Emerging Threat Alert: Israeli Conflict and Industries Impacted

The conflict between Israel and Palestine has resulted in cyberattacks by politically motivated hackers, commonly known as hacktivists. According to CyberKnow, a security research group, more than 60 groups have launched attacks on Israeli and Palestinian territories. Although pro-Palestine hacking groups have been more active, it is expected that pro-Israel groups may also emerge. Additionally, state-backed hacking groups, especially those associated with Iran, have a history of targeting Israel through espionage and disruptive attacks. These cyber conflicts have wide-ranging effects, impacting various industries. It is crucial for organizations to maintain a high threat level, as more hacking groups are likely to join the Israel-Hamas conflict. Currently, the following industries have been impacted:

1. **Travel and Tourism:** Airlines and travel companies often suspend or modify flights to Israel during times of conflict. Travelers may cancel or postpone their plans, leading to revenue losses in the tourism industry. Cruise operators may also adjust itineraries to avoid areas of conflict.
2. **Energy:** Energy companies operating in the region, like Chevron, may be affected. There can be disruptions in the production and transportation of oil and natural gas. For instance, Israel's Ministry of Energy ordered Chevron to shut down the Tamar natural gas field.
3. **Banking and Finance:** Financial institutions with offices in Israel, such as Goldman Sachs, JPMorgan Chase, Bank of America, Morgan Stanley, and Citigroup, may ask employees to work from home or make operational changes in response to security concerns.
4. **Logistics:** Logistics companies like FedEx and UPS may temporarily suspend services or flights in and out of the conflict zone. They often have contingency plans to ensure the safety of their shipments.
5. **Technology:** Tech companies with offices in the region, such as Nvidia, may cancel events or shift their workloads to other regions as needed to ensure employee safety.
6. **Retail and Consumer Goods:** Retail giants like H&M and Inditex have temporarily closed their stores in Israel, which can impact sales and operations.
7. **Pharmaceuticals:** Pharmaceutical companies like Eli Lilly and Co closely monitor the situation to ensure the safety of their staff and an uninterrupted supply of medicines to patients in the region.

The impact on these industries may fluctuate based on factors such as the conflict's intensity, duration, geographic location, and the specific companies involved. It is essential to remain vigilant as cyber hacktivists continue to target various industries, potentially affecting your organization.
_____

The CRITICAL**START**® Cyber Research Unit will continue to monitor the situation and work closely with the SOC and Security Engineering team to implement any relevant detections. For future updates the CTI team will post updates via Cyber Operations Risk & Response™ Bulletins and on the Critical Start Intelligence Hub.

References:
1. https://www.axios.com/2023/10/10/israel-palestine-hamas-companies-businesses
2. https://www.aljazeera.com/economy/2023/10/10/how-global-firms-are-reacting-to-the-israel-hamas-conflict
3. https://www.csis.org/analysis/energy-market-implications-israel-hamas-conflict
4. https://cybernews.com/cyber-war/palestine-israel-scada-under-attack/
5. https://www.informationweek.com/it-leadership/israel-s-vital-tech-industry-braces-for-war
6. https://gbhackers.com/hack-private-power-station-in-israel/
7. https://thehackernews.com/2023/10/gaza-linked-cyber-threat-actor-targets.html
8. https://www.csoonline.com/article/655223/israel-palestine-conflict-extends-to-cyberspace.html
9. https://www.controlrisks.com/our-thinking/insights/israel-hamas-conflict-to-heighten-cyber-espionage-and-disruptive-cyber-threats?utm_referrer=https://www.google.com