USSC

Security Operations Center в полевых условиях

Руслан Амиров

Директор Центра мониторинга ИБ

USSC-SOC

Структура доклада

1. Инцидент информационной безопасности
2. Теоретический экскурс
3. Расследование инцидента
4. Результаты расследования
5. Выводы

Звонок Заказчика

Время 19:30 (стандартный рабочий день в УЦСБ заканчивается в 18:30)

Заказчик: «Случилась неприятность!»

- Нарушитель получил доступ к ИТ-инфраструктуре и к конкретным ИТ-сервисам
- Один из наиболее критичных сервисов скомпрометирован: хакер имеет доступ к Интернет-банку (ДБО)
- У Заказчика производство, остановить работу которого нельзя
- Оплаты подрядчикам тоже прекратить нельзя
- Нарушитель требует 4 000 000 рублей в криптовалюте

Заказчик: «Что делать?»

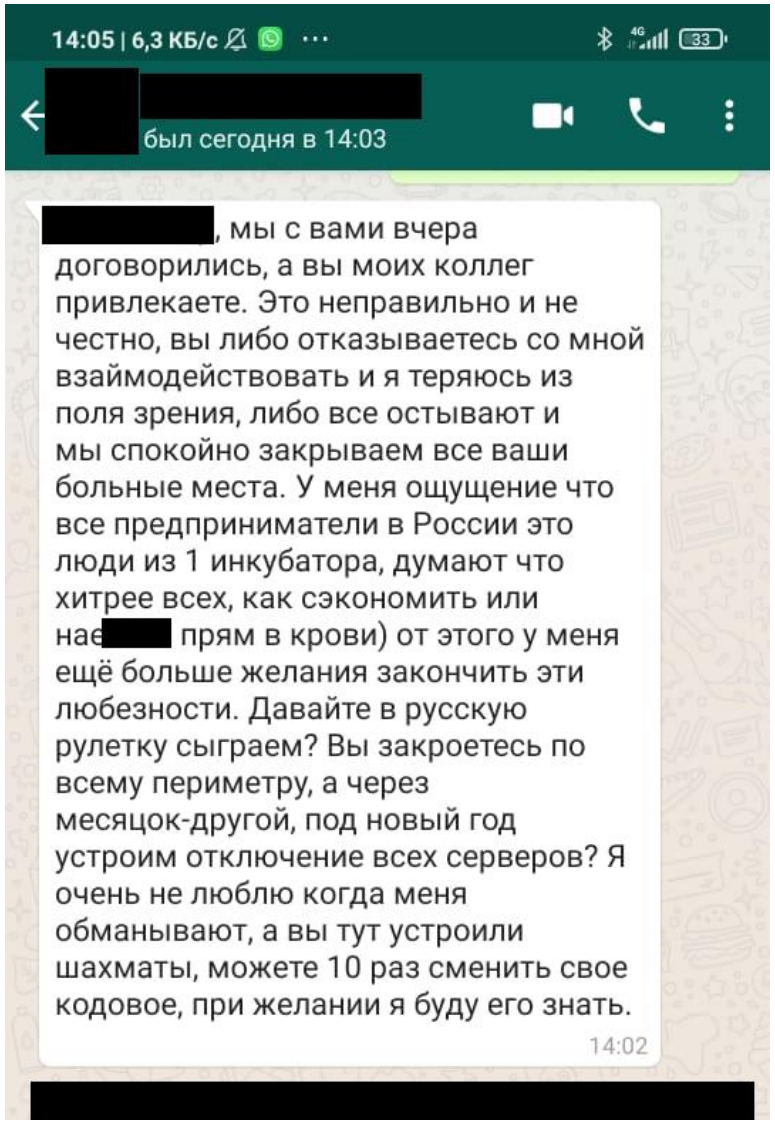
УЦСБ: «SOC берет задачу в работу»

Второй звонок Заказчика

На следующий день:

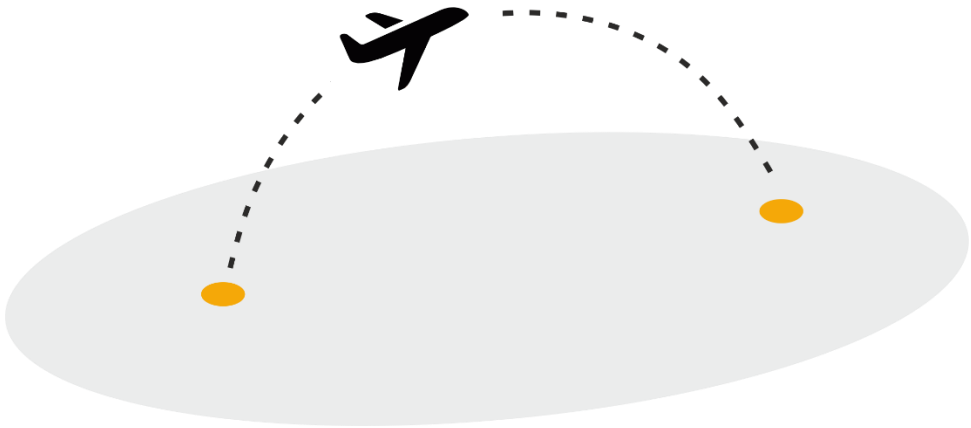
Заказчик пересылает сообщение от нарушителя в WhatsApp и в тот же момент звонит ->

Нарушитель угрожает обрушить всю инфраструктуру и отрезать доступ к Интернет-банку даже после смены кодового слова



Второй звонок Заказчика

В то время, пока мы получали обновленную информацию, офис-менеджер уже оформлял гостиницу для сотрудников УЦСБ, которые уже вылетели утром



Заказчик находится вне УрФО

Командированные сотрудники:

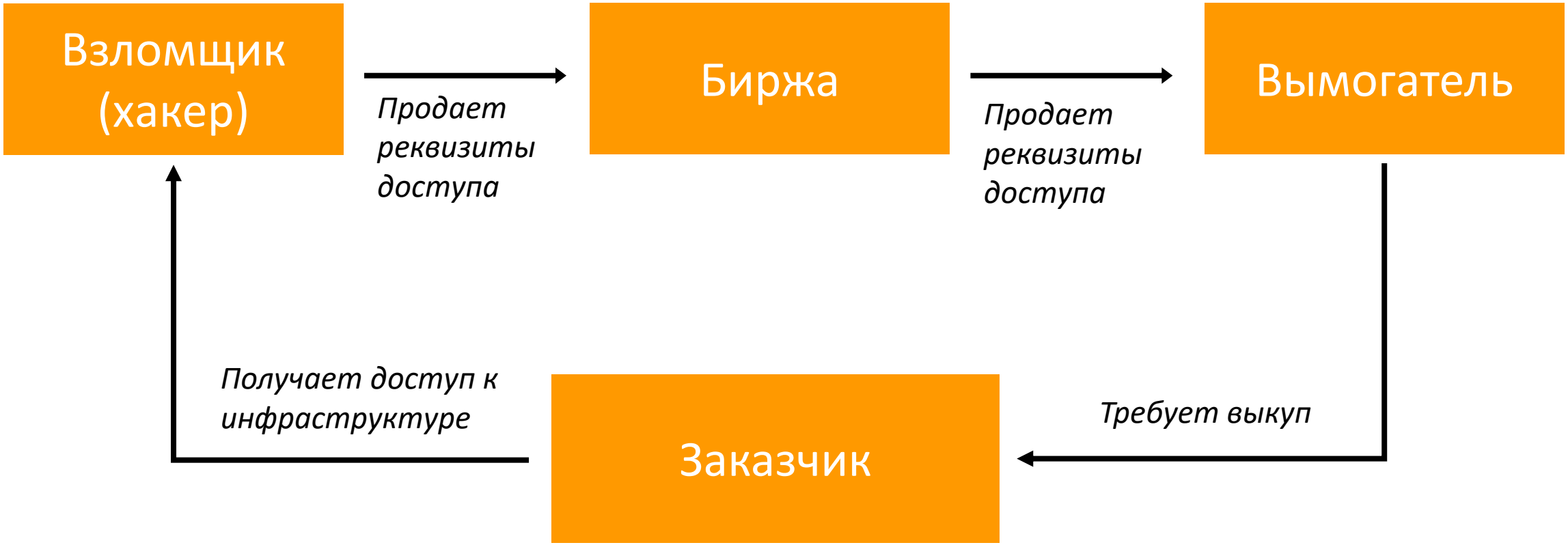
- Специалист по Offensive Security
- Специалист по сетевой безопасности
- Специалист по прикладной безопасности

Сотрудников Заказчик встретил на собственном авто

Криминальная составляющая инцидента

USSC

Структура преступного бизнеса в киберпространстве



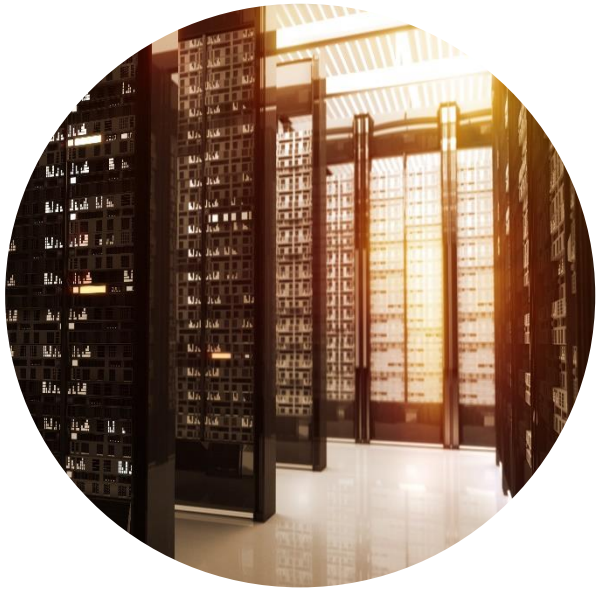
Security Operation Center

USSC

- Эффективное **обнаружение и предотвращение** атак, а также устранение причин возникновения инцидентов
- **Готовые** сценарии мониторинга инцидентов
- **Своевременное** оповещение о возникновении угроз для бизнес-процессов
- **Рекомендации** по корректировке защитных мер, подготовка критериев, аналитическая работа
- Помощь в **расследовании** инцидентов ИБ и сборе **доказательной базы** для суда
- **Выявление, регистрация, учет** инцидентов, подготовка **отчетности**
- **Объективная** картина состояния защищенности компании. Повышение уровня компании по **устойчивости** к атакам
- **Уменьшение времени** реакции на инциденты
- **Снижение риска** проникновения в инфраструктуру
- **Минимизация** последствий, ущерба, затрат на локализацию и устранение инцидента

Security Operation Center (SOC) – Центр мониторинга и реагирования на инциденты информационной безопасности (центр ГосСОПКА)

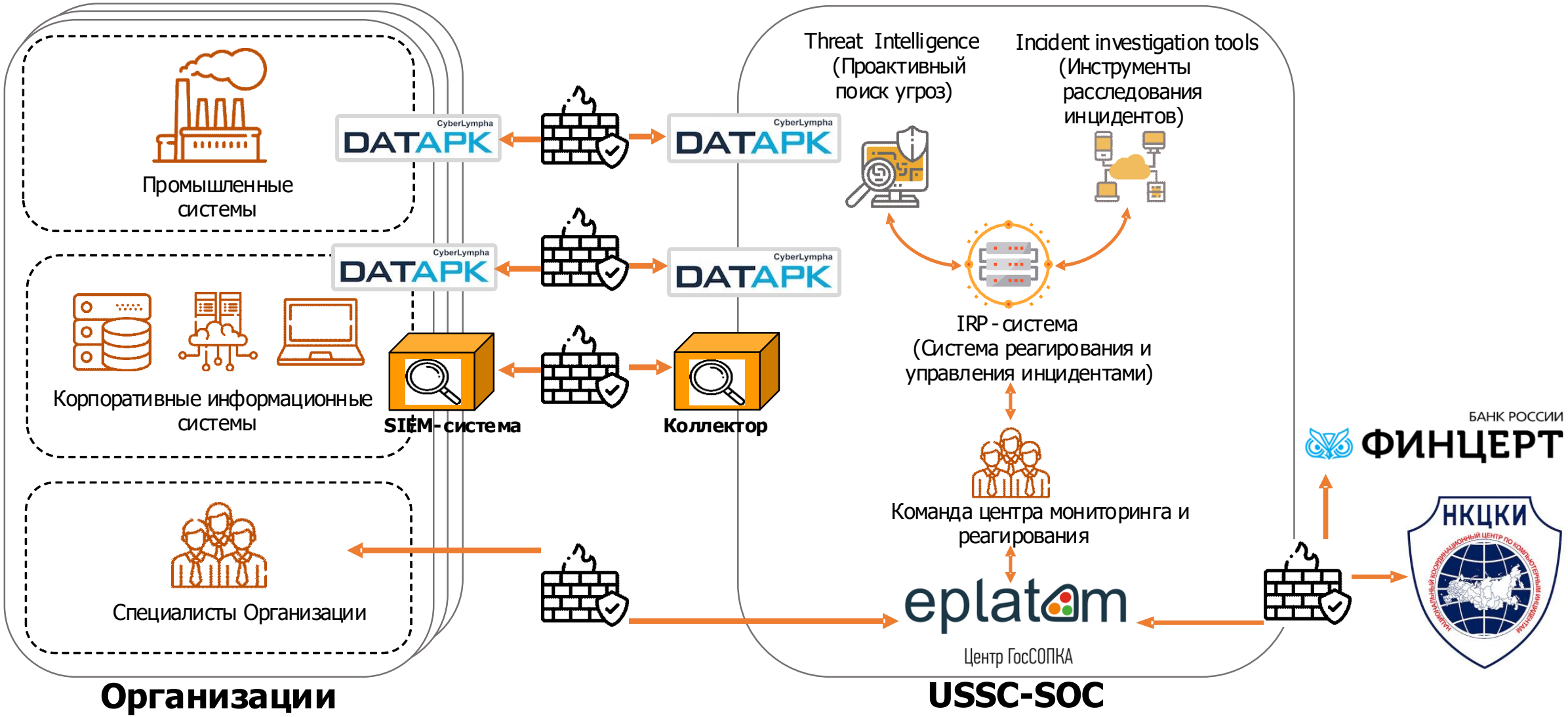
Варианты построения SOC



Аутсорсинговый SOC
сервис, предоставляемый сторонней компанией, обладающей необходимыми компетенциями и лицензиями, в рамках договора с организацией

Создание **собственного SOC**, самостоятельно организацией

Архитектура USSC-SOC



Организационно-штатная структура USSC-SOC

Услуги УЦСБ

Аутсорсинговый SOC	Собственный SOC
Предоставление услуг Центра мониторинга и реагирования на инциденты информационной безопасности (SOC)	Проектирование систем управления инцидентами ИБ (включая подключение к ГосСОПКА)
Взаимодействие с ГосСОПКА	Готовое решение под ключ ПАК «DATAPK-ГосСОПКА»
Взаимодействие с CERT/CSIRT/SOC	Поставка программных и технических средств для системы управления информационной безопасностью (СУИБ): DATAPK, ePlat4m, SIEM, ViPNet

Проведение тестирования на проникновение, в том числе с использованием методов социальной инженерии

Расследование инцидентов информационной безопасности

Security Awareness (повышение осведомленности работников)

War Gaming (проведение киберучений)

SOC / центр ГосСОПКА на базе УЦСБ

SOC/ГосСОПКА за

3 месяца

Запуск базовых функций SOC / центра ГосСОПКА менее чем за 3 месяца

8x5

с 9:30 до 18:30 в рабочие дни

10x5

с 8:00 до 19:00 в рабочие дни

24x7

круглосуточно

Время обслуживания определяется регламентом предоставления услуги

Время реагирования на инцидент

<60 мин

Расследование инцидента

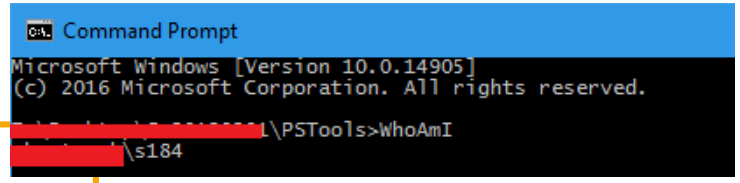
1. Сотрудники в командировке на объекте Заказчика имеют на руках **результаты анализа** предварительной информации об инциденте
2. **Руководство осуществляется стратегическое** (из SOC) и по месту (руководитель работ)
3. Введены ограничения для нарушителя – ограничение контура
4. Уточнение первичной информации – ведется по 2 направлениям:
    - «безопасность изнутри»
    - «безопасность снаружи»
5. Ведется глубокий **анализ путей развития атаки**
6. **Ликвидация последствий**

Расследование инцидента

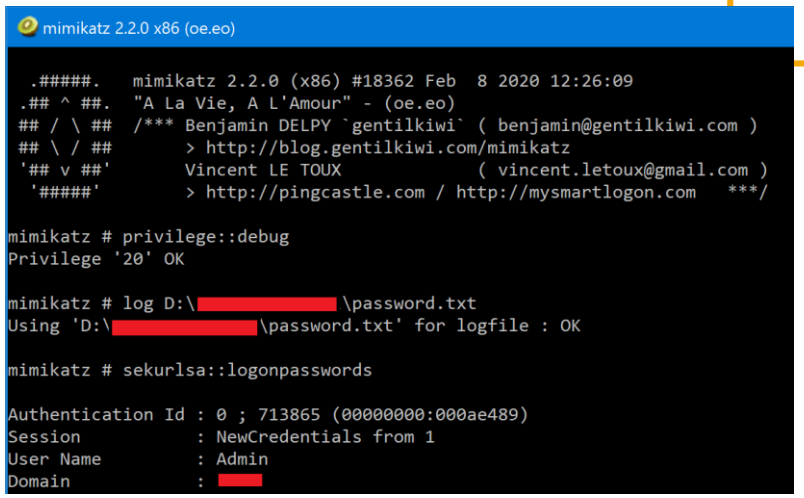
USSC

Спам-рассылка или уязвимость

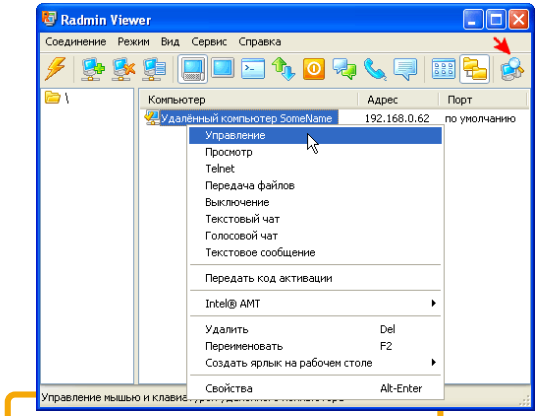
Получение реквизитов учетной записи с ограниченным доступом



Повышение привилегий



Закрепление в инфраструктуре



Результаты

- **Инцидент ликвидирован**: из инфраструктуры Заказчика удалены программные закладки и средства удаленного администрирования
- **Ограничен доступ к внешним сетям**, проведен инструктаж персонала Заказчика по основам информационной безопасности при использовании корпоративных сервисов и сети Интернет
- **Заказчик принял решение** не обращаться в правоохранительные органы и не предавать инцидент огласке
- **Фактический ущерб был сведен к нулю**, Заказчику удалось избежать лишних затрат и репутационных потерь

Выводы

- Использование профессиональных сервисов по обеспечению информационной безопасности, как по отдельности, так и в пакете услуг в рамках аутсоринга, позволяет снизить риски реализации угроз
- В данном конкретном случае своевременное обращение к специалистам позволило в кратчайшие сроки восстановить ИТ-инфраструктуру в состояние до взлома
- При выявлении инцидентов на раннем этапе можно значительно снизить потенциальный ущерб

USSC

СПАСИБО ЗА ВНИМАНИЕ!

ВОПРОСЫ?

Вопросы по USSC-SOC можете направлять сюда: soc@ussc.ru

Руслан Амиров

Директор Центра мониторинга ИБ

+7 (343) 379-98-34 (доб. 1203)

ramirov@ussc.ru

УРАЛЬСКИЙ ЦЕНТР СИСТЕМ БЕЗОПАСНОСТИ | USSC.RU