SOLAR

Мессенджеры и видеоконференции как возможные каналы утечки данных: главные риски и как с ними справиться

МИХАИЛ МОИСЕЕВ
Старший аналитик Центра технологий кибербезопасности

5 октября 2023

Как утекают конфиденциальные данные?

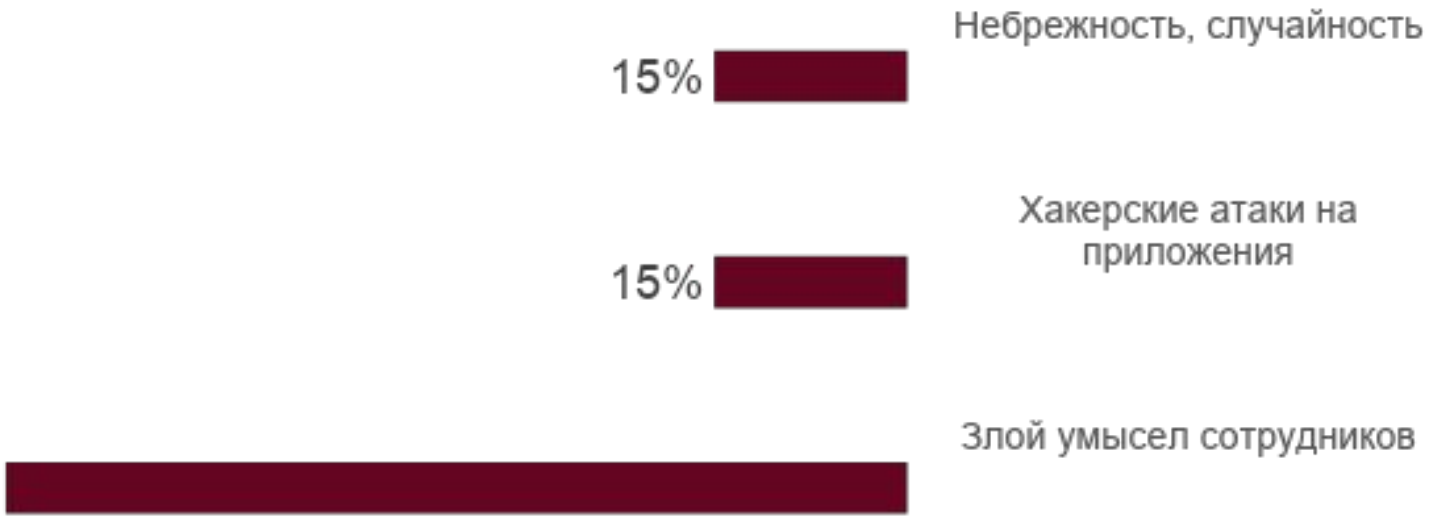
35%

сотрудников фотографируют экраны мониторов, снимают скринкасты (и во время ВКС)*

33%

сливов конфиденциальной информации осуществляются через мессенджеры*

Большая часть утечек происходит в результате «человеческого фактора» - намеренного или случайного слива данных**



* По данным исследования КРОК и EveryTag: ссылка

** По данным «Солар»: ссылка

ВКС и мессенджеры: возможности и риски

Повседневный инструмент для работы команд (в том числе распределенных):

- Рабочие чаты вперемешку с личными
- Постоянная отправка файлов, сообщений
- Аудио-, видеозвонки
- Демонстрация содержимого экрана

Один из самых популярных каналов утечки конфиденциальной информации:

- Бывшие сотрудники остаются в рабочих чатах
- Случайная отправка документа не в тот чат, не тому адресату
- Случайная отправка личной информации в рабочий чат
- Намеренная передача конфиденциальной информации в мессенджере своему «подельнику»

Источник: Солар, 2022

Истории утечек данных (1/2)

SOLAR

Бывшие сотрудники в рабочих чатах

Автодилер

- Сеть филиалов по всей стране.
- Количество сотрудников: 1000+
- Рабочий чат в мессенджере для обсуждения цен, поставок, планов со всеми сотрудниками.
- Свободный доступ к чату для любого сотрудника. Слабое администрирование чата.
- Как результат – неконтролируемое обращение с корпоративной информации и потенциальный слив данных.

Медвежья услуга

Отправка рабочих документов руководителю

- Руководитель регулярно просил своего помощника высылать ему ряд документов через мессенджер.
- Помощник таким образом стал нарушителем политик безопасности, не подозревая, что руководитель может передавать данные третьим сторонам и использовать это в корыстных целях.

Истории утечек данных (2/2)

SOLAR

Ошибся чатом

«Простите, ошибся чатом»

- Менеджер случайно отправил заказчику часть переписки со своим руководителем, в которой обсуждался сам заказчик.
- Потеряла ли компания этого заказчика – история умалчивает.
- Пример из другой компании: одному заказчику случайно отправили договоры других заказчиков, с массой критичных данных.

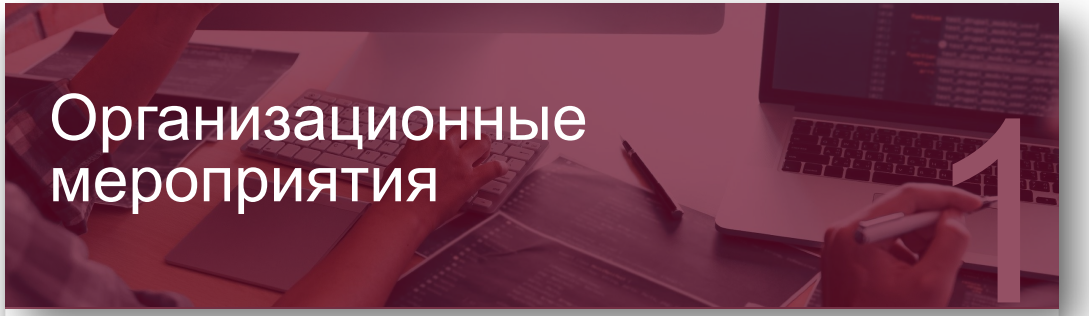
Зашел в ВКС по обороне

Несложный брутфорс PIN-кода ВКС

- Журналист подключился к закрытой ВКС министров обороны стран ЕС.
- В Твиттере (сейчас X) один из министров опубликовал фотографию, на которую попали пять из шести цифр кода для подключения к конференции.
- Журналист путем перебора вычислил недостающий символ, ввел код и присоединился к видеозвонку.

SOLAR

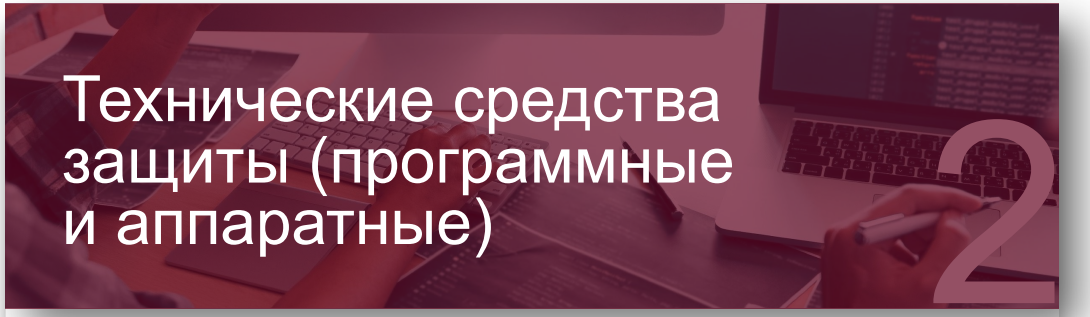
Как защитить информацию от утечки?



Организационные мероприятия

1

Разработка политики безопасности, положений, регламентов и инструкций по работе с конфиденциальными данными.



Технические средства защиты (программные и аппаратные)

2

Могут включать широкий спектр решений: начиная от СКУД и заканчивая системами защиты информации от несанкционированного доступа и DLP-решениями.

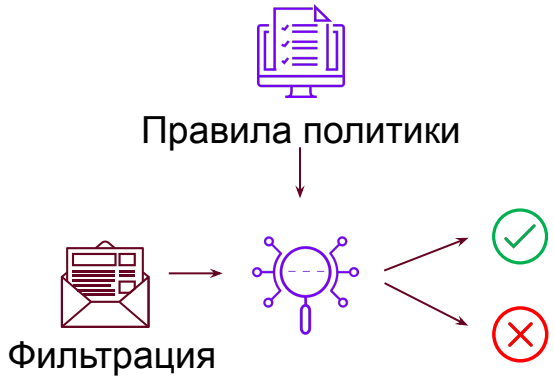
Принцип работы DLP-системы

Перехват

- Корпоративная, веб-почта
- Печать
- Мессенджеры, ВКС
- Публикации в сети
- Съемные носители
- Веб-запросы
- Файловые ресурсы

- Буфер обмена, нажатие клавиш
- Подключение к Wi-Fi
- Звук с микрофона
- Снимки экрана
- Видео с экрана

Фильтрация



Анализ

- Досье на персоны и группы
- Досье на информацию
- Аналитика и отчетность
- Анализ поведения пользователей
- Управление событиями и инцидентами
- Архив коммуникаций

1. Обнаружение и предотвращение нарушений в режиме реального времени

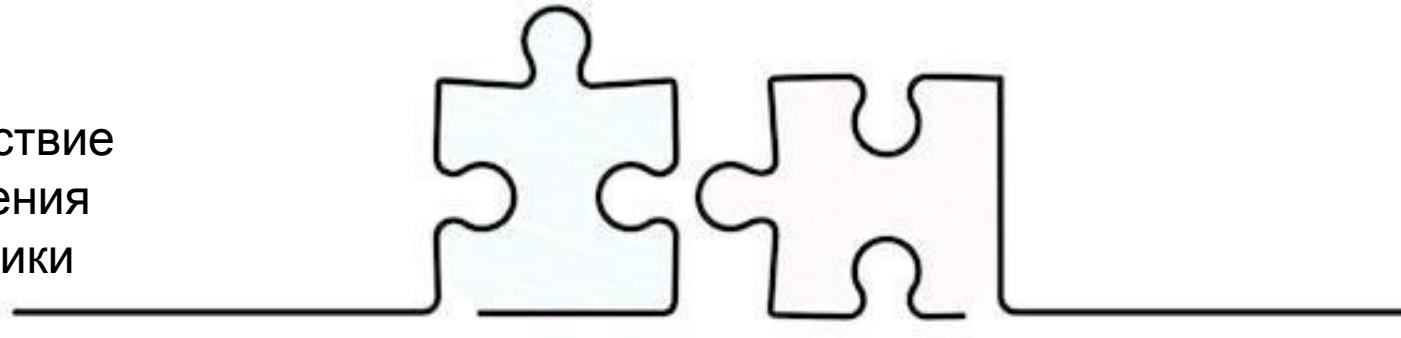
2. Незамедлительная реакция системы (<1 сек) на нарушения политики безопасности:

- Создание события
- Оповещение сотрудника безопасности
- Блокировка или помещение сообщений в карантин

SOLAR

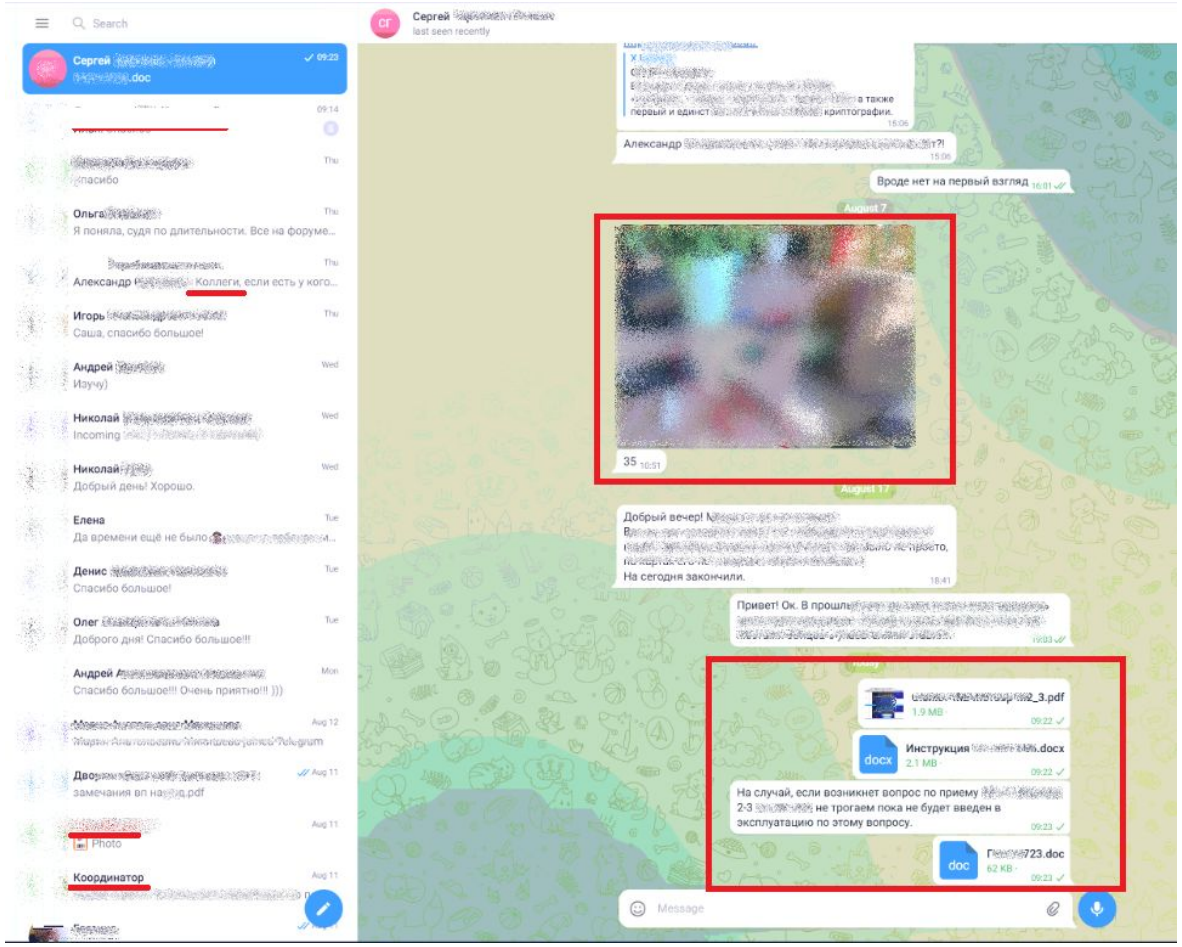
Интеграция DLP-систем с средствами ВКС: синергия возможностей

- Безопасное пространство корпоративных коммуникаций
- Перехват трафика на уровне сервера, без использования агента. Сообщения перехватываются по протоколу ICAP.
- Сообщения отправляются на анализ и соответствие политикам в онлайн-режиме. Передача сообщения заблокируется, если сработает действие политики Заблокировать.



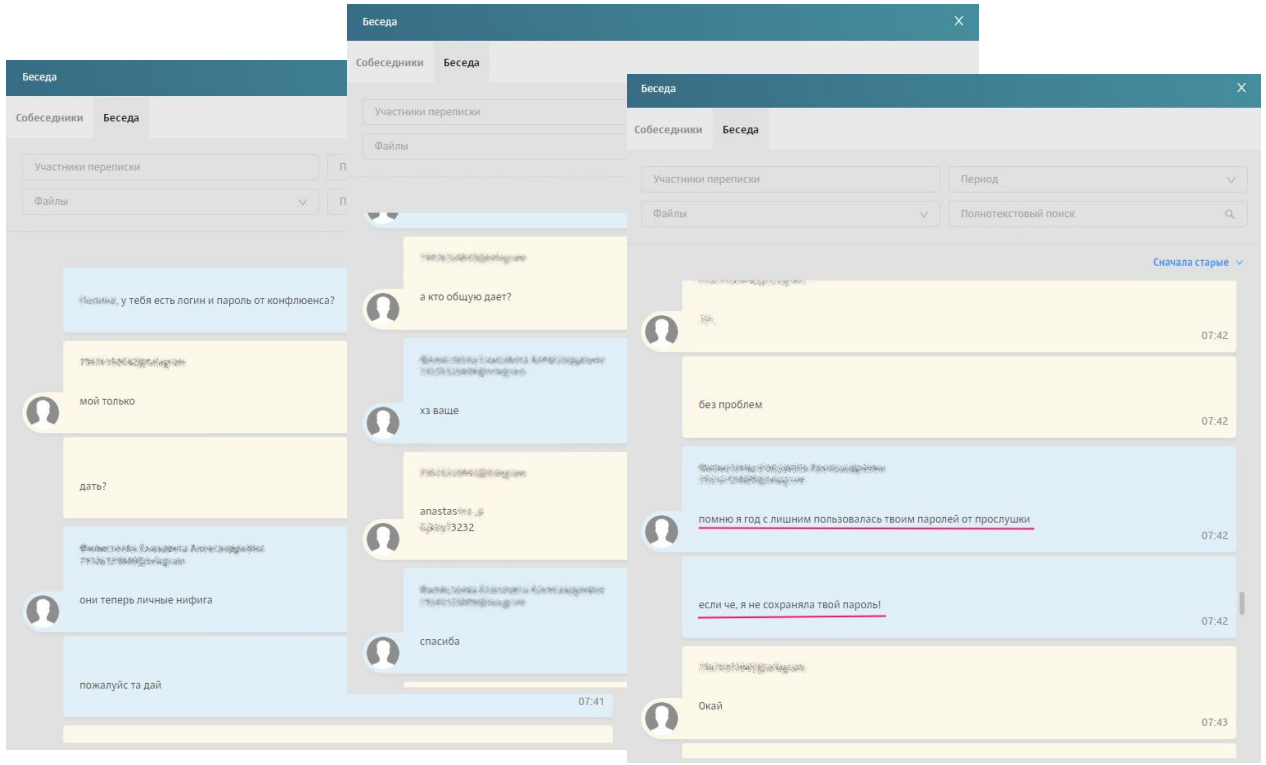
Кейсы из практики внедрения Solar Dozor

Благодаря перехвату переписки в мессенджере, удалось выявить факт отправки сотрудником чувствительных данных. Сотрудник передавал инструкции, фотографии и другие данные по разработкам третьим лицам.



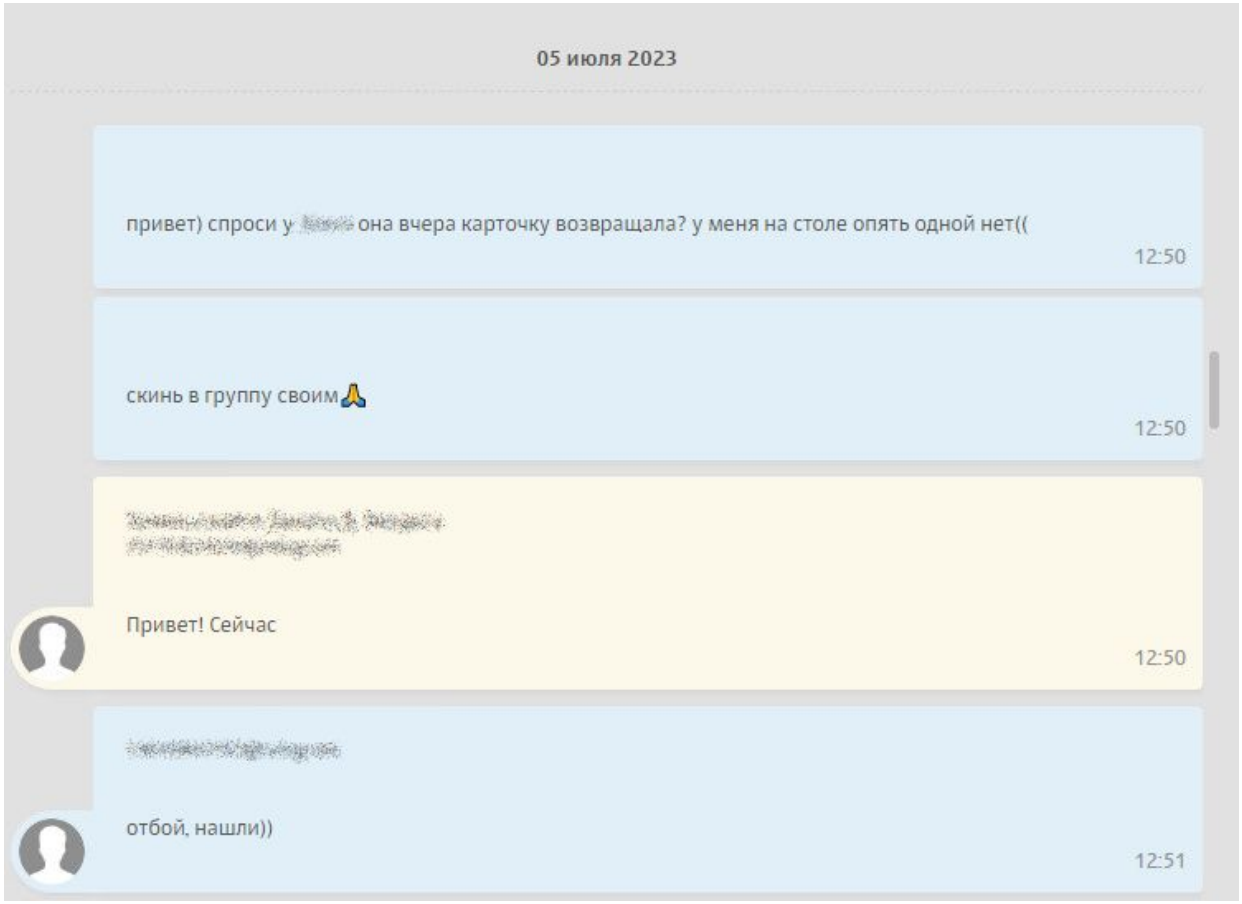
Кейсы из практики внедрения Solar Dozor

Сотрудники передавали пароли от корпоративной системы третьим лицам - тем, кто не должен иметь к ним доступ вообще.
С помощью Solar Dozor удалось выявить и пресечь нарушения парольной политики.



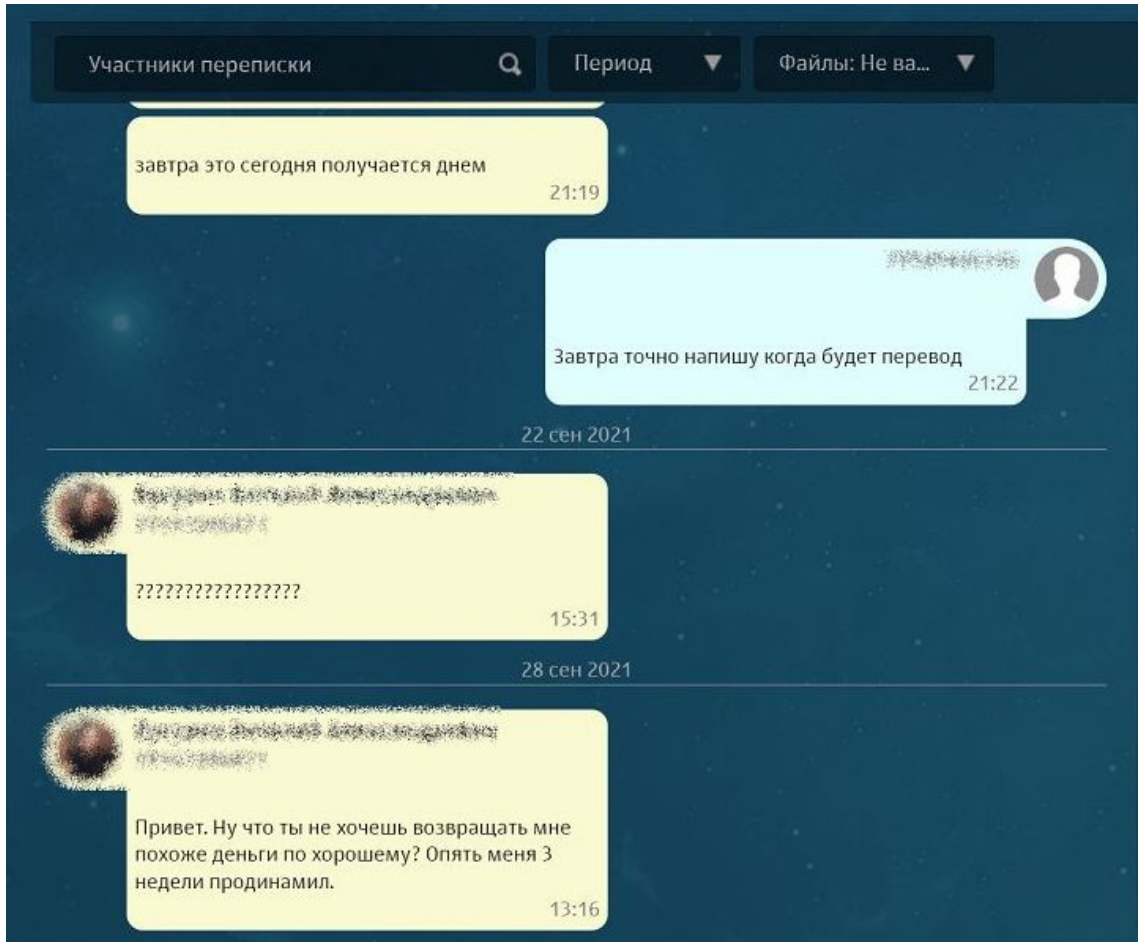
Кейсы из практики внедрения Solar Dozor

Выявлен случай халатного отношения к картам для СКУД.
Сотрудники обсуждали потерю карточки своей коллеги (кто потерял и где найти).
Оказалось, что практически любой, зная, где лежит карточка, мог подойти и воспользоваться ею для прохода в закрытые помещения.



Кейсы из практики внедрения Solar Dozor

Обнаружена переписка, где третьи лица предъявляют сотруднику требования по возврату долгов. Этот кейс интересен с точки зрения профилирования. Ведь нередко именно такие люди решаются на незаконные действия с целью получения прибыли.



Кейсы из практики внедрения Solar Dozor

ЧТО СЛУЧИЛОСЬ

Сотрудники информационной безопасности обнаружили в трафике сотрудника Василия подозрительные сообщения. В мессенджере передавал непонятные цифры. Как оказалось – это были номера карты.

РЕЗУЛЬТАТЫ

Изучив историю в других мессенджерах и сопоставив всё это с деятельностью Василия (а он работал в тендерном отделе), стало понятно, что Василий передавал важную информацию по тендеру конкурентам, и в итоге именно этот конкурент и выиграл.
При этом выяснилось, что Василий планировал ещё одну подобную «акцию», однако деятельность инсайдера была пресечена.

SOLAR

Ключевой фактор успеха – постоянное поддержание DLP-системы в актуальном состоянии

Спасибо за внимание!
Вопросы?

Михаил Моисеев

Старший аналитик Центра технологий кибербезопасности компании «Солар»

m.moiseev@rt-solar.ru