



USSC



Security Operations Center В ПОЛЕВЫХ УСЛОВИЯХ

Руслан Амиров

Директор Центра мониторинга ИБ

USSC-SOC

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

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?»

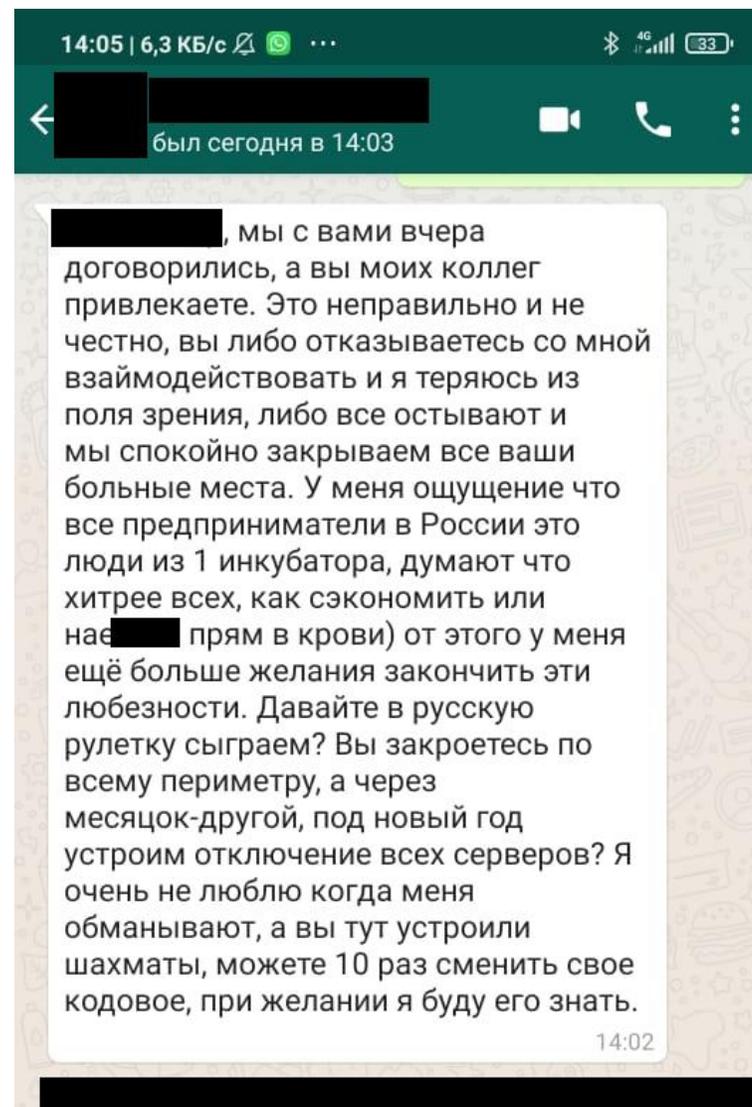
УЦСБ: «SOC берет задачу в работу»



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



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

Заказчик находится вне УрФО

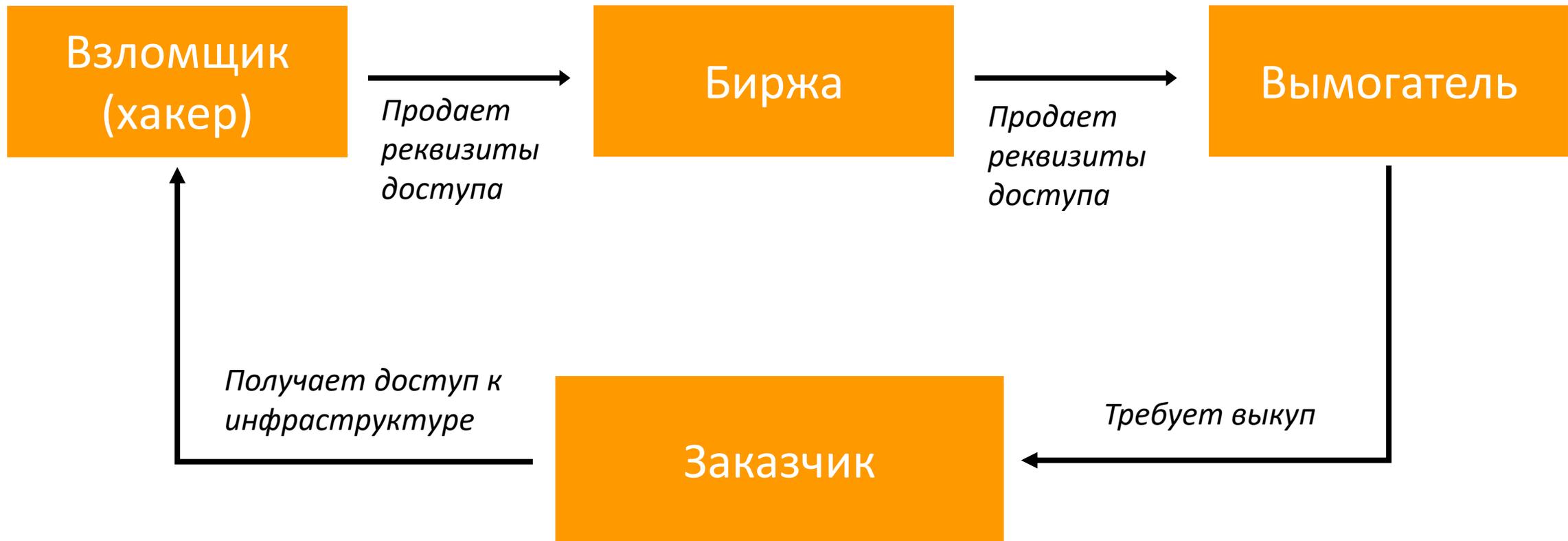
Командированные сотрудники:

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

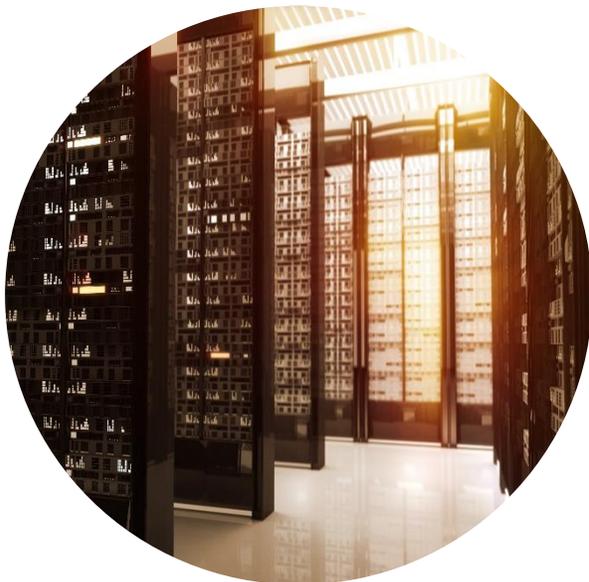
Сотрудников Заказчик встретил на собственном авто



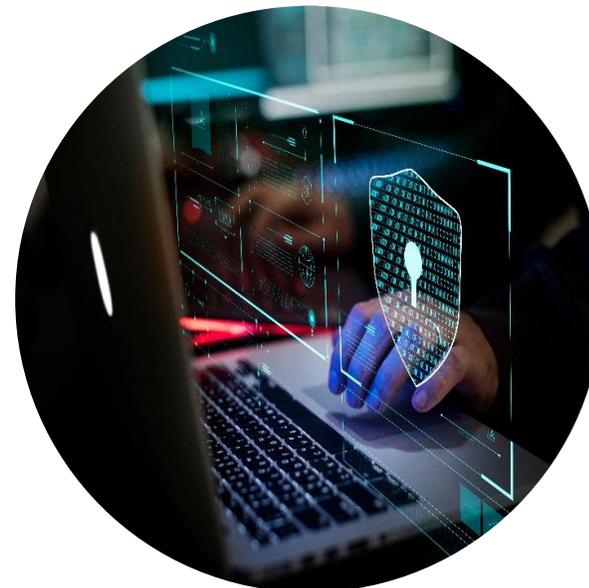
Структура преступного бизнеса в киберпространстве



- 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

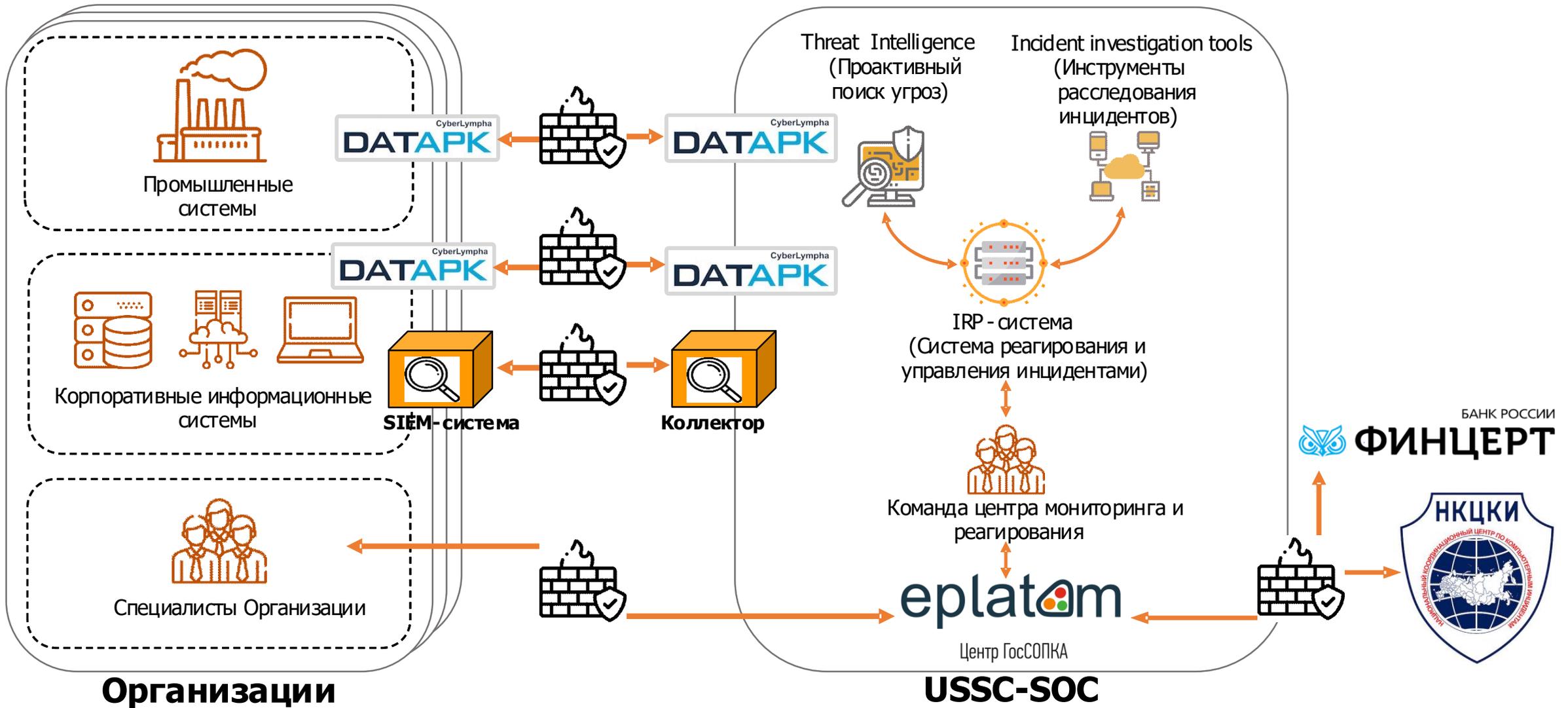


Аутсорсинговый SOC
сервис, предоставляемый сторонней компанией, обладающей необходимыми компетенциями и лицензиями, в рамках договора с организацией



Создание **собственного SOC**, самостоятельно организацией

Архитектура USSC-SOC



Руководство SOC



Аутсорсинговый SOC

Предоставление услуг Центра мониторинга и реагирования на инциденты информационной безопасности (SOC)

Взаимодействие с ГосСОПКА

Взаимодействие с CERT/CSIRT/SOC

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)

Собственный SOC

Проектирование систем управления инцидентами ИБ (включая подключение к ГосСОПКА)

Готовое решение под ключ ПАК «ДАТАРК-ГосСОПКА»

Поставка программных и технических средств для системы управления информационной безопасностью (СУИБ): ДАТАРК, ePlat4m, SIEM, ViPNet



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

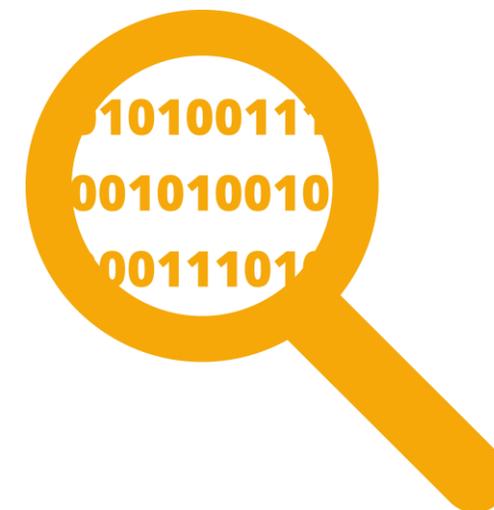
Время обслуживания
определяется регламентом
предоставления услуги



Время реагирования на
инцидент

< 60 мин

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

Спам-рассылка
или уязвимость



Получение
реквизитов учетной
записи с
ограниченным
доступом

```
Command Prompt
Microsoft Windows [Version 10.0.14905]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\user>whoami
user\s184
```

Повышение
привилегий

```
mimikatz 2.2.0 x86 (oe.eo)

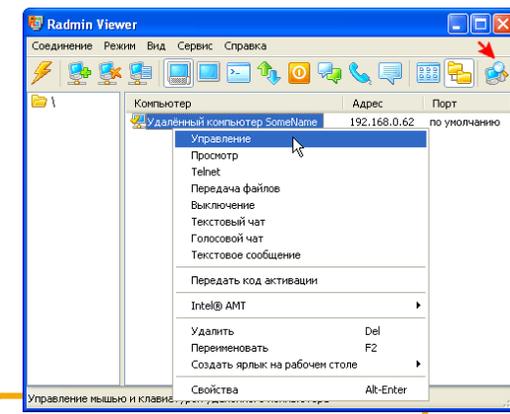
.#####. mimikatz 2.2.0 (x86) #18362 Feb  8 2020 12:26:09
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v #' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com **/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # log D:\[redacted]\password.txt
Using 'D:\[redacted]\password.txt' for logfile : OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 713865 (00000000:000ae489)
Session           : NewCredentiaals from 1
User Name          : Admin
Domain             : [redacted]
```



Закрепление в
инфраструктуре

- **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

- 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

Корпоративный центр мониторинга

USSC-SOC

Руслан Амиров

Директор Центра мониторинга ИБ

+7 (343) 379-98-34 (доб. 1203)

ramirov@ussc.ru



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

УРАЛЬСКИЙ ЦЕНТР
СИСТЕМ БЕЗОПАСНОСТИ | **USSC.RU**

