Покупка домена привела к атаке на цепочку поставок, затронувшей более 100 000 сайтов.

Более 100 000 сайтов подверглись массовой атаке на цепочку поставок со стороны сервиса Polyfill.io — это сервис, предоставляющий полифиллы (фрагменты кода), которые позволяют использовать современные функции веб-стандартов в старых браузерах, которые их не поддерживают.

 Polyfill.io автоматически определяет, какие полифиллы необходимы для текущего браузера пользователя, и загружает только их, минимизируя таким образом размер загружаемого кода. Это помогает разработчикам обеспечить кроссбраузерную совместимость и улучшить производительность веб-приложений." data-html="true" data-original-title="Polyfill.io" >Polyfill.io после того, как китайская компания Компания Funnull специализируется на услугах по распределению контента (CDN), защите от DDoS-атак и оптимизации веб-сайтов. Компания предоставляет решения для ускорения загрузки сайтов, защиты от различных видов онлайн-угроз и оптимизации производительности веб-приложений." data-html="true" data-original-title="Funnull" >Funnull приобрела домен, а скрипт сервиса был изменен для перенаправления пользователей на вредоносные и мошеннические сайты.

Polyfill — это фрагмент кода (обычно JavaScript — это язык программирования, с помощью которого web-страницам придается интерактивность. С его помощью создаются приложения, которые включаются в HTML-код. Вся уникальность данного языка программирования заключается в том, что он поддерживается практически всеми браузерами и полностью интегрируется с ними." data-html="true" data-original-title="JavaScript" >JavaScript), добавляющий современную функциональность старым браузерам, которые не поддерживают его изначально. Например, Polyfill добавляет функции JavaScript, недоступные в старых браузерах, но присутствующие в современных.

Сервис polyfill.io используется сотнями тысяч сайтов, чтобы позволить всем посетителям использовать одну и ту же кодовую базу, даже если их браузеры не поддерживают те же современные функции, что и более новые.

Как объясняет ИБ-компания Sansec, в феврале китайская компания Funnull купила домен и учетную запись Polyfill на GitHub — это платформа для хостинга и совместной разработки программного обеспечения.

 Одним из ключевых аспектов GitHub является его социальная составляющая. Разработчики могут подписываться на интересующие их проекты, следить за обновлениями, вносить свои предложения и комментарии, а также взаимодействовать с другими разработчиками, делая процесс

разработки быстрее и эффективнее.

 GitHub является популярным инструментом в сообществе разработчиков и служит платформой для сотен тысяч открытых и закрытых проектов в различных областях программного обеспечения." data-html="true" data-original-title="GitHub" >Github. С тех пор домен был пойман на внедрении вредоносного ПО на мобильные устройства через любой сайт, встраивающий cdn.polyfill.io.

Специалисты Sansec обнаружили, что модифицированный скрипт используется для перенаправления на фиктивный сайт букмекерской конторы и другие мошеннические страницы. Это делается через поддельный домен Google Analytics (www[.]googie-anaiytics[.]com) или редиректы, такие как kuurza.com/redirect?from=bitget.

Отличительной чертой вредоносного кода является его способность уклоняться от анализа: он активируется только на определенных мобильных устройствах в строго определенное время и отключается при обнаружении в системе администратора или службы веб-аналитики.

В ответ на возрастающую угрозу, сервисы Cloudflare и Fastly создали собственные зеркала Polyfill.io, чтобы обеспечить безопасное использование скриптов на затронутых сайтах. Кроме того, при продаже Polyfill.io разработчик проекта предупредил, что он никогда не владел сайтом Polyfill.io и что все веб-сайты должны немедленно удалить его.

Пост разработчика Polyfill.io

Google также вступила в борьбу с угрозой, предупредив рекламодателей о риске нежелательных перенаправлений с их лендинг-страниц. Отмечается, что Bootcss, Bootcdn и Staticfile также вызывают нежелательные перенаправления, потенциально добавляя тысячи, если не сотни тысяч сайтов, пострадавших от атак в цепочке поставок. Если Google обнаружит такие редиректы во время регулярных проверок рекламных мест, соответствующая реклама будет отклонена.