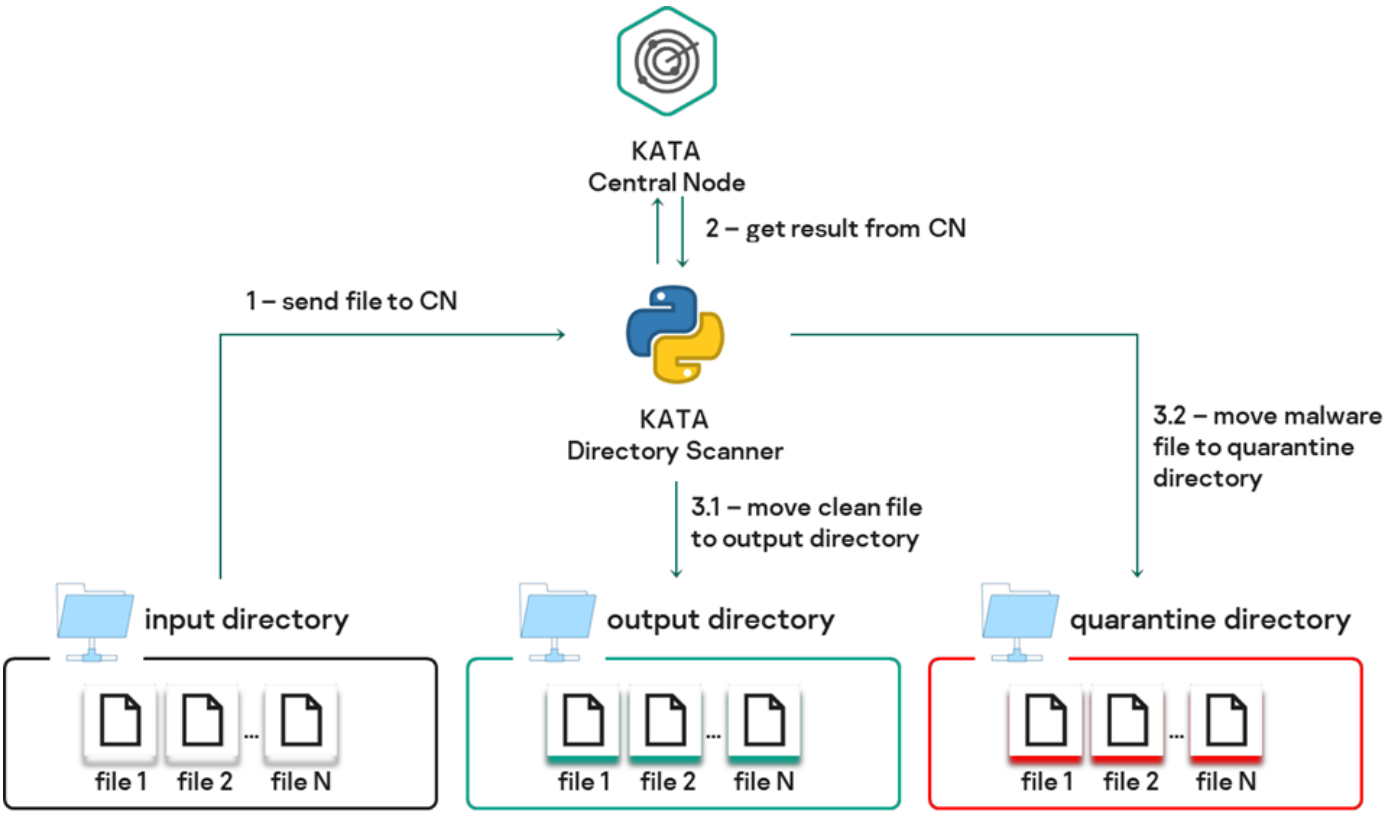
????????? KATA Directory Scanner

????????? KATA Directory Scanner (????? – KDS) ????????? ????????????? ??????????? KATA ? ???????????? ??? ???????????? ????? ????? ?? ??????? ???????????? ??.

???????? ?????????????:

- на KATA CN монтируется три общих ресурса: input, output и quarantine;
- на KATA CN устанавливается сервис KDS;
- KDS отслеживает появление новых файлов в директории input и отправляет их по API на анализ в KATA;
- KDS по API получает вердикты от KATA;
- в случае, если признаки вредоносного ПО не обнаружены, файлы перемещаются в директорию output; во всех остальных случаях файлы перемещаются в директорию quarantine.



?????????? ? ??????????:

Компонент KDS не является официально поддерживаемым компонентом KATA, предназначен для демонстрации расширения функциональных возможностей KATA с использованием API и предоставляется «как есть».

- Один экземпляр сервиса KDS предназначен для работы с тремя директориями.
- В директории input сканируются и отправляются на анализ только файлы. Вложенные директории не сканируются, их иерархия не восстанавливается в директориях output и quarantine.
- Файлы размером более 100 Мб пропускаются и остаются в директории input без изменений.
- В директорию quarantine перемещаются все файлы с вердиктом отличным от «not detected», в том числе, если произошла ошибка сканирования («error») или превышен таймаут ожидания («timeout»).
- Если файл уже существует в директории input или quarantine, то он заменяется новым.

?????????? ?????:

Для того чтобы скачать файлы: **kata-dir-scanner.service, kata_dir_scanner.py** и **kata_dir_scanner.conf**, обратитесь к команде pre-sale инженеров команды AntiApt.

????????? ?? ??????? KATA CN

ВАЖНО! Заранее скачайте пакет **cifs-utils.deb**, загрузите его на CN и установите с помощью команды:

```
apt install ./cifs-utils.deb
```

1. Подключитесь к KATA CN по SSH. Перейдите в раздел Technical Support Mode.
2. Создайте структуру директорий input, output и quarantine.

   ```
   mkdir /mnt/in


   mkdir /mnt/out


   mkdir /mnt/qrnt
   ```

3. Создайте файл с учетными данными для доступа к общим ресурсам (username и password замените на свои).

   ```
   vi /root/.kata-secret


   username=<username>
   ```

```
password=<password>
```

ВАЖНО! Пользователь должен иметь доступ к проверяемой директории

4. Добавьте в конец файла **/etc/fstab** следующие строки (удаленный хост замените на свои).

```
\\<IP or FQDN>\in /mnt/in cifs credentials=/root/.kata-secret 0 0

\\<IP or FQDN>\out /mnt/out cifs credentials=/root/.kata-secret 0 0

\\<IP or FQDN>\qrnt /mnt/qrnt cifs credentials=/root/.kata-secret 0 0
```

5. Примонтируйте все ресурсы.

```
mount -a
```

6. Подготовьте ключевую информацию.

```
openssl req -x509 -newkey rsa:2048 -keyout ./server.key -out ./server.crt -days 365 -
nodes

cat server.crt server.key > cert.pem
```

7. Инициализируйте подключение сторонней системы к KATA. Для этого необходимо отправить любой файл на проверку с использованием подготовленного сертификата.

```
Подготавливаем UUID:

python3 -c "import uuid; print(uuid.uuid4())"

curl -k --noproxy '*' --cert ./cert.pem --key ./server.key -F scanId=f2df00bc-c6b0-
4bcf-b20b-040e02f08de9 -F objectType=file -F content=@ -X

POST https://localhost:443/kata/scanner/v1/sensors//scans
```

8. Подтвердите запрос на подключение со стороны KATA CN.

9. Создайте директорию.

```
mkdir /opt/kata-dir-scanner/
```

10. Скопируйте в **/opt/kata-dir-scanner/** следующие файлы.

```
kata_dir_scanner.py
```

```
kata_dir_scanner.conf

cert.pem

server.key
```

11. Скопируйте в **/etc/systemd/system/** следующий файл.

```
kata-dir-scanner.service
```

12. Отредактируйте конфигурационный файл (измените system_id на свой).

```
vi kata_dir_scanner.conf
{
"in_dir": "/mnt/in/",
"out_dir": "/mnt/out/",
"qrnt_dir": "/mnt/qrnt/",
"cert_pem": "/opt/kata-dir-scanner/cert.pem",
"cert_key": "/opt/kata-dir-scanner/server.key",
"kata_cn_addr": "localhost",
"system_id": ""
}
```

13. Запустите сервис KDS.

```
systemctl daemon-reload

systemctl start kata-dir-scanner.service

systemctl status kata-dir-scanner.service
```

14. Добавьте сервис в автозагрузку.

```
systemctl enable kata-dir-scanner.service
```

15. Установка и настройка сервиса KDS завершена. Логи работы KDS можно посмотреть используя следующую команду:

```
tail -f /var/log/kata-dir-scanner.log
```

16. События, связанные с обнаружением вредоносного ПО, доступны в web-консоли KATA.

????????? ? ????????????? ?????? ??????????:

1. В директории **/opt/kata-dir-scanner/** создайте файл **exclude_list.txt**. В **exclude_list.txt** построчно запишите имена файлов и расширения, которые нужно исключить из пересылки на анализ в KATA.

   Например:

   File1.txt

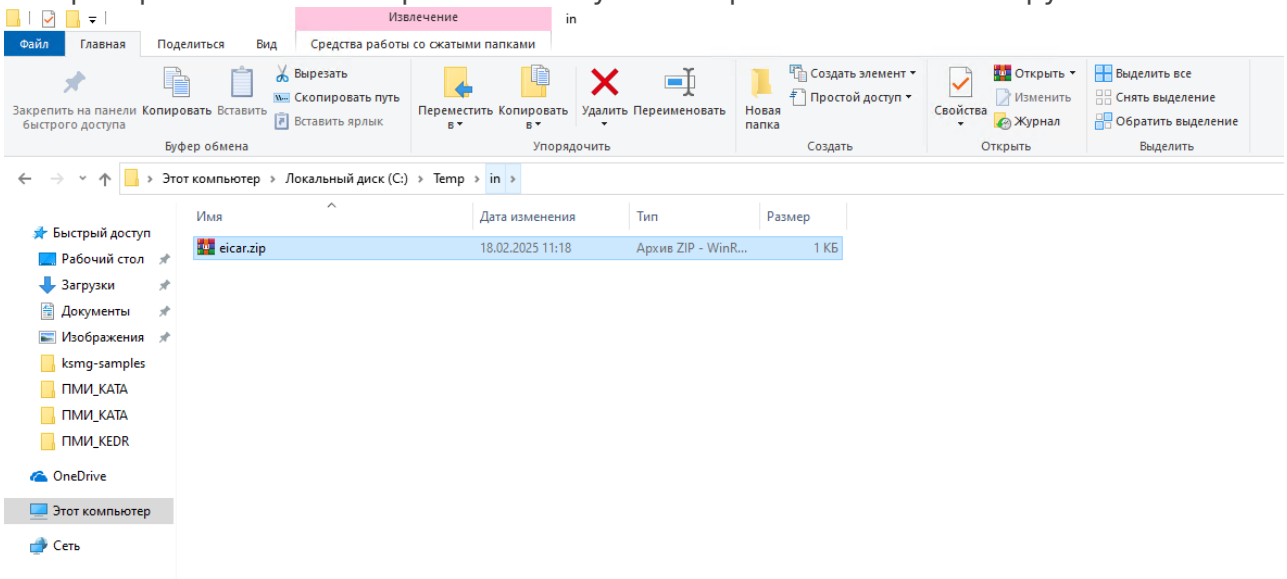
   ***.doc**

   File2.py

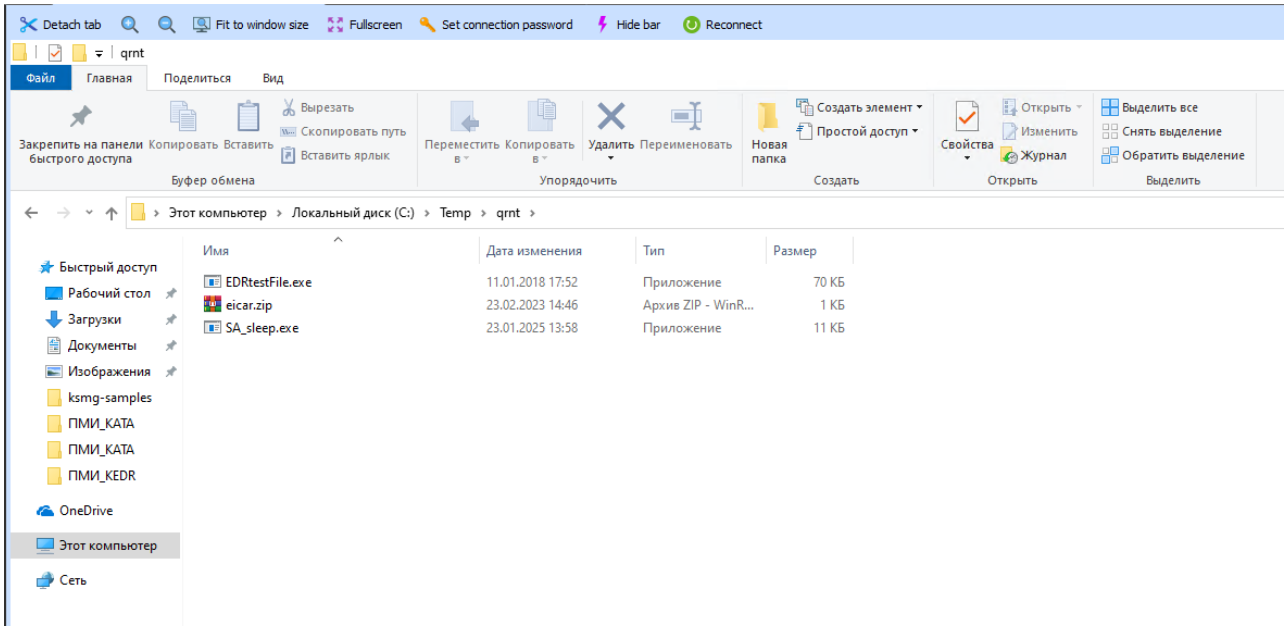
   ***.pdf**

?????? ?????? KDS:

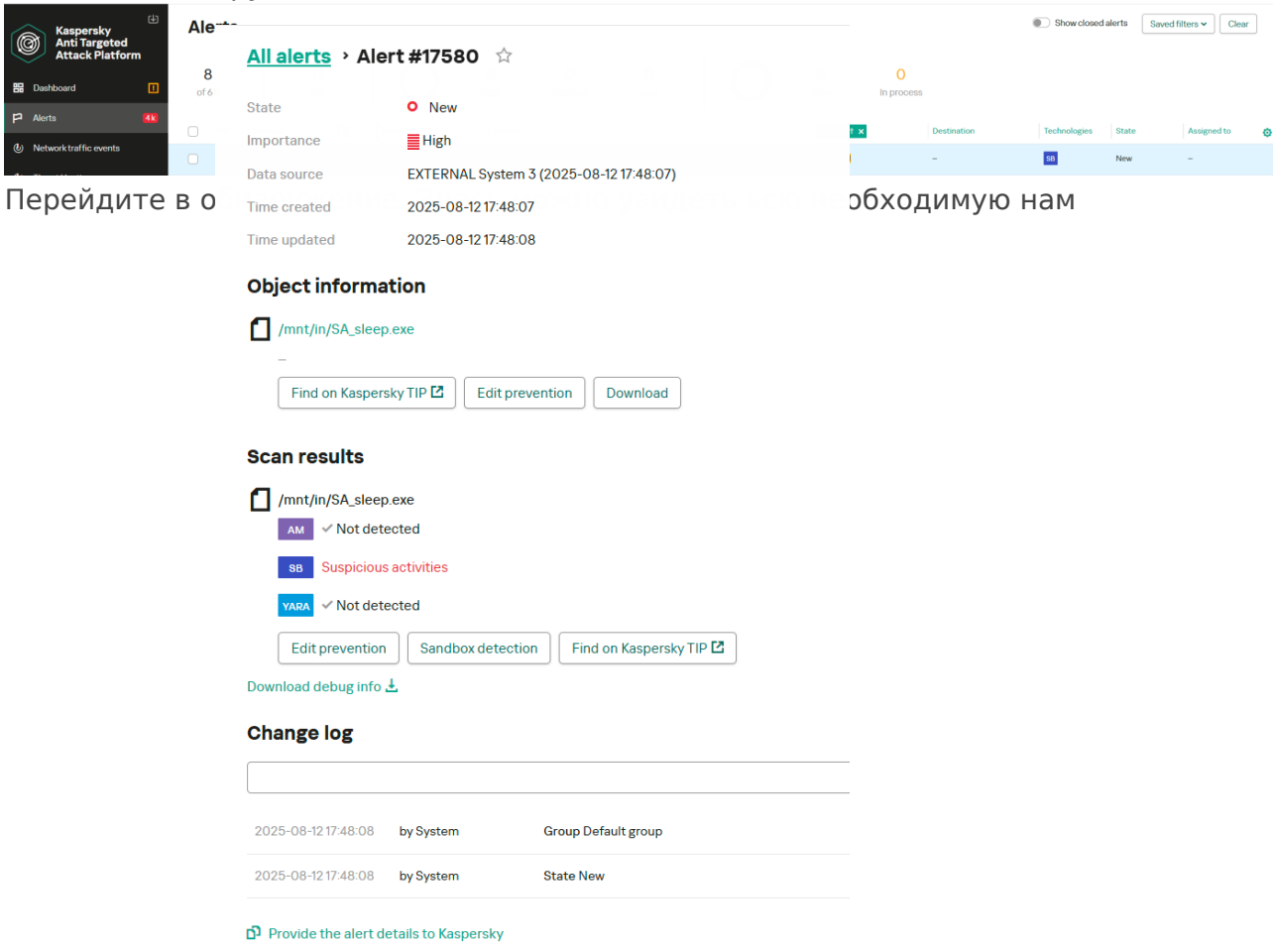
1. На проверяемом хосте открываем папку in и сохраните тестовый вирус.



2. Перейдите в папку qrnt. Вирусный файл был автоматически отправлен в папку qrnt.

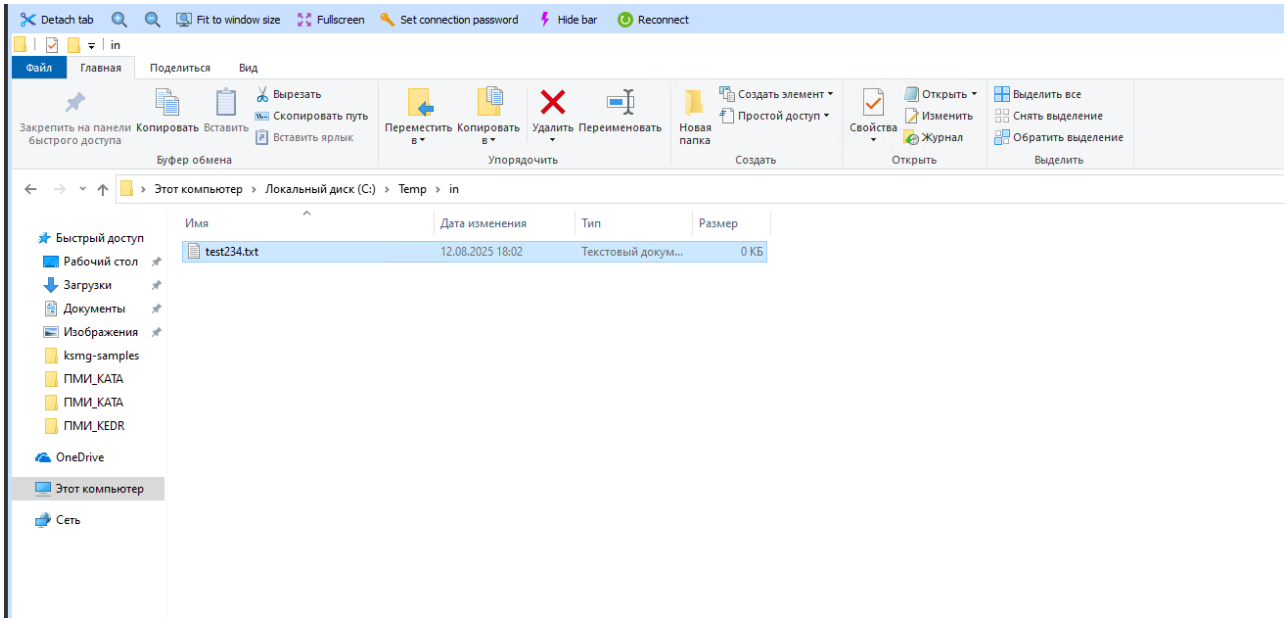


3. Перейдите в web-консоль KATA CN, зайдите в раздел обнаружения и видим сработку на тестовый вирус.

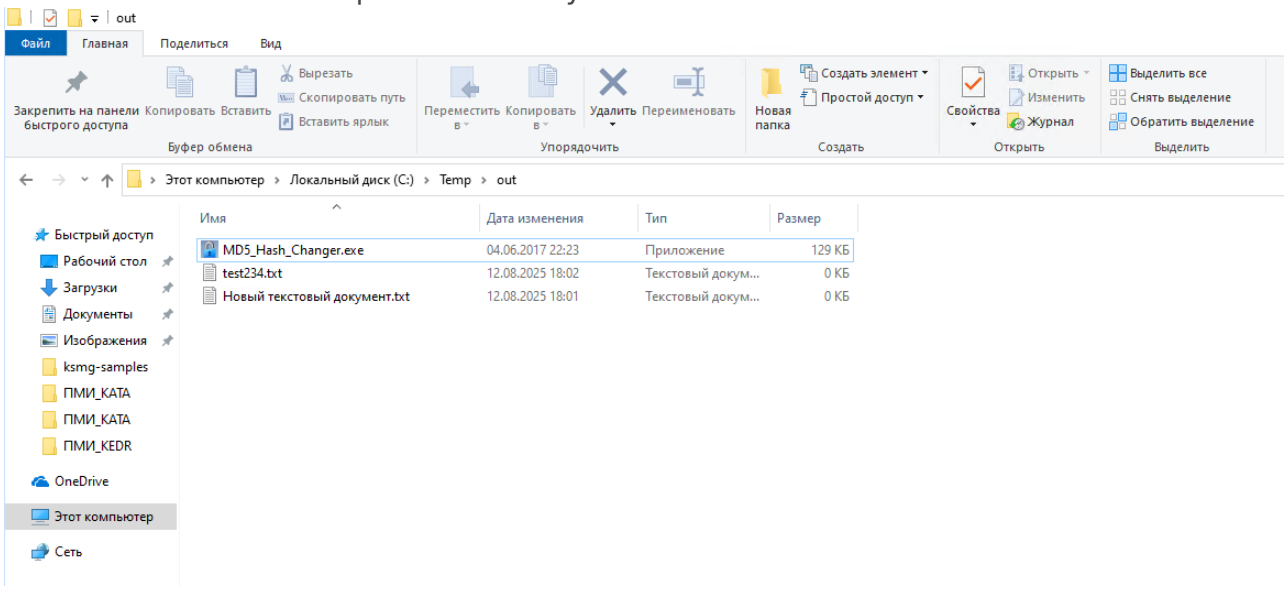


4. Перейдите в о обходимую нам информацию.

5. На проверяемом хосте откройте папку in и сохраните обычный текстовый документ.



6. Перейдите в папку out, тестовый файл test_KDS не является вирусным и поэтому был автоматически отправлен в папку out.



Revision #13
Created 15 July 2025 10:23:48 by Александр
Updated 6 February 2026 10:49:29 by Кирилл