Десятки тысяч сайтов оказались под прицелом цифровых диверсантов.

Несколько легитимных плагинов WordPress — это бесплатная платформа для управления контентом веб-сайтов (CMS), которая позволяет пользователям создавать и управлять своими собственными веб-сайтами без необходимости обладать специальными знаниями в области программирования. С помощью WordPress можно создавать различные типы сайтов, включая блоги, интернет-магазины, корпоративные сайты и другие типы веб-ресурсов. Платформа имеет открытый исходный код, что позволяет разработчикам создавать расширения и темы для WordPress, чтобы расширять его функциональность и адаптировать внешний вид сайта под свои нужды." data-html="true" data-original-title="WordPress" >WordPress подверглись атаке с внедрением вредоносного кода, который позволяет создавать несанкционированные учётные записи администраторов, что даёт возможность злоумышленникам выполнять произвольные действия.

Исследователь безопасности Wordfence — это компания, специализирующаяся на кибербезопасности и защите веб-сайтов, особенно на платформе WordPress. Компания также разрабатывает и предлагает одноимённый плагин безопасности, который помогает владельцам сайтов защититься от вредоносных программ, взломов и других кибератак.

 Плагин Wordfence предоставляет различные функции, включая мониторинг активности на сайте, блокировку вредоносного трафика, обнаружение и блокировку попыток взлома, защиту от перебора паролей и другие механизмы безопасности. Он также предлагает возможность сканирования веб-сайта на наличие уязвимостей и предупреждает владельцев о потенциальных угрозах.

 Компания Wordfence также предоставляет услуги мониторинга безопасности, которые позволяют владельцам сайтов быть в курсе актуальных угроз и обнаруживать нарушения безопасности в реальном времени. Они также предлагают консультационные услуги и помощь в восстановлении сайта после кибератак." data-html="true" data-original-title="Wordfence" >Wordfence Хлоя Чемберлен сообщила, что вредоносное ПО пытается создать новую учётную запись администратора и затем отправляет эти данные на сервер, контролируемый атакующими. Кроме того, угроза включает добавление вредоносного 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 в футер сайтов, что приводит к распространению SEO-спама.

Учётные записи администраторов имеют имена «Options» и «PluginAuth», а информация о них передаётся на IP-адрес 94.156.79[.]8.

Как злоумышленникам удалось скомпрометировать плагины, пока неизвестно, но первые признаки атаки датируются 21 июня 2024 года.

Сейчас данные плагины удалены из каталога WordPress для проведения проверки:

Пользователям данных плагинов рекомендуется проверить свои сайты на наличие подозрительных учётных записей администраторов и удалить их, а также устранить любой вредоносный код.