**Harvest под ударом: эксперт Едемская о растущей угрозе двойного вымогательства**

Финтех-компания Harvest стала жертвой атаки вымогателей Run Some Wares. Злоумышленники использовали тактику двойного вымогательства: зашифровали данные и угрожают их публикацией. Среди украденной информации — финансовые документы, юридические записи и данные сотрудников. Этот инцидент подчеркивает растущую угрозу кибератак, особенно для компаний, работающих с чувствительной информацией. **Екатерина Едемская, инженер-аналитик компании «Газинформсервис»,** подчеркивает текущие тенденции в сфере киберугроз, особенно для компаний, работающих с конфиденциальными данными.

*«Использование тактики «двойного вымогательства», при которой атакующие не только шифруют данные, но и угрожают их публикацией, является одной из самых опасных форм кибератак в настоящее время. Утечка значительного объема информации, включая финансовые документы, юридические записи и данные сотрудников, резко повышает риски для компании и ее клиентов, угрожая репутационными и финансовыми потерями»,* — объясняет Едемская.

Эксперт подчёркивает необходимость комплексной защиты данных: от надежного шифрования и безопасного хранения до строгих протоколов доступа и аутентификации. Не менее важным является мониторинг даркнета и внешних источников для своевременного обнаружения утечек данных. Раннее выявление и реагирование на угрозы, связанные с раскрытием данных, помогает минимизировать последствия. Учитывая высокую степень подготовки атакующих, компаниям необходимы стратегии долгосрочного реагирования, включая регулярное тестирование планов восстановления после атак, чтобы *минимизировать время простоя и потенциальные убытки от таких инцидентов.*

*«Инцидент с Harvest служит важным напоминанием о том, что киберугрозы становятся все более сложными и многоуровневыми. Для защиты от таких атак организациям необходимо не только внедрять передовые технические решения, но и развивать «культуру безопасности» на уровне всей компании, обучая сотрудников правильному обращению с данными и реагированию на угрозы. В этом контексте, использование системы поведенческой аналитики, такой как Ankey ASAP от компании "Газинформсервис", может значительно повысить уровень защищенности. Эта система эффективно обнаруживает аномалии и подозрительные действия на ранних стадиях атаки, используя методы машинного обучения и UEBA, что позволяет оперативно реагировать на угрозы и минимизировать риски»,* — отмечает киберспециалист.

**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.