🗼 xi-tauw 8 июля 2020 в 04:10

## От комментария на Хабре к уязвимости в антивирусе Dr. Web

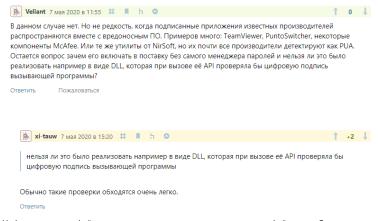
Блог компании Перспективный мониторинг, Информационная безопасность\*

Относительно недавно на хабре появилась статья «Стилер паролей в антивирусном ПО Avira Free Antivirus» от пользователя @Veliant. Автор обнаружил, что в стандартной поставке упомянутого антивируса присутствует компонент, который позволяет простым образом извлечь пароли из хранилища браузера Chrome.

В комментариях произошла дискуссия, можно ли считать это уязвимостью. Но меня зацепил один комментарий автора:

нельзя ли это было реализовать например в виде DLL, которая при вызове её API проверяла бы цифровую подпись вызывающей программы?

Дело в том, что буквально перед этим я исследовал несколько программ, которые точно так же полагались на проверку цифровой подписи. И такую проверку было очень легко обойти.



Цифровая подпись файла соответствует только самому исполняемому файлу, но работающая программа это не только исполняемый файл. Существует несколько способов повлиять на работу программы, не меняя исполняемый файл: можно подменить библиотеки, которые загружаются или сделать инъекцию кода прямо в памяти.

Я посмотрел на профиль автора: «Работает в: Доктор Веб». А что если посмотреть, не используется ли в продуктах этой компании проверка, о которой говорит автор? Я решил посмотреть и, спойлер, нашел уязвимость, которая позволяет повысить свои привилегии до системных пользователю Dr.Web Security Space для Windows.

# Разведка

Я не разбираюсь в продуктах Доктор Веб, поэтому взял первое попавшееся, что можно было скачать на сайте — это был Dr.Web Security Space 12 для Windows. При настройках по умолчанию данный продукт проводит проверку обновлений каждые полчаса. И в механизме обновления была обнаружена уязвимость.

Ниже я предлагаю видео эксплуатации с описанием того, что происходит на видео с привязкой ко времени. Там же будет описание, в чем же конкретно состояла уязвимость.

## Видео эксплуатации

https://youtu.be/q7Kqi7kE59U

Демонстрация проходит на ОС Windows 10 x64 от пользователя без прав администратора. 0:00-0:12 через консоль Windows показываю, что текущий пользователь не является администратором

0:12-0:24 показываю установленную версию Dr.Web Security Space

0:24-0:29 в папке на рабочем столе находится файл drweb\_eop\_upd\_dll.dll (исходные коды и файл

0:29-0:34 показываю, что в папке C:\ProgramData\Doctor Web\Updater\etc находится 3 файла 0:34-0:47 копирую библиотеку drweb\_eop\_upd\_dll.dll в папке на рабочем столе и один экземпляр называю version.dll, другой — cryptui.dll

0:47-0:56 копирую файл C:\Program Files\Common Files\Doctor Web\Updater\drwupsrv.exe в папку на рабочем столе, рядом с dll.

0:56-1:00 запускаю скопированный файл

Запускаемый файл drwupsrv.exe из папки на рабочем столе загружает расположенную рядом

Web\Updater\etc\drwupsrv.xml.new. На папку C:\ProgramData и вглубь у пользователя есть права на создание файлов, поэтому это легальная операция. Если попробовать создать такой файл вручную, то, вероятно, защитные механизмы Dr.Web предотвращают такую операцию. Но в эксплуатации создание файла проходит от имени drwupsrv.exe, что вероятно обходит внутренние проверки и файл создается. Фактически, это обход той самой проверки подписи о которой и идет речь в начале статьи.

1:00-1:22 демонстрирую созданный файл и его содержимое. В общем смысле файл совпадает по содержимому с файлом C:\ProgramData\Doctor Web\Updater\etc\drwupsrv.xml, но все пути указывают папку на рабочем столе (C:\Users\User\Desktop\dwtest)

1:22-2:00 ничего не происходит (на этом этапе я ожидаю процесса обновления ПО, который по умолчанию происходит раз в полчаса и ожидаемое время можно найти в логах)

2:00-2:14 судя по всему, взяв созданный файл конфигурации, обновлятор видит, что в папке C:\User\Desr\Desktop\dwtest нет файлов ПО Dr.Web, начинает туда файлы ПО копировать.

Среди копируемых файлов есть файл dwservice.exe, который запускается в момент обновления от имени пользователя NT AUTHORITY\SYSTEM. Данный файл загружает в себя библиотеку cryptui.dll, которая была в папке C:\Users\User\Desktop\dwtest. Код библиотеки просто запускает интерактивную консоль, которую и видно на экране. Командой whoami убеждаюсь, что получены права системы.

#### Итог

Отчет об уязвимости был отправлен в Доктор Веб и, вроде бы, разработчики все поправили.

### Таймлайн:

15.05.2020 — Обращение в техподдержку с просьбой предоставить security-контакт.

20.05.2020 — Получаю ответ, что можно передать отчет в данном обращении

20.05.2020 — Передаю отчет

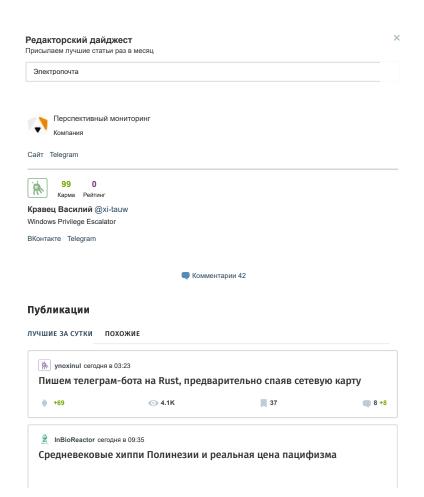
14.06.2020 — Получаю ответ, что для 12 версии уязвимость исправлена. Ожидают портирование для версии 11.

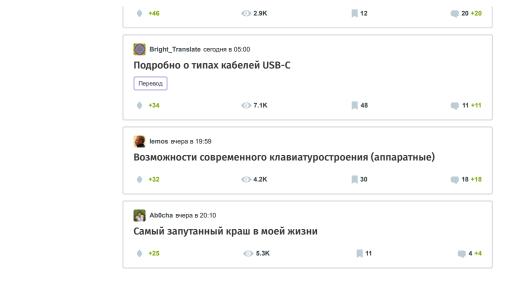
07.07.2020 — Разработчики подтверждают, что исправления выпущены.

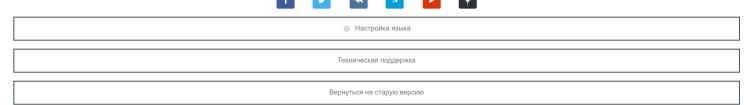
This article in english.

**Теги:** dr web, eop, lpe, уязвимость, антивирус

Хабы: Блог компании Перспективный мониторинг, Информационная безопасность







© 2006–2022, Habr