

How your .NET software supply chain is open to attack

and how to fix it

Andrei EPURE

Engineering Manager at  **sonar**

Software supply chain

Source code

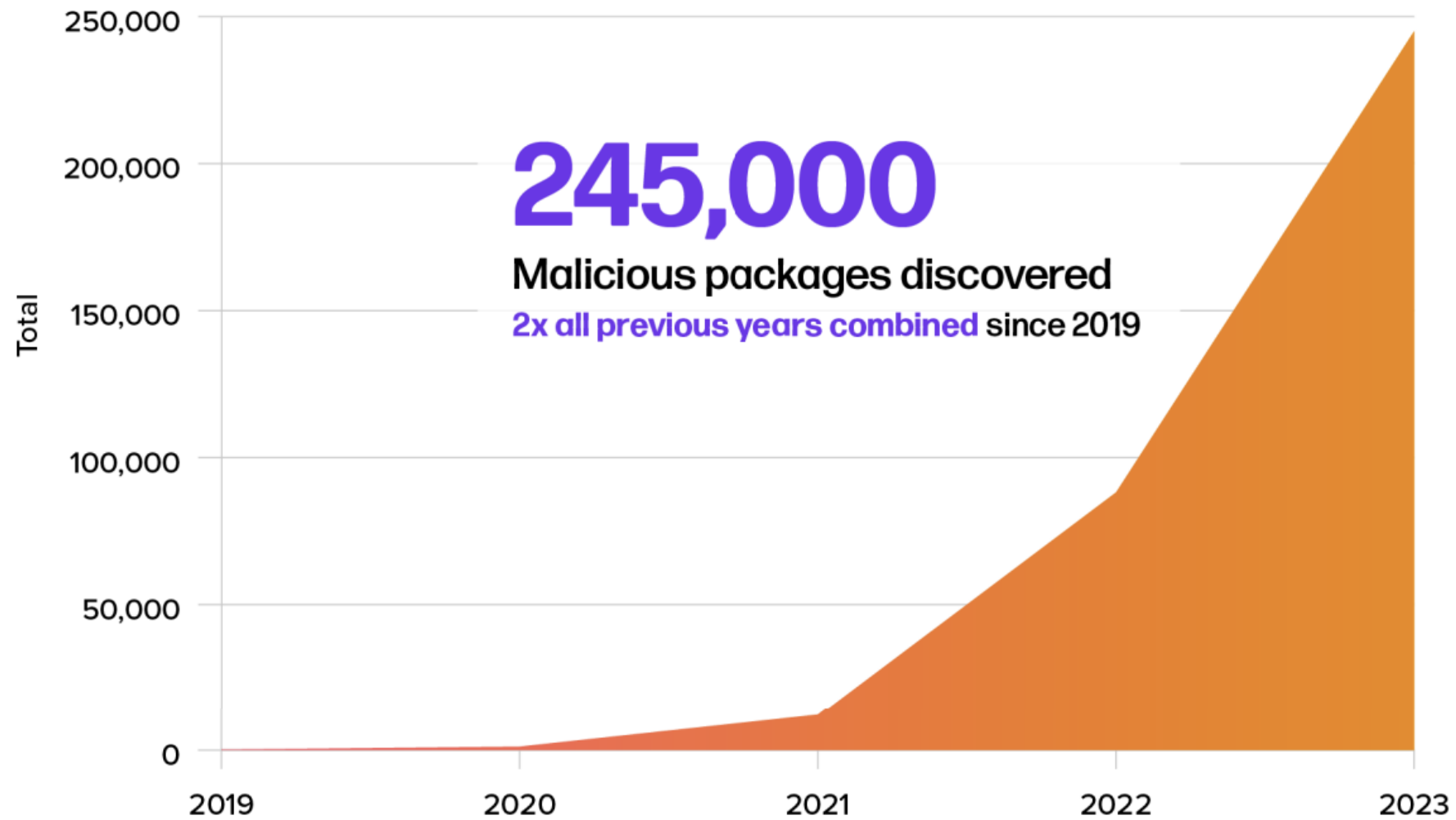
Libraries

Package managers (NuGet, NPM, PyPI)

Build tools, CI/CD, etc

FIGURE 1.7

NEXT GENERATION SOFTWARE SUPPLY CHAIN ATTACKS (2019-2023)



Source: [Sonatype's "9th State of the Software Supply Chain report" \(2023\)](#)

sonar



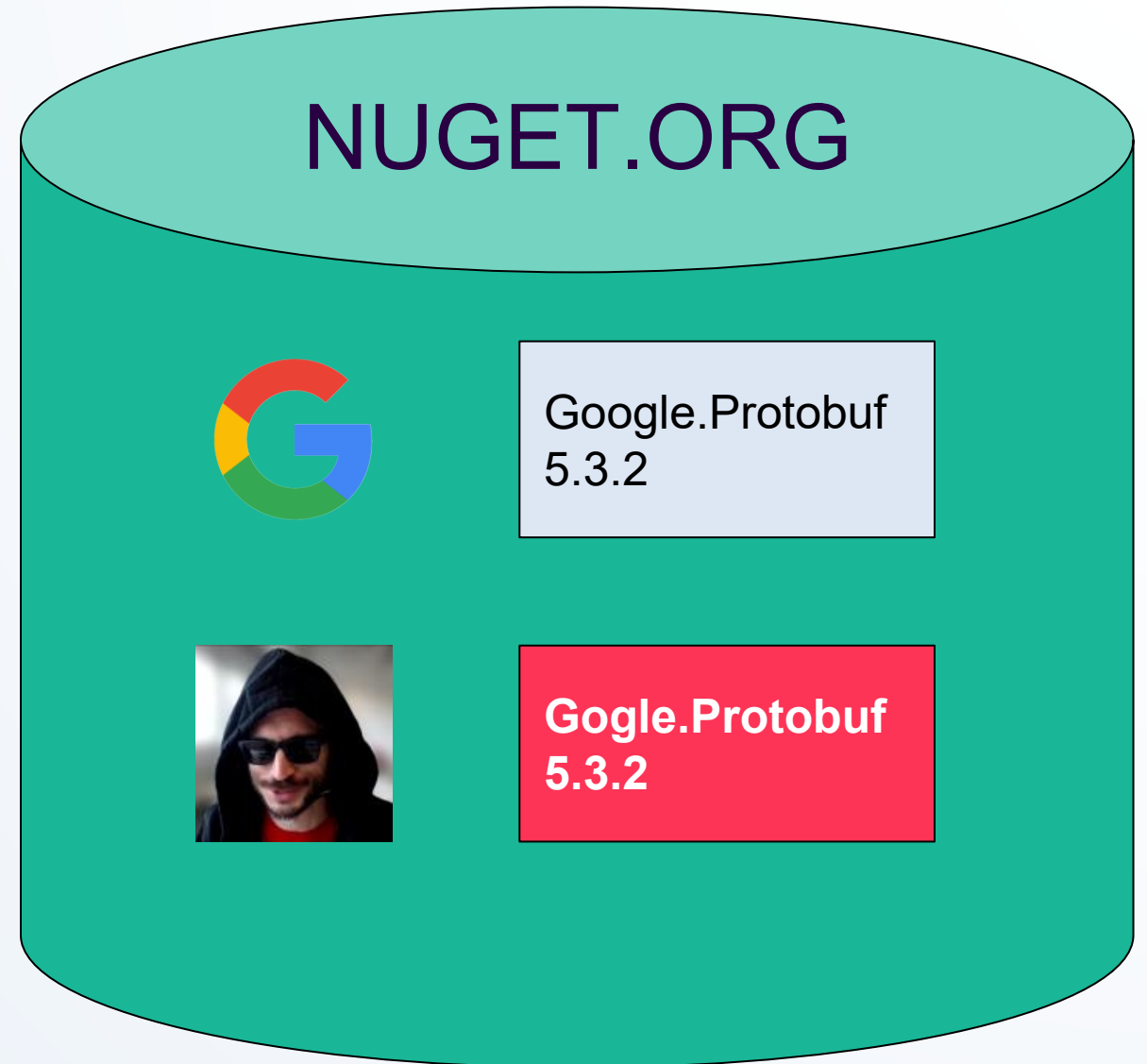
Agenda

1. Typosquatting
 2. Dependency confusion
- 
- Attack &
Defense

Typosquatting

To err is human

dotnet add package
Gogle.Protobuf -v 5.3.2



Typosquatting (2016) - Nikolai Tschacher

NPM and PyPi

17K infected PCs

50% admin privilege

Source: incolumitas.com

Typosquatting (2022)

Threat Research | July 5, 2022

Update: IconBurst npm software supply chain attack grabs data from apps and websites

27K downloads

Source: [ReversingLabs](#)

AndreiEpure.ro

Typosquatting (2023)

BLOG HOME >

Attackers are starting to target .NET developers with malicious-code NuGet packages

By Natan Nehorai, Application Security Researcher | Brian Moussalli, JFrog Malware Research Team Leader | March 20, 2023
🕒 12 min read

SHARE:   

Source: [JFrog](#)

Oct 12, 2023 / 6 min read / Research

Source: [Phylum](#)

Phylum Discovers SeroXen RAT in Typosquatted NuGet Package

Typosquatting DEMO



Mr. Evil Hacker

In production

← → ↻ 🔒 nuget.org/packages/Google.Protobuf/3.21.4

👋 What do you think about NuGet.org? We're looking for feedback from developers like you. [Take the survey.](#)

nuget Packages Upload Statistics Documentation Downloads Blog Sign in

Search for packages...

Google.Protobuf 3.21.4

⊗ **This package has been deleted from the gallery.** It is no longer available for install/restore.

🔗 Used By ⌚ **Versions**

Version	Downloads	Last updated
---------	-----------	--------------

Downloads
Full stats →

Total **494**

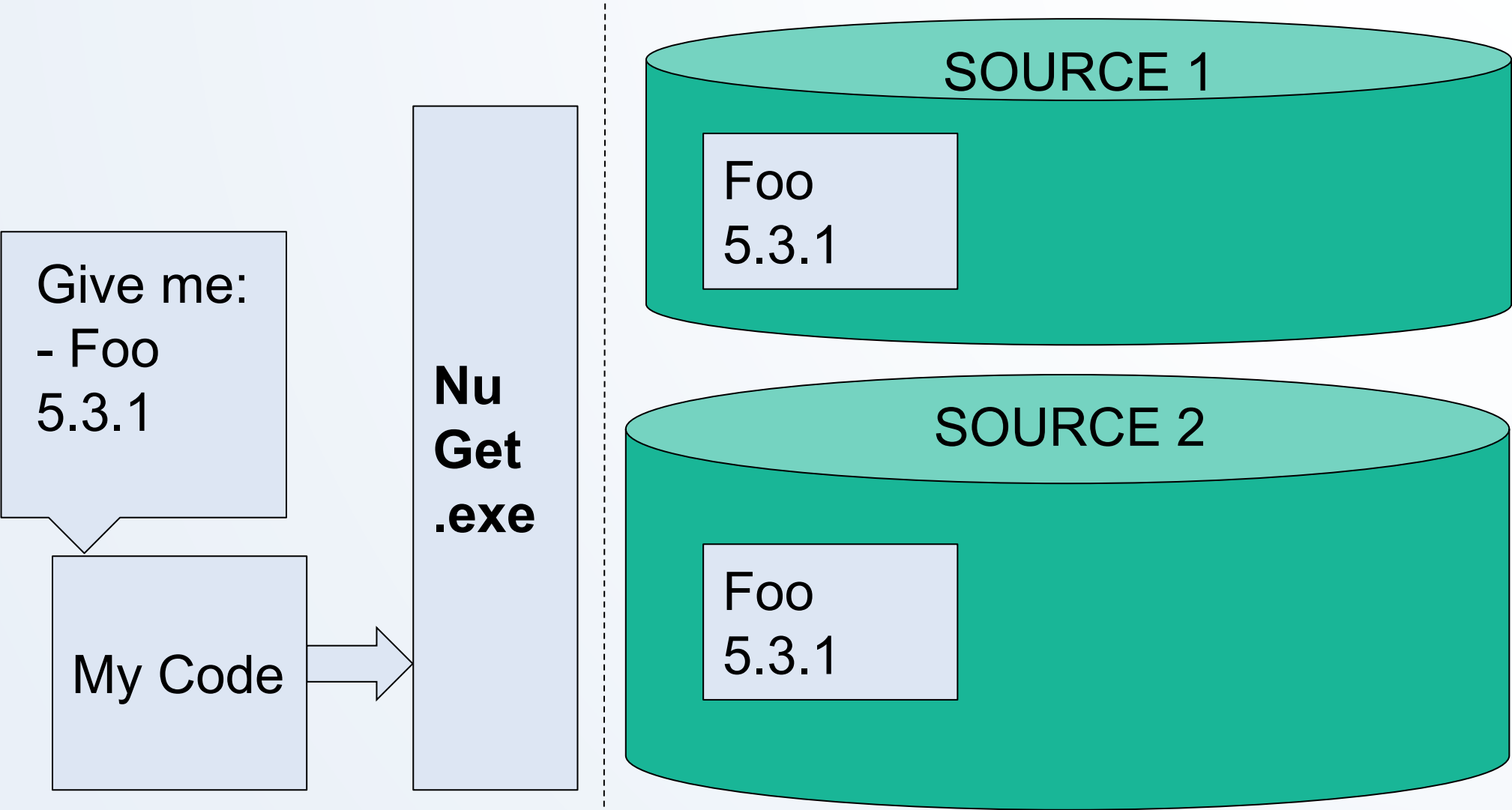
Current version **174**

Per day average **1**

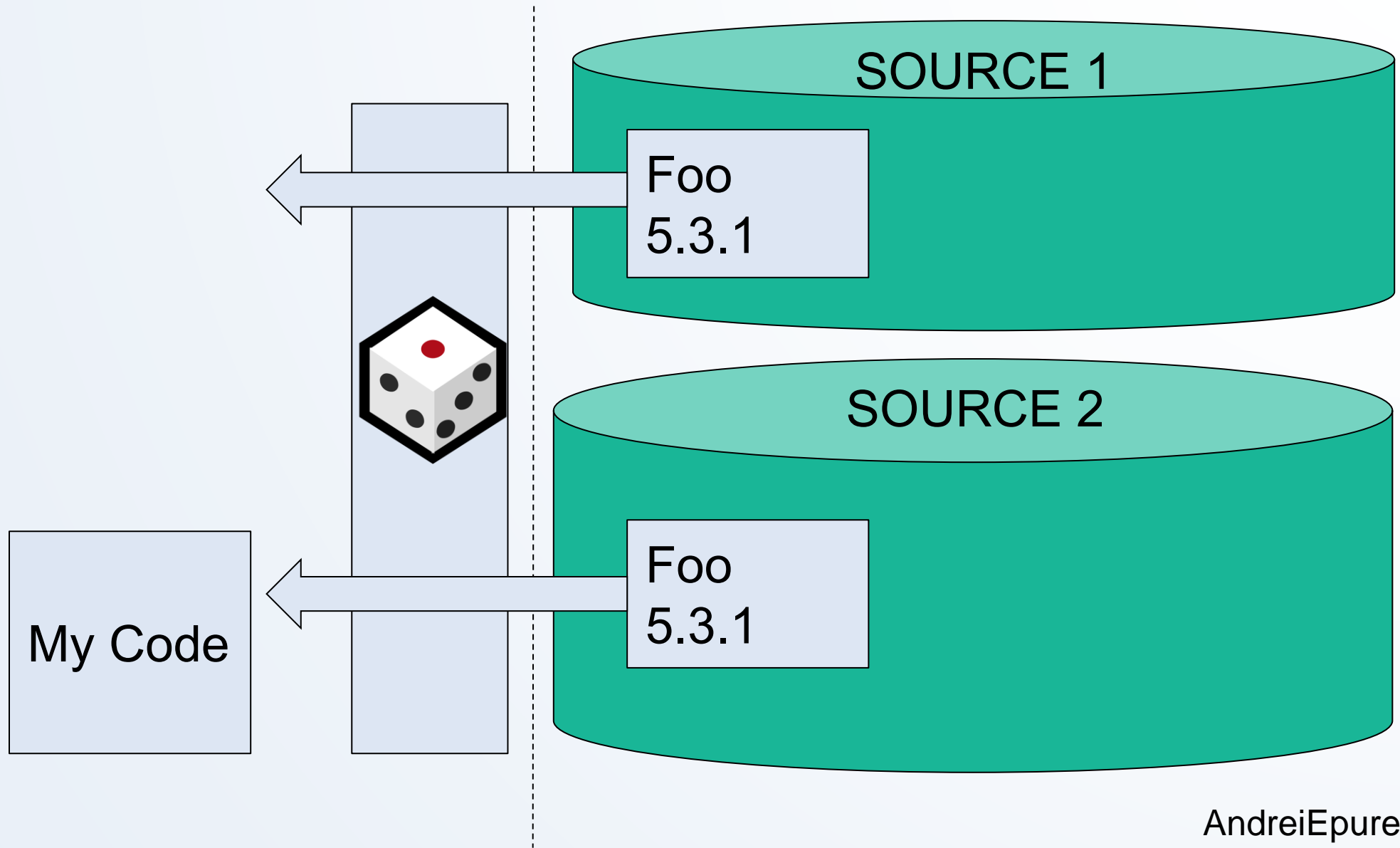
About

⌚ Last updated 9 months ago

NuGet Package Resolution



NuGet Package Resolution

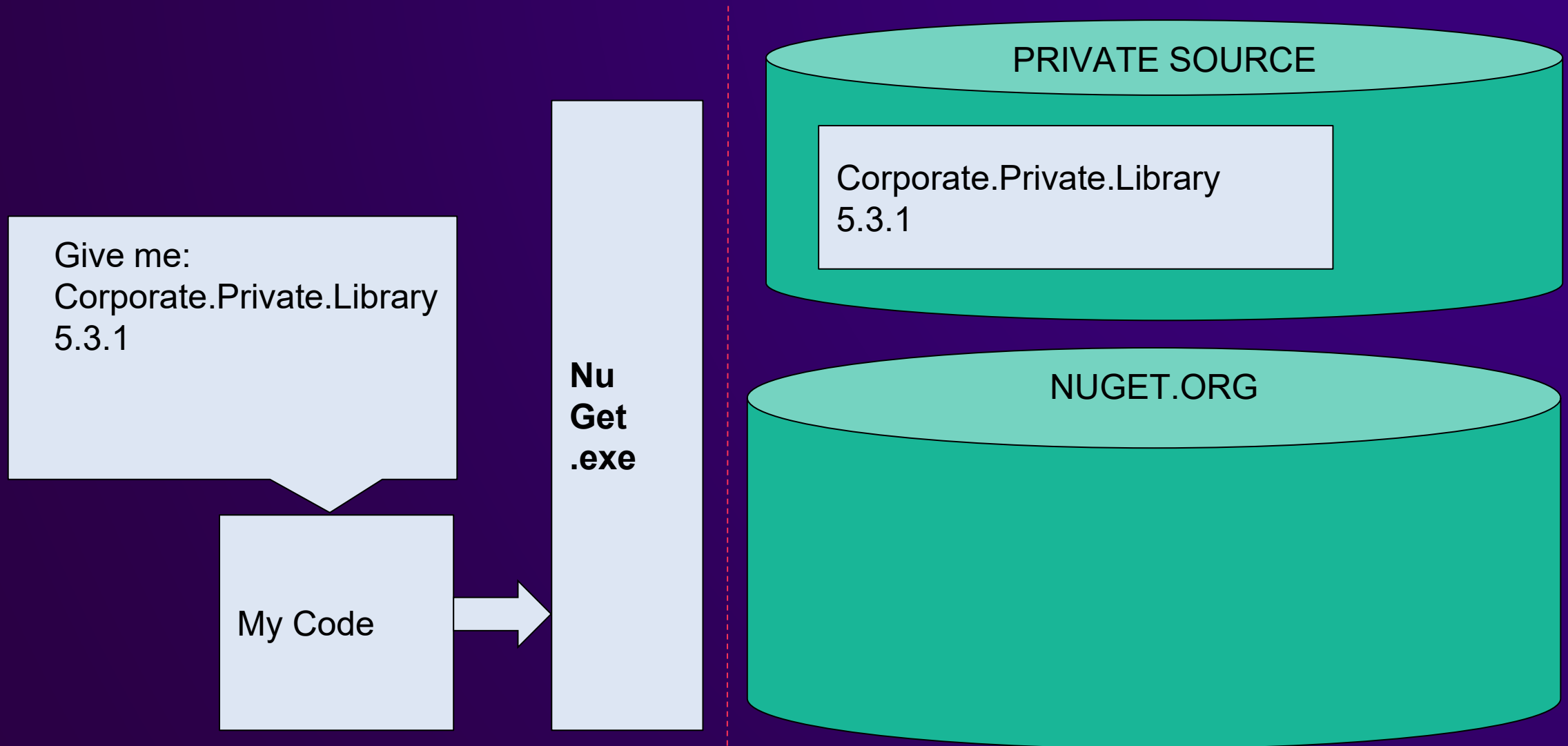


Dependency Confusion

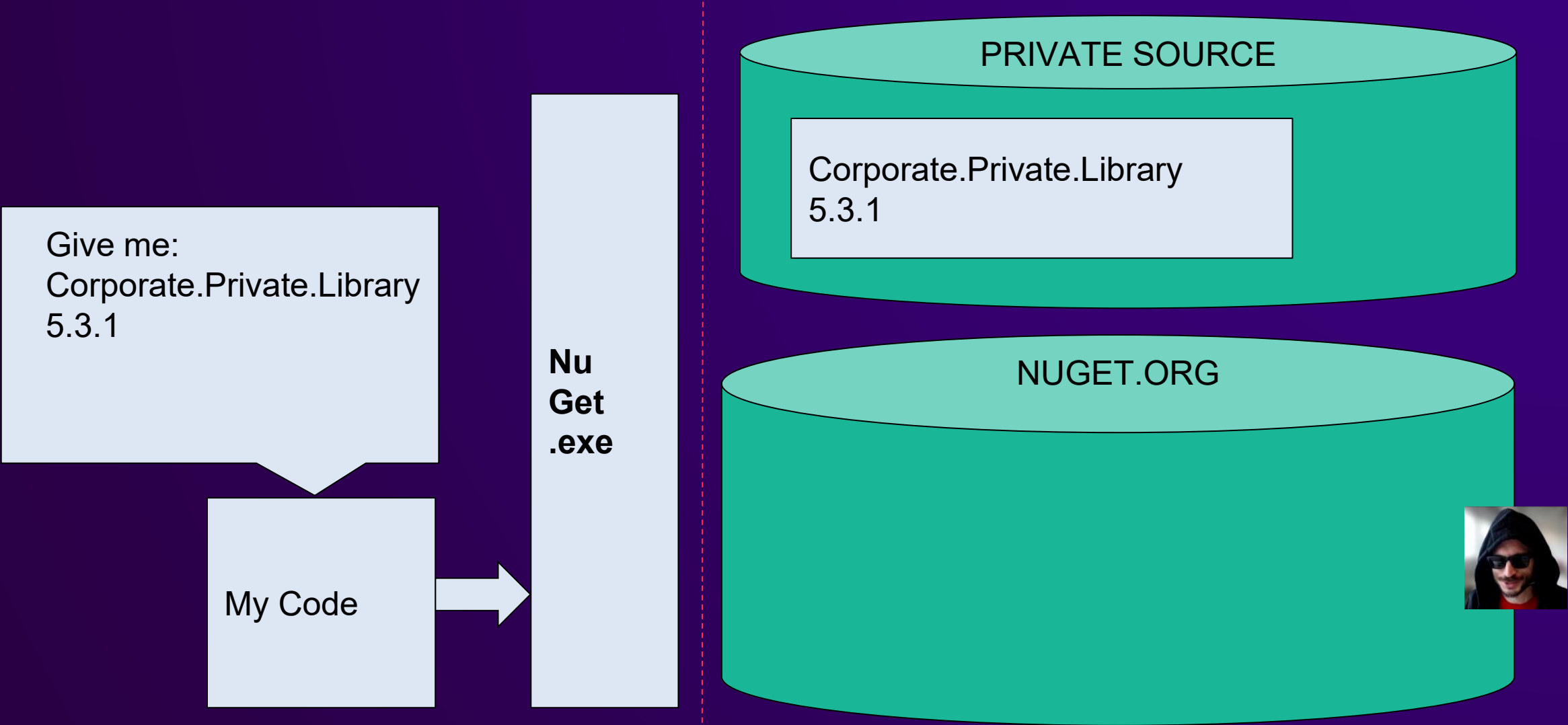


Mr. Evil Hacker

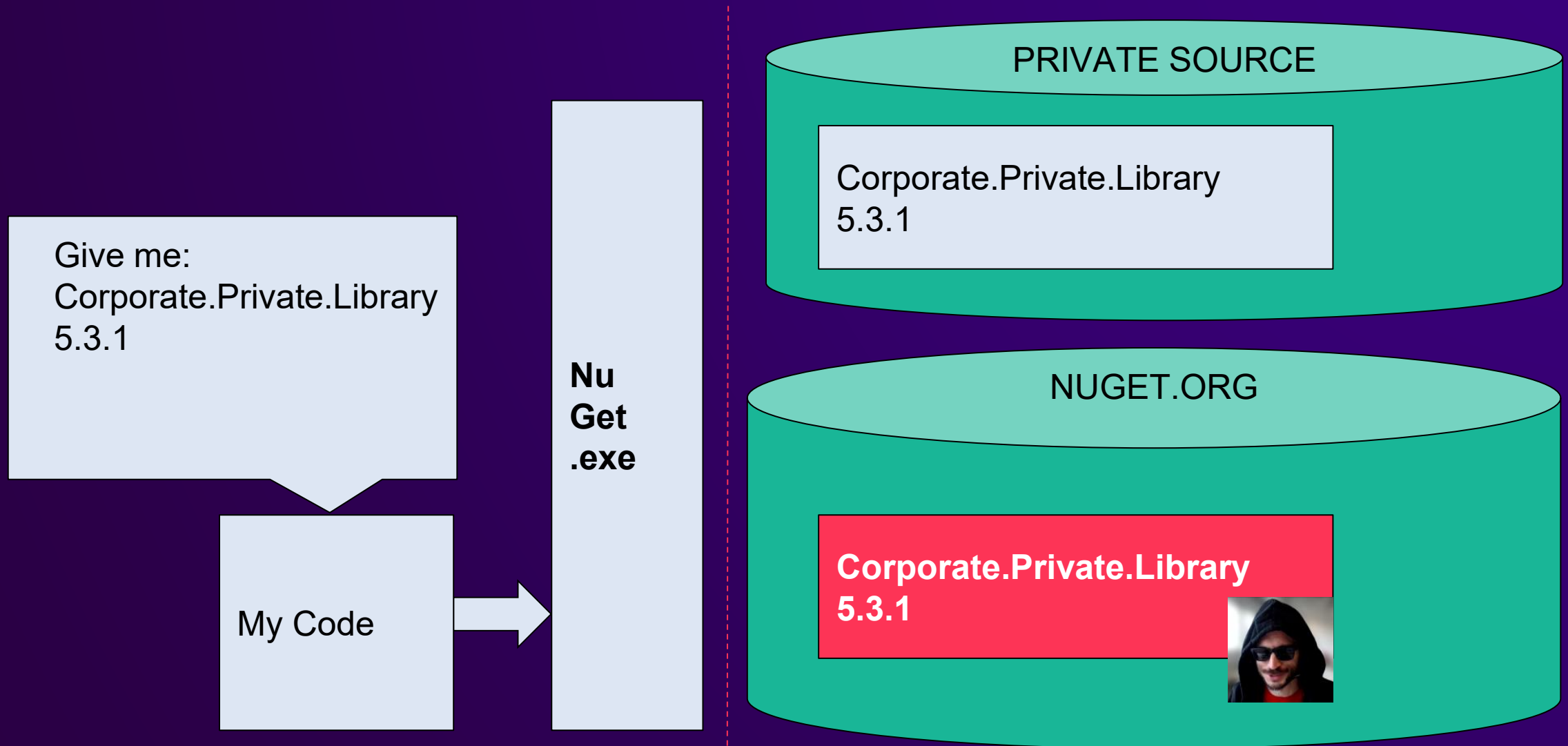
Dependency confusion



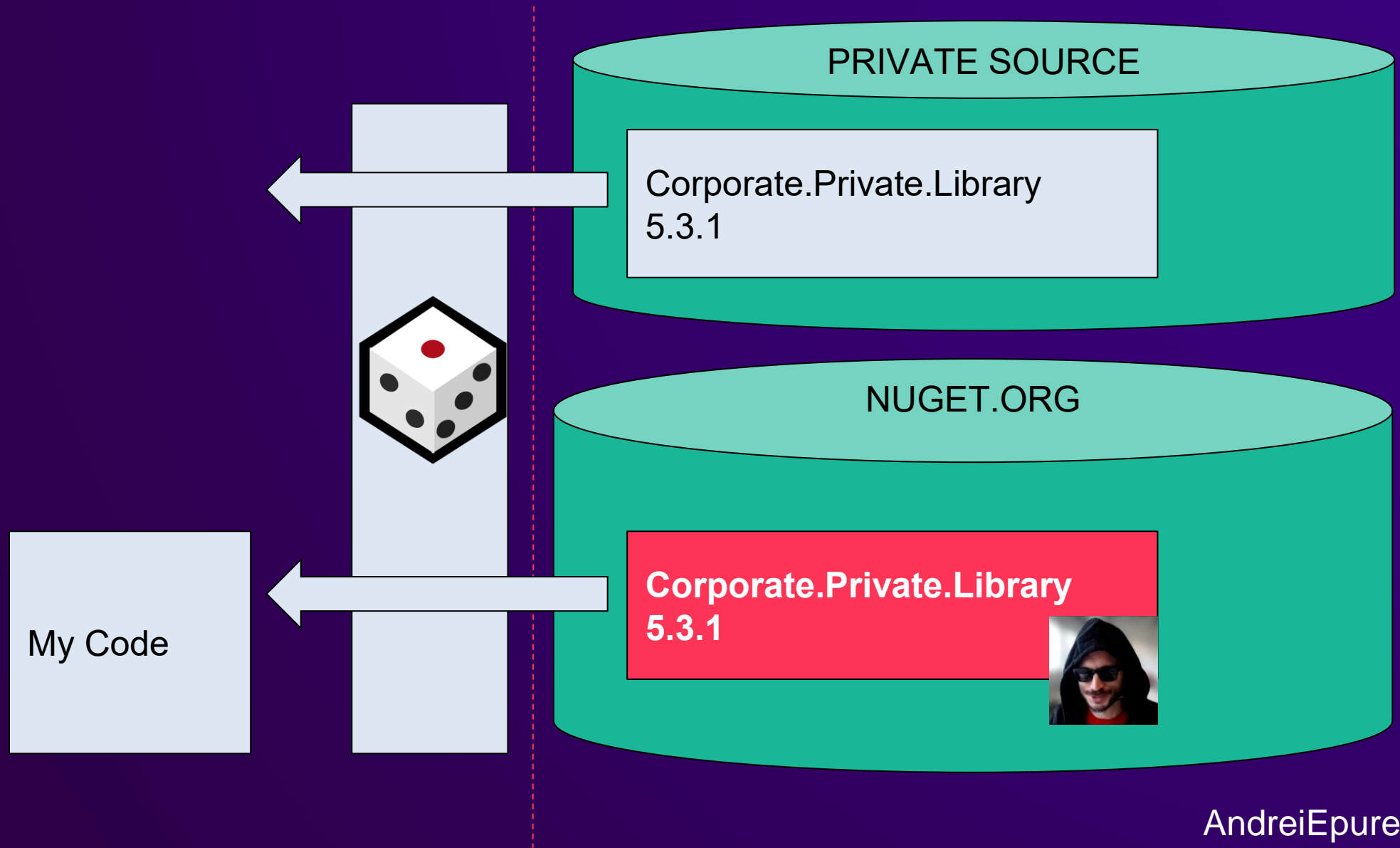
Dependency confusion



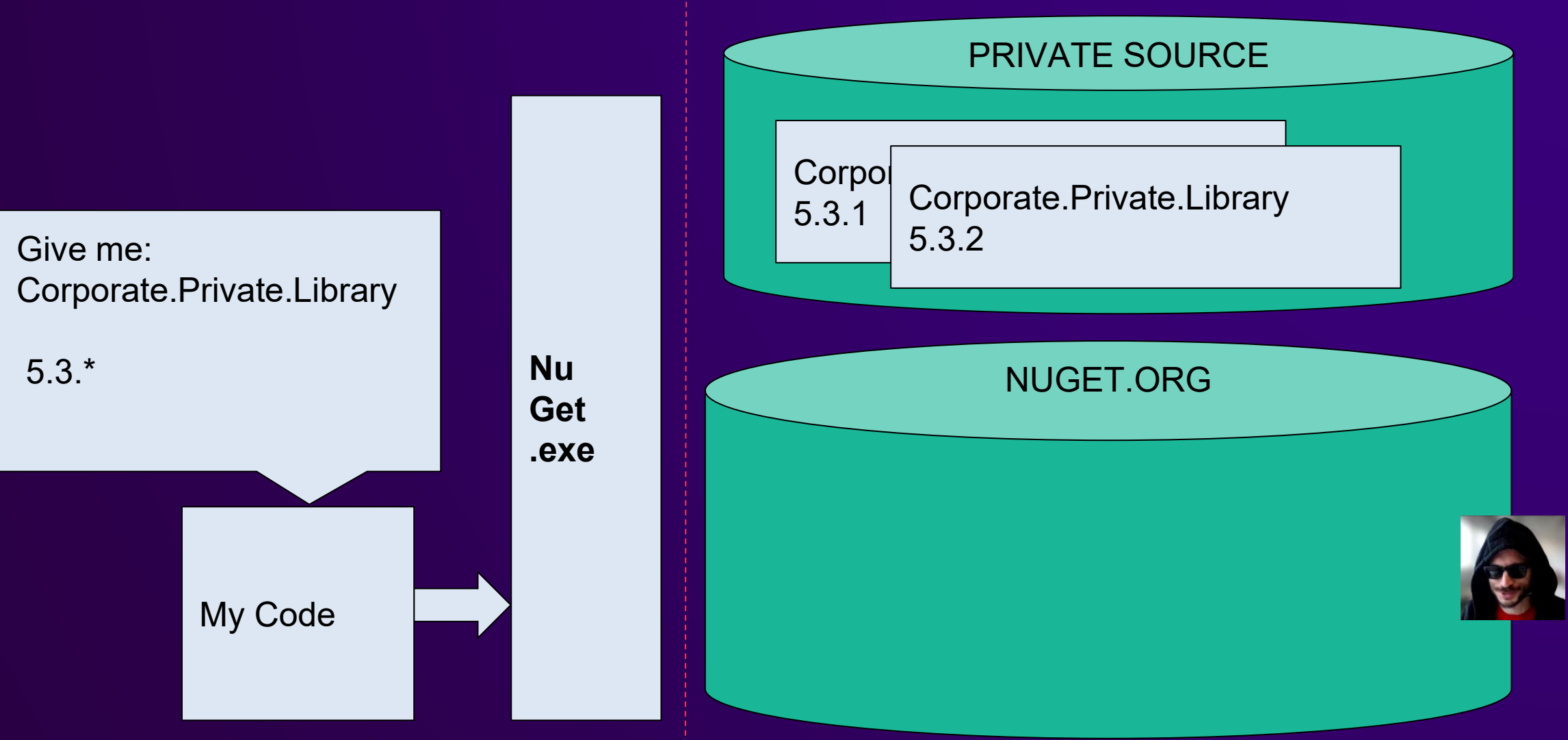
Dependency confusion



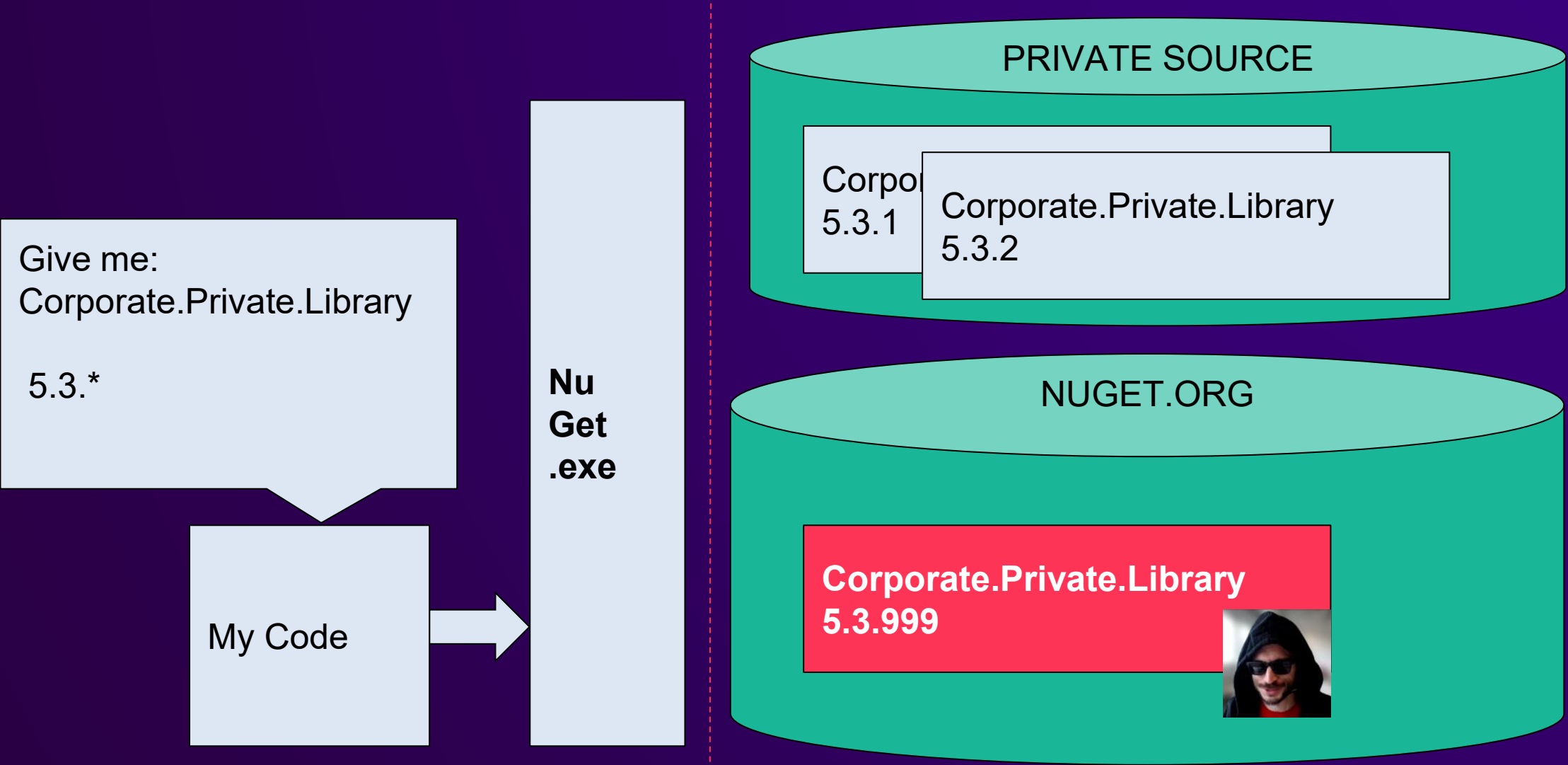
Dependency confusion



Dependency confusion



Dependency confusion



Dependency confusion

Here you are:

Corporate.Private.Library
5.3.999

Nu
Get
.exe

My Code

PRIVATE SOURCE

Corpor
5.3.1

Corporate.Private.Library
5.3.2

NUGET.ORG

Corporate.Private.Library
5.3.999



Dependency confusion

In 2020, security researcher Alex Bîrsan  used

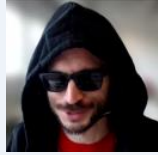
dependency confusion to hack into:

- Microsoft \$ 40K
- Apple \$ 30K
- Shopify \$ 30K
- Paypal \$ 30K
- ... and another 31 big companies

Bug
bounties

Dependency confusion DEMO

Do not let

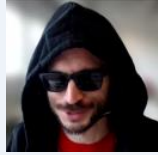


win!

1. `<clear>`
2. Package Source Mapping **or** single source
3. `<trustedSigners>`

More details in: [How to secure your NuGet supply chain](#)

Do not let



win!

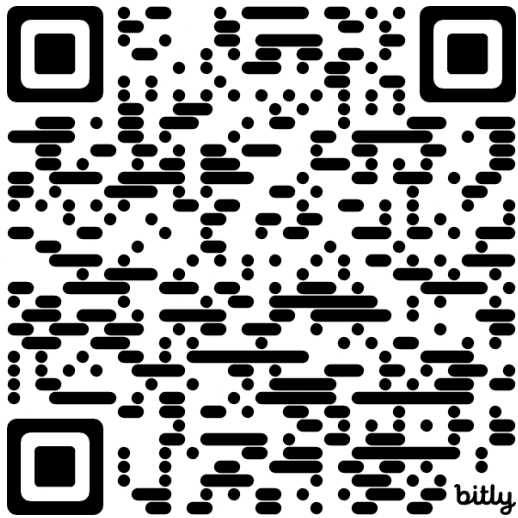
4. Fixed versions

5. Sign your packages

6. Reserve prefixes on nuget.org

More details in: [How to secure your NuGet supply chain](#)

Q & A



feedback form & slides on

AndreiEpure.ro