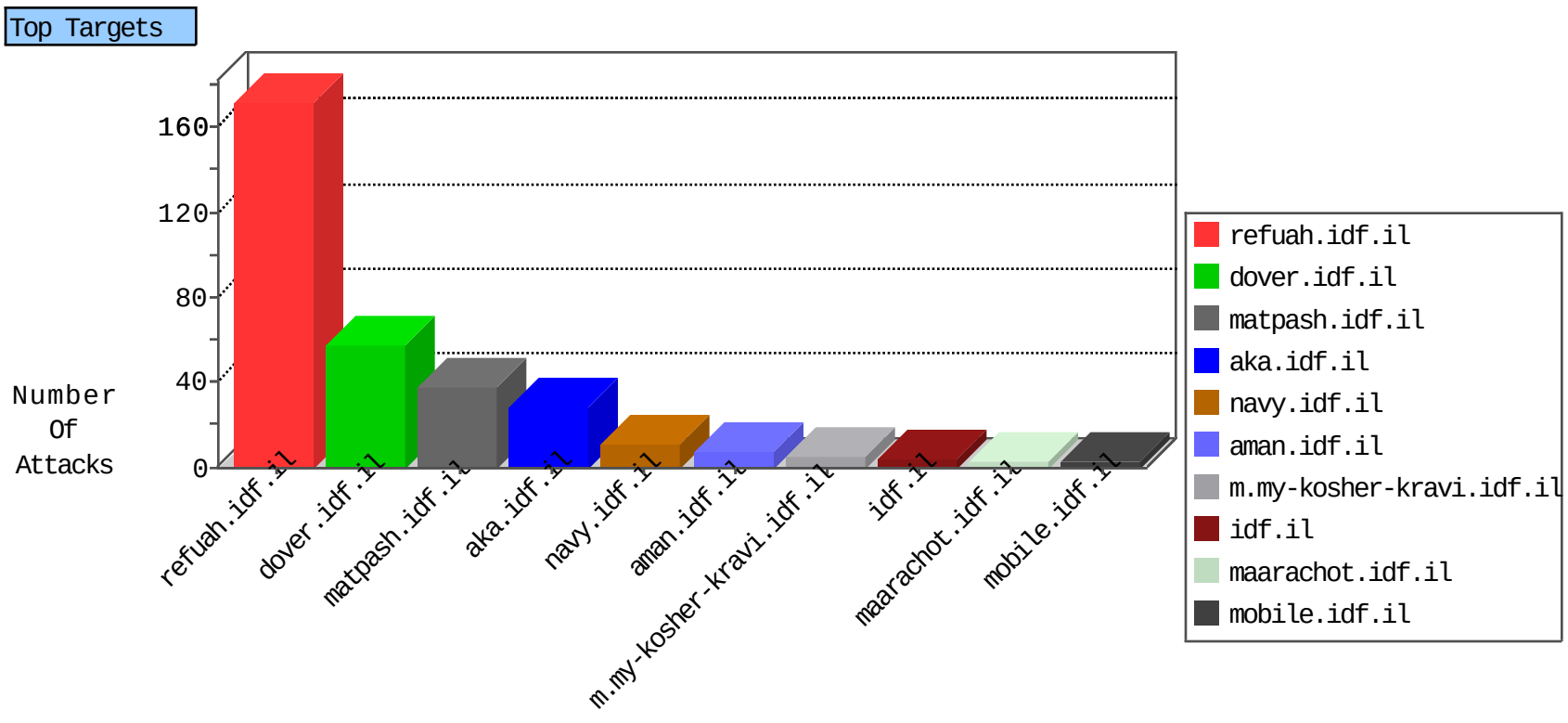
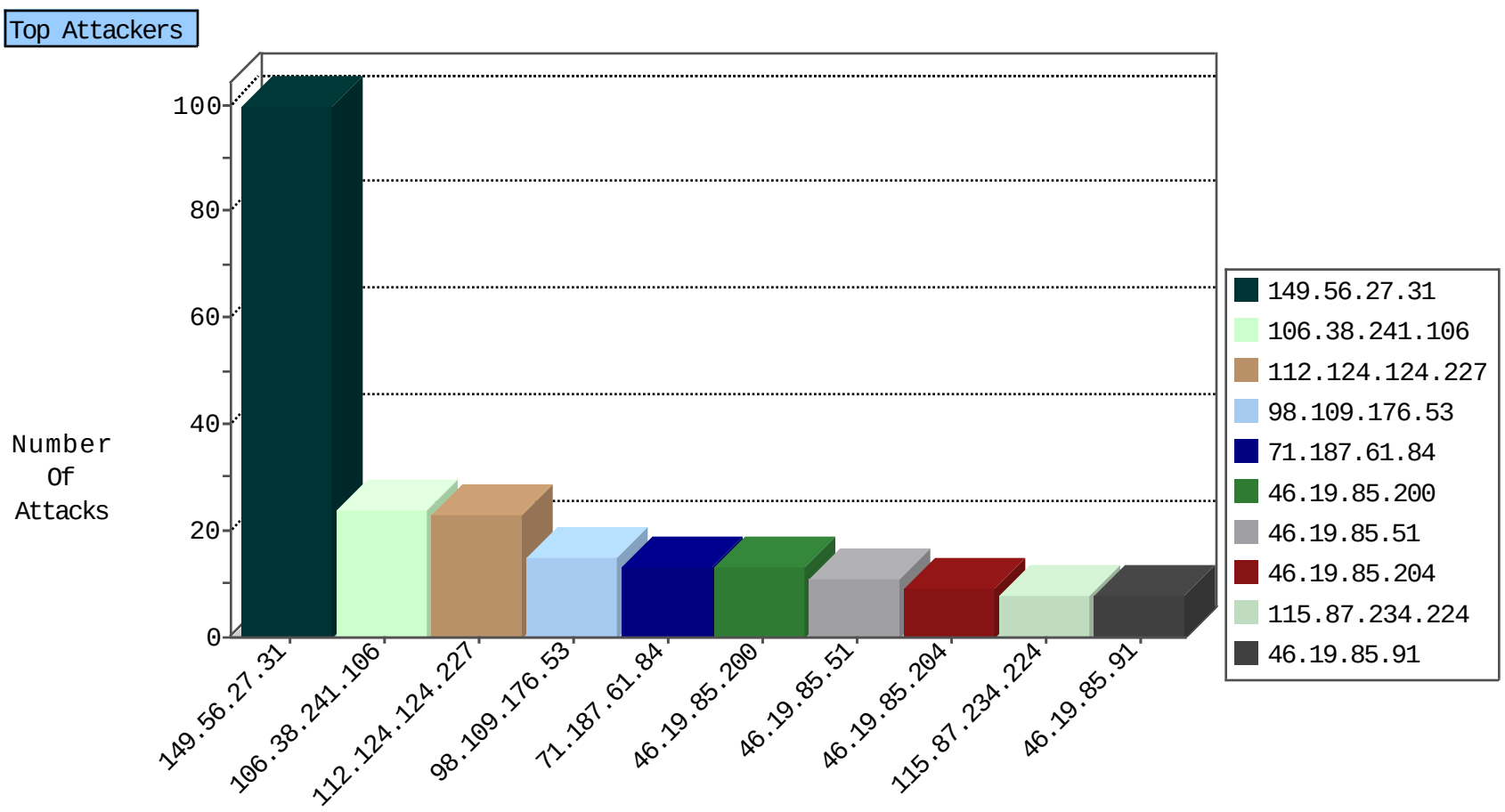
10-02-2016-06:04:02 to 10-02-2016-07:04:02

# IDF Under Attack Daily Report



10-02-2016-06:04:02 to 10-02-2016-07:04:02

## Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 109.67.123.183 | Israel | 147.237.77.216 | dover.idf.il | SYN Flood delete reset | drop | 5 |

10-02-2016-06:04:02 to 10-02-2016-07:04:02

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 106.38.241.106 | China | 147.237.77.176 | matpash.idf.il | C1000071: HTTP: User Agent Sogou+web+spider | Permit | 13 |

10-02-2016-06:04:02 to 10-02-2016-07:04:02

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 190.214.49.3 | 147.237.8.46 | Ecuador | e.chinuch.idf.il | ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force | 2 |
| 91.201.236.155 | 147.237.0.33 | Ukraine | idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 52.187.42.85 | 147.237.77.235 | United States | sviva.idf.il | ET SCAN Potential SSH Scan | 1 |
| 41.215.36.46 | 147.237.77.227 | Kenya | e.hamaz.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 183.60.48.25 | 147.237.76.39 | China | mobile.meitav.idf.il | ET SCAN Potential SSH Scan | 1 |
| 176.47.77.71 | 147.237.77.216 | Saudi Arabia | dover.idf.il | ET DROP Spamhaus DROP Listed Traffic Inbound | 1 |
| 91.224.161.69 | 147.237.0.34 | Netherlands | tikshuv.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.201.236.158 | 147.237.0.17 | Ukraine | m.my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 2048 | 1 |
| 91.201.236.155 | 147.237.0.33 | Ukraine | idf.il | ET SCAN NMAP -sS window 4096 | 1 |
| 91.201.236.155 | 147.237.0.33 | Ukraine | idf.il | ET SCAN NMAP -f -sS | 1 |
| 46.172.91.21 | 147.237.72.14 | Ukraine | dover.idf.il(old) | ET SCAN NMAP -sS window 1024 | 1 |
| 183.129.160.229 | 147.237.0.34 | China | tikshuv.idf.il | ET SCAN Potential SSH Scan | 1 |
| 183.60.48.25 | 147.237.0.17 | China | m.my-kosher-kravi.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.224.161.69 | 147.237.76.38 | Netherlands | e.e.meitav.idf.il | ET SCAN Potential SSH Scan | 1 |
| 91.201.236.158 | 147.237.0.17 | Ukraine | m.my-kosher-kravi.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 91.201.236.158 | 147.237.0.17 | Ukraine | m.my-kosher-kravi.idf.il | ET SCAN NMAP -f -sS | 1 |

10-02-2016-06:04:02 to 10-02-2016-07:04:02

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 149.56.27.31 | United States | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 62 |
| 149.56.27.31 | United States | 147.237.76.42 | refuah.idf.il | SYN Attack | | monitor | 26 |
| 149.56.27.31 | United States | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 12 |
| 85.64.130.93 | Israel | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 8 |
| 46.19.85.200 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 46.19.85.204 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 7 |
| 98.109.176.53 | United States | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 6 |
| 77.124.39.199 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 6 |
| 46.19.85.200 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 6 |
| 112.124.124.227 | China | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different sequence | monitor | 5 |
| 112.124.124.227 | China | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 5 |
| 112.124.124.227 | China | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 5 |
| 112.124.124.227 | China | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different sequence | alert | 5 |
| 46.19.85.91 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | alert | 4 |
| 46.19.85.91 | Israel | 147.237.77.216 | dover.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 4 |
| 98.109.176.53 | United States | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different sequence | monitor | 4 |
| 46.19.85.51 | Israel | 147.237.77.176 | matpash.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 71.187.61.84 | United States | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different sequence | alert | 3 |
| 112.124.124.227 | China | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 3 |
| 2.55.56.220 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Invalid Retransmission | Invalid segment retransmission. Packet dropped. | drop | 3 |
| 212.143.142.56 | Israel | 147.237.77.216 | dover.idf.il | drop | First packet isn't SYN | drop | 3 |
| 71.187.61.84 | United States | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different sequence | monitor | 3 |
| 71.187.61.84 | United States | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 3 |
| 24.184.77.28 | United States | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 2 |
| 71.187.61.84 | United States | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 2 |
| 98.109.176.53 | United States | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 2 |
| 79.181.99.166 | Israel | 147.237.72.156 | aman.idf.il | Bad TCP sequence | | monitor | 2 |
| 159.192.248.80 | Thailand | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 2 |
| 71.187.61.84 | United States | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 2 |
| 115.87.234.224 | Thailand | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 2 |
| 46.19.85.204 | Israel | 147.237.76.86 | navy.idf.il | Bad TCP sequence | Invalid ACK number | alert | 2 |
| 27.34.32.45 | Nepal | 147.237.72.166 | aka.idf.il | Bad TCP sequence | SYN+ACK retransmit with different window scale | monitor | 2 |
| 98.109.176.53 | United States | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different sequence | alert | 2 |
| 46.19.86.3 | Israel | 147.237.77.176 | matpash.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 24.184.77.28 | United States | 147.237.76.42 | refuah.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | alert | 2 |
| 115.87.234.224 | Thailand | 147.237.72.166 | aka.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 2 |
| 41.37.67.148 | Egypt | 147.237.77.216 | dover.idf.il | drop | SAM rule | drop | 2 |
| 46.19.85.51 | Israel | 147.237.77.176 | matpash.idf.il | Block HTTP Non Compliant | illegal header format detected: Illegal start line in request | monitor | 1 |
| 77.138.125.108 | France | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 159.192.248.80 | Thailand | 147.237.72.166 | aka.idf.il | drop | First packet isn't SYN | drop | 1 |
| 115.87.234.224 | Thailand | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 67.224.154.90 | Puerto Rico | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | SYN retransmit with different sequence | monitor | 1 |
| 108.172.55.87 | Canada | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 216.154.212.80 | United States | 147.237.77.170 | maarachot.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |
| 80.246.137.1 | Israel | 147.237.72.166 | aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 163.172.220.201 | United Kingdom | 147.237.77.216 | dover.idf.il | SYN Attack | SYN -> SYN-ACK -> Timeout | monitor | 1 |
| 46.19.85.51 | Israel | 147.237.77.176 | matpash.idf.il | Bad TCP sequence | Invalid ACK number | alert | 1 |
| 71.244.142.181 | United States | 147.237.77.176 | matpash.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 141.212.122.19 | United States | 147.237.76.200 | eitan.aka.idf.il | SYN Attack | SYN -> SYN-ACK -> RST | monitor | 1 |
| 69.174.160.32 | United States | 147.237.76.42 | refuah.idf.il | Bad TCP sequence | Invalid ACK number | monitor | 1 |

10-02-2016-06:04:02 to 10-02-2016-07:04:02

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 66.249.65.51 | Israel | 147.237.77.216 | dover.idf.il | Multiple Unauthorized URL Access from 66.249.65.51 | Block | 5 |
| 77.138.197.114 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx | Block | 3 |
| 64.118.104.215 | United States | 147.237.77.216 | dover.idf.il | SSL Untraceable Connection - Open Mode | None | 1 |
| 185.27.106.161 | Israel | 147.237.72.166 | aka.idf.il | Unknown Parameter asm in www.aka.idf.il/main/giyus/yahash2017/lobby.aspx | None | 1 |
| 66.249.65.185 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/994-8941-he/refuah.aspx | Block | 1 |
| 46.19.85.51 | Israel | 147.237.77.176 | matpash.idf.il | Abnormally Long Request method | Block | 1 |
| 66.249.64.124 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized URL Access to www.aka.idf.il/lomdim/forum/ | Block | 1 |
| 5.102.242.124 | Israel | 147.237.0.19 | madim.atal.idf.il | Suspicious Response Code | Block | 1 |
| 66.249.76.52 | Israel | 147.237.0.17 | m.my-kosher-kravi.idf.il | Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx | None | 1 |
| 46.19.85.51 | Israel | 147.237.77.176 | matpash.idf.il | Illegal HTTP Version | Block | 1 |
| 80.178.191.219 | Israel | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/main/sachar/ | Block | 1 |
| 27.34.108.219 | Nepal | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 1 |
| 66.249.79.8 | Israel | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to www.navy.idf.il/1132-8613-he/navy.aspx.aspx | Block | 1 |
| 46.19.85.51 | Israel | 147.237.77.176 | matpash.idf.il | Malformed URL asp.net_sessionid=qyf5cm451vaf5l45o4xlvmv1 | Block | 1 |
| 80.246.130.242 | Israel | 147.237.76.42 | refuah.idf.il | Parameter Type Violation searchText in www.refua.atal.idf.il/1653-he/refuah.aspx | Block | 1 |
| 66.249.65.52 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/hebrew/organization/paratroopers | Block | 1 |
| 40.77.169.101 | United States | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/1133-14686-he/dover.aspx (hebrew) | Block | 1 |
| 77.138.124.163 | France | 147.237.72.166 | aka.idf.il | Multiple Unauthorized Method for Known URL from 77.138.124.163 | Block | 1 |
| 46.19.85.51 | Israel | 147.237.77.176 | matpash.idf.il | Unknown HTTP Request Method 4839.1461754585.; in URL asp.net_sessionid=qyf5cm451vaf5l45o4xlvmv1 | Block | 1 |
| 157.55.39.144 | United States | 147.237.76.86 | navy.idf.il | Unauthorized URL Access to navy.idf.il/main/home/default.aspx | Block | 1 |
| 66.249.65.182 | Israel | 147.237.76.42 | refuah.idf.il | Unauthorized URL Access to 147.237.76.42/994-8804-he/refuah.aspx | Block | 1 |
| 46.4.74.42 | Germany | 147.237.72.166 | aka.idf.il | Unauthorized Method HEAD for www.aka.idf.il/miluim/templates/inner.asp | Block | 1 |
| 77.138.124.163 | France | 147.237.72.166 | aka.idf.il | Unauthorized Method POST for aka.idf.il/rights/asp/home.asp | Block | 1 |

10-02-2016-06:04:02 to 10-02-2016-07:04:02