**Новая схема атаки на атомную промышленность: как защититься от социальной инженерии?**

Руководитель лаборатории исследований кибербезопасности аналитического центра кибербезопасности компании «Газинформсервис» Вадим Матвиенко предупреждает о растущей угрозе сложных кибератак с использованием социальной инженерии. Недавние исследования специалистов «Лаборатории Касперского» подтверждают тревожную тенденцию: киберпреступники всё чаще используют психологические уловки и сложные методы маскировки вредоносного ПО, чтобы обмануть пользователей и получить доступ к их системам. В числе новых целей хакеров — предприятия атомной промышленности.

Специалисты обнаружили новую волну ключевой операции хак-группы Lazarus — DreamJob. Злоумышленники заражают инфраструктуру компаний через файловые архивы, которые распространяются под видом тестов на оценку навыков кандидатов на ИТ-позиции. Эти атаки требуют от организаций переосмысления своих стратегий кибербезопасности. Важно понимать, что традиционных мер защиты часто недостаточно для противодействия подобным угрозам.

*«Понимание психологии потенциальных жертв и использование современных методов маскировки своих действий, чтобы казаться легитимными действиями пользователей, — такой тренд прослеживается при анализе кибератак, осуществляемых АРТ-группировками. Учитывая сложность выявления и высокий уровень риска, для обеспечения информационной безопасности требуется комплексный подход. Центры мониторинга информационной безопасности, такие как SOC компании "Газинформсервис", помогают обнаружить подобные угрозы и оперативно отреагировать на них»*, — отметил **Вадим Матвиенко**.

Так, киберэксперт рекомендует компаниям пересмотреть свои стратегии информационной безопасности, уделив особое внимание обучению сотрудников и внедрению систем мониторинга безопасности для обнаружения угроз и реагирования на них в режиме реального времени.

Напомним, старт работы коммерческого SOC (Security Operations Center) компании «Газинформсервис» был объявлен в мае этого года. Специалисты компании в зависимости от состава услуг и возможностей заказчика используют различные схемы подключения и меняют состав решения, но в базе всегда присутствуют SIEM, VM, XDR и UEBA.

**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.