Банк развития и модернизации промышленности

Уважаемые клиенты!

Настоящим письмом доводим до Вас информацию о случаях хищений денежных средств у клиентов-юридических лиц, использующих систему 1С для передачи платежных поручений в систему ДБО.
Реализация атаки выглядит следующим образом:

Краткое описание атаки:

1. Клиент формирует с помощью 1С платежное поручение и отправляет их на выгрузку в систему ДБО;

2. 1С, как правило, формирует текстовый файл **1c_to_kl.txt**, содержащий служебную информацию, перечень расчетных счетов, период, остатки и обороты по счетам и т.д.;

3. Вредоносная компьютерная программа отслеживает появление этого файла и производит подмену реквизитов получателя (название остается неизменным, подменяется счет и ИНН получателя);

4. Информация обрабатывается через ДБО. В некоторых случаях от клиента требовалось подтверждение проведения платежа по СМС – он его подтверждал.

Основные меры противодействия:

1. Использовать антивирусное средство, поддерживать его базы в актуальном состоянии, не реже 1 раза в неделю проводить полное сканирование системы, в которой генерируется файл **1c_to_kl.txt;**

2. Выполнять все рекомендации по работе с вложениями, пришедшими из подозрительных источников, не открывать вложения-исполняемые файлы и не включать макросы в документах Microsoft Office, если не уверены в надежности отправителя;

3. Проверять суммы платежей и не подтверждать подозрительные операции по СМС, если есть такая возможность.