**Мошенники обходят CAPTCHA: как защитить компанию от социальной инженерии?**

Недавняя новость о масштабной фишинговой кампании с поддельными CAPTCHA для распространения стиллера Lumma подчёркивает актуальность защиты от мошенников. Киберэксперт «Газинформсервиса» отмечает, что продукты поведенческой аналитики, такие как Ankey ASAP, становятся незаменимыми для защиты компаний. Они позволяют выявлять подозрительные действия сотрудников-жертв социальной инженерии, предотвращая потенциальный ущерб.

*«Про социальную инженерию в этом году знает каждый специалист ИБ — против неё ежедневно внедряются новые организационные и технические меры. Но не каждый сотрудник организации понимает, что подвергается воздействию социальной инженерии, и тем самым может нанести вред работе всей компании. Поведенческая аналитика продукта Ankey ASAP поможет вовремя поймать вредоносные действия, совершаемые сотрудником. Функциональность продукта настроена так, что он будет ориентироваться на терминальные команды, выявляя нелегитимные действия пользователя»,* — отметила менеджер по продукту Ankey ASAP компании «Газинформсервис» **Яна Заковряжина**.

Напомним, о масштабной кампании по распространению стиллера Lumma накануне сообщили специалисты Guardio Labs. Для мошеннической схемы авторы вредоносной активности использовали легитимную рекламную сеть.

**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.