**Rezet (Rare Wolf) снова на охоте: к чему готовиться промышленным предприятиям?**

Группировка кибершпионов Rezet (Rare Wolf) снова атакует российские промышленные предприятия, маскируя вредоносные письма под приглашения на семинары по стандартизации оборонной продукции. Киберэксперт, аналитик L2 GSOC компании «Газинформсервис» Андрей Жданухин, предупреждает, что традиционные средства защиты могут оказаться бессильны без вовлечения самих сотрудников в обеспечение безопасности, и подчёркивает необходимость комплексного подхода к защите.

В январе 2025 года аналитики FACCT зафиксировали массовые атаки группировки Rezet (она же Rare Wolf) на российские промышленные предприятия. Объектами атак на этот раз стали предприятия химической, пищевой и фармацевтической промышленности.

*«Эта атака показывает, что злоумышленники продолжают совершенствовать методы социальной инженерии, используя максимально приближенные к реальности сценарии. Маскировка под официальные приглашения на мероприятия указывает на целенаправленный подход и детальную подготовку. И, вероятнее всего, для этого они используют современные нейросети»,* — отмечает киберэксперт.

В своих атаках хакеры обычно используют фишинговые рассылки, что произошло и на этот раз. Заражение системы происходило при запуске вложенного архива с pdf-документом и полезной нагрузкой.

*«Это говорит о том, что традиционные средства защиты, такие как антивирусы и почтовые фильтры, могут быть недостаточно эффективны без вовлечённости самих сотрудников в процесс обеспечения безопасности. Важно, что атаки затронули промышленные предприятия, поскольку они часто имеют более сложную инфраструктуру и могут быть менее защищены на уровне конечных пользователей. Это в очередной раз подчёркивает необходимость внедрения не только технических мер защиты, но и комплексного подхода к кибербезопасности. Компании должны развивать внутреннюю культуру безопасности, проводить обучающие мероприятия для сотрудников и усиливать контроль за внешним периметром организации, используя профессиональные услуги центра мониторинга, например GSOC»,* — добавил **Андрей Жданухин.**

**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.