Уклонение от средств защиты: 1 Часть. – Telegraph

telegra.ph/Uklonenie-ot-sredstv-zashchity-1-CHast-07-12

Life-Hack - Linux/Хакинг/Хакер/ИБ/Osint July 12, 2024

Сокрытие процессов от антивирусного программного обеспечения (AV) - важная задача не только для хакеров, создающих вирусы, но и для специалистов по тестированию на проникновение. Существует много способов сокрытия процессов, и одним из них является Herpaderping.

Microsoft позволяет разработчикам антивирусного ПО получать с помощью API все нужные им события например:

```
PsSetCreateProcessNotifyRoutineEx
```

Когда создается процесс, AV сразу узнает об этом, получая соответствующий Callback. Теперь он может анализировать исполняемый файл и принять решение, разрешить данный процесс или нет.

Процесс содержит виртуальное адресное пространство, исполняемый код, открытые дескрипторы для системных объектов, контекст безопасности, уникальный идентификатор процесса, переменные среды, класс приоритета, минимальный и максимальный размеры рабочего множества и как минимум один поток выполнения.

Суть в том, что уведомление CreateProcessNotify — совсем не про создание процесса. Callback полетит в тот момент, когда внутри данного процесса возникнет первый поток (thread). Поток — это базовая единица, в которой ОС выделяет процессорное время. Поток может выполнять любую часть кода процесса.

Рассмотрим этапы создания процесса:

1) В начале для исполняемого файла мы получаем дескриптор (handle), который запускаем, например таким образом:

```
hFile = CreateFile(“C:\Windows\System32\svchost.exe”)
```

2) Создается image section например:

```
hSection = NtCreateSection(hFile, SEC_IMAGE)
```

3) Image section представляет собой особый раздел и служит для отображения файла (или части файла) в память. Раздел соответствует PE-файлам и может быть создан только в них. Создается процесс в image section например:

```
hProcess = NtCreateProcessEx(hSection)
```

4) Назначаются аргументы и переменные среды например:

```
CreateEnvironmentBlock/NtWriteVirtualMemory
```

5) Создается поток для выполнения процесса например:

```
NtCreateThreadEx
```

Имейте ввиду: процессы запускаются из исполняемых файлов, но информация внутри исполняемого файла может меняться относительного того, что находится в image section (так как она кешируется memory manager).

Herpaderping

Нам потребуется mimikatz.exe, целевой исполняемый файл (тут можно указывать что угодно, у нас это будет hack.exe) и любой файл, не вызывающий подозрений у антивирусных программ.

Herpaderping по шагам:

1) Write — Создаем и открываем hack.exe, копируем в него mimikatz.exe, дескриптор не закрываем.

2) Map — Создаем image section и мапим содержимое в память.

3) Modify — Создаем процесс с дескриптором ранее созданного раздела. После этого меняем содержимое файла hack.exe, копируя туда что-нибудь легитимное. Помните важный момент из раздела про создание процесса? Так вот это он и есть: с этого момента то, что у нас в памяти, и то, что хранится в файле, отличается.

4) Execute — Создаем initial thread. Только сейчас антивирусу летит process creation callback. Различие содержимого в файле и в памяти сводит с ума AV, он не может понять, можно ли разрешать выполнение этого процесса.

5) Close — Закрываем открытый дескриптор.

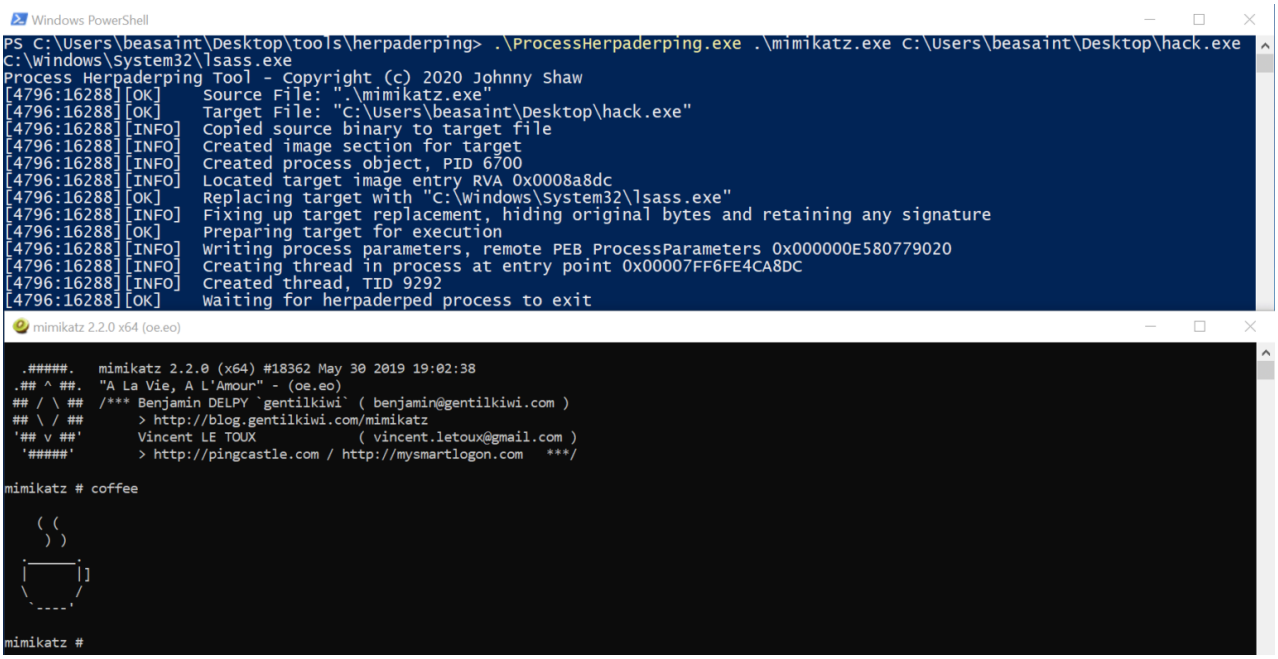
Herpaderping на практике

Клонирум проект из GitHub и собираем его:

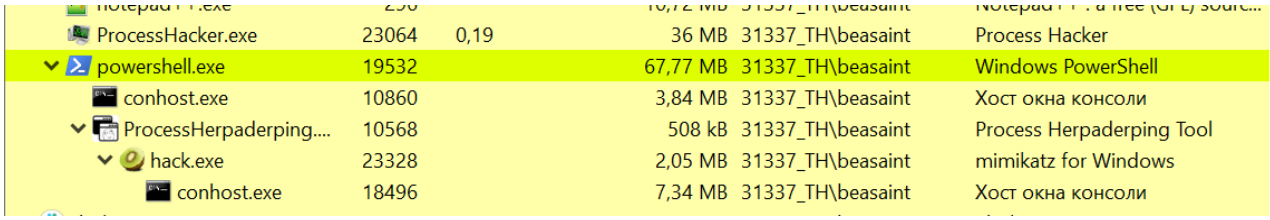
```
git clone https://github.com/jxy-s/herpaderping.git
cd .\herpaderping\
git submodule update --init –recursive
```

Выполняем команду:

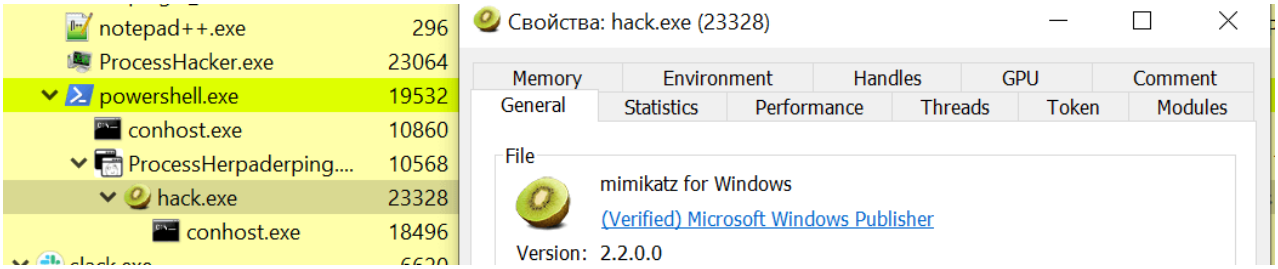
```
ProcessHerpaderping.exe mimikatz.exe hack.exe lsass.exe
```



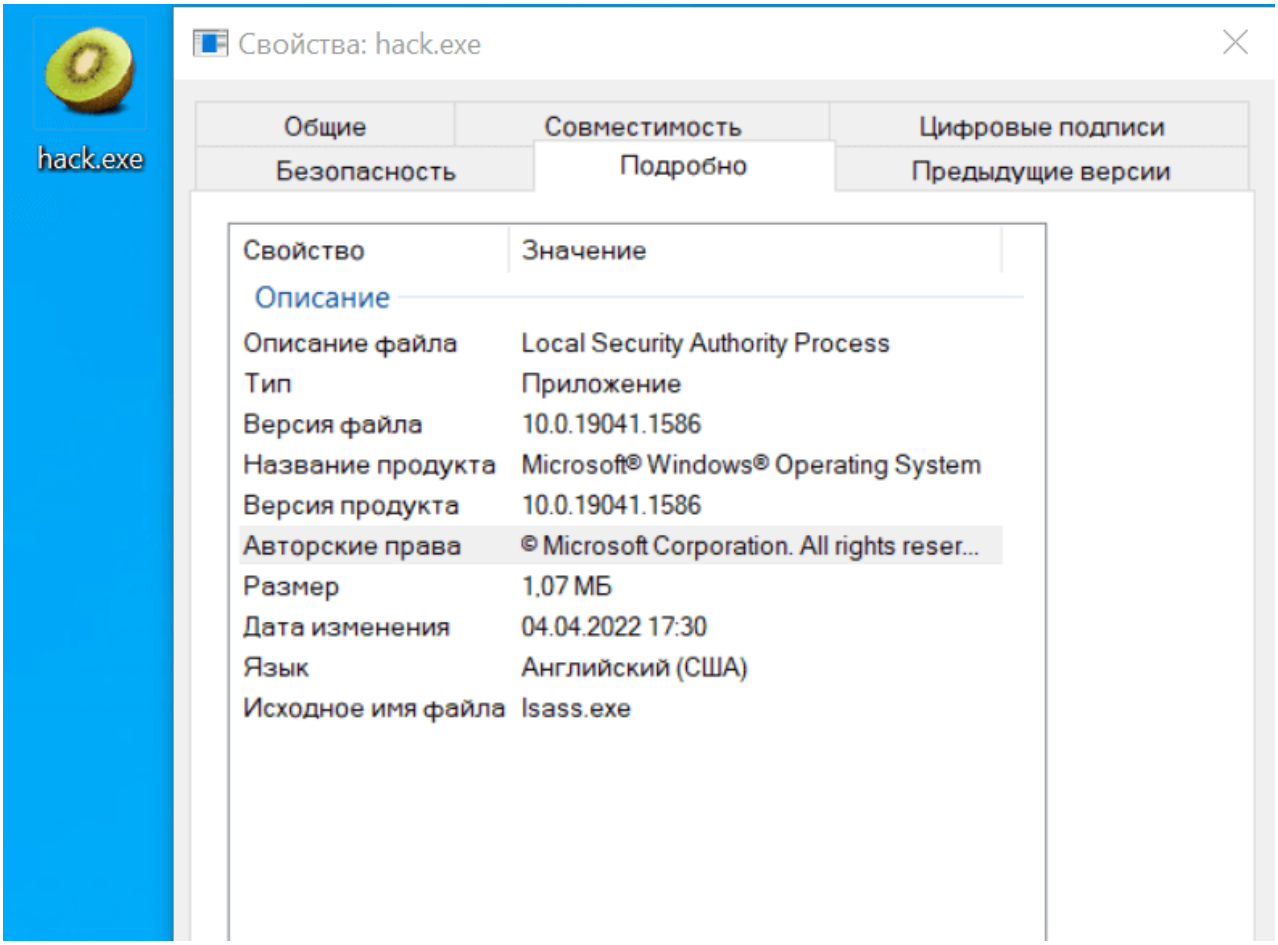
Как мы видим, все выполнилось успешно, AV не среагировал. Давайте взглянем, что покажет нам ProcessHacker.



У нас исполняется не mimikatz.exe, а hack.exe. А еще у нашего приложения hack.exe есть сертификат, выданный Microsoft.



Ну а сам hack.exe спокойно лежит на рабочем столе.


hack.exe
Свойства: hack.exe
Общие
Совместимость
Цифровые подписи
Безопасность
Подробно
Предыдущие версии
Свойство
Значение
Описание
Описание файла
Local Security Authority Process
Тип
Приложение
Версия файла
10.0.19041.1586
Название продукта
Microsoft® Windows® Operating System
Версия продукта
10.0.19041.1586
Авторские права
© Microsoft Corporation. All rights reser...
Размер
1,07 МБ
Дата изменения
04.04.2022 17:30
Язык
Английский (США)
Исходное имя файла
lsass.exe