SYNACKTIV

Hooking Windows Named Pipes

Sthack 2025

23/05/2025

Whoami

SYNACKTIV

Thomas Borot

Pentester/Developer

thomas.borot@synacktiv.com

Synacktiv

SYNACKTIV

- French offensive security company
- 180 security experts
- 4 departments :
  - Pentest / Redteam
  - Reverse Engineering / Vulnerability Research
  - Development
  - Incident Response
- Hexacon

Overview

SYNACKTIV

- Windows Named Pipes presentation and APIs
- Common attacks to intercept and modify data
- Common mitigations against MitM attacks
- How to bypass mitigations
- Demo

Windows Named Pipes

SYNACKTIV

Bidirectional channel between a **client** and a **server**.

```
PS > .\pipelist64.exe

Pipe Name                                          Instances         Max Instances
---------                                          ---------         -------------
InitShutdown                                               3                    -1
lsass                                                      9                    -1
ntsvcs                                                     3                    -1
scerpc                                                     3                    -1
Winsock2\CatalogChangeListener-2ec-0                       1                     1
Winsock2\CatalogChangeListener-3e0-0                       1                     1
epmapper                                                   3                    -1
Winsock2\CatalogChangeListener-254-0                       1                     1
LSM_API_service                                            3                    -1
Winsock2\CatalogChangeListener-1d8-0                       1                     1
atsvc                                                      3                    -1
```

Windows Named Pipes APIs

SYNACKTIV

Server:

`handle = CreateNamePipe("\\.\pipe\example_pipe")` -> listen on "example_pipe"

Client:

`handle = CreateFile("\\.\pipe\example_pipe")` -> connects to "example_pipe"

Both:

`WriteFile(handle, "hello world!")` -> sends "hello world!" to the server

`data = ReadFile(handle)` -> reads data from the pipe

Other Windows APIs can be used to perform asynchronous read and writes

Example

SYNACKTIV

```
PS > .\pipe.exe -mode sync -servermode -pipename "example_pipe"
[INFO] CreateNamedPipeW("\\.\pipe\example_pipe", ...) -> 308
[INFO] ConnectNamedPipe(308, 0) -> 1
[INFO]   New client connected
[INFO] ReadFile(308, readBuffer, 2048, pNbBytesRead, 0) -> 1
[INFO]   Got data (22 bytes): "Client says tutJxQNpew"
[INFO] WriteFile(308, "Server says FSrHdjnLcr", 22, pNbBytesWritten, 0) -> 1
[INFO]   Wrote 22 bytes
```

```
PS > .\pipe.exe -mode sync -pipename "example_pipe"
[INFO] CreateFileW("\\.\pipe\example_pipe", ...) -> 332
[INFO]   Connected to existing pipe
[INFO] WriteFile(332, "Client says tutJxQNpew", 22, pNbBytesWritten, 0) -> 1
[INFO]   Wrote 22 bytes
[INFO] ReadFile(332, readBuffer, 2048, pNbBytesRead, 0) -> 1
[INFO]   Got data (22 bytes): "Server says FSrHdjnLcr"
```

What else?

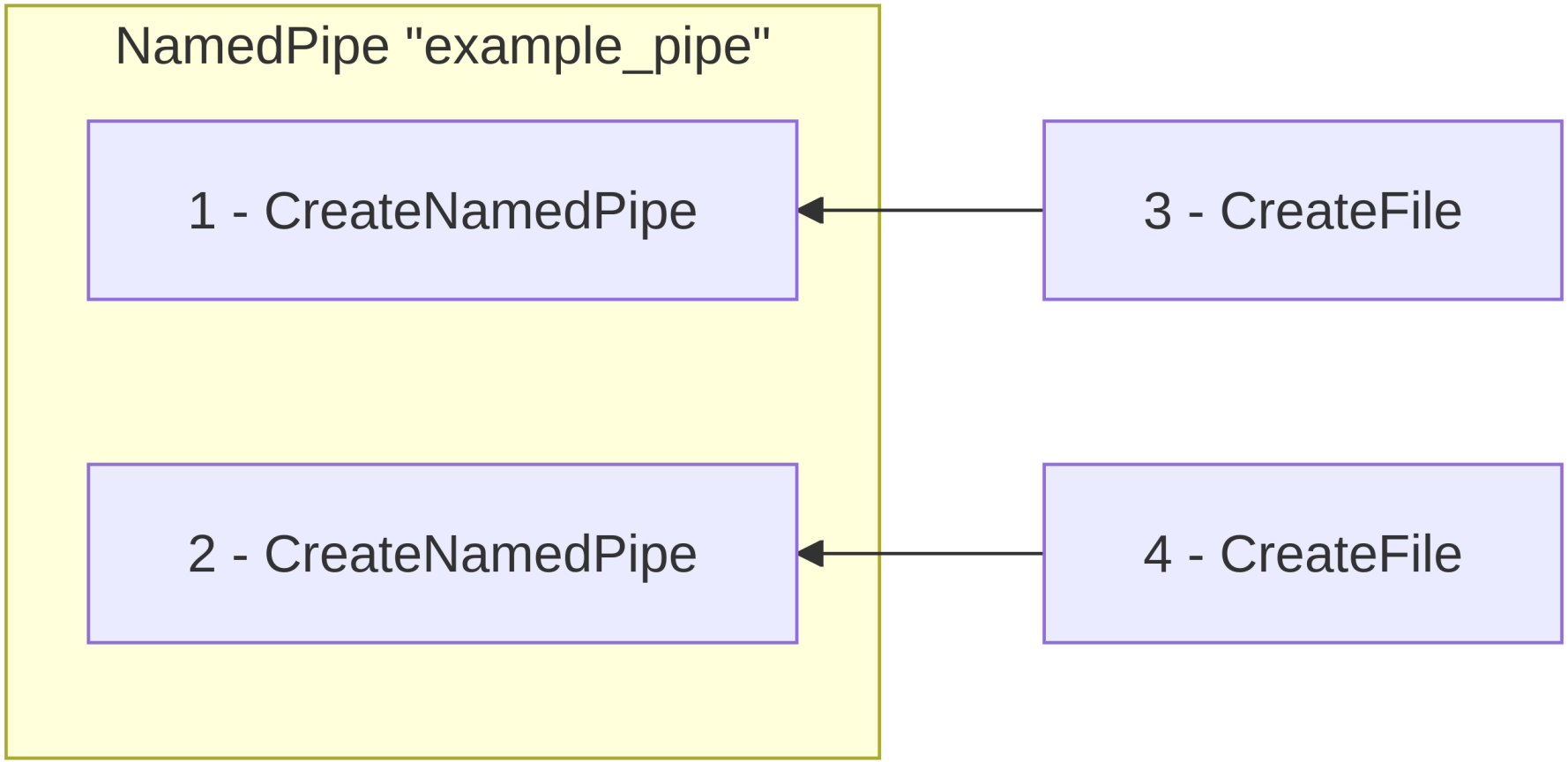
SYNACKTIV

```
PS > .\accesschk64.exe \\.\pipe\ntsvcs

\\.\pipe\ntsvcs
  RW Everybody
  RW AUTORITE NT\ANONYMOUS LOGON
  RW BUILTIN\Administrators
```

Listen for several clients

SYNACKTIV



Listen for several clients

SYNACKTIV

```
PS > .\pipelist64.exe
Pipe Name                                          Instances         Max Instances
---------                                          ---------         -------------
ntsvcs                                                 4                 -1
```

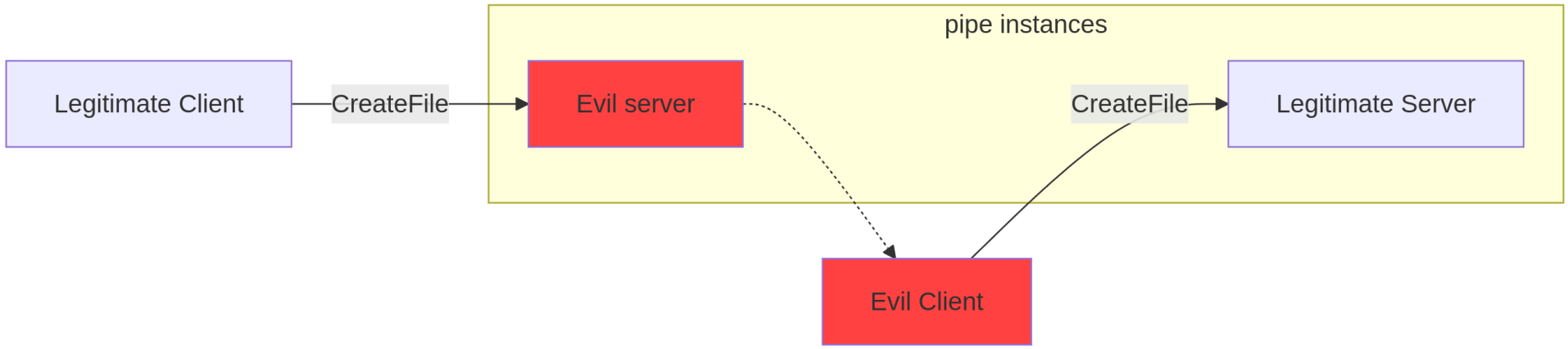
```
PS > .\pipe.exe -mode sync -pipename "ntsvcs"
[INFO] CreateNamedPipeW("\\.\pipe\ntsvcs", ...) -> 340
[INFO] ConnectNamedPipe(308, 0)
```

```
PS > .\pipelist64.exe
Pipe Name                                          Instances         Max Instances
---------                                          ---------         -------------
ntsvcs                                                 5                 -1
```

We can listen on top of an existing pipe instance

Common attacks

SYNACKTIV



Mitigations

SYNACKTIV

What if the server checks that the connecting process:

- Has a specific Process ID (PID)
- Was created from an exe file that has a specific sha256

Bypassing mitigations

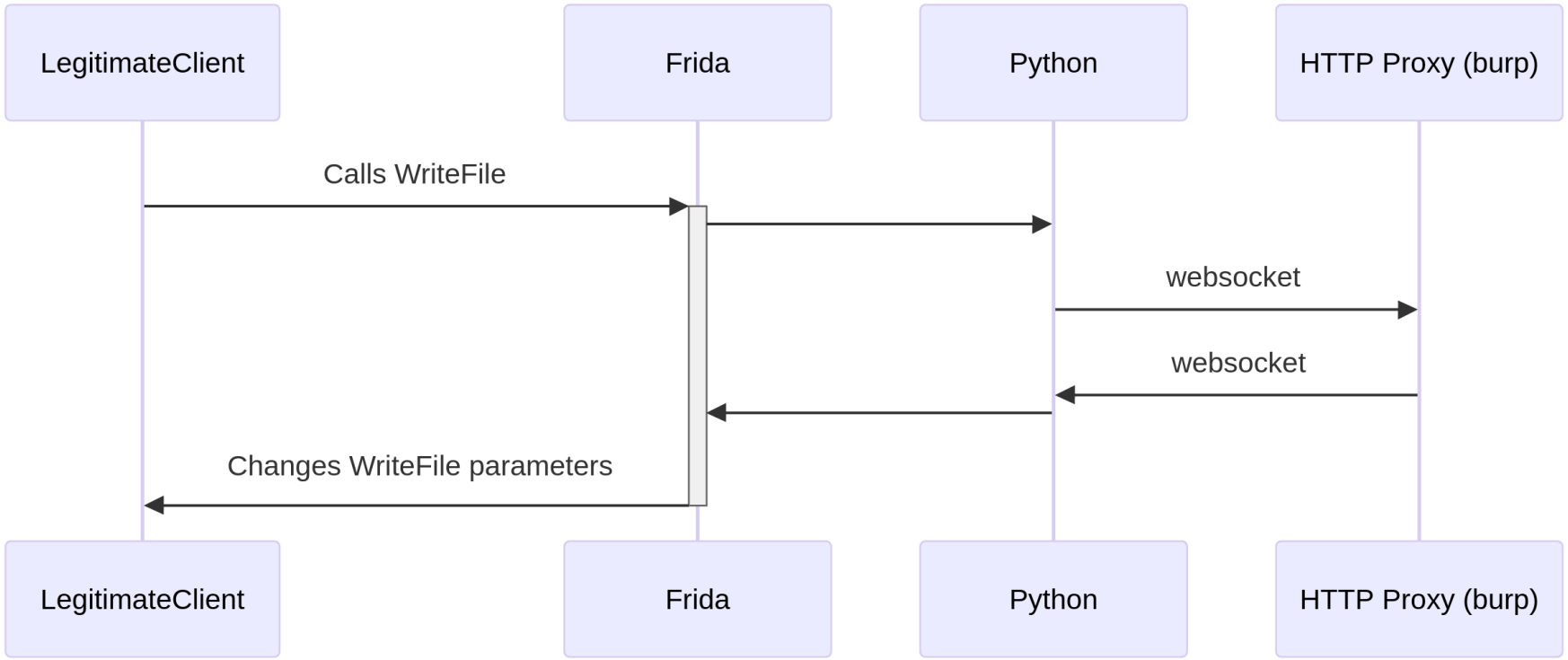
SYNACKTIV

- Injecting a payload into a legitimate process at run-time
- Redirecting every calls to `ReadFile` and `WriteFile`

Demo time

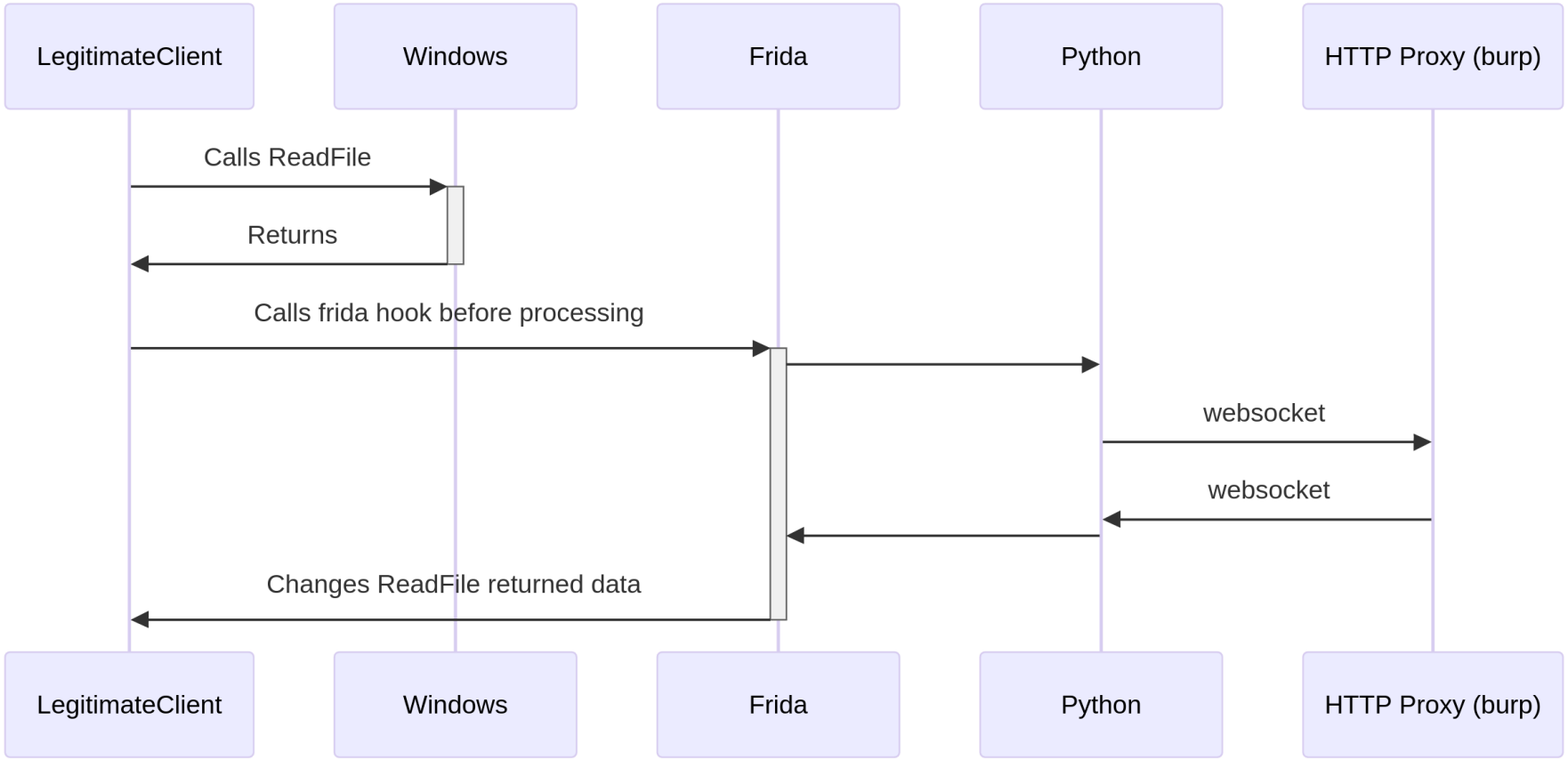
WriteFile flow

SYNACKTIV



ReadFile flow

SYNACKTIV



SYNACKTIV

https://www.linkedin.com/company/synacktiv

https://x.com/synacktiv

https://bsky.app/profile/synacktiv.com

https://synacktiv.com