

HOW YOUR .NET SOFTWARE SUPPLY CHAIN IS OPEN TO ATTACK

AND HOW TO FIX IT

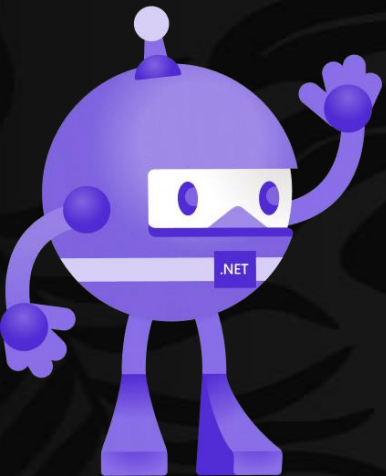
Andrei Epure







ANDREI EPURE





my talk, my opinions

Agenda

1. Remember SolarWinds
2. Refresh NuGet concepts
3. How to attack
4. How to defend

Agenda

1. Remember SolarWinds
2. Refresh NuGet concepts
3. How to attack
4. How to defend

SolarWinds breach (2020)

Orion: Network Management System

Used by 30K organizations

SolarWinds breach (2020)

attackers

build machines (2019)

injected malware in Orion (2020)

SolarWinds breach (2020)

malware to 18K customers

US departments (e.g. Defense, State, etc)

Microsoft, Intel, Cisco etc

FireEye

SolarWinds breach (2020)

FireEye

stolen credentials

employee noticed

investigation

SolarWinds breach (2020)



Supply chain attacks can be catastrophic.

Why do I care?



used by 400K organizations

Why should YOU care?

think

Agenda

1. Remember SolarWinds
2. Refresh NuGet concepts
3. How to attack
4. How to defend

Who in this room...

... uses NuGet?

NuGet Concepts

1. Software Supply Chain
2. package
3. targets
4. version
5. source
6. resolution

(1) Software supply chain

Source code

Libraries

NuGet

Build tools, CI/CD, etc

(1) Software supply chain

NuGet

> dotnet restore

(2) NuGet Package

compiled libraries

metadata

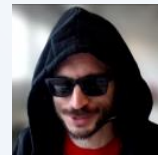
MSBuild target files

(2) NuGet Package

compiled libraries

metadata

MSBuild target files



(3) MSBuild targets

Task = action

Target = collection of tasks

(4) NuGet Version

fixed: *1.2.3*

range: *(, 1.2.3]*

floating: *1.2.**

Who in this room...

... changed a nuget.config file?

(5) NuGet Package Source

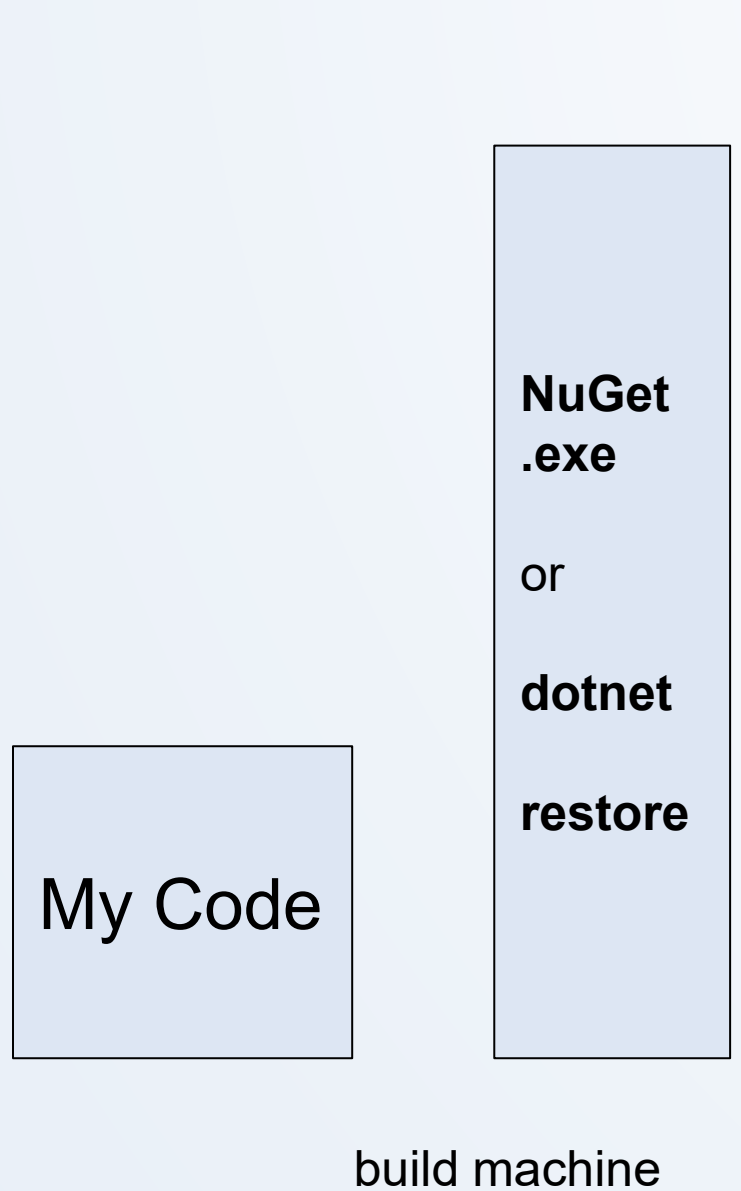
feed

central storage

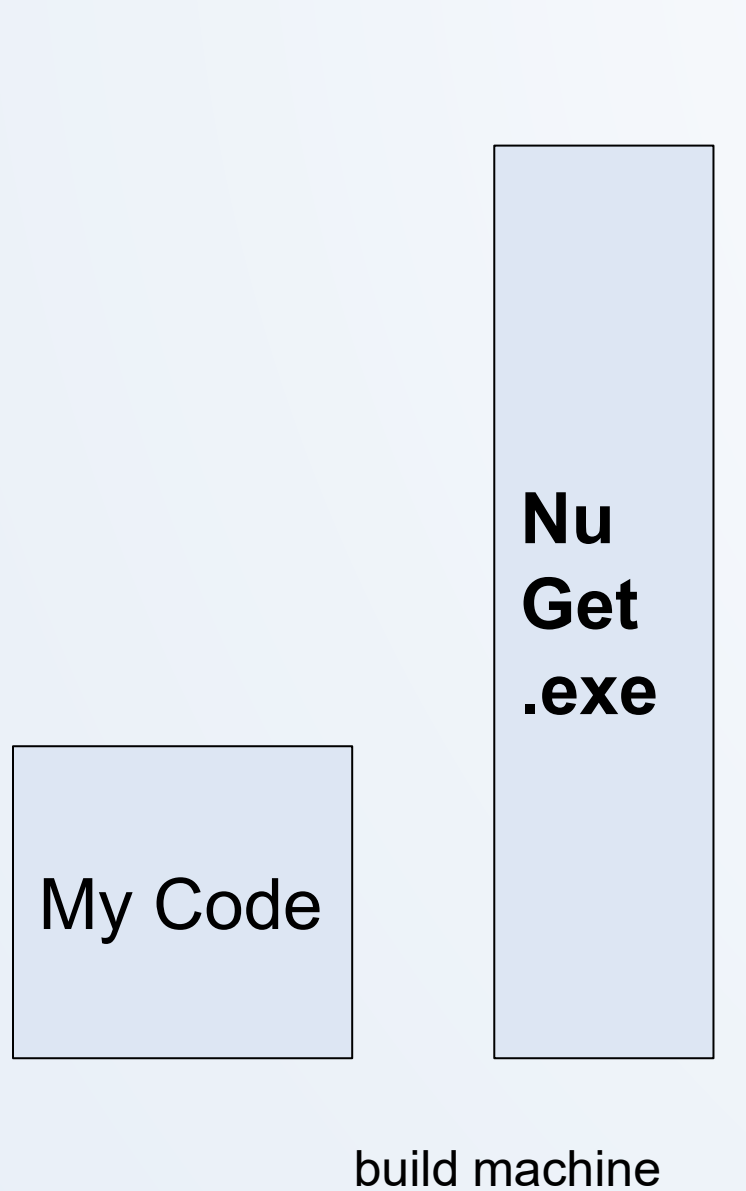
Who in this room...

... uses both public (nuget.org) and private
package sources?

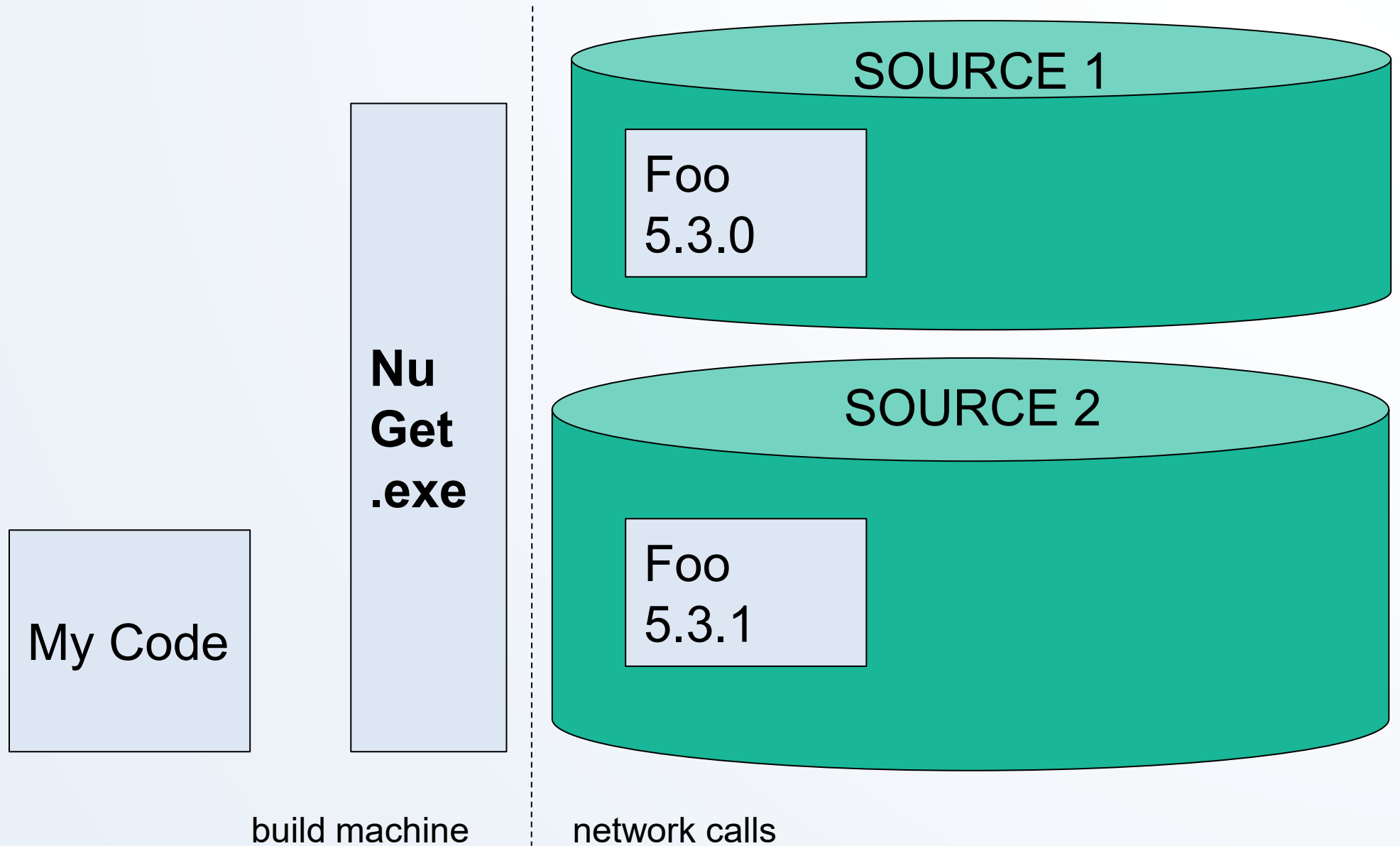
(6) NuGet Package Resolution



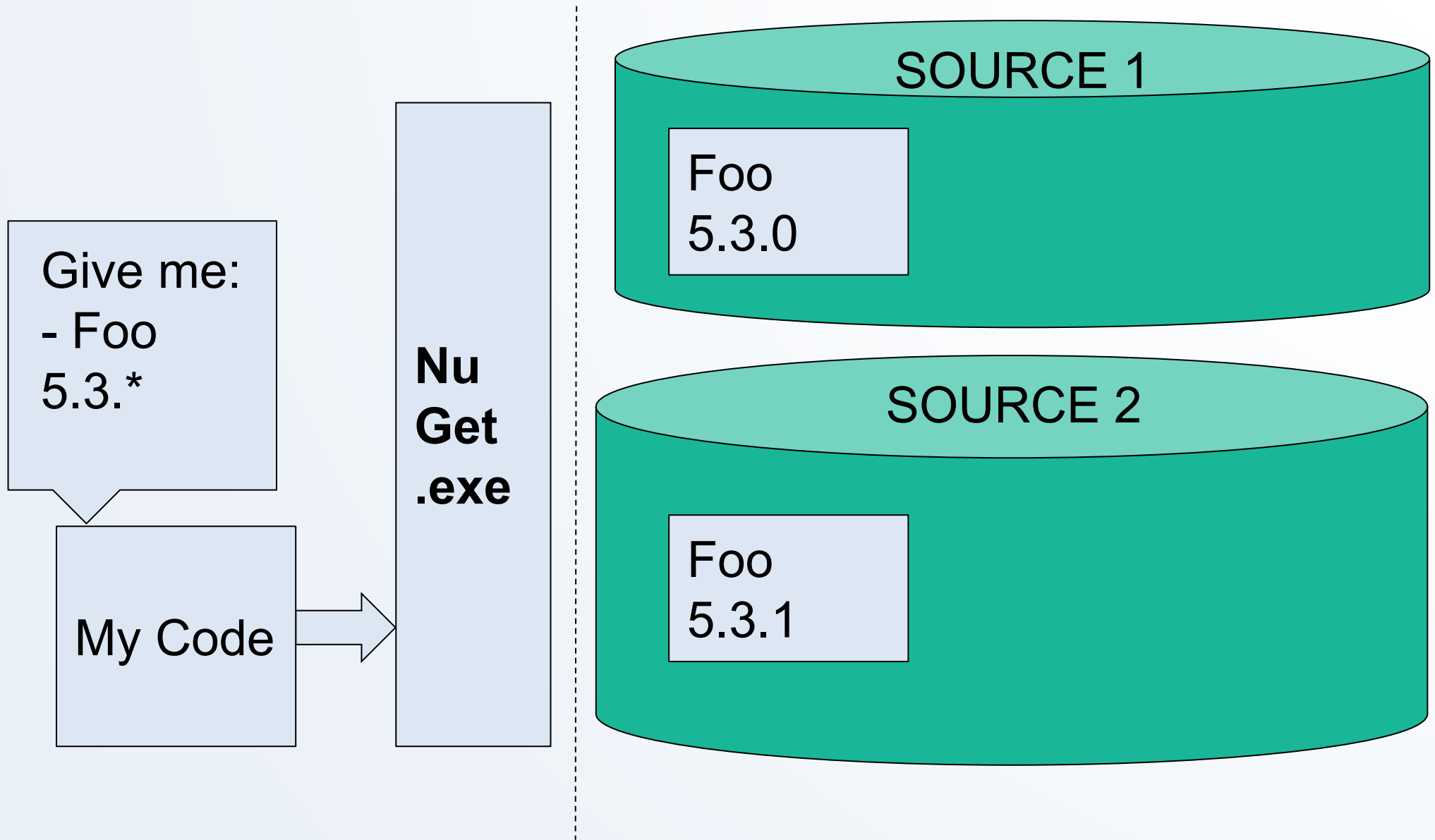
(6) NuGet Package Resolution



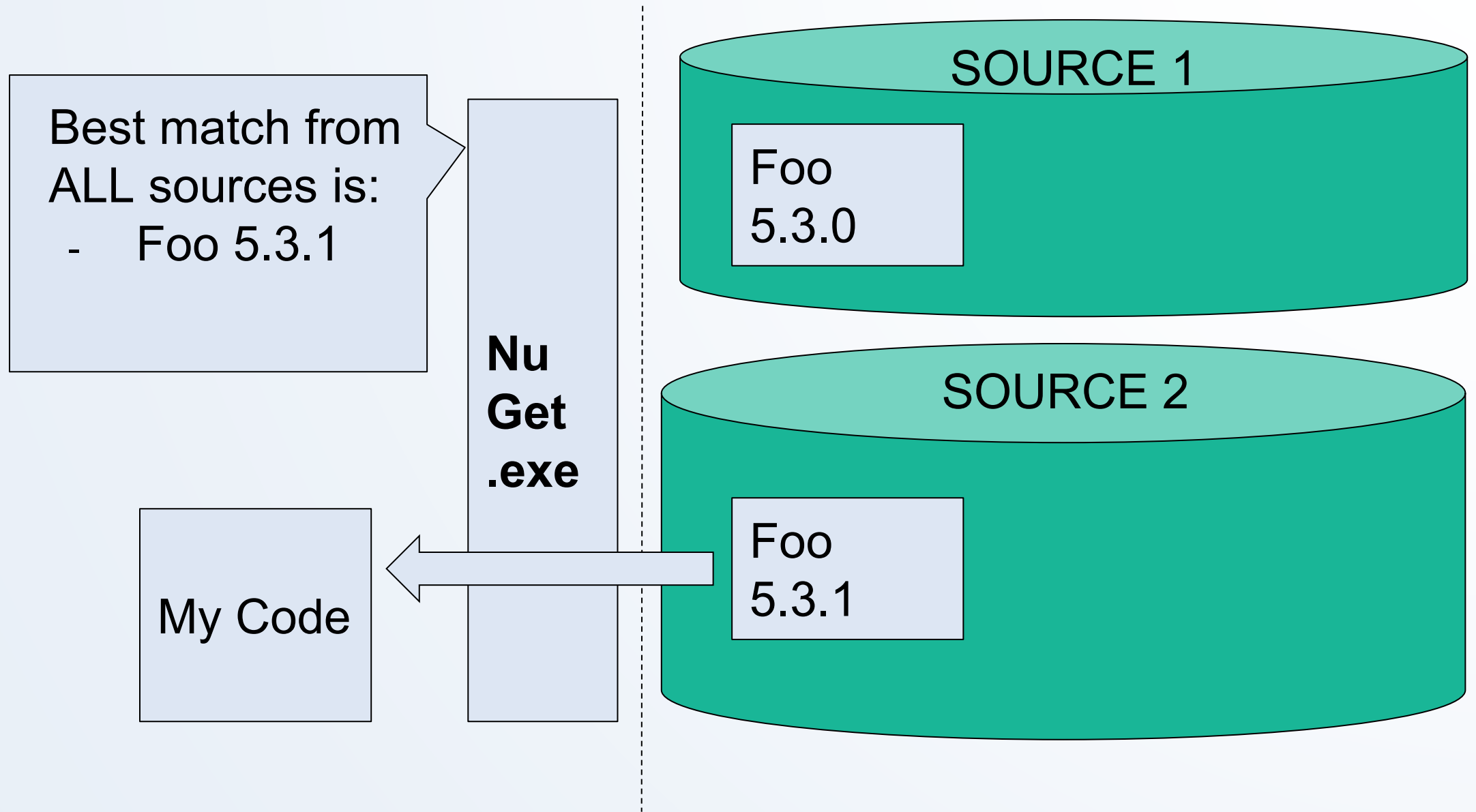
(6) NuGet Package Resolution



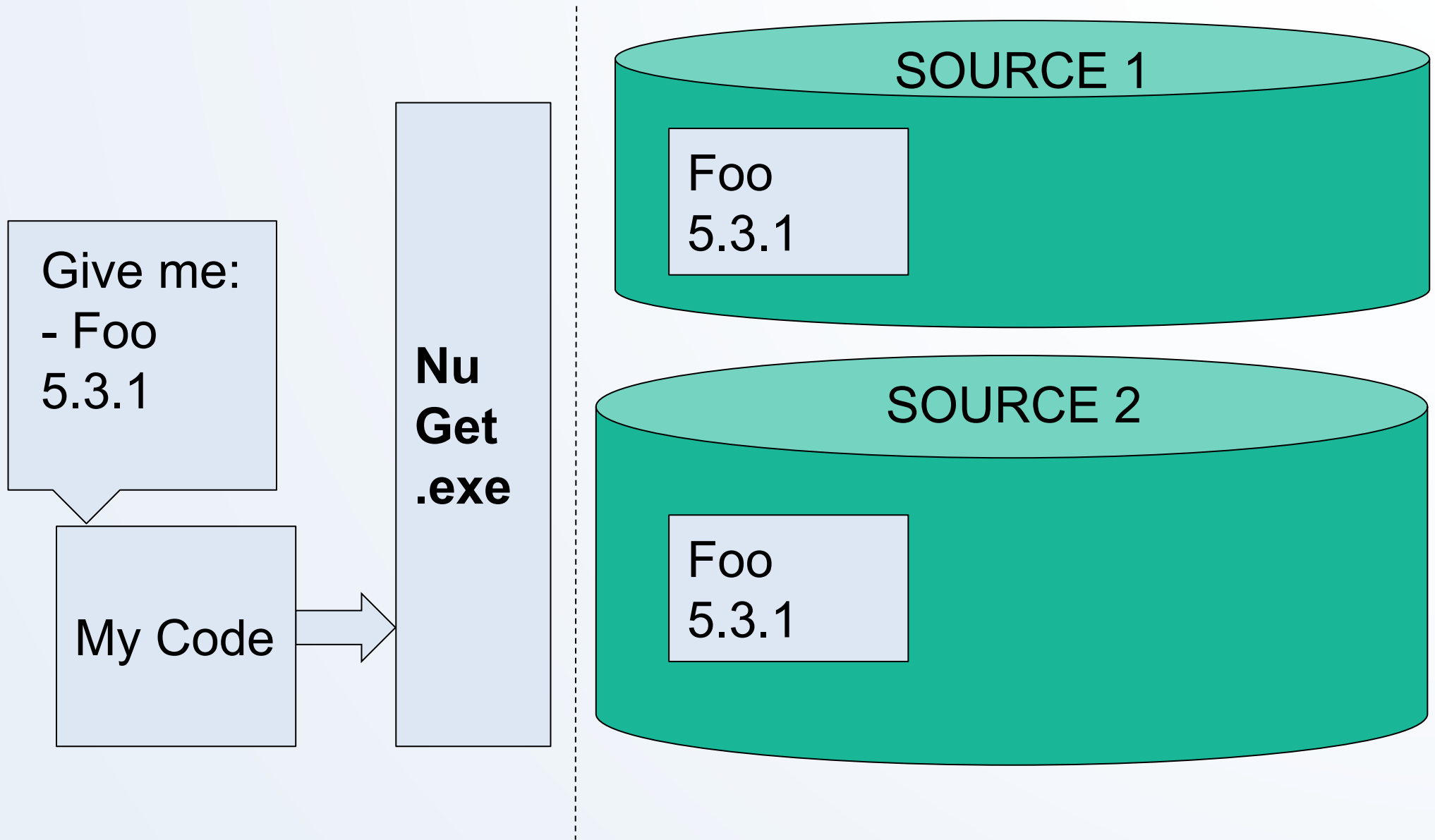
(6) NuGet Package Resolution



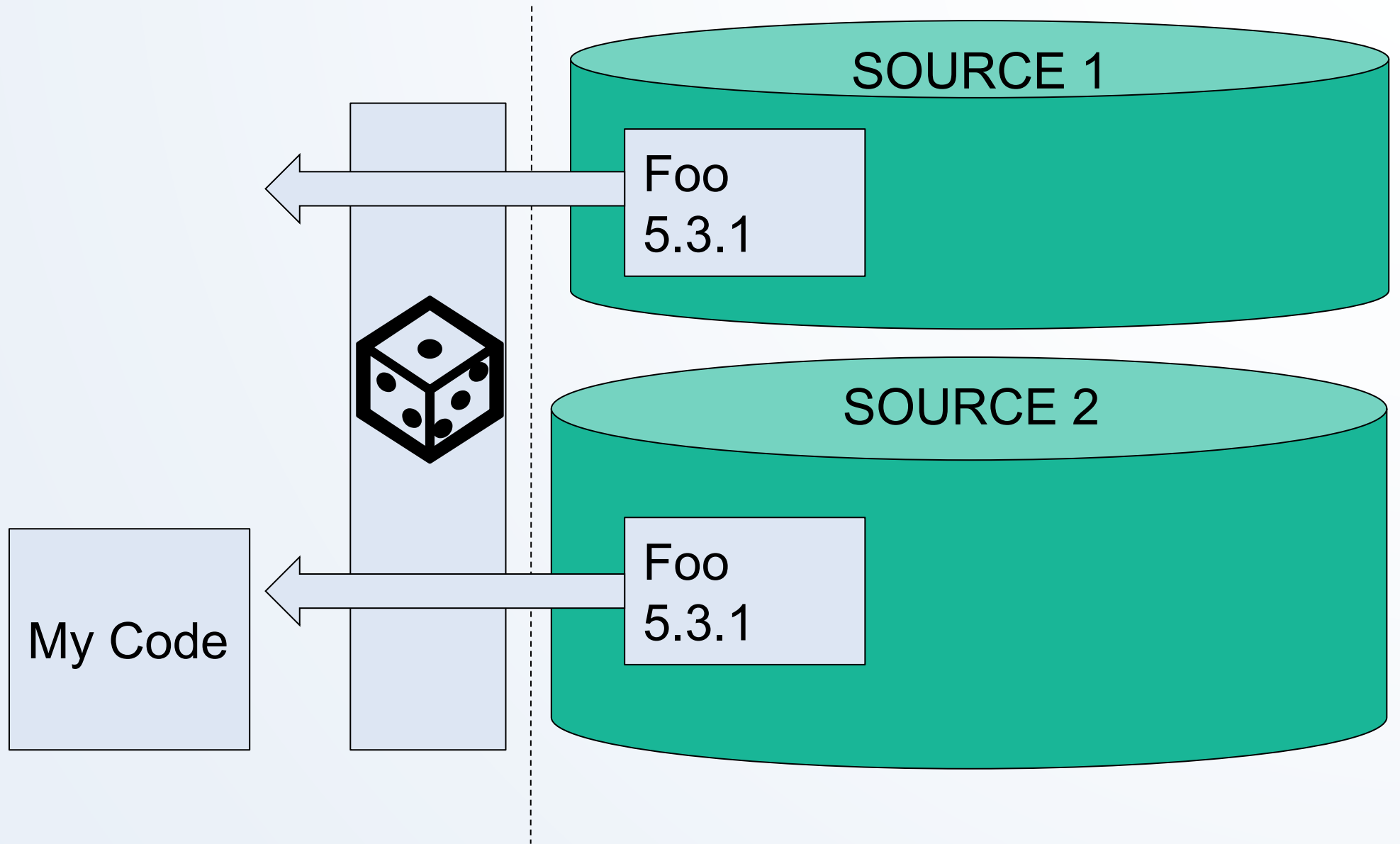
(6) NuGet Package Resolution



(6) NuGet Package Resolution



(6) NuGet Package Resolution



Agenda

1. Remember SolarWinds
2. Refresh NuGet concepts
3. **How to attack**
4. How to defend

Attacks



Mr. Evil Hacker

Attacks

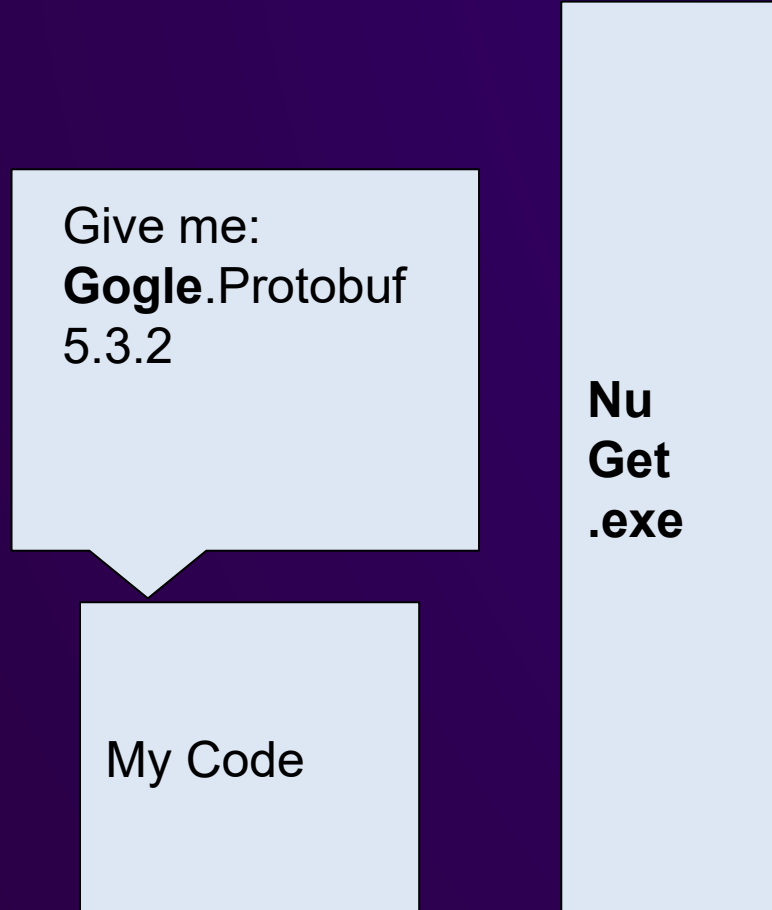
Typosquatting

Dependency confusion

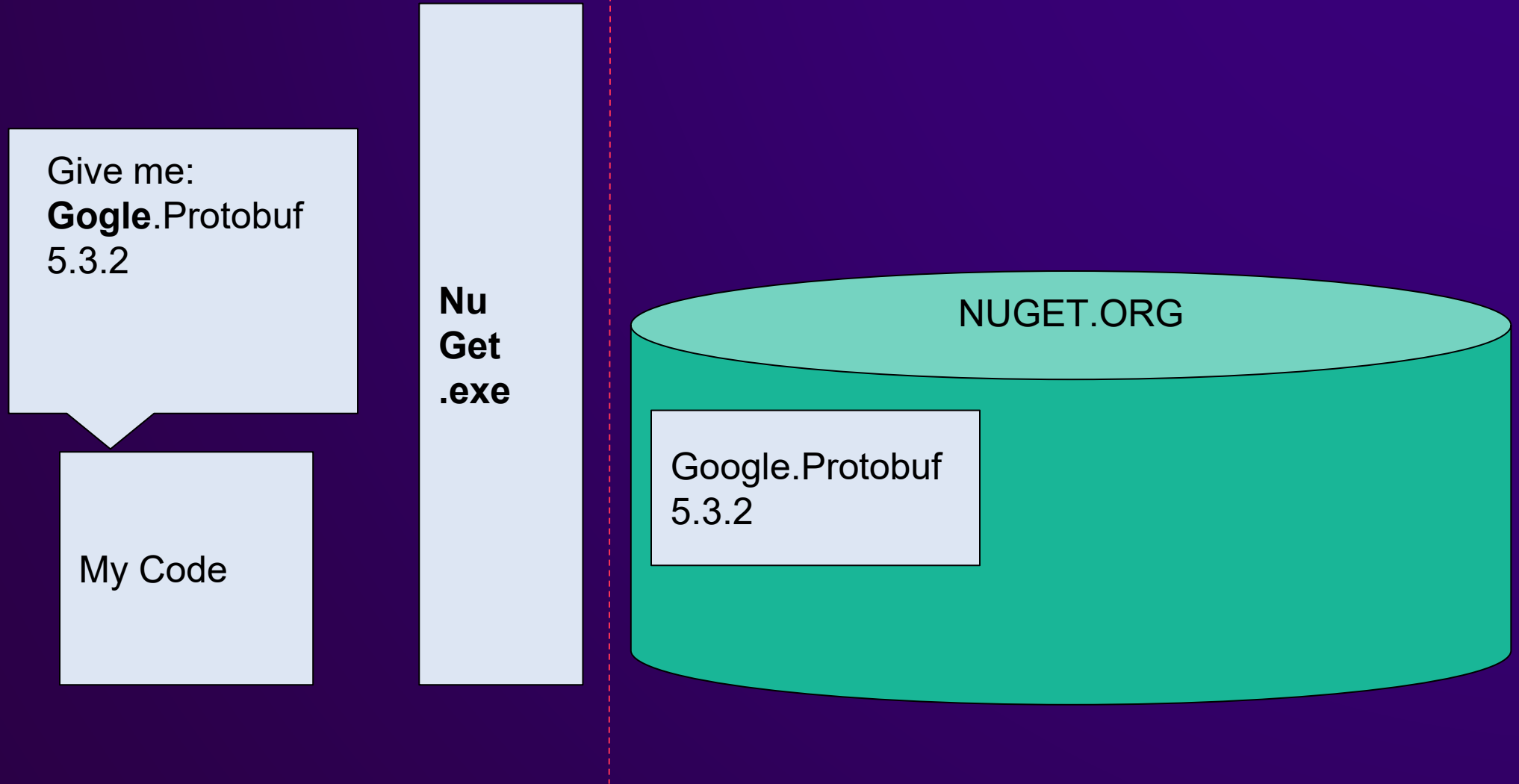
Typosquatting

To err is human

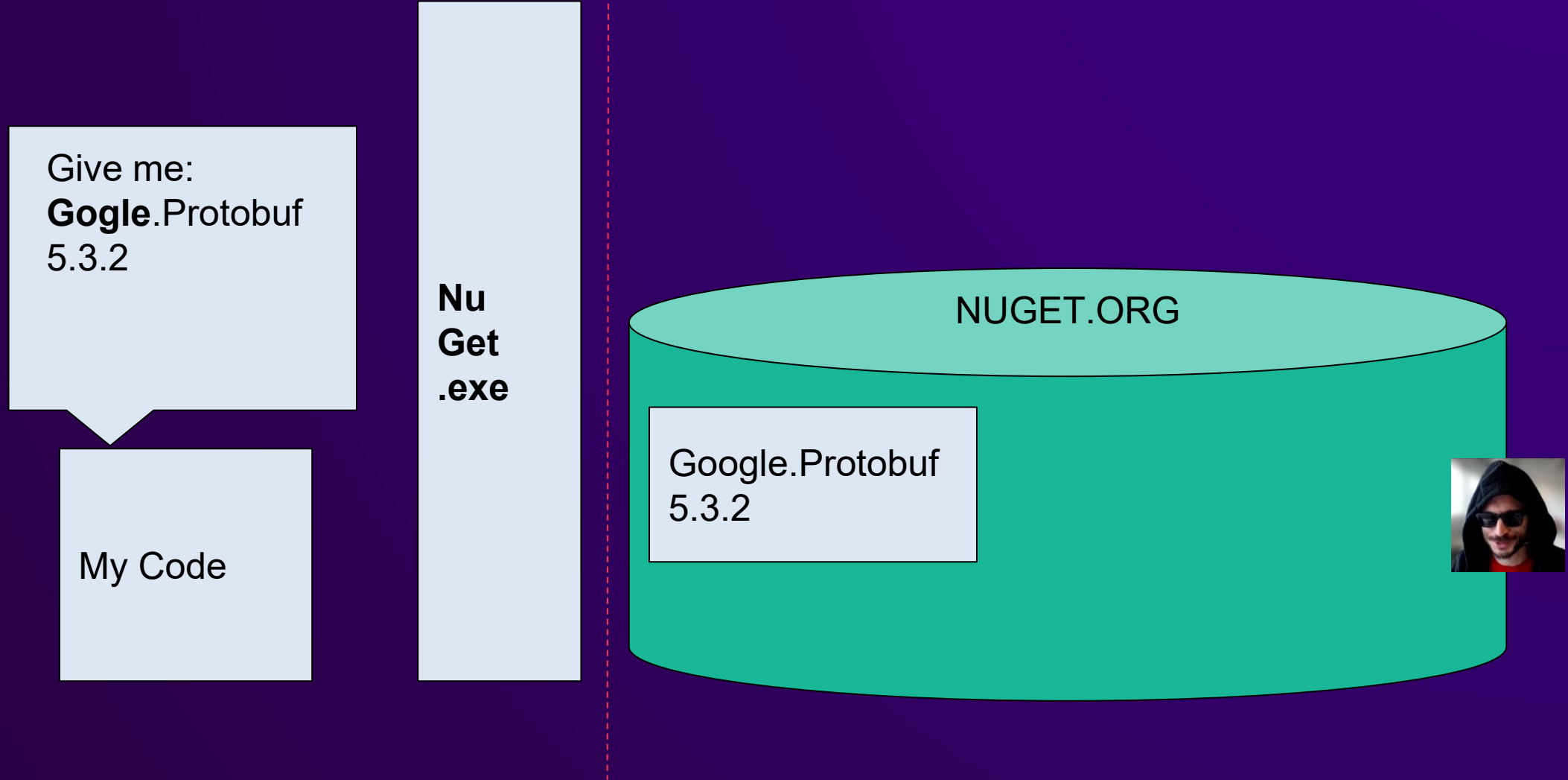
Typosquatting



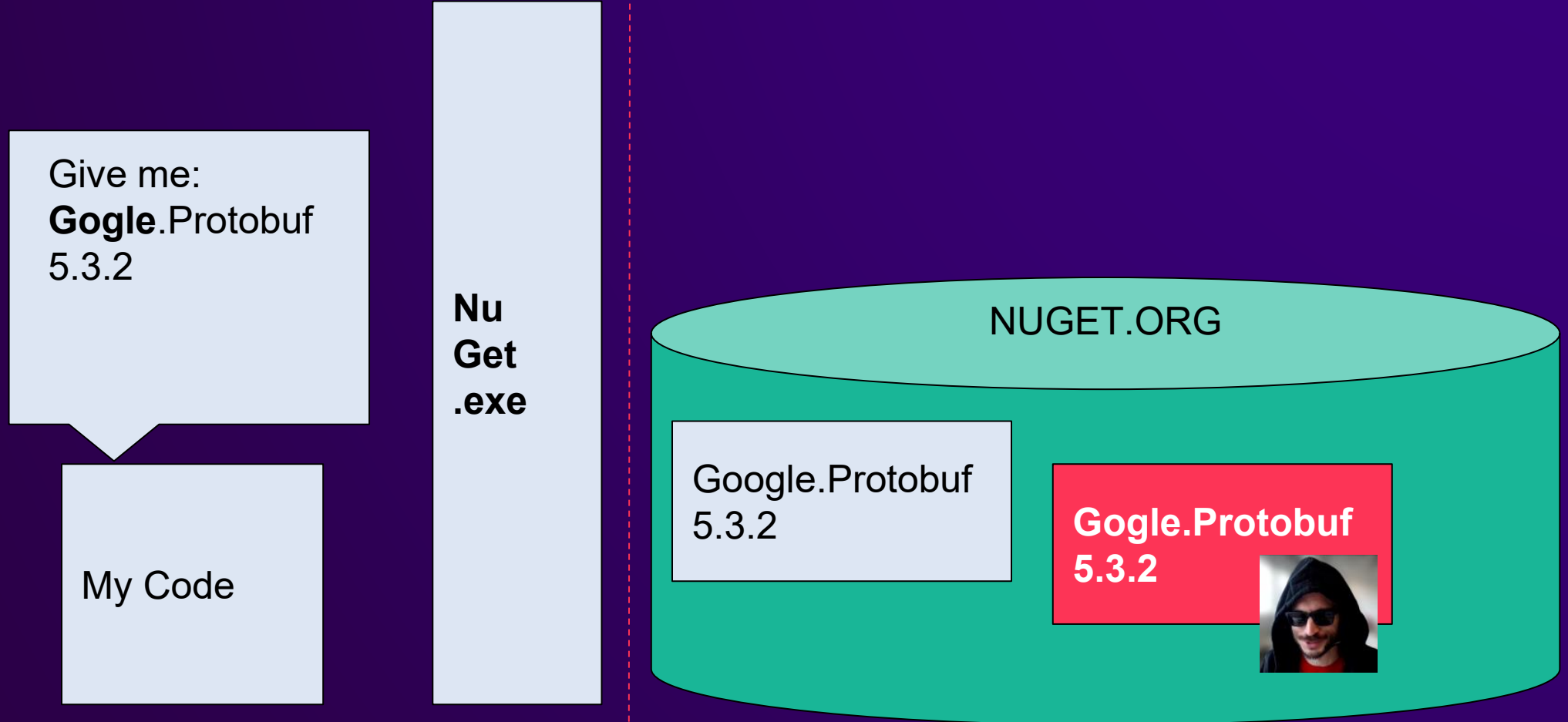
Typosquatting



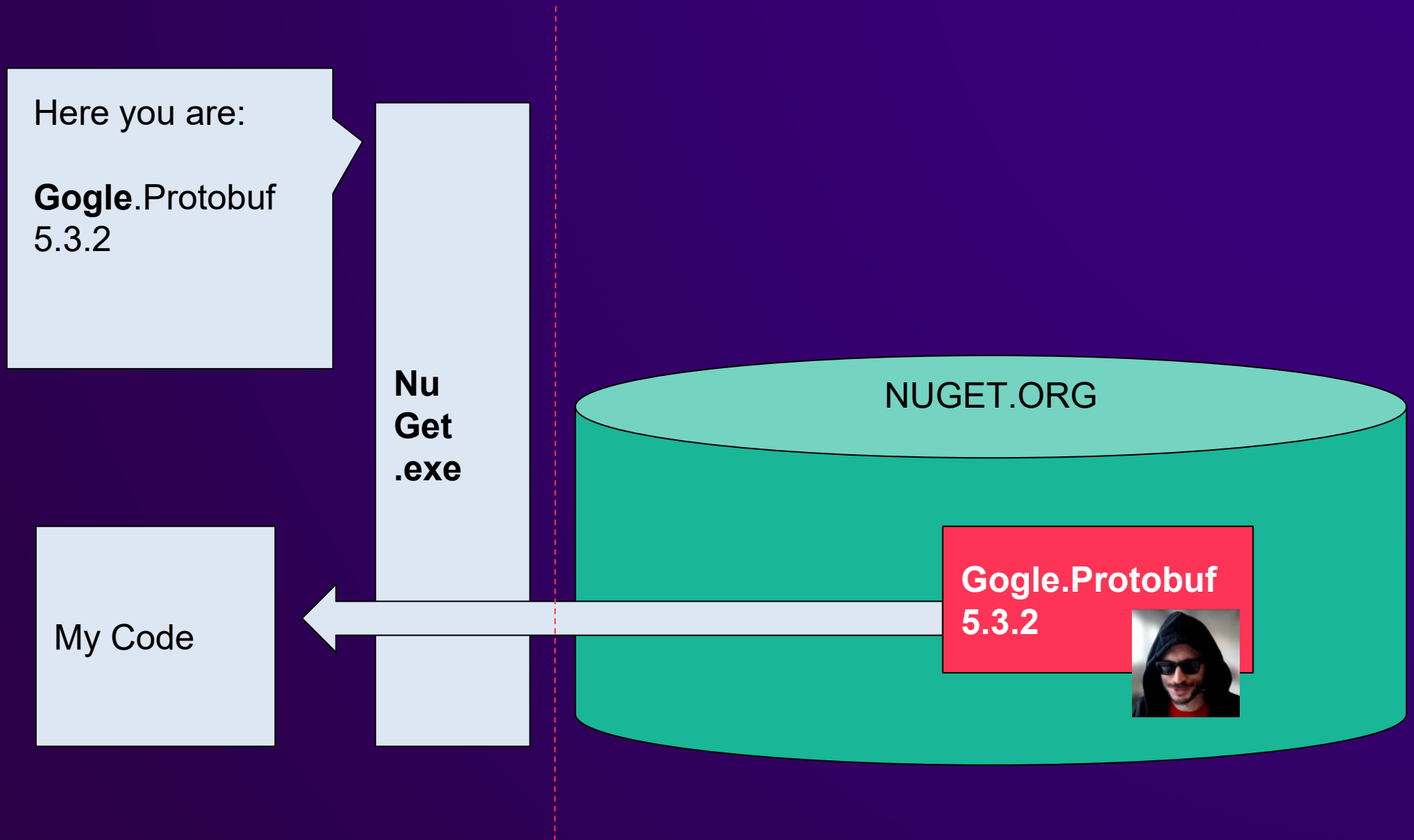
Typosquatting



Typosquatting



Typosquatting



Demo 0

Typosquatting

[2016] NPM and PyPi

17K infected PCs

50% admin

Typosquatting

[2022] NPM IconBurst malwares

27K downloads

Form data exfiltration

Typosquatting

← → ↻ 🔒 nuget.org/packages/Gogle.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...

Gogle.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**

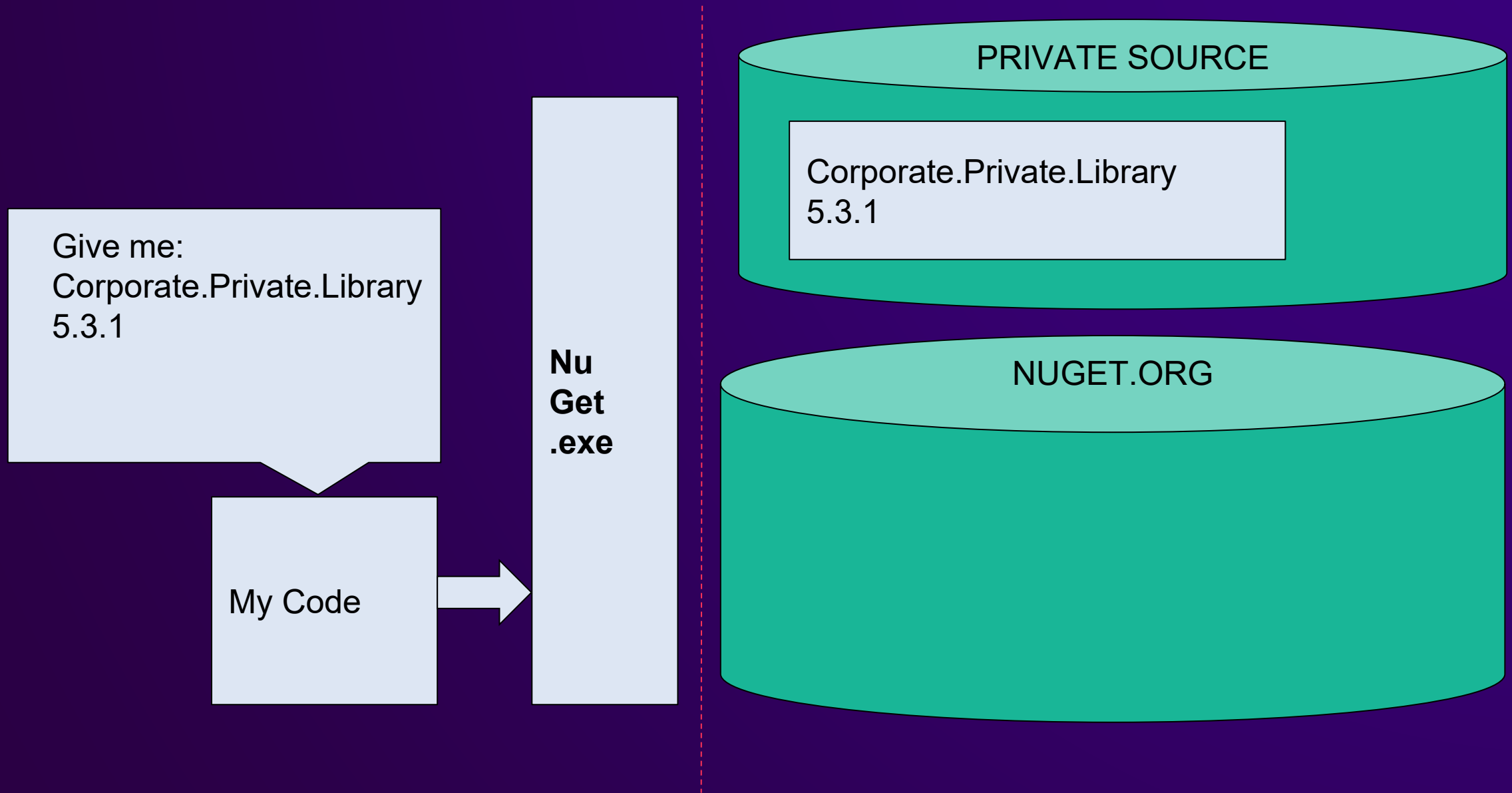
Per day average **1**

About

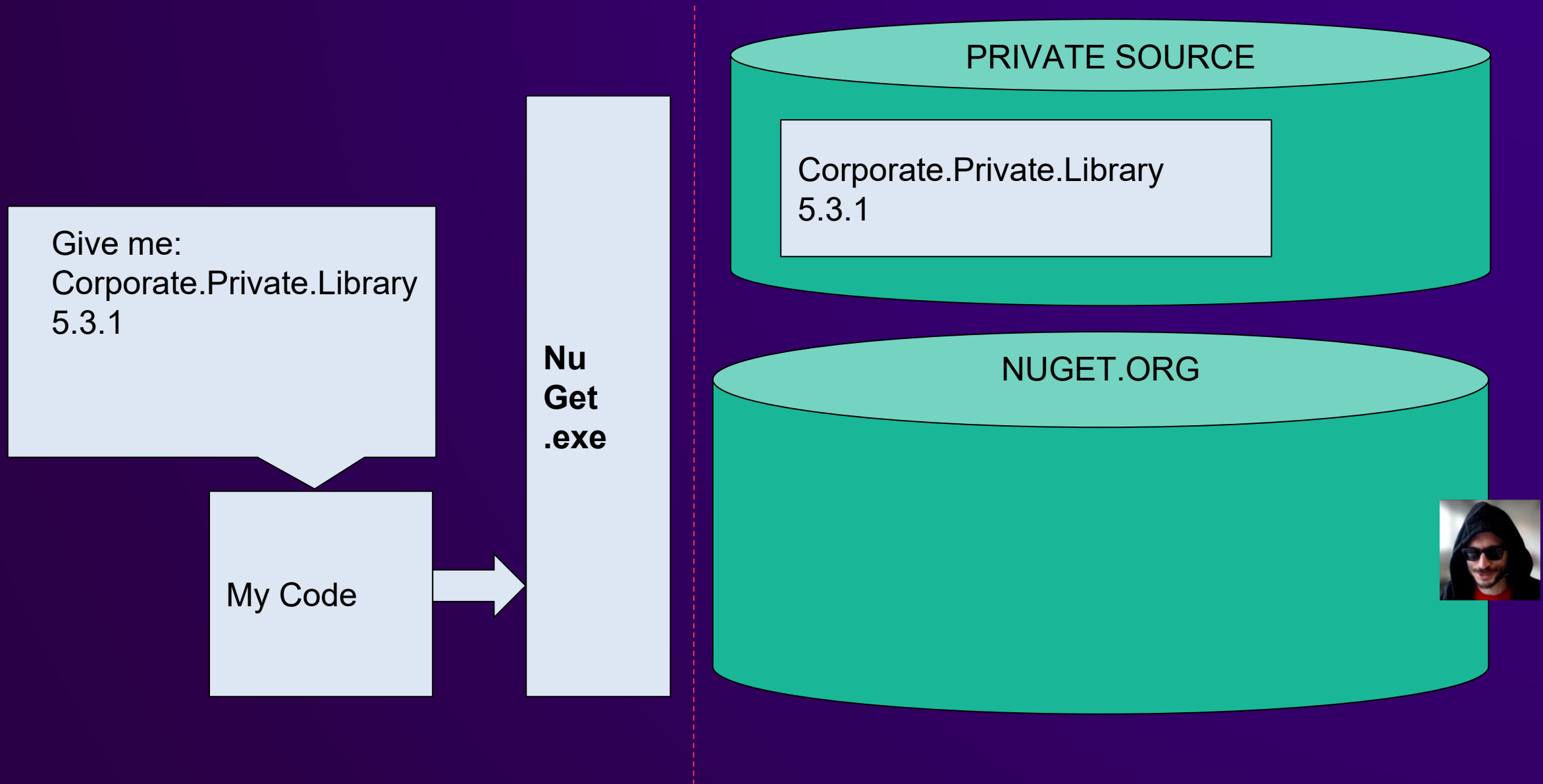
⌚ Last updated 9 months ago

Dependency confusion

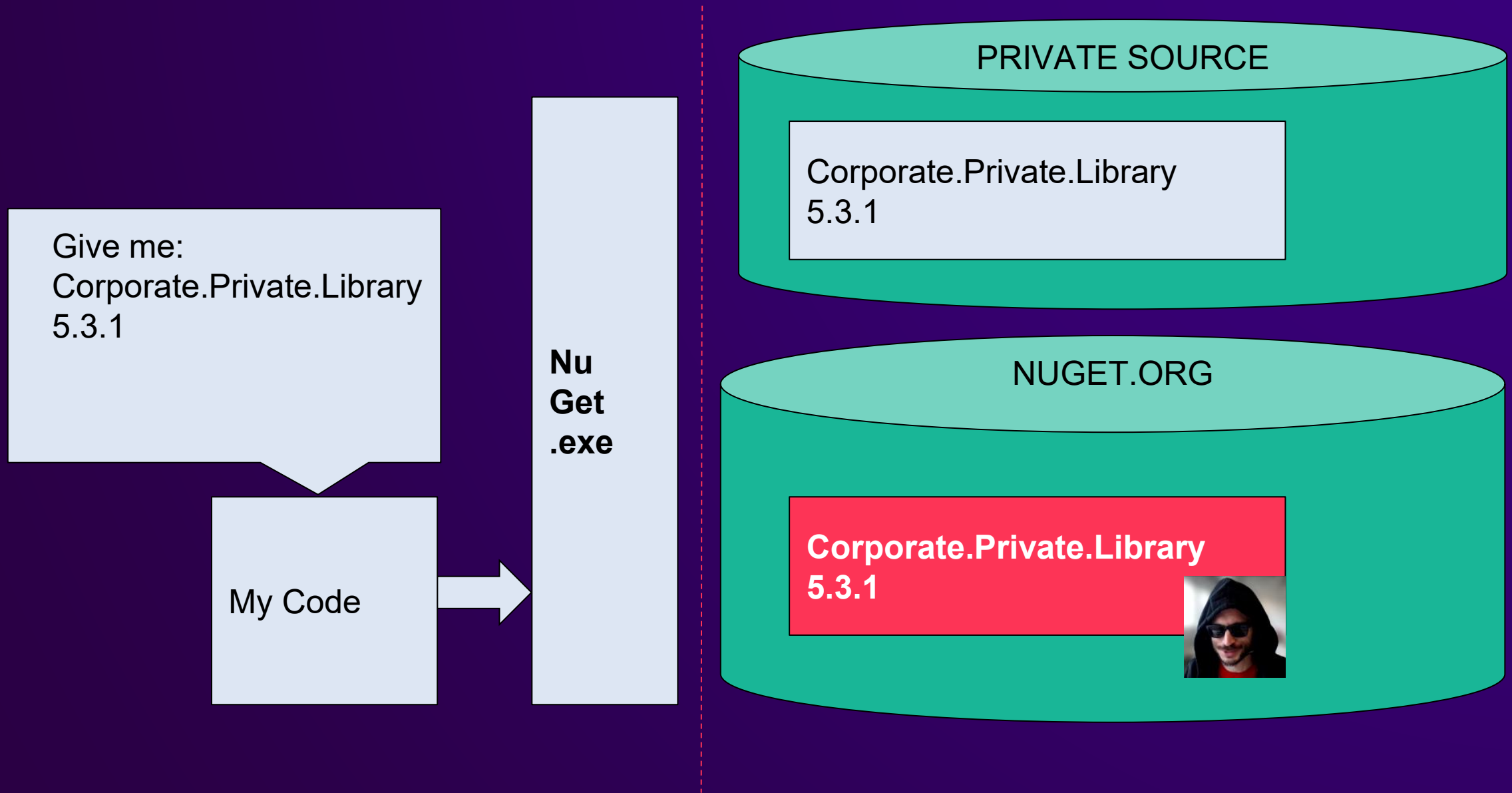
Dependency confusion



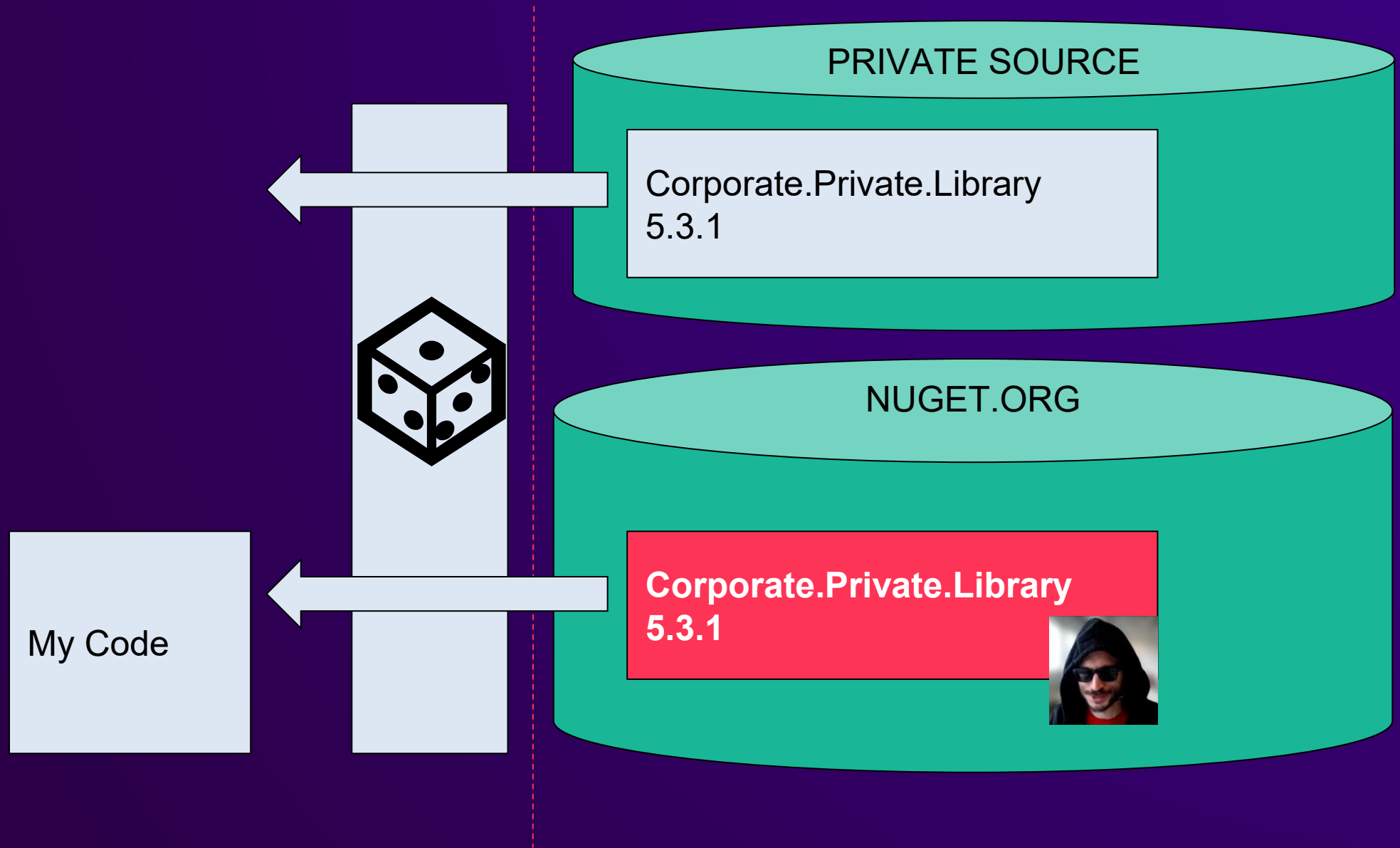
Dependency confusion



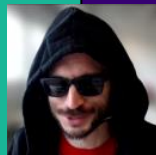
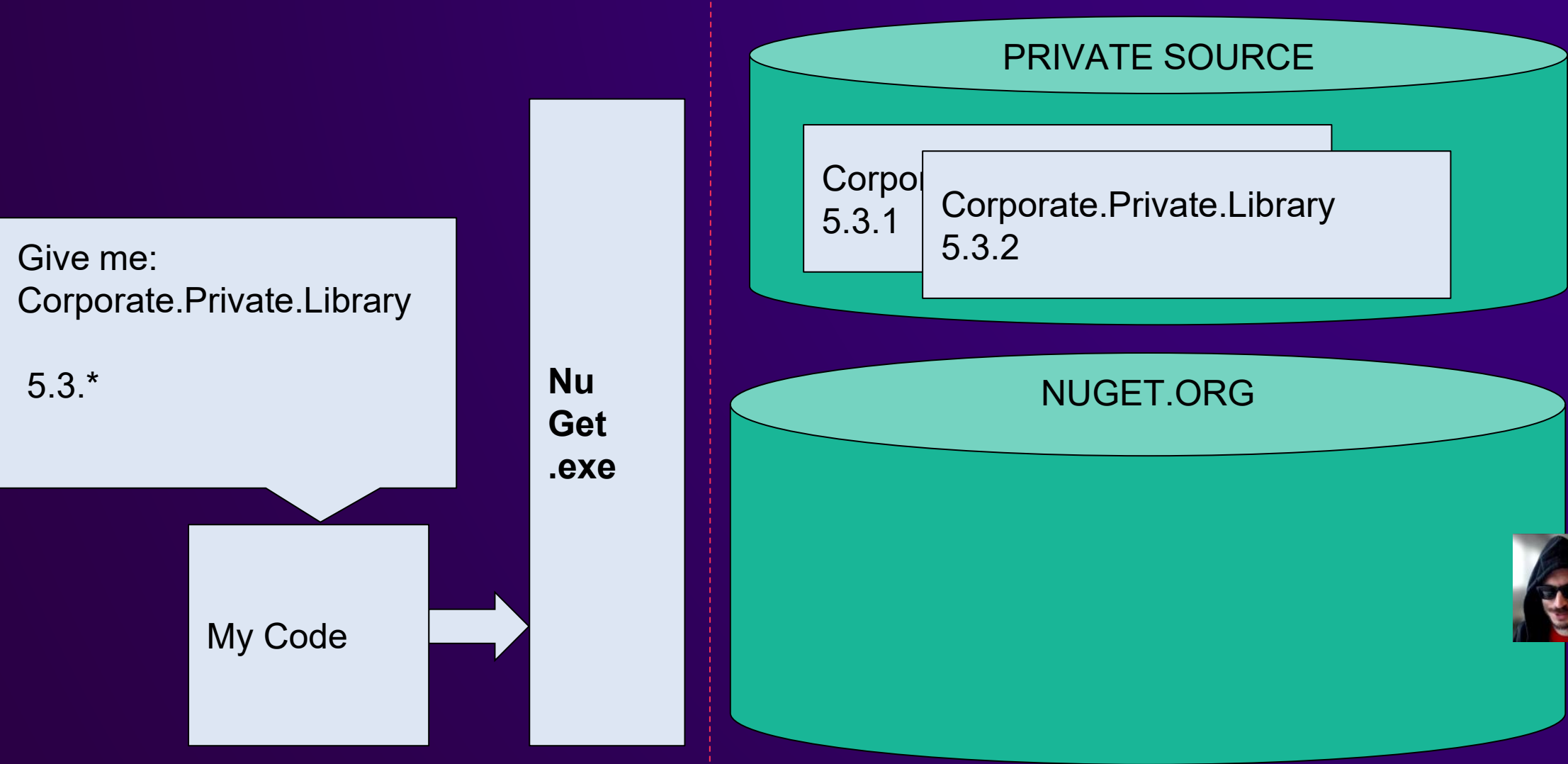
Dependency confusion



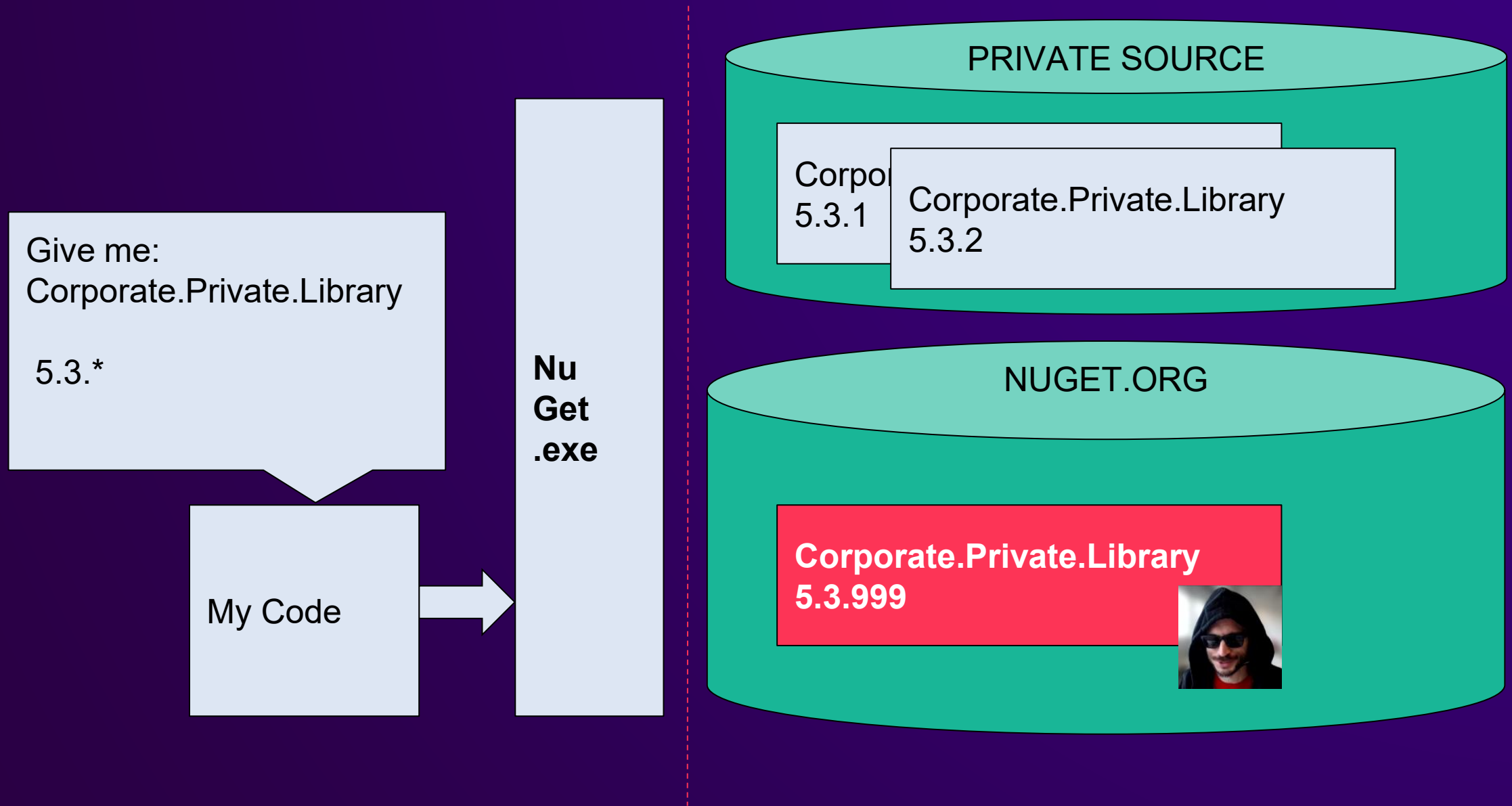
Dependency confusion



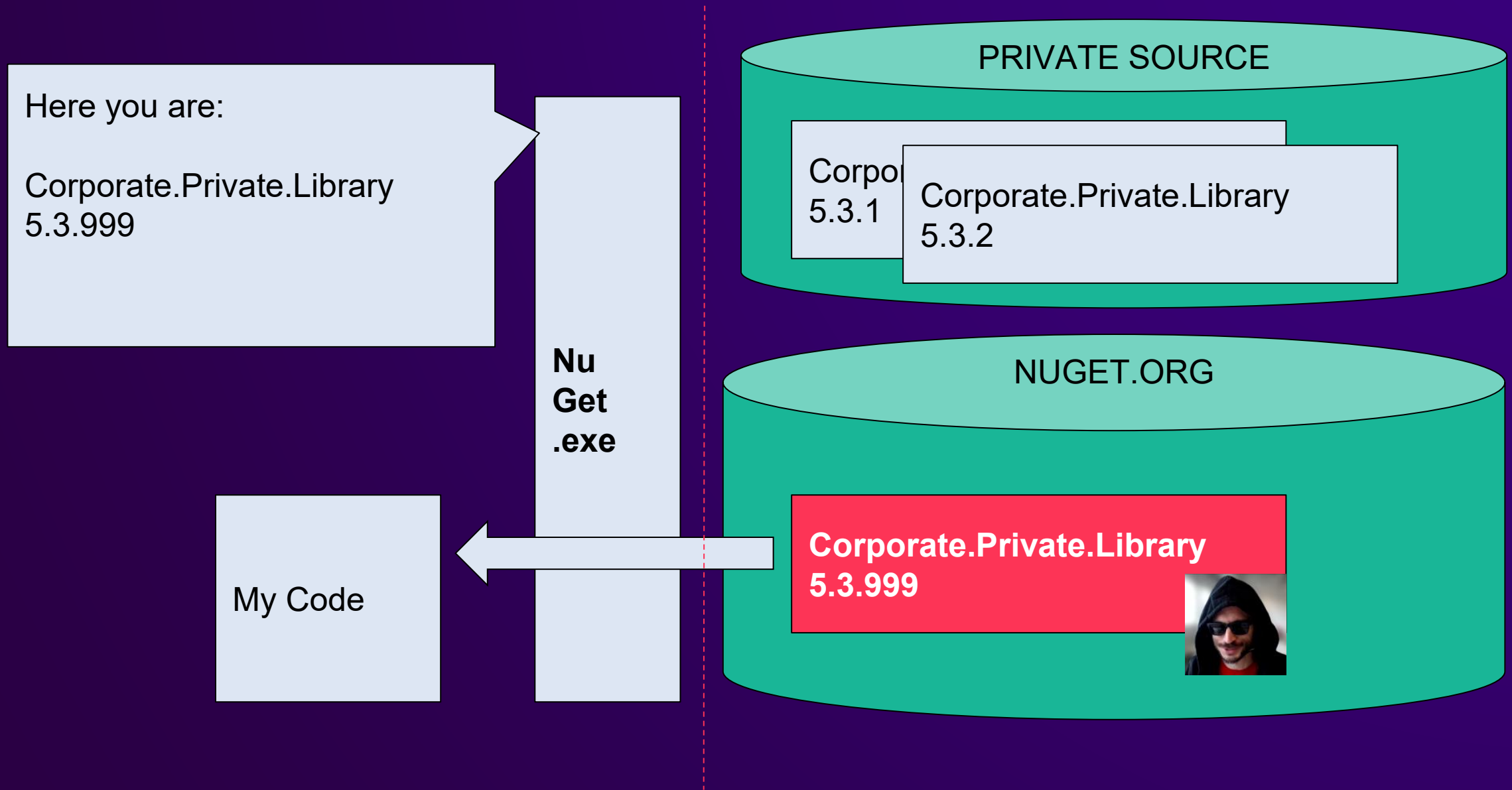
Dependency confusion



Dependency confusion



Dependency confusion



Demo 1

Agenda

1. Remember SolarWinds
2. Refresh NuGet concepts
3. How to attack
4. How to defend

Vulnerable Configurations (1)

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <activePackageSource>
    <add key="NuGet.org"
          value="https://api.nuget.org/v3/index.json" />
  </activePackageSource>
</configuration>
```

Vulnerable Configurations (2)

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <activePackageSource>
    <add key="NuGet.org"
          value="https://api.nuget.org/v3/index.json" />
    <add key="MyPrivateRepo"
          value="https://MyPrivateRepo/nuget" />
  </activePackageSource>
</configuration>
```

How to defend

As a consumer

Who in this room...

... uses Package Source Mapping?

Package Source Mapping

protects against dependency confusion

Demo 2

Package Source Mapping

Required for Central Package
Management

Package Source Mapping

PackageSourceMapper

<trustedSigners>

protect against typosquatting

<trustedSigners>

repository certificate

accepted <owners>

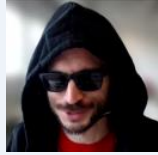
<owner> certificate

Demo 3

<clear>

avoid unexpected behavior

Do not let



win!

1. Package Source Mapping
2. `<trustedSigners>`

How to defend

As a publisher

Reserve Prefix

public

packages name prefix

private

Reserve Prefix

SonarSource - reserve ID prefixes for nuget.org

External



Fri, Jun 11, 2021, 6:31 PM



Andrei Epure <andrei.epure@sonarsource.com>

to account, Dotnet ▾

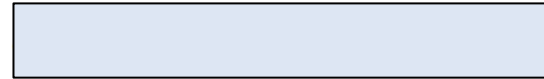
Hello,

We would like to reserve the following two package prefixes for the SonarSource owner [0]:

- "SonarAnalyzer" - it is used by our two Roslyn analyzers: SonarAnalyzer.CSharp [1] and SonarAnalyzer.VisualBasic [2]
- "SonarSource" - it contains our company's name and could be used by attackers in phishing campaigns

Please find below our self-evaluation:

Reserve Prefix



@microsoft.com>

to nuget.org, Dotnet, me ▾

Hi,

I have reserved SonarAnalyzer* and SonarSource* for organization SonarSource.

Let me know if you have any questions or run into any issues!

Best,

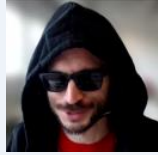
NuGet Admin

Sign Packages

<author> certificate validation

Demo 4

Do not let



win!

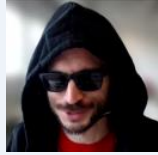
Reserve prefixes on nuget.org

public

packages

private

Do not let




win!


1. Package Source Mapping
2. <trustedSigners>
3. Reserve prefixes on nuget.org

Credits

Credits

In 2020, security researcher Alex Bîrsan  used *dependency confusion* to hack into:

Credits

In 2020, security researcher Alex Bîrsan  used *dependency confusion* to hack into:

- Microsoft
- Apple
- Shopify
- Paypal
- ... and another 31 big companies ...

Credits

In 2020, security researcher Alex Bîrsan  used

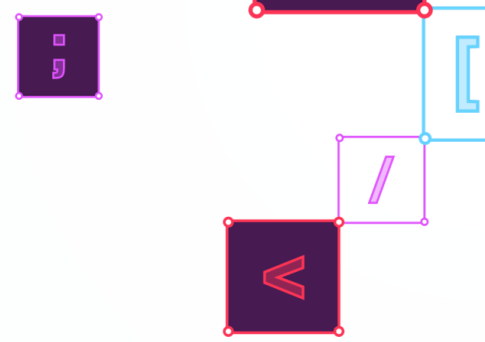
dependency confusion to hack into:

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

Bug
bounties

Goodie

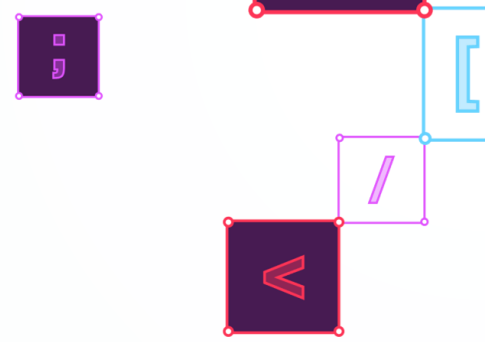
Screen wipe



Hiring

- .NET Developer Advocate
- .NET Ecosystem Product Manager

sonarsource.com/company/careers



FEEDBACK FORM + RESOURCES:

andreiepure.ro