Time Is of the Essence: Discovering Co-Evolving Browser Extensions via Update Patterns

Eric Olsson

May 25, 2026

1 Abstract

Thousands of browser extensions are published to the Chrome Web Store daily, and malicious ones routinely survive review for months or years. A common defense is to expand from a known malicious seed by linking extensions through shared code, domains, or developer metadata. However, coordinated campaigns increasingly diversify these properties to evade clustering. In this paper, we demonstrate that *temporal update patterns* provide a valuable signal for resisting this evasion, because the signal emerges from shared behavior among extensions rather than identifying properties of any single one. We develop a framework that clusters co-evolving extensions by the similarity of their update timeseries to detect coordinated groups. Applied to Chrome Web Store data from 2022–2025, our method uncovers a malvertising campaign of 146 extensions including 65 previously unreported extensions with over two million combined users, with the temporal update signal revealing these extensions even though their code, domain, and developers are divided. We further identify a novel attack vector exploited by this campaign: *spammy updates*, in which attackers publish frequent, near-empty updates solely to trigger on-update events to redirect users to attacker-controlled domains, including malvertising networks.