Here is a potential LinkedIn post based on the article you provided:

"Cache poisoning is a cyber-attack where hackers manipulate web caches, you don't want to be a victim of such attacks. What is a web cache you may ask? Web caching involves storing a copy of a piece of content. A web cache stores copies of web pages or parts of web content temporarily. Learn more about web caching here [insert listing with bolded punctuation below]:

Browser Cache: Stores a copy of recently visited web pages, images, and other content

CDN Cache: Stores copies of web resources in multiple worldwide locations

Reverse Proxy Cache: Sits between users and the web server, caching content to reduce server load and improve response times

Web caching serves content faster but comes with vulnerabilities that can be exploited by hackers. Here is a summary of how cache poisoning works and some methods to avoid it [insert listing with numbered points and bolded punctuation below]:

1. The attacker identifies cached resources on a web page, crafts a request with harmful content that looks like a legitimate request, and tricks the cache into storing the malicious content.

2. When a user requests the cached resource, the cache serves the manipulated data instead of the legitimate one.

Cache poisoning poses a significant risk to web applications and users. You can protect your web apps from cache poisoning by learning how it works and using proper precautions. Protect yourself and read the Stealth Security newsletter for more articles on offensive and defensive cybersecurity.