Издание ArsTechnica выяснило, что разработчики браузерных расширений монетизируют свой труд, продавая доступ к сайтам для платных клиентов через браузеры ничего не подозревающих пользователей.

По подсчётам исследователя информационной безопасности Джона Такнера из SecurityAnnex, специализированные расширения для браузеров установлены на 1 млн устройств. Эти расширения отключают ключевые средства защиты и сканируют веб-сайты от имени платных служб. Расширения используются для различных целей, включая управление закладками, увеличение громкости динамиков и генерацию случайных чисел. Все расширения используют библиотеку JavaScript MellowTel-js для монетизации рассылки.

Эксперт утверждает, что монетизация осуществляется за счёт использования расширений для парсинга веб-сайтов (сбора и обобщения информации) в интересах платных клиентов, включая рекламодателей. MellowTel-js предоставляет пропускную способность для доступа к общедоступным данным с веб-сайтов. Это весьма экономичный способ парсинга.

Подобная практика считается легальной, однако Такнер указывает на нарушение конфиденциальности и внедрение скрытого фрейма на страницу при использовании MellowTel. MellowTel также проблематична, так как сайты, которые открываются таким образом, неизвестны конечным пользователям, что требует доверия к MellowTel в проверке безопасности и достоверности каждого сайта.

По мнению Такнера, MellowTel представляет опасность для корпоративных сетей, которые ограничивают типы кода и сайты, разрешённые для запуска пользователями. И если этой библиотекой начнут пользоваться злоумышленники, учитывая количество установленных расширений, масштаб атак на компьютеры и слежки будет огромным.