**Киберэксперт призывает не терять бдительность: инфостилер вновь атакует Windows-системы**

Вредоносное ПО Skuld вновь атакует, на этот раз поражая не только Windows-системы, но и экосистему npm (Node Package Manager). Инженер-аналитик компании «Газинформсервис» Никита Титаренко призывает организации усилить меры кибербезопасности, особенно в предновогодний период и в праздники. По его словам, решение Ankey ASAP с модулем UEBA позволяет эффективно противостоять угрозам, подобным Skuld.

Недавно команда по исследованию угроз Socket обнаружила вредоносную кампанию, проникшую в экосистему npm; киберпреступники развернули инфостилер Skuld всего через несколько недель после аналогичной атаки, нацеленной на разработчиков Roblox. Злоумышленники целенаправленно атакуют доверительные отношения разработчиков с открытыми репозиториями, используя цепочку поставок программного обеспечения в качестве точки входа.

Так, злоумышленник, используя учётную запись ‘k303903’, распространил инфостилер, похищающий пароли, файлы cookie и историю браузера, более чем в 600 проектах, прежде чем пакеты были удалены. Этот инцидент повторяет предыдущую атаку и подчёркивает риски использования непроверенных пакетов npm, требуя от разработчиков внедрения строгих мер безопасности. Распространяется Skuld, вероятно, через фишинговые письма, содержащие вредоносные вложения.

*«Злоумышленники довольно часто маскируют доставку и использование вредоносного ПО под легитимную активность, что помогает им оставаться "в тени", совершая кибератаку. К сожалению, стандартные системы защиты информации могут пропустить подобного рода атаку, так как в ходе её реализации атакующий встраивается в легитимные процессы и маскирует вредоносные файлы под стандартные. Выявить скрытую атаку поможет система, имеющая "под капотом" модуль UEBA, с помощью которого можно отследить подозрительное поведение любой сущности на устройстве (пользователя, файла или процесса) и своевременно пресечь попытку злоумышленника нанести вред организации. Одной из таких систем является платформа расширенной аналитики Ankey ASAP»,* — отметил **Никита Титаренко**.

**Справка о компанпии:**

[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.