Циклические перенаправления превращают онлайн-рекламу в гигантскую финансовую ловушку.

Исследователи выявили две мошеннические сети, которые ежедневно перенаправляют сотни миллионов онлайн-реклам на всплывающие окна на сомнительных сайтах. В докладе от 30 мая компания Human Security – это компания, специализирующаяся на кибербезопасности. Основная цель компании заключается в обеспечении защиты информации и данных от киберугроз путем разработки и предоставления разнообразных решений и услуг. Это может включать в себя меры по обнаружению и предотвращению кибератак, защиту личных данных, мониторинг сетевой активности и оценку уязвимостей в компьютерных системах. Human Security также может заниматься обучением сотрудников компаний и организаций основам кибербезопасности для снижения рисков." data-html="true" data-original-title="Human Security" >Human Security назвала эти сети «Merry-Go-Round» или операция «Карусель» за характерный способ циклического показа рекламы на ограниченном числе доменов.

В период своего пика «Карусель» демонстрировала пользователям 782 миллиона рекламных объявлений ежедневно. В настоящее время операция продолжает работать, показывая в среднем 200 миллионов объявлений в день, приводя к огромным доходам злоумышленников и аналогичным потерям рекламодателей.

«Масштаб и величина этой операции поражают», — отмечает Уилл Гербиг, директор по борьбе с мошенничеством в Human Security. «Чтобы понять масштаб: обычный пользователь видит около 5000 объявлений в день [с отключенным блокировщиком рекламы]. Так что 780 миллионов — это эквивалентно ежедневной рекламной нагрузке 150 000 человек».

Рекламные компании теряют огромные суммы денег из-за подобного рода мошенничества с самого начала существования онлайн-рекламы. Закрытый рынок размещения рекламы, где посредники автоматизируют процесс покупки и продажи онлайн-пространства, создаёт дистанцию между покупателем и продавцом, чем и пользуются мошенники.

«Карусель» работает относительно просто, но эффективно. Начинается всё с невидимого оверлея, наложенного на сайт с пиратским контентом или материалами для взрослых. Любой клик перенаправляет пользователя в новую вкладку с ожидаемым контентом, в то время как оригинальное окно переходит на домен «Карусели», демонстрирующий пользователю сотни рекламных объявлений в фоне.

«Карусель» использует различные методы для избежания обнаружения. Например, первый показанный пользователю домен включает HTML-код, запрещающий поисковым системам индексировать сайт и проверять содержащиеся в нём ссылки. Дополнительный JavaScript-код сбрасывает информацию о реферере, чтобы скрыть связи между доменами «Карусели» и сайтами, запустившими цикл.

Лучший трюк «Карусели» — это маскировка. Если подозревающий мошенничество рекламодатель напрямую посещает один из доменов, он видит простую, безобидную страницу. И лишь при редиректе с определённых сайтов пользователю показывается настоящая форма «Карусели» со множеством рекламных объявлений на странице.

Обнаружение и остановка таких операций, как «Карусель», сложны. К счастью, рекламодателям есть простой способ избежать потерь бюджета — не доверять размещение рекламы посредникам.

«Важно знать, у кого покупается рекламное пространство», — советует Гербиг. «Чем ближе отношения с партнёрами, тем меньше вероятность попасть на мошенников».

К счастью, конечным пользователям подобные операции не угрожают. Они лишь используют их для незаконного заработка, что, впрочем, тоже способствует достижению мошенниками своих целей. Чтобы не играть на руку киберпреступникам, стоит в обязательном порядке использовать в браузере блокировщик рекламы, а также не посещать сомнительные веб-сайты.