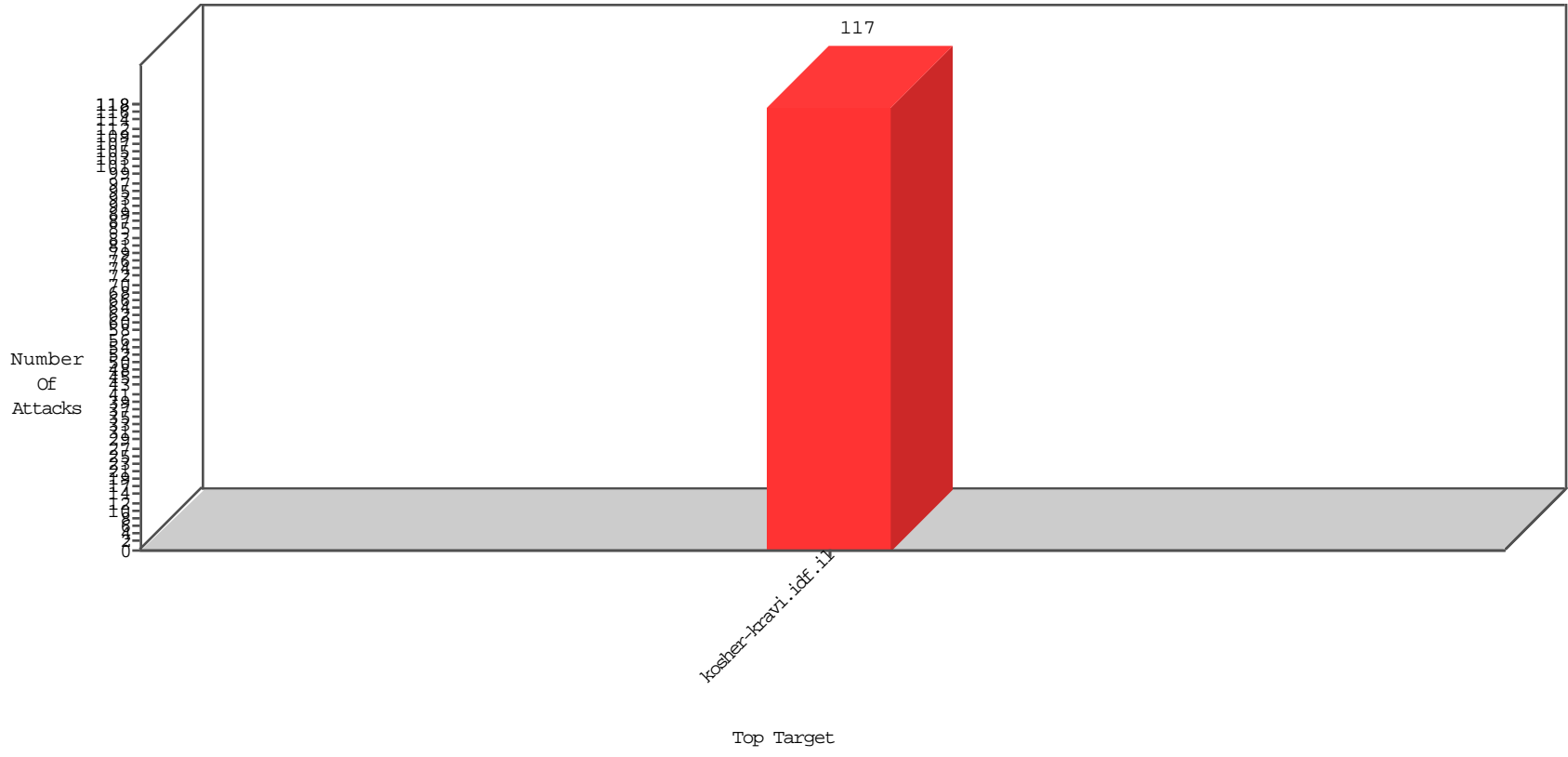


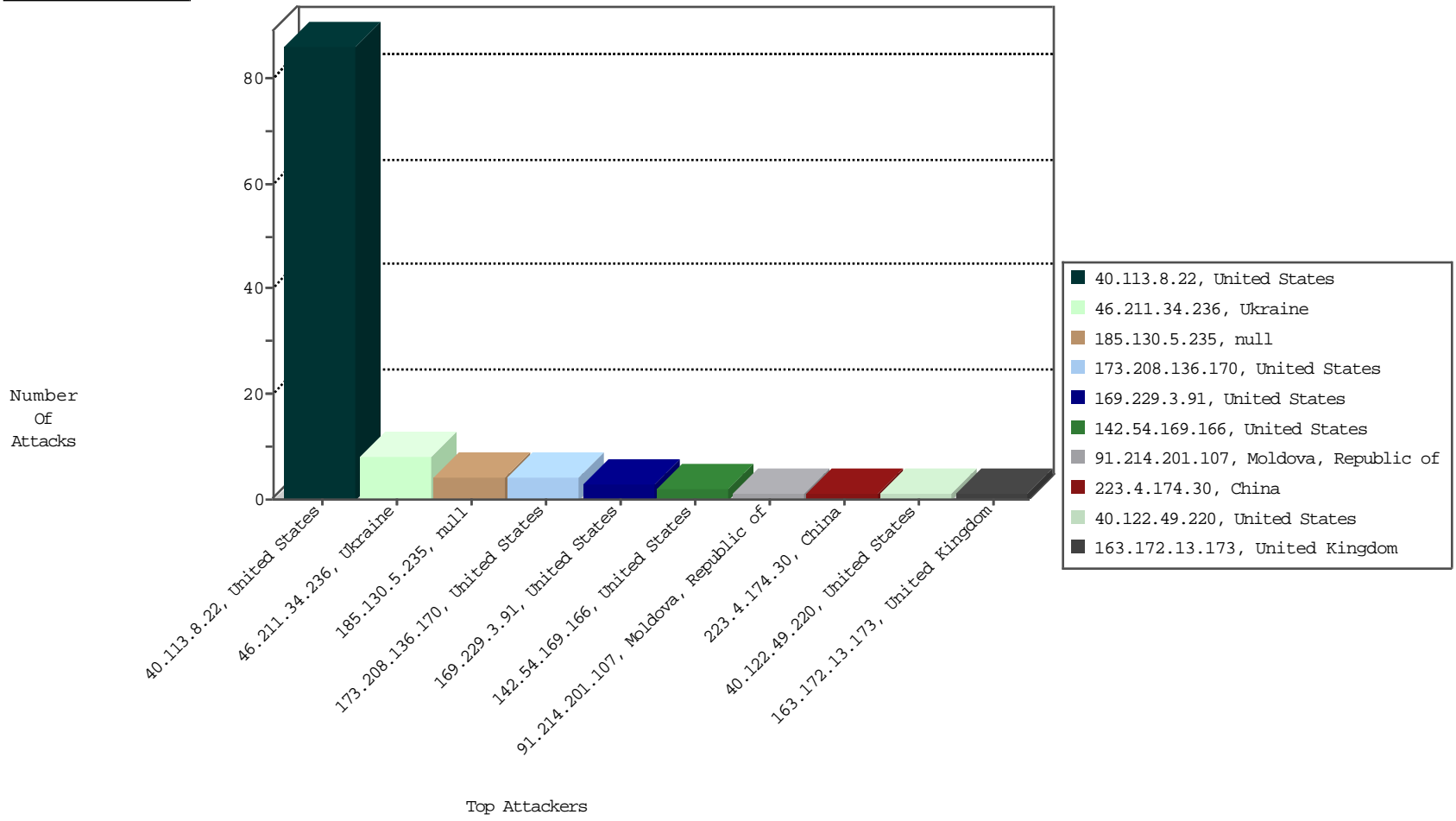
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



01-18-2016 to 01-19-2016

Top Attackers In DDoS-Defence

| Attacker Address | Attacker Geo | Target Address | Site | Signature | Device Action | DP_location.Location | Count |
|------------------|---------------|----------------|---------------------|----------------|---------------|----------------------|-------|
| 142.54.169.166 | United States | 147.237.0.15 | kosher-kravi.idf.il | block-sp-trafl | forward | DP-Tehila | 1 |

Top Attackers In IPS

| Attacker Address | Attacker Geo | Target Address | Site | Signature | Device Action | Count |
|------------------|---------------|----------------|---------------------|--|---------------|-------|
| 40.113.8.22 | United States | 147.237.0.15 | kosher-kravi.idf.il | 20086: HTTP: Muieblackcat Security Scanner | Block | 82 |
| 40.113.8.22 | United States | 147.237.0.15 | kosher-kravi.idf.il | 20085: HTTP: Muieblackcat Security Scanner Initial Request | Block | 2 |
| 185.130.5.235 | | 147.237.0.15 | kosher-kravi.idf.il | 20086: HTTP: Muieblackcat Security Scanner | Block | 2 |
| 185.130.5.235 | | 147.237.0.15 | kosher-kravi.idf.il | 20085: HTTP: Muieblackcat Security Scanner Initial Request | Block | 1 |
| 188.165.15.119 | France | 147.237.0.15 | kosher-kravi.idf.il | C228: HTTP: AhrefBot crawler | Block | 1 |
| 40.122.49.220 | United States | 147.237.0.15 | kosher-kravi.idf.il | 10711: HTTP: ZmEu Vulnerability Scanner | Block | 1 |

Top Attackers In IDS

| Attacker Address | Attacker Geo | Target Address | Site | Signature | Count |
|------------------|----------------|----------------|--------------------|---|-------|
| 40.113.8.22 | United States | 147.237.0.15 | kosher-kravi.idf.i | ET WEB_SERVER Muieblackcat scanner | 2 |
| 83.14.28.82 | Poland | 147.237.0.15 | kosher-kravi.idf.i | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 1 |
| 163.172.13.173 | United Kingdom | 147.237.0.15 | kosher-kravi.idf.i | ET SCAN NMAP -sS window 1024 | 1 |
| 223.4.174.30 | China | 147.237.0.15 | kosher-kravi.idf.i | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 46.211.34.236 | Ukraine | 147.237.0.15 | kosher-kravi.idf.i | SERVER-WEBAPP admin.php access | 1 |
| 91.201.236.114 | Ukraine | 147.237.0.15 | kosher-kravi.idf.i | ET SCAN NMAP -sS window 1024 | 1 |
| 185.130.5.235 | | 147.237.0.15 | kosher-kravi.idf.i | ET WEB_SERVER Muieblackcat scanner | 1 |

Top Attackers In FW

| Attacker Address | Attacker Geo | Target Address | Site | Name | Signature | Device Action | Count |
|------------------|----------------|----------------|--------------------|---|--|---------------|-------|
| 173.208.136.170 | United States | 147.237.0.15 | kosher-kravi.idf.i | Block HTTP Non Compliant | Failed to handle connection data | monitor | 52 |
| 173.208.136.170 | United States | 147.237.0.15 | kosher-kravi.idf.i | drop | SAM rule | drop | 29 |
| 5.102.254.212 | Israel | 147.237.0.15 | kosher-kravi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 20 |
| 94.188.248.70 | Israel | 147.237.0.15 | kosher-kravi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 16 |
| 213.8.204.45 | Israel | 147.237.0.15 | kosher-kravi.idf.i | drop | SAM rule | drop | 14 |
| 46.19.85.254 | Israel | 147.237.0.15 | kosher-kravi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 12 |
| 94.188.248.70 | Israel | 147.237.0.15 | kosher-kravi.idf.i | Bad TCP sequence | Invalid ACK number | alert | 10 |
| 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 |
| 46.19.85.214 | Israel | 147.237.0.15 | kosher-kravi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 5.102.254.159 | Israel | 147.237.0.15 | kosher-kravi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 80.246.130.99 | Israel | 147.237.0.15 | kosher-kravi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 216.243.31.2 | United States | 147.237.0.15 | kosher-kravi.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 2 |
| 64.125.239.240 | United States | 147.237.0.15 | kosher-kravi.idf.i | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 1 |
| 184.105.139.118 | United States | 147.237.0.15 | kosher-kravi.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 40.113.8.22 | United States | 147.237.0.15 | kosher-kravi.idf.i | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 1 |
| 141.212.122.165 | United States | 147.237.0.15 | kosher-kravi.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 109.253.200.111 | Israel | 147.237.0.15 | kosher-kravi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 202.112.51.96 | China | 147.237.0.15 | kosher-kravi.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 46.19.85.163 | Israel | 147.237.0.15 | kosher-kravi.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 183.2.207.27 | China | 147.237.0.15 | kosher-kravi.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 2.52.169.68 | Israel | 147.237.0.15 | kosher-kravi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 169.229.3.91 | United States | 147.237.0.15 | kosher-kravi.idf.i | drop | SAM rule | drop | 1 |
| 141.212.121.192 | United States | 147.237.0.15 | kosher-kravi.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 71.6.216.38 | United States | 147.237.0.15 | kosher-kravi.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 184.105.247.208 | United States | 147.237.0.15 | kosher-kravi.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 40.122.49.220 | United States | 147.237.0.15 | kosher-kravi.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 176.13.6.161 | Israel | 147.237.0.15 | kosher-kravi.idf.i | Bad TCP sequence | Invalid ACK number | alert | 1 |
| 141.212.122.166 | United States | 147.237.0.15 | kosher-kravi.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 109.253.223.117 | Israel | 147.237.0.15 | kosher-kravi.idf.i | Bad TCP sequence | Invalid ACK number | alert | 1 |
| 80.246.130.99 | Israel | 147.237.0.15 | kosher-kravi.idf.i | Bad TCP sequence | Invalid ACK number | alert | 1 |
| 184.105.139.100 | 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 | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 141.212.122.81 | 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 |
| 185.130.5.235 | | 147.237.0.15 | kosher-kravi.idf.i | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 1 |
| 46.19.85.56 | Israel | 147.237.0.15 | kosher-kravi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 176.13.6.161 | Israel | 147.237.0.15 | kosher-kravi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 141.212.122.203 | United States | 147.237.0.15 | kosher-kravi.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 109.253.223.117 | Israel | 147.237.0.15 | kosher-kravi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 184.105.139.107 | United States | 147.237.0.15 | kosher-kravi.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 141.212.122.82 | United States | 147.237.0.15 | kosher-kravi.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 109.253.200.111 | Israel | 147.237.0.15 | kosher-kravi.idf.i | Bad TCP sequence | Invalid ACK number | alert | 1 |
| 80.82.64.68 | Netherlands | 147.237.0.15 | kosher-kravi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 191.240.136.5 | Brazil | 147.237.0.15 | kosher-kravi.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 46.19.85.163 | Israel | 147.237.0.15 | kosher-kravi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 180.76.15.10 | China | 147.237.0.15 | kosher-kravi.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 141.212.122.204 | United States | 147.237.0.15 | kosher-kravi.idf.i | SYN Attack | SYN -> SYN-ACK -> RST | reject | 1 |
| 128.232.110.28 | United Kingdom | 147.237.0.15 | kosher-kravi.idf.i | SYN Attack | SYN -> SYN-ACK -> Timeout | reject | 1 |
| 81.218.66.107 | Israel | 147.237.0.15 | kosher-kravi.idf.i | Bad TCP sequence | Invalid ACK number | monitor | 1 |

01-18-2016 to 01-19-2016

Top Attackers In WAF

| Attacker Address | Attacker Geo | Target Address | Site | Signature | Device Action | Count |
|------------------|----------------------|----------------|--------------------|--|---------------|-------|
| 173.208.136.170 | United States | 147.237.0.15 | kosher-kravi.idf.i | Multiple Admin Blocking from 173.208.136.170 | Block | 3 |
| 46.211.34.236 | Ukraine | 147.237.0.15 | kosher-kravi.idf.i | PHP Attempt | Block | 2 |
| 46.211.34.236 | Ukraine | 147.237.0.15 | kosher-kravi.idf.i | Multiple Unauthorized URL Access from 46.211.34.236 | Block | 2 |
| 169.229.3.91 | United States | 147.237.0.15 | kosher-kravi.idf.i | Illegal Byte Code Character in Method [[#21]]Â Â²[[#15]]Ã&OÃ„Â-Ã?B | Block | 1 |
| 173.208.136.170 | United States | 147.237.0.15 | kosher-kravi.idf.i | Multiple Unauthorized URL Access from 173.208.136.170 | Block | 1 |
| 136.243.48.84 | Germany | 147.237.0.15 | kosher-kravi.idf.i | Unauthorized URL Access to kosher-kravi.idf.il/shared/usercontrols/headerupper/ | Block | 1 |
| 46.211.34.236 | Ukraine | 147.237.0.15 | kosher-kravi.idf.i | Admin Blocking | Block | 1 |
| 169.229.3.91 | United States | 147.237.0.15 | kosher-kravi.idf.i | Illegal Byte Code Character in URL | Block | 1 |
| 46.211.34.236 | Ukraine | 147.237.0.15 | kosher-kravi.idf.i | Unauthorized URL Access to kosher-kravi.idf.il/wp-login.php | Block | 1 |
| 141.212.122.81 | United States | 147.237.0.15 | kosher-kravi.idf.i | Unauthorized URL Access to /x | Block | 1 |
| 46.211.34.236 | Ukraine | 147.237.0.15 | kosher-kravi.idf.i | Multiple Admin Blocking from 46.211.34.236 | Block | 1 |
| 169.229.3.91 | United States | 147.237.0.15 | kosher-kravi.idf.i | Unknown HTTP Request Method [[#21]]Â Â²[[#15]]Ã&OÃ„Â-Ã?B in URL | Block | 1 |
| 80.82.64.68 | Netherlands | 147.237.0.15 | kosher-kravi.idf.i | Unauthorized URL Access to alemaral.org/wp-content/themes/akhbar24/images/alemarah.jpg | Block | 1 |
| 142.54.169.166 | United States | 147.237.0.15 | kosher-kravi.idf.i | Unauthorized URL Access to www.tgobet.com/ | Block | 1 |
| 91.214.201.107 | Moldova, Republic of | 147.237.0.15 | kosher-kravi.idf.i | Unauthorized URL Access to 147.237.0.15/ | Block | 1 |

01-18-2016 to 01-19-2016