**Zip-ловушка: новая уязвимость обходит защиту Mark-of-the-Web**

Исследователи обнаружили уязвимость CVE-2025-0411 в программе для сжатия файлов 7-Zip, позволяющую злоумышленникам обходить механизм защиты Mark-of-the-Web (MOTW). Для защиты эксперт компании «Газинформсервис» Никита Титаренко рекомендует своевременно обновлять ПО и использовать в арсенале поведенческую аналитику центра мониторинга и реагирования GSOC.

MOTW — важный элемент безопасности Windows, предупреждающий пользователей о потенциальной опасности файлов, загруженных из интернета. Он добавляет к файлам из внешних источников специальный атрибут, позволяющий системе распознавать их как потенциально вредоносные. CVE-2025-0411 позволяет хакерам удалить этот атрибут, существенно повышая риск заражения. Без предупреждения MOTW вредоносный код, скрытый в архиве, может запуститься без ведома пользователя. Уязвимость затрагивает все поддерживаемые версии Windows. Отметим, что Microsoft уже выпустила патч для устранения этой уязвимости.

*«Данная уязвимость может позволить злоумышленникам создать архив, при распаковке которого файлы утрачивают метку "Mark of the Web", сигнализирующую о том, что файл был загружен из интернета. Следовательно, у пользователя, который обращается к файлам внутри подобного архива, не будет предупреждения перед их запуском. Это представляет серьёзную угрозу для безопасности пользователей, так как файлы могут хранить в себе вредоносный код, который может выполниться на целевой машине пользователя без каких-либо уведомлений. Для предотвращения развития атак пользователям следует своевременно обновлять ПО, которое установлено на устройстве, а организациям — обращаться к услугам центра мониторинга информационной безопасности, например GSOC, специалисты которого могут отслеживать подозрительную активность пользователей и устройств, оперативно выявлять и предотвращать угрозы, минимизируя риски и последствия для организации»,* — отметил инженер-аналитик компании «Газинформсервис» **Никита Титаренко**.

**Справка о компании:**

[ООО «Газинформсервис»](https://www.gaz-is.ru/) — отечественный разработчик программных и программно-аппаратных средств обеспечения информационной безопасности и комплексной инженерно-технической охраны. Компания специализируется на создании систем обеспечения информационной безопасности объектов и ИБ-систем для корпораций энергетической и транспортной отраслей, органов государственной власти, промышленных предприятий, а также учреждений финансового сектора и телекоммуникационных компаний.