**Киберэксперт Жданухин предостерёг от хакеров-ждунов**

Специалисты Solis Security и Intezer обнаружили новую тактику киберпреступной группы XE Group, которая с 2024 года проводит целенаправленные кражи данных, используя уязвимости нулевого дня и скрытно компрометируя системы управления заказами. Киберэксперт, аналитик L2 GSOC компании «Газинформсервис» Андрей Жданухин, предупреждает о возрастающей опасности атак так называемых «хакеров-ждунов» и подчёркивает необходимость комплексного подхода к защите.

Эксперт отмечает, что деятельность киберпреступной группировки XE Group, которая с 2024 года сосредоточилась на целенаправленной краже информации, эксплуатируя уязвимости нулевого дня в цепочках поставок и компрометируя системы управления заказами, поражает своей скрытностью. *«Злоумышленники использовали критические уязвимости в программном обеспечении VeraCore, что позволило им загружать вредоносные файлы на сервер, извлекать данные из базы и получать доступ к учётным записям. В одном из случаев они даже повторно активировали веб-оболочку, установленную ещё в 2020 году, что говорит нам о том, что атакующие могут выжидать долгие годы прежде, чем напасть снова».*

*«Уже сейчас существуют методы защиты от подобных угроз.* *В частности, программный модуль SafeERP Platform Security предназначен для выявления небезопасных настроек ПО и средств защиты, контроля целостности программных объектов и доступа к критически важным элементам информационных систем. Кроме того, здесь может помочь инструмент Efros DefOps, который обеспечивает контроль конфигураций и состояний рабочей среды сетевого оборудования, платформ виртуализации и операционных систем. Использование этих решений может существенно повысить уровень защиты корпоративных систем от подобных атак», —* отмечает киберэксперт **Андрей** **Жданухин**, — *«Надёжная кибербезопасность достигается за счёт развития культуры безопасности в целом, обучения персонала и использования профессиональных сервисов мониторинга (например, GSOC)».*

**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.