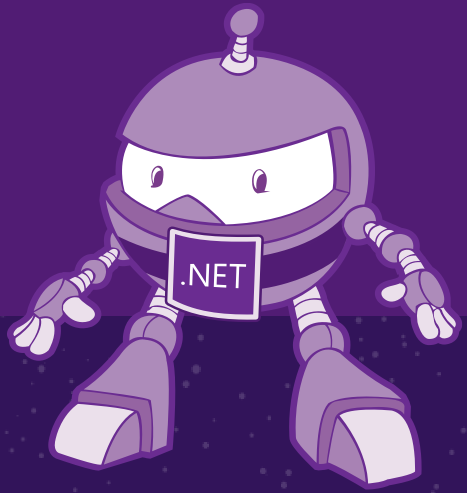
Secure your NuGet eco-system

Karan Nandwani
Program Manager, Microsoft
@karann9



Supply-chain attacks target package managers

.NET

Homebrew

TL;DR

- Attacker identified a GitHub personal access token with recently elevated scopes was leaked from Homebrew’s Jenkins that gave them access to git push on Homebrew/brew and Homebrew/homebrew-core.
- This could have let them modify formulae (packages) potentially placing a backdoor on any machine that installed it.

Takeaway

- Tools should be able to detect package tampering
- Tools should be able to identify the package’s real author

npm

TL;DR

- “ESLint” author account compromised
- Attacker published a malicious version that harvested credentials
- 4,500 account credentials leaked before package was taken down

Takeaway

- Username and password security is NOT enough

TL;DR

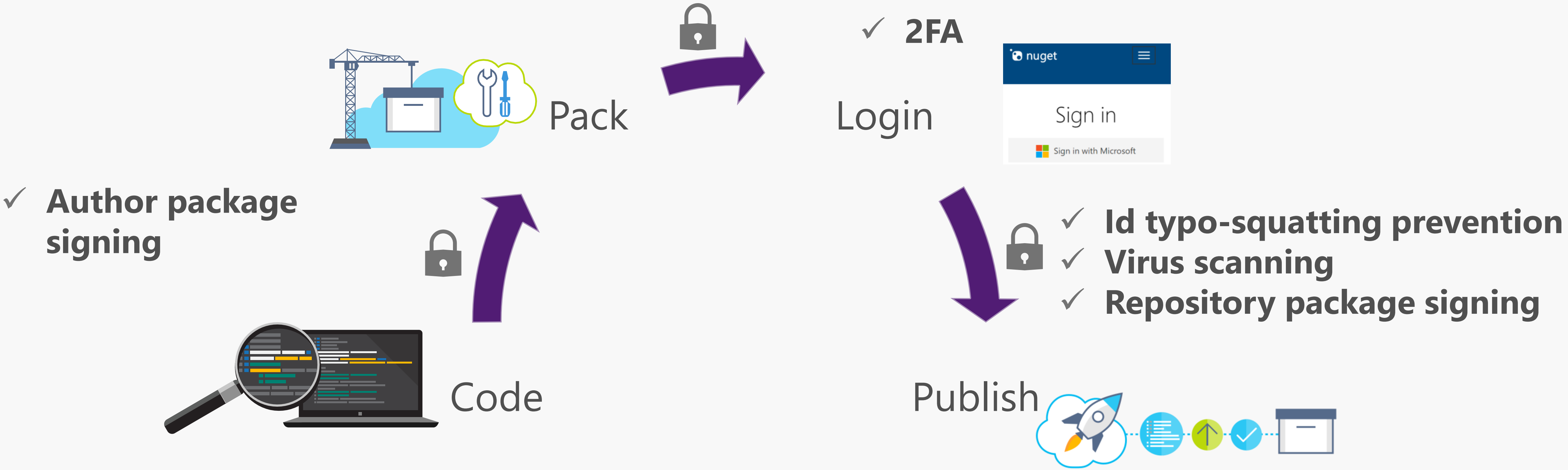
- Attacker published 38 similarly named packages to "cross-env", a package with over 2.5 million weekly downloads
- Malicious packages sent environment variables set on the victim's machine to a private server
- Attack went undetected for 2 weeks

Takeaway

- Repositories should protect against typo-squatting
- Users should be able to define which publishers to trust

NuGet Workflow and Best practices

.NET



✓ **Author package signing**

Code

Pack

✓ **2FA**

Login

nuget

Sign in

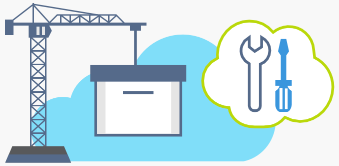
Sign in with Microsoft

✓ **Id typo-squatting prevention**
✓ **Virus scanning**
✓ **Repository package signing**

Publish

Code

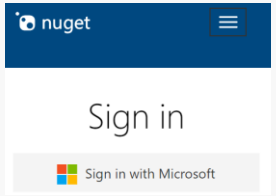
- ✓ **Author package signing**



Pack

Login

- ✓ **2FA**



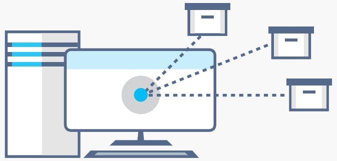
Sign in

Sign in with Microsoft

- ✓ **Id typo-squatting prevention**
- ✓ **Virus scanning**
- ✓ **Repository package signing**

Publish

Install



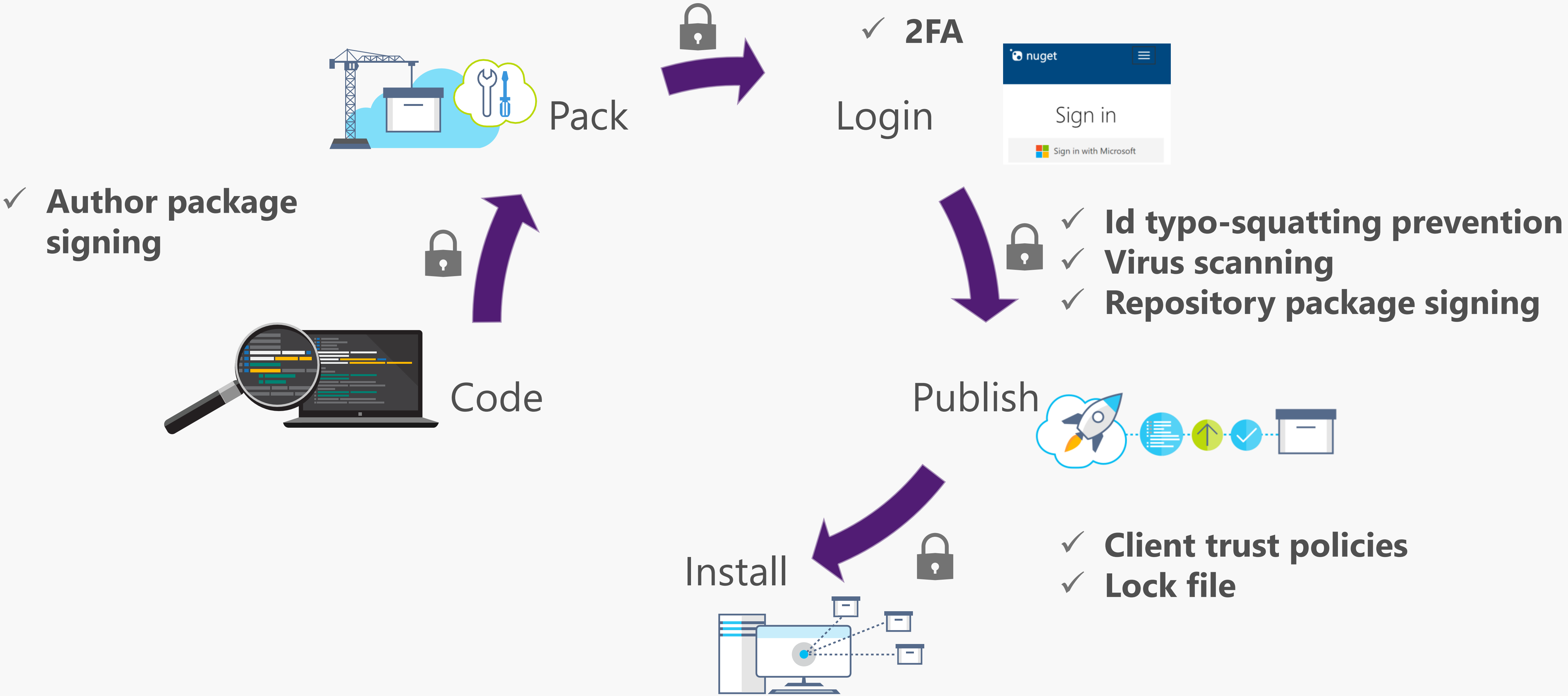
Client Trust policies

- Requires packages to be signed
- Trust package author
  - Author signed
  - Agnostic to package source
- Trust packages on NuGet.org owned by specific users/accounts
  - NuGet.org (repository) signed
  - Trust packages coming from a repository that supports repository signing

Demo – Client trust policies

Client Trust policies

- Define trusted Repositories, Publishers (NuGet.org), and Authors
- Author trust policies are independent of source repository
- Guarantees package authenticity and integrity



Code

✓ Author package signing

Pack

✓ 2FA

Login

nuget

Sign in

Sign in with Microsoft

✓ Id typo-squatting prevention

✓ Virus scanning

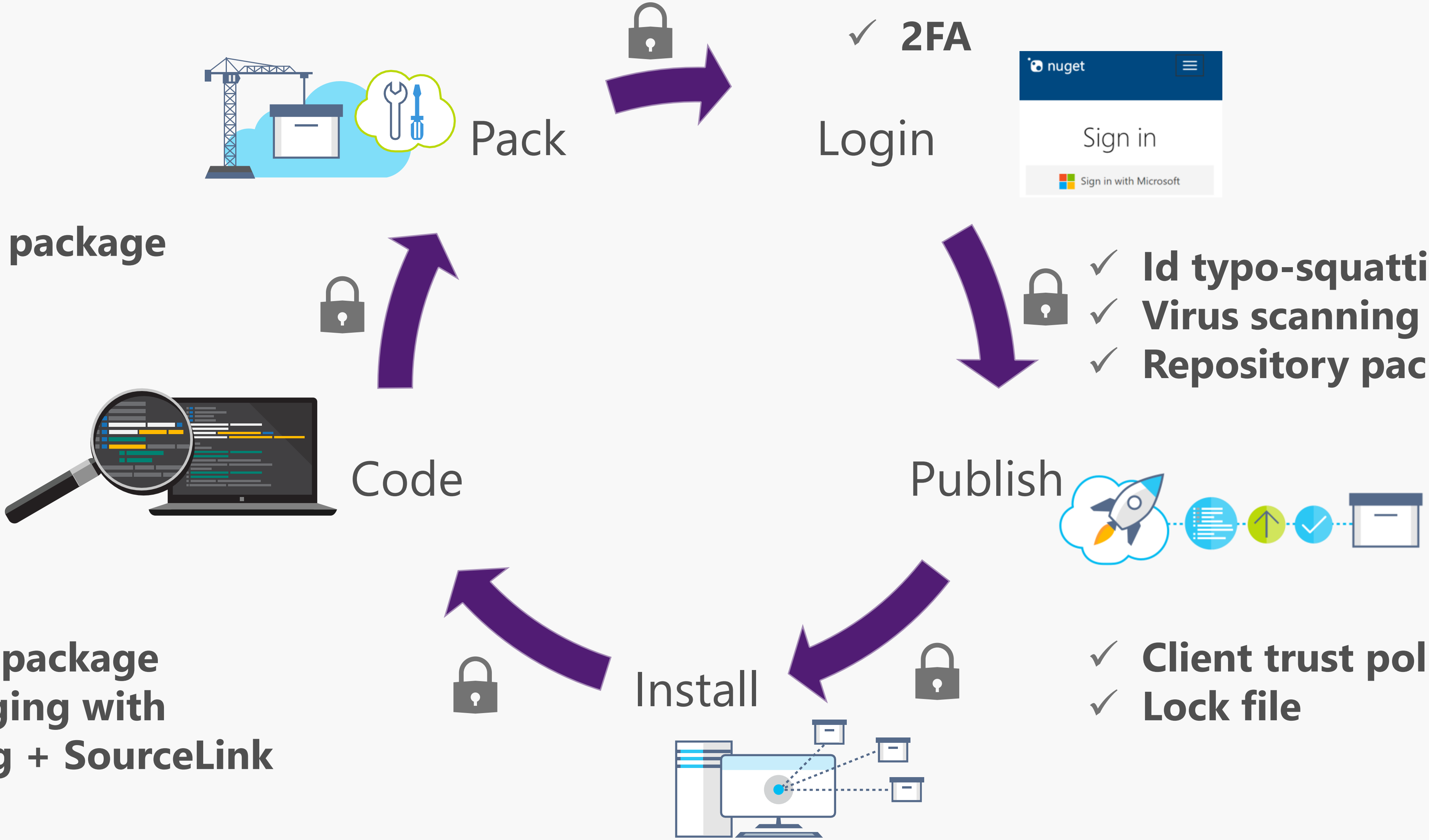
✓ Repository package signing

Publish

✓ Client trust policies

✓ Lock file

Install



- ✓ **2FA**

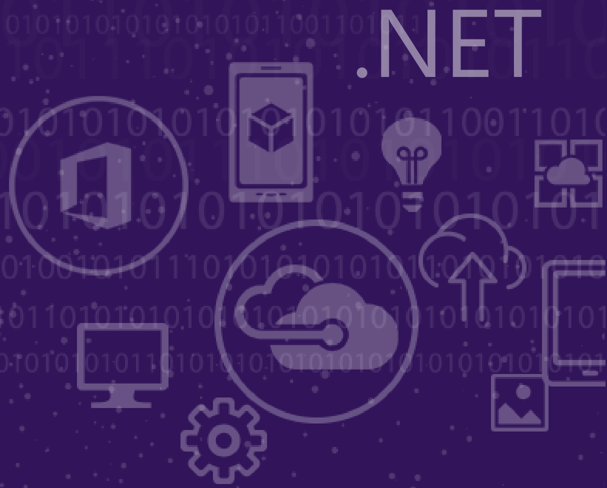
- ✓ **Id typo-squatting prevention**
- ✓ **Virus scanning**
- ✓ **Repository package signing**

- ✓ **Client trust policies**
- ✓ **Lock file**

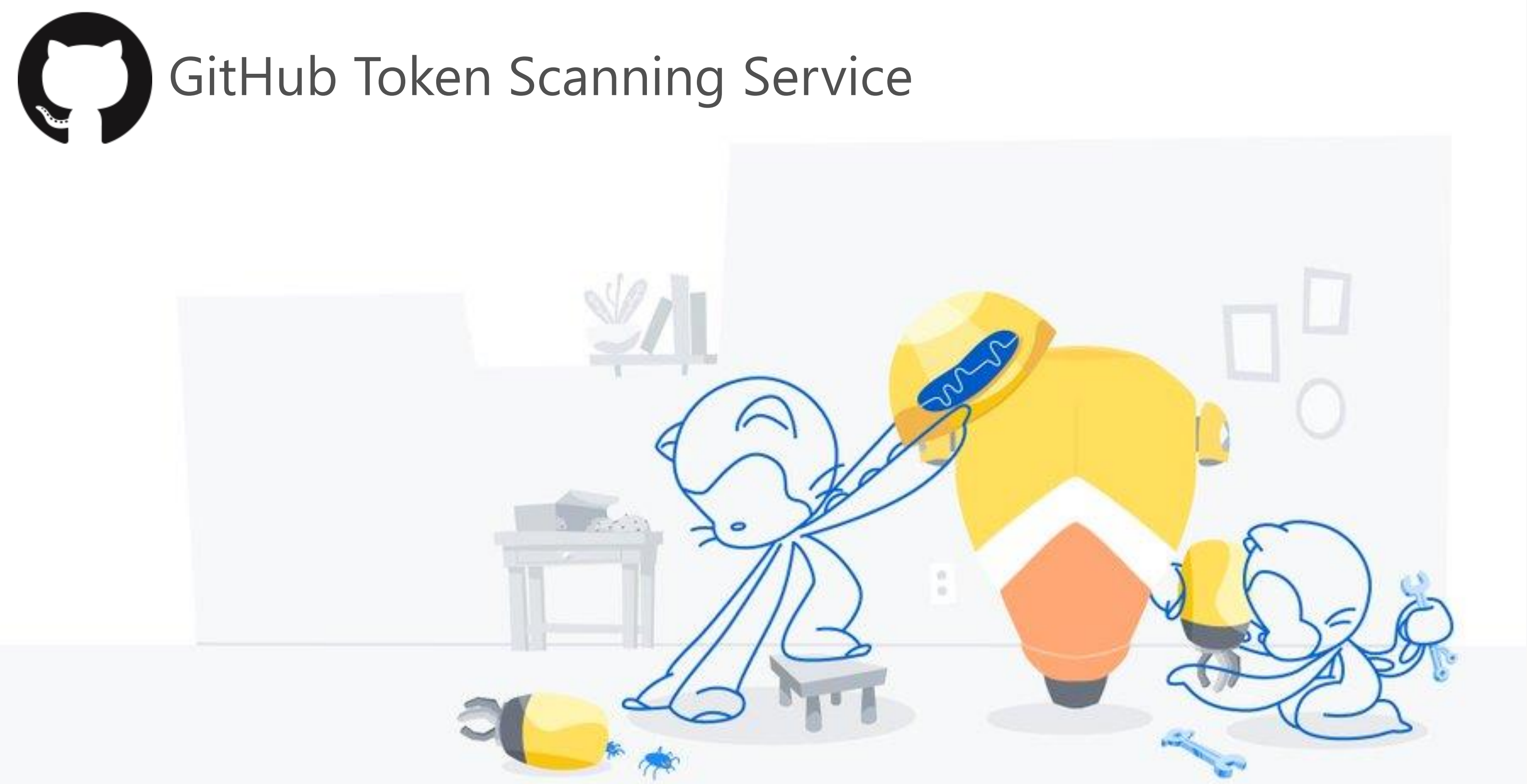
- ✓ **Author package signing**

- ✓ **Secure package debugging with .snupkg + SourceLink**

Sneak Peek

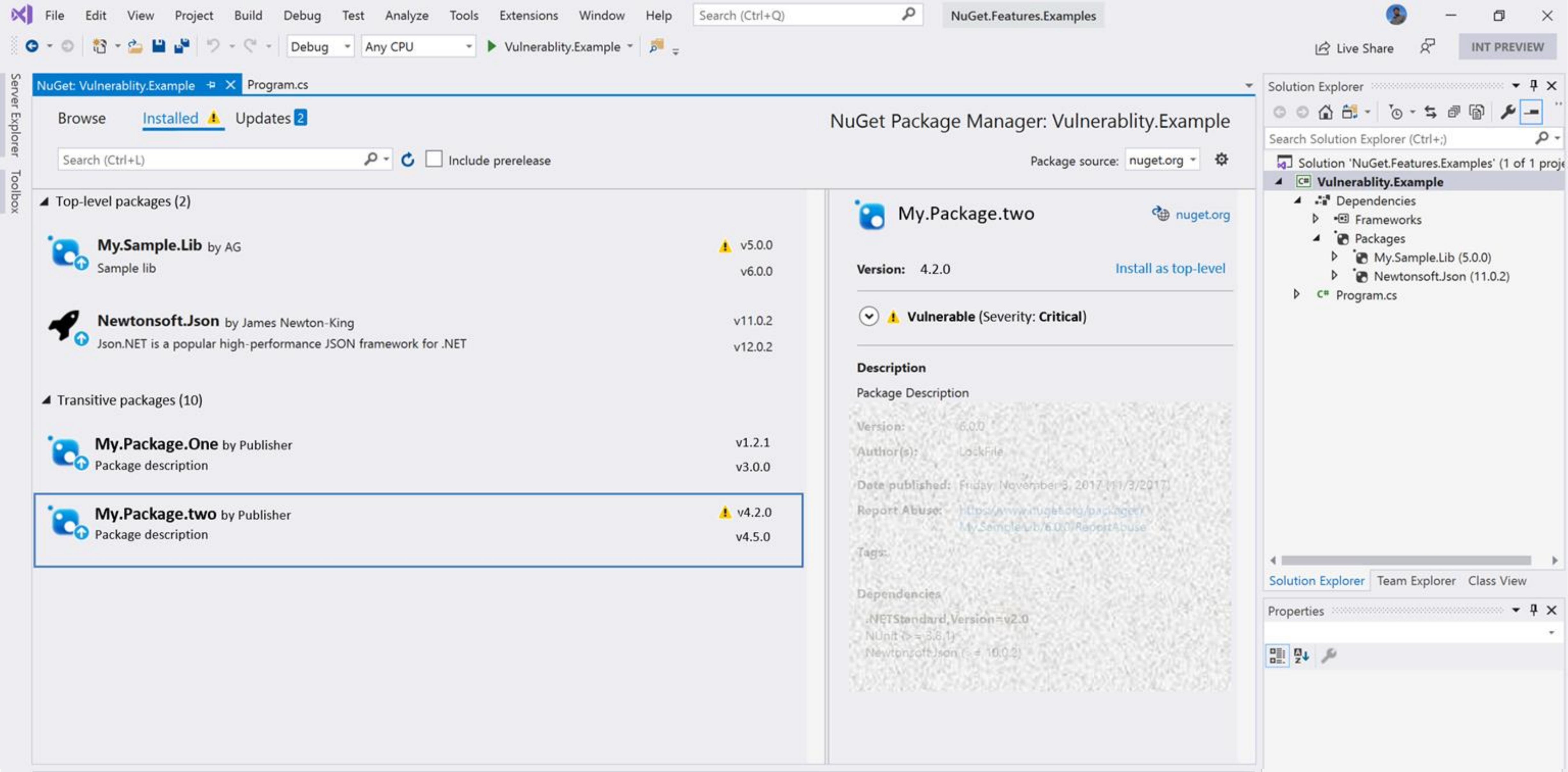


Protect against accidental leaks of API keys



GitHub Token Scanning Service

Flag vulnerable packages



NuGet Package Manager: Vulnerablity.Example

◢ Top-level packages (2)

My.Sample.Lib by AG ⚠ v5.0.0
Sample lib v6.0.0

Newtonsoft.Json by James Newton-King v11.0.2
Json.NET is a popular high-performance JSON framework for .NET v12.0.2

◢ Transitive packages (10)

My.Package.One by Publisher v1.2.1
Package description v3.0.0

My.Package.two by Publisher ⚠ v4.2.0
Package description v4.5.0

My.Package.two nuget.org

Version: 4.2.0 Install as top-level

⚠ **Vulnerable** (Severity: **Critical**)

Description

Package Description

Version: 6.0.0

Author(s): LockFile

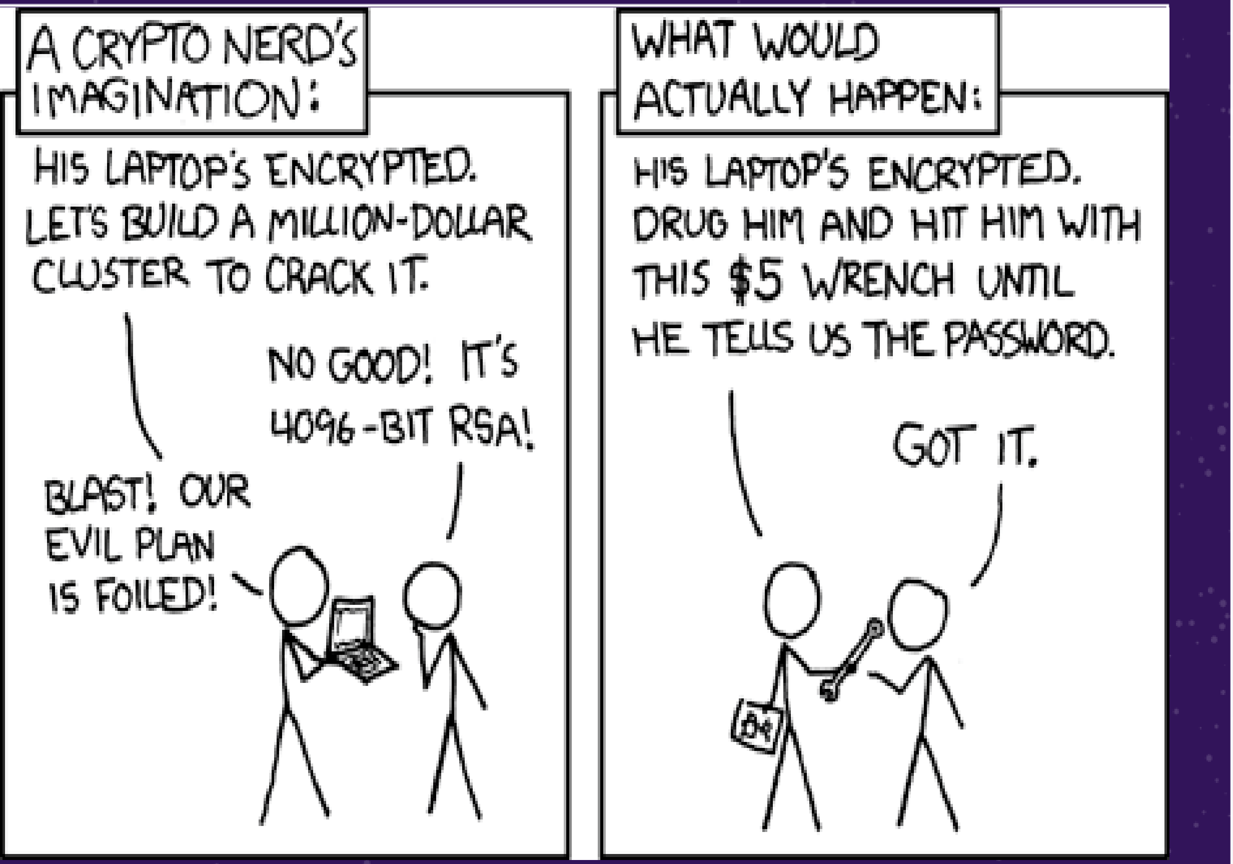
Date published: Friday, November 3, 2017 (11/3/2017)

Report Abuse: https://www.nuget.org/packages/My.Sample.Lib/6.0.0/ReportAbuse

Tags:

Dependencies

.NETStandard,Version=v2.0
NUnit (>= 3.8.1)
Newtonsoft.Json (>= 10.0.2)


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

https://aka.ms/secureNuGet

Code Sample Title

```
Code Sample
```