

Module 1: Groundwork – Security Essentials

Demo 2 – Solution

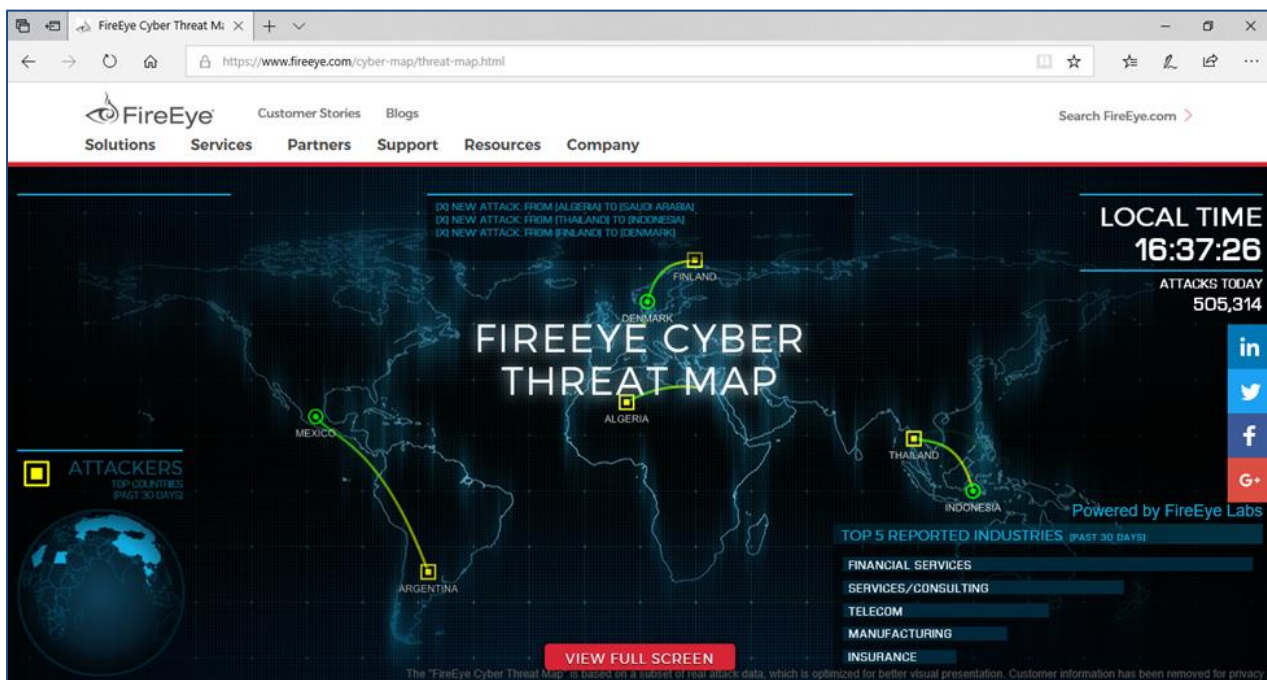
edureka!

edureka!

© Brain4ce Education Solutions Pvt. Ltd.

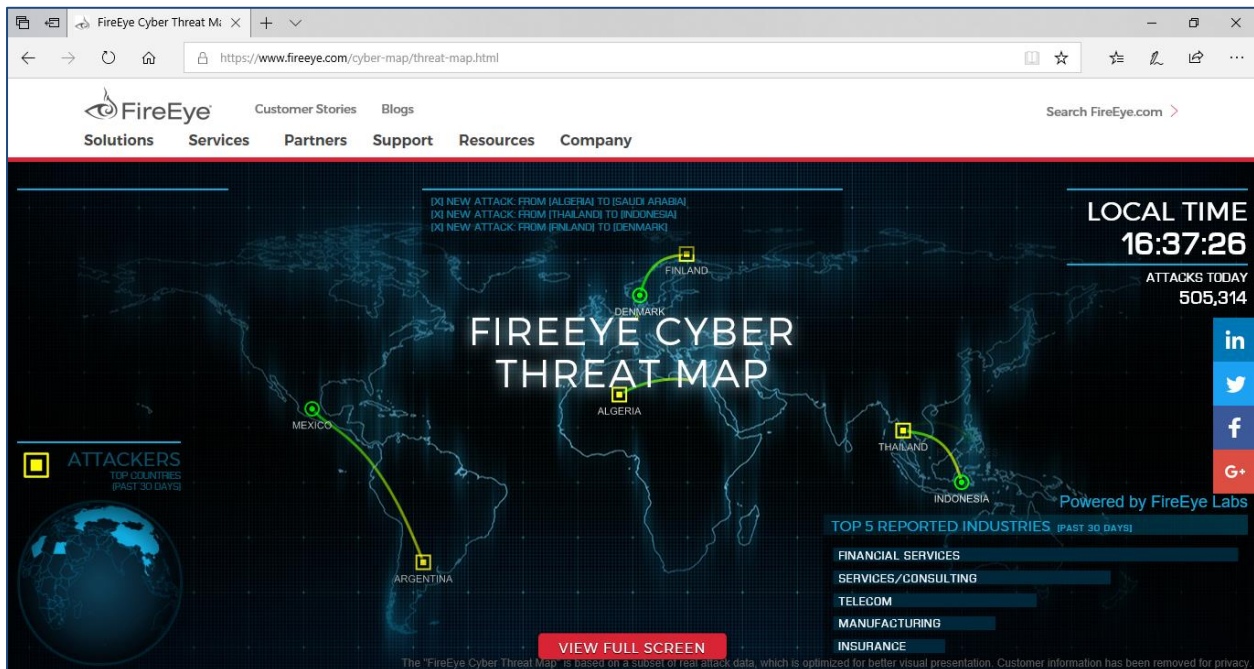
Demo 2 : Internet Threat Scenario

- Monitor the global cyber threat scenario including hacking, bots, and malware attacks using live threat maps
- Identify hacking attempts or cyber-attacks from different parts of the world as they happen in real time
- Use the link: <https://www.fireeye.com/cyber-map/threat-map.html>

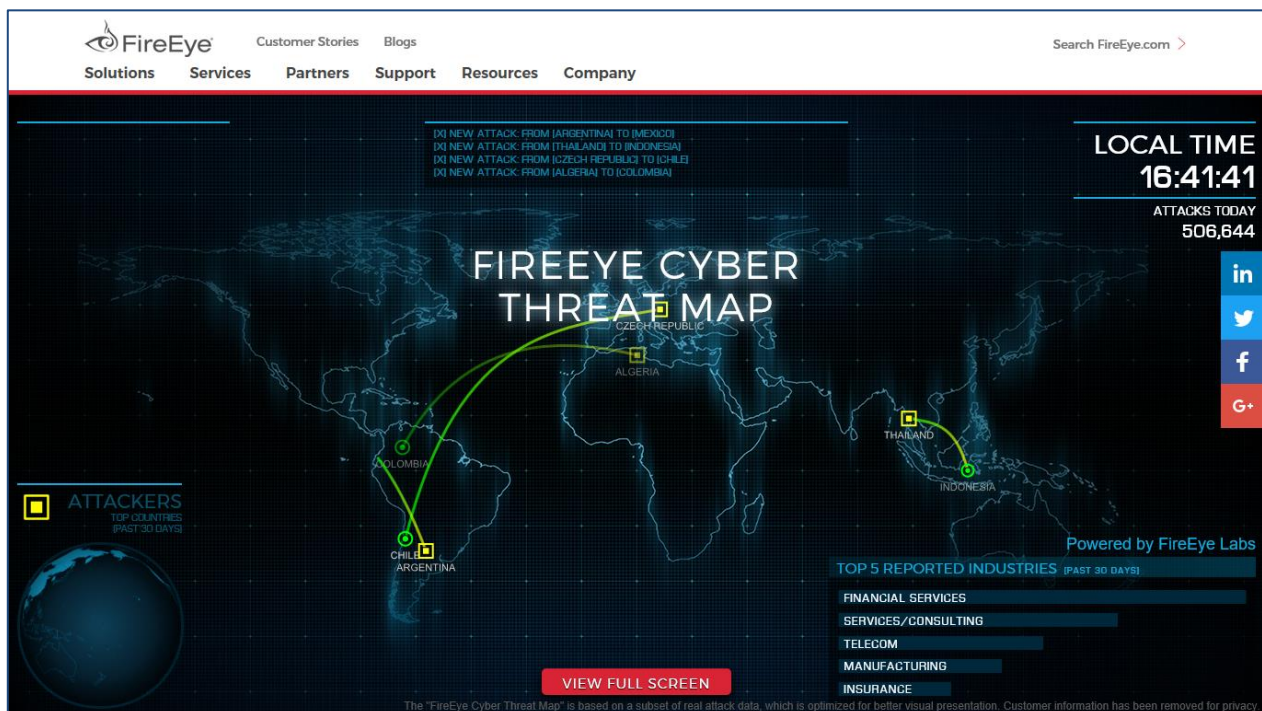


Demo 2 – Solution

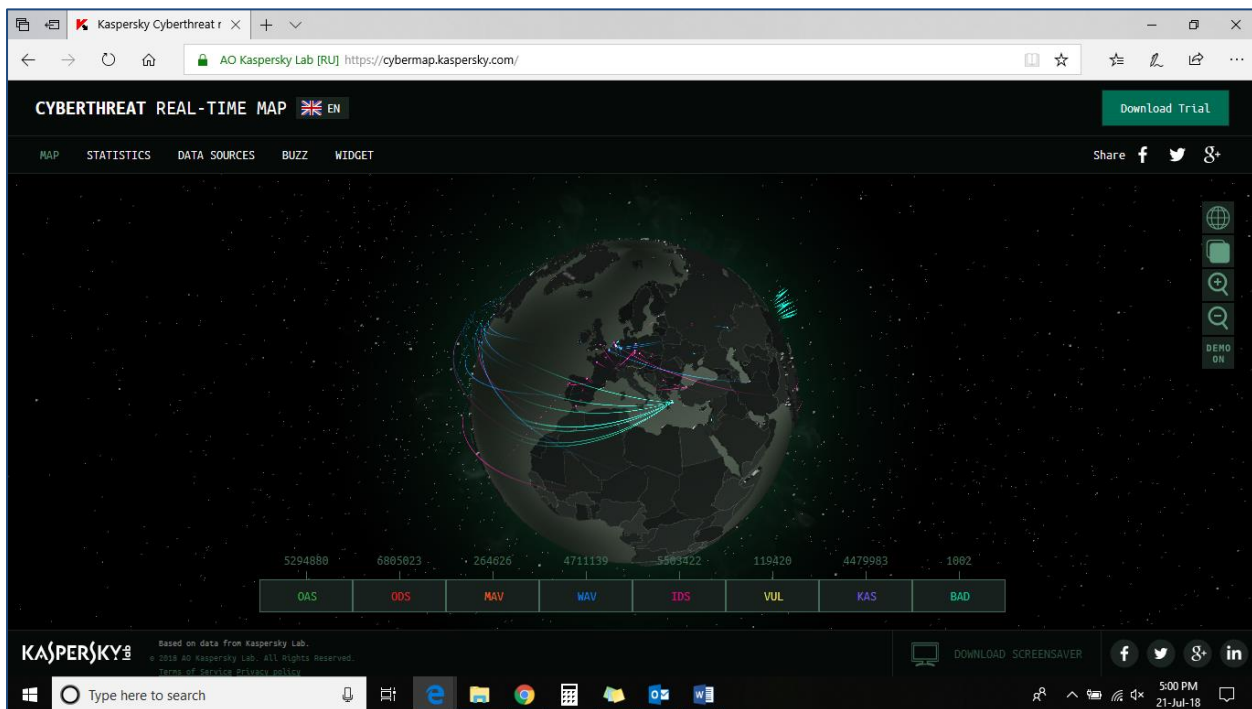
- **Step 1:** Open the FireEye cyber threat map by opening the following URL:
<https://www.fireeye.com/cyber-map/threat-map.html>



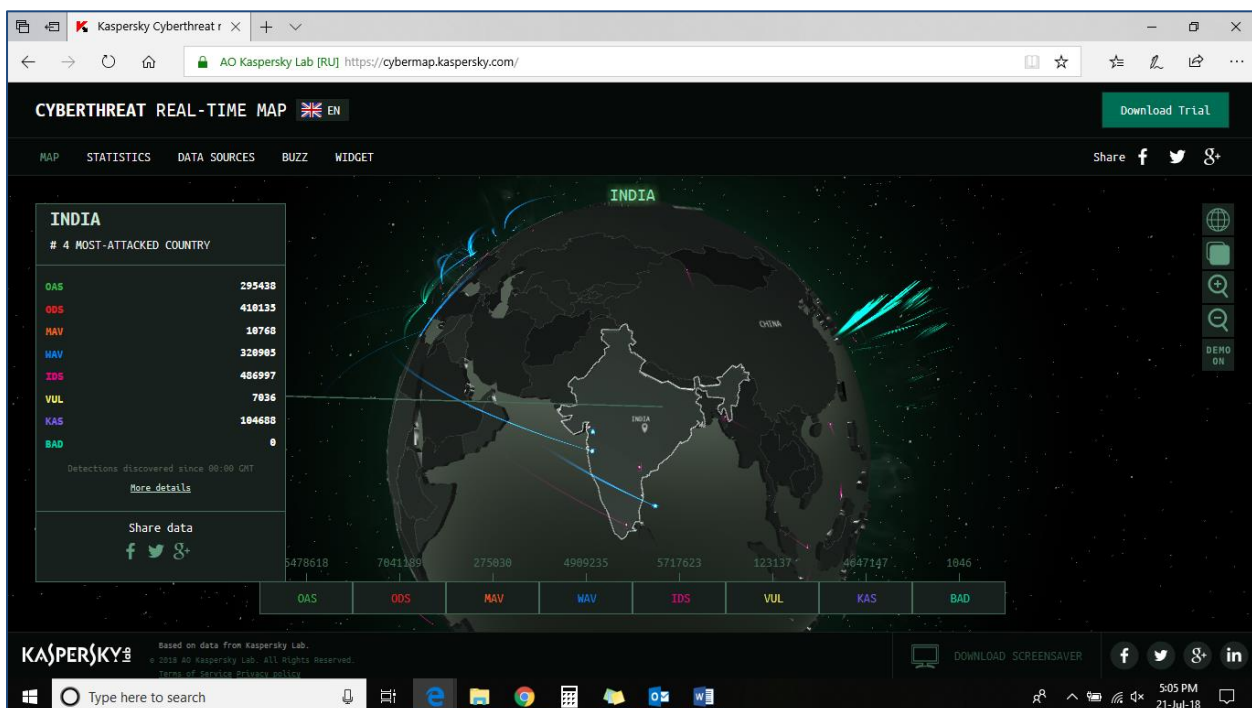
- **Step 2:** Click on “View Full Screen” for full screen view. You can view top 5 industries hit by cyberattacks on the bottom right hand side and most attack originating countries on the bottom left hand side



- **Step 3:** Open Kaspersky Cyber threat real-time map from the following link:
<https://cybermap.kaspersky.com/>



- **Step 4:** To view the country specific details click on the country on the map.
Example: India



- **Step 5:** To view the overall statistics of detected attacks click on the Statistics tab on the screen



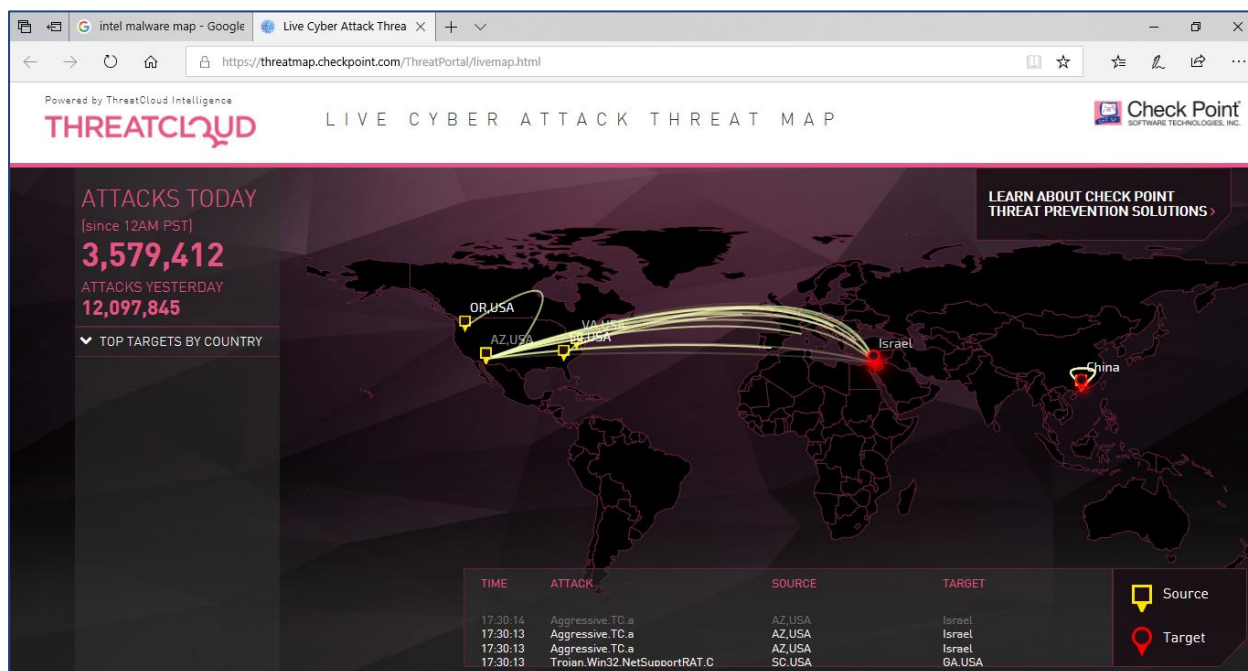
- **Step 6:** Click on the “Data Sources” tab to view the details of different sources of attack detection

The screenshot shows the 'CYBERTHREAT REAL-TIME MAP' interface with the 'DATA SOURCES' tab selected. The page displays detailed information for various detection sources:

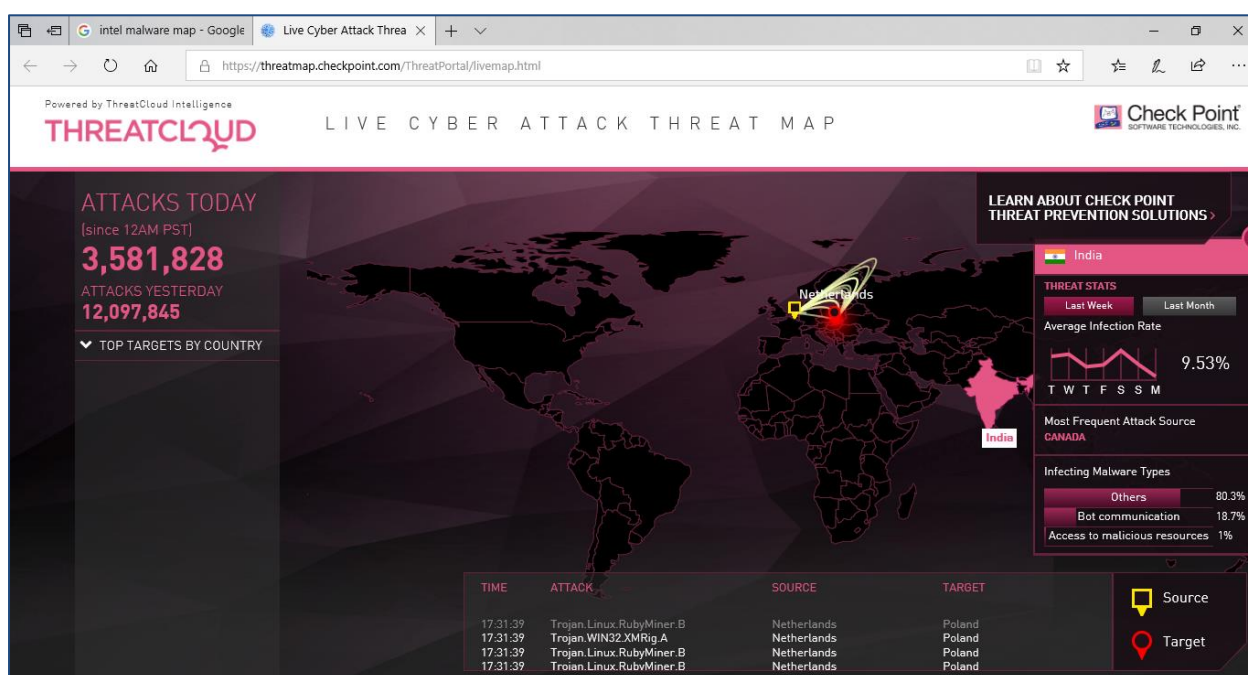
- OAS - On-Access Scan:** OAS (On-Access Scan) shows malware detection flow during On-Access Scan, i.e. when objects are accessed during open, copy, run or save operations.
- ODS - On-Demand Scan:** ODS (On Demand Scanner) shows malware detection flow during On-Demand Scan, when the user manually selects the 'Scan for viruses' option in the context menu.
- MAV - Mail Anti Virus:** MAV (Mail Anti-Virus) shows malware detection flow during Mail Anti-Virus scan when new objects appear in an email application (Outlook, The Bat, Thunderbird). The MAV scans incoming messages and calls OAS when saving attachments to a disk.
- WAV - Web Anti-Virus:** WAV (Web Anti-Virus) shows malware detection flow during Web Anti-Virus scan when the html page of a website opens or a file is downloads. It checks the ports specified in the Web Anti-Virus settings.
- IDS - Intrusion Detection Scan:** IDS (Intrusion Detection System) shows network attacks detection flow.
- VUL - Vulnerability Scan:** VUL (Vulnerability Scan) shows vulnerability detection flow.
- KAS - Kaspersky Anti-Spam:** KAS (Kaspersky Anti-Spam) shows suspicious and unwanted email traffic discovered by Kaspersky Lab's Reputation Filtering technology.
- BAD - Botnet Activity Detection:** BAD (Botnet Activity Detection) shows statistics on identified IP-addresses of DDoS-attacks victims and botnet C&C servers. These statistics were acquired with the help of the DDoS Intelligence system (part of the solution Kaspersky DDoS Protection).

The page also features promotional banners for 'ESSENTIAL PROTECTION FOR YOUR PC AGAINST MALWARE' and 'PREMIUM PROTECTION FOR YOUR PC AGAINST MALWARE AND INTERNET THREATS', both offering a 'FREE TRIAL'.

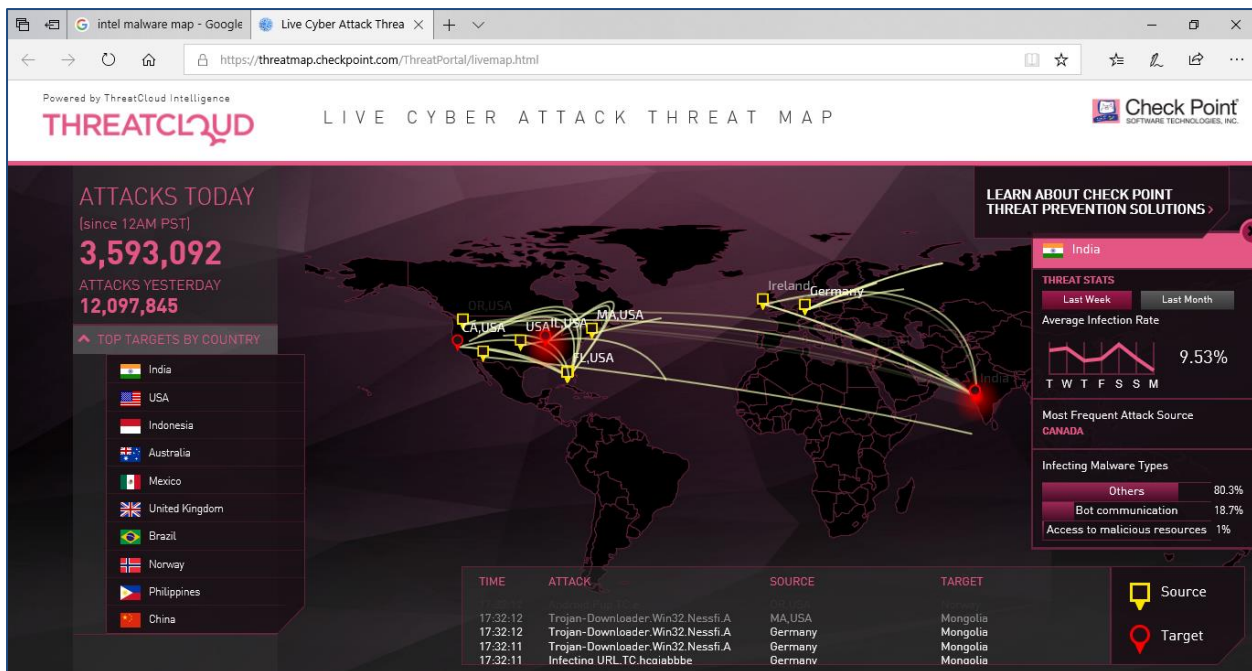
- **Step 7:** Open the Checkpoint Live Cyber Attack Threat Map by clicking on the following URL: <https://threatmap.checkpoint.com/ThreatPortal/livemap.html>



- **Step 8:** Click on a particular country for getting country specific details of cyber attacks



- **Step 9:** To view the top targets by country list click on the “Top Targets by Country” dropdown



edureka!