Злоумышленники придумали способ незаметной кражи конфиденциальных данных.

Согласно отчету Sucuri, неизвестные хакеры используют малоизвестные плагины 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 для внедрения вредоносного PHP — это скриптовый язык программирования, широко используемый для разработки веб-приложений. Он может быть встроен в HTML-код и обычно работает на сервере, обрабатывая запросы от клиентов. PHP применяется для создания динамических веб-страниц, работы с базами данных, формирования и отправки электронной почты, управления сессиями и cookie, а также для многих других задач на веб-сервере." data-html="true" data-original-title="PHP" >PHP-кода на сайты жертв и кражи платежных данных. Специалисты Sucuri – это компания, которая занимается безопасностью веб-сайтов и защитой от кибератак. Она предоставляет такие услуги, как сканирование на уязвимости, защиту от DDoS-атак и вредоносных программ, а также быстрое восстановление веб-сайта в случае взлома. Sucuri основана в 2010 году и имеет штаб-квартиру в Сан-Диего, Калифорния, США. Компания также предлагает услуги по оптимизации производительности веб-сайтов и контролю целостности контента. Sucuri работает со многими популярными CMS, такими как WordPress, Joomla и Drupal." data-html="true" data-original-title="Sucuri" >Sucuri 11 мая обнаружили кампанию, в ходе которой злоумышленники использовали плагин Dessky Snippets . Плагин, позволяющий пользователям добавлять собственный PHP-код, имеет более 200 активных установок.

В подобных атаках хакеры используют уязвимости в плагинах WordPress или легко угадываемые учетные данные для получения доступа администратора. После этого они устанавливают дополнительные плагины для дальнейшей эксплуатации. Плагин Dessky Snippets используется для внедрения серверного вредоносного ПО на PHP, которое занимается скимингом банковских карт на скомпрометированных сайтах и кражей финансовых данных.

Вредоносный код сохраняется в параметре dnsp_settings таблицы wp_options и изменяет процесс оформления заказа в WooCommerce — популярная платформа электронной коммерции для WordPress с открытым исходным кодом, которую

используют примерно 40% всех интернет-магазинов." data-html="true" data-original-title="WooCommerce" >WooCommerce. Код манипулирует формой выставления счета, добавляя поля для ввода данных платежной карты – имя, адрес, номер карты, дата истечения срока действия и CVV-номер. Собранные данные затем передаются на URL-адрес «hxxps://2of[.]cc/wp-content/».

Характеристики вредоносной кампании

Особенностью кампании является отключение атрибута автозаполнения (autocomplete="off") в форме выставления счета. Это снижает вероятность того, что браузер предупредит пользователя о вводе конфиденциальной информации. Также поля формы остаются пустыми до тех пор, пока пользователь не заполнит их вручную, что снижает подозрения.

Рекомендации для владельцев сайтов WordPress

Владельцам сайтов WordPress, особенно тем, кто предлагает функции электронной коммерции, рекомендуется поддерживать свои сайты и плагины в актуальном состоянии. Используйте надежные пароли для предотвращения атак методом перебора и регулярно проверяйте сайты на наличие признаков вредоносного ПО или любых несанкционированных изменений.

Ранее стало известно, что киберпреступники начали эксплуатировать критическую уязвимость в плагине WP Automatic для WordPress, что позволяет создавать учетные записи с административными привилегиями и устанавливать бэкдоры для долгосрочного доступа.