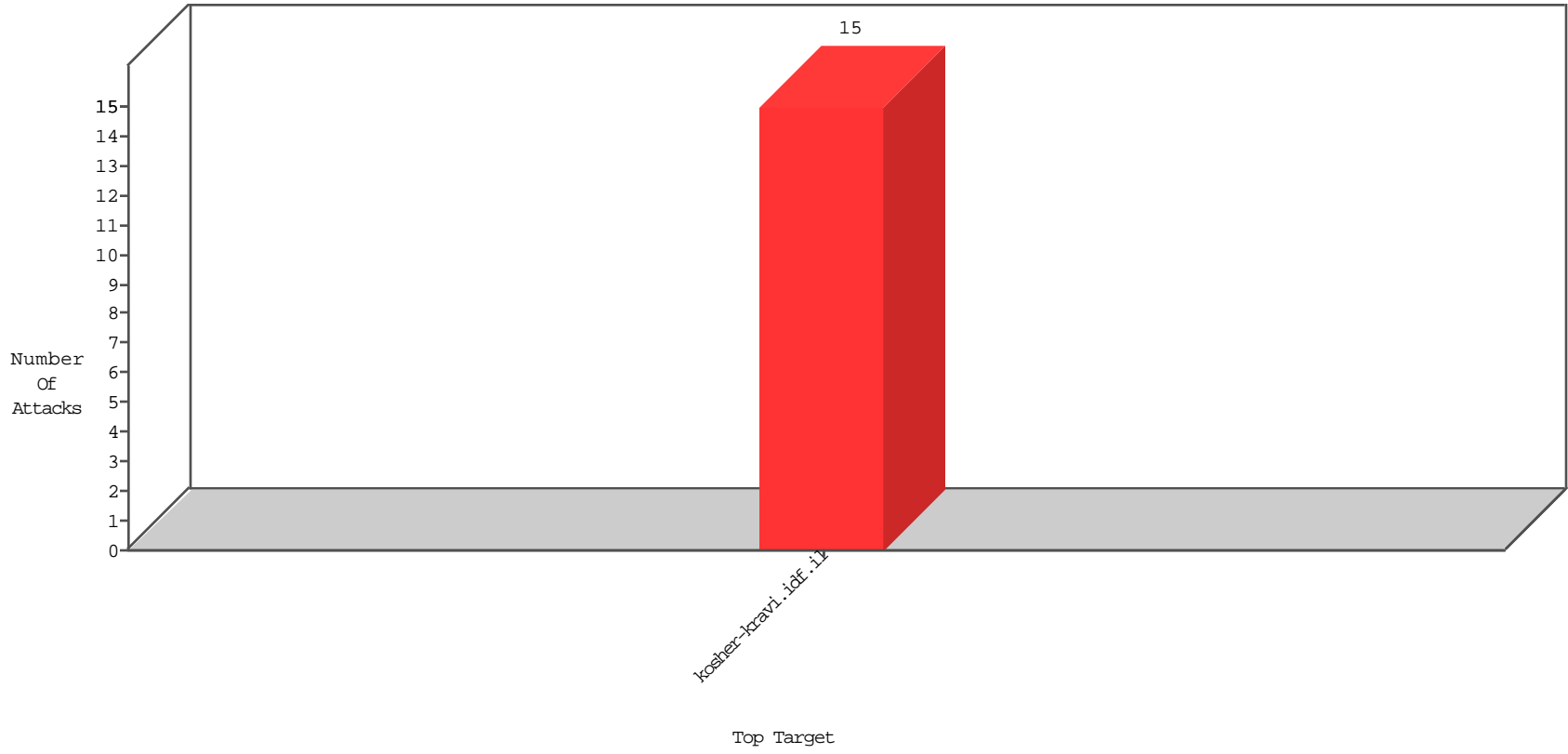


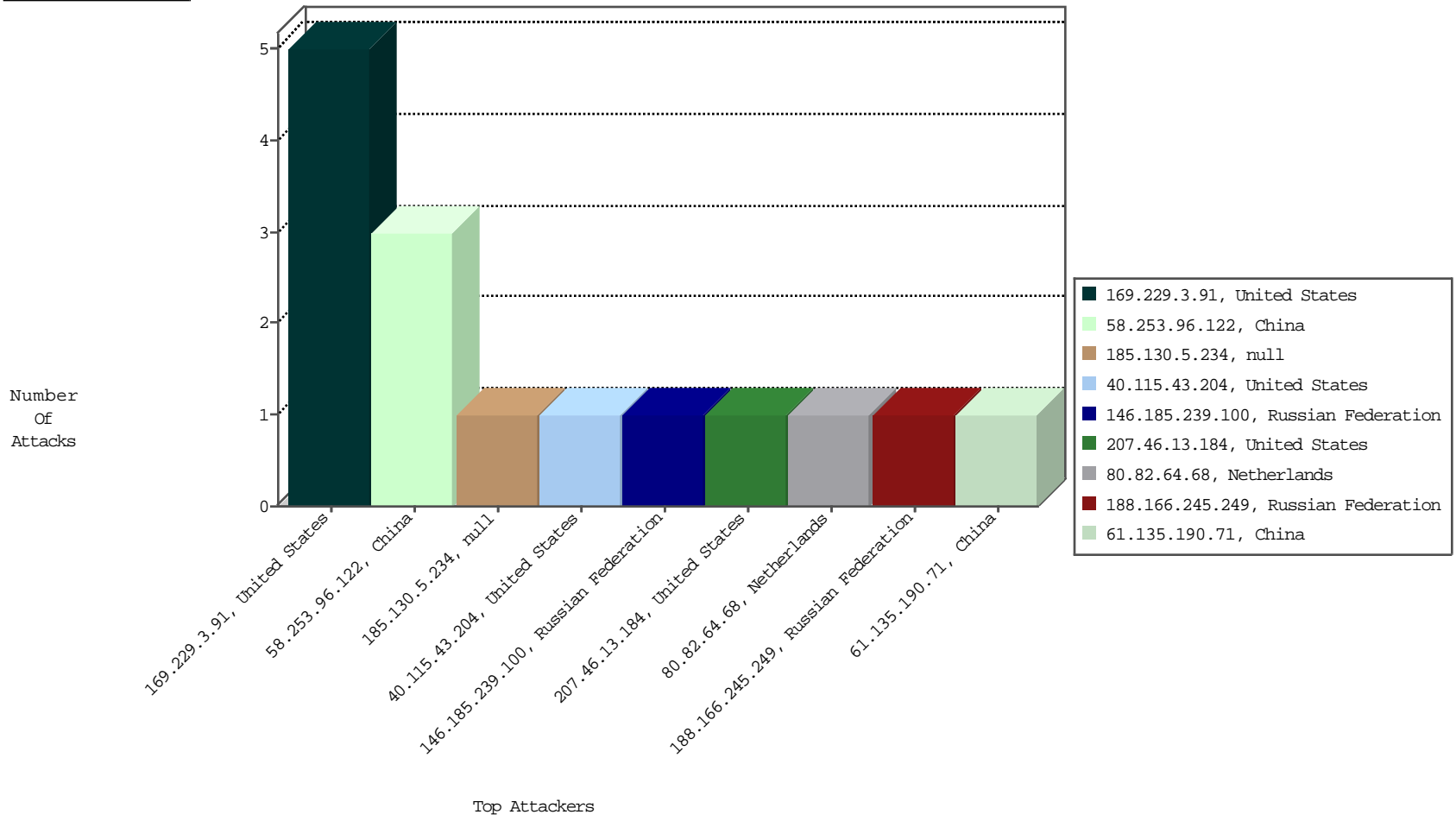
# Focused IP Under Attack Daily Report



## Top Targets



## Top Attackers



01-25-2016 to 01-26-2016

Top Attackers In DDoS-Defence

| Attacker Address | Attacker Geo       | Target Address | Site                | Signature      | Device Action | DP_location.Location | Count |
|------------------|--------------------|----------------|---------------------|----------------|---------------|----------------------|-------|
| 146.185.239.100  | Russian Federation | 147.237.0.15   | kosher-kravi.idf.il | block-sp-traf1 | drop          | BBL-Frankfurt        | 1     |

01-25-2016 to 01-26-2016

Top Attackers In IPS

| Attacker Address | Attacker Geo  | Target Address | Site                | Signature                               | Device Action | Count |
|------------------|---------------|----------------|---------------------|---|---------------|-------|
| 40.115.43.204    | 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 |
|------------------|--------------------|----------------|---------------------|------------------------------|-------|
| 188.166.245.249  | Russian Federation | 147.237.0.15   | kosher-kravi.idf.il | ET SCAN NMAP -sS window 1024 | 1     |
| 58.253.96.122    | China              | 147.237.0.15   | kosher-kravi.idf.il | ET SCAN NMAP -sS window 2048 | 1     |
| 185.130.5.234    |                    | 147.237.0.15   | kosher-kravi.idf.il | ET SCAN Potential SSH Scan   | 1     |
| 58.253.96.122    | China              | 147.237.0.15   | kosher-kravi.idf.il | ET SCAN NMAP -f -sS          | 1     |
| 58.253.96.122    | China              | 147.237.0.15   | kosher-kravi.idf.il | ET SCAN NMAP -sS window 3072 | 1     |

## Top Attackers In FW

| Attacker Address | Attacker Geo       | Target Address | Site               | Name  | Signature  | Device Action | Count |
|------------------|--------------------|----------------|--------------------|---|--|---------------|-------|
| 68.180.229.94    | United States      | 147.237.0.15   | kosher-kravi.idf.i | drop  | SAM rule   | drop          | 66    |
| 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     |
| 5.102.254.190    | Israel             | 147.237.0.15   | kosher-kravi.idf.i | Bad TCP sequence                                | Invalid ACK number   | monitor       | 8     |
| 216.243.31.2     | United States      | 147.237.0.15   | kosher-kravi.idf.i | SYN Attack                                      | SYN -> SYN-ACK -> RST  | reject        | 2     |
| 184.105.139.122  | United States      | 147.237.0.15   | kosher-kravi.idf.i | SYN Attack                                      | SYN -> SYN-ACK -> RST  | reject        | 1     |
| 144.172.234.107  | Canada             | 147.237.0.15   | kosher-kravi.idf.i | drop  | SAM rule   | drop          | 1     |
| 80.82.64.68      | Netherlands        | 147.237.0.15   | kosher-kravi.idf.i | Bad TCP sequence                                | Invalid ACK number   | alert         | 1     |
| 176.13.1.218     | Israel             | 147.237.0.15   | kosher-kravi.idf.i | Bad TCP sequence                                | Invalid ACK number   | alert         | 1     |
| 80.246.130.246   | Israel             | 147.237.0.15   | kosher-kravi.idf.i | Bad TCP sequence                                | Invalid ACK number   | monitor       | 1     |
| 216.218.206.79   | United States      | 147.237.0.15   | kosher-kravi.idf.i | SYN Attack                                      | SYN -> SYN-ACK -> RST  | reject        | 1     |
| 146.185.239.102  | Russian Federation | 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     |
| 40.115.43.204    | United States      | 147.237.0.15   | kosher-kravi.idf.i | SYN Attack                                      | SYN -> SYN-ACK -> Timeout  | reject        | 1     |
| 176.13.1.218     | Israel             | 147.237.0.15   | kosher-kravi.idf.i | Bad TCP sequence                                | Invalid ACK number   | monitor       | 1     |
| 141.212.121.192  | United States      | 147.237.0.15   | kosher-kravi.idf.i | SYN Attack                                      | SYN -> SYN-ACK -> RST  | alert         | 1     |
| 71.6.216.48      | United States      | 147.237.0.15   | kosher-kravi.idf.i | SYN Attack                                      | SYN -> SYN-ACK -> RST  | reject        | 1     |
| 216.218.206.118  | 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     |
| 46.19.86.74      | Israel             | 147.237.0.15   | kosher-kravi.idf.i | Bad TCP sequence                                | Invalid ACK number   | monitor       | 1     |
| 184.105.139.116  | United States      | 147.237.0.15   | kosher-kravi.idf.i | SYN Attack                                      | SYN -> SYN-ACK -> RST  | reject        | 1     |
| 141.212.121.192  | United States      | 147.237.0.15   | kosher-kravi.idf.i | SYN Attack                                      | SYN -> SYN-ACK -> RST  | reject        | 1     |
| 79.176.134.202   | 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 | Block HTTP Non Compliant                        | illegal header format detected: Malformed HTTP format in request | monitor       | 1     |
| 80.246.130.246   | Israel             | 147.237.0.15   | kosher-kravi.idf.i | Bad TCP sequence                                | Invalid ACK number   | alert         | 1     |
| 64.125.239.174   | United States      | 147.237.0.15   | kosher-kravi.idf.i | SYN Attack                                      | SYN -> SYN-ACK -> Timeout  | reject        | 1     |

01-25-2016 to 01-26-2016

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 [[#28]]Ã?<br>F[[#15]]Ã%[[#8]]HÃ-1Ã%Ã,,Ãf0Ã²Ã¹Ã¹mH[[#23]][[#25]]OÃ¹+h[[#4]]yuÃ¥Ã..<br>Ã->Ãž[[#27]]Ã@8Ãµ%Ã,Ã&bÃ%Ãf(Ã²{oÃ | Block         | 1     |
| 80.82.64.68      | Netherlands   | 147.237.0.15   | kosher-kravi.idf.i | Unauthorized URL Access to gassam.ps/prisoner-52-murid_salim_al_akhras.html  | Block         | 1     |
| 169.229.3.91     | United States | 147.237.0.15   | kosher-kravi.idf.i | Malformed URL  | 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 [[#28]]Ã?<br>F[[#15]]Ã%[[#8]]HÃ-1Ã%Ã,,Ãf0Ã²Ã¹Ã¹mH[[#23]][[#25]]OÃ¹+h[[#4]]yuÃ¥Ã..<br>Ã->Ãž[[#27]]Ã@8Ãµ%Ã,Ã&bÃ%Ãf(Ã²{oÃ in URL    | Block         | 1     |
| 169.229.3.91     | United States | 147.237.0.15   | kosher-kravi.idf.i | Illegal Byte Code Character in Header Name   | Block         | 1     |
| 207.46.13.184    | United States | 147.237.0.15   | kosher-kravi.idf.i | Unauthorized URL Access to<br>kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/   | Block         | 1     |
| 61.135.190.71    | China         | 147.237.0.15   | kosher-kravi.idf.i | Unauthorized URL Access to 147.237.0.15/   | Block         | 1     |

01-25-2016 to 01-26-2016