AUTO-SYS-OPS

Improve security

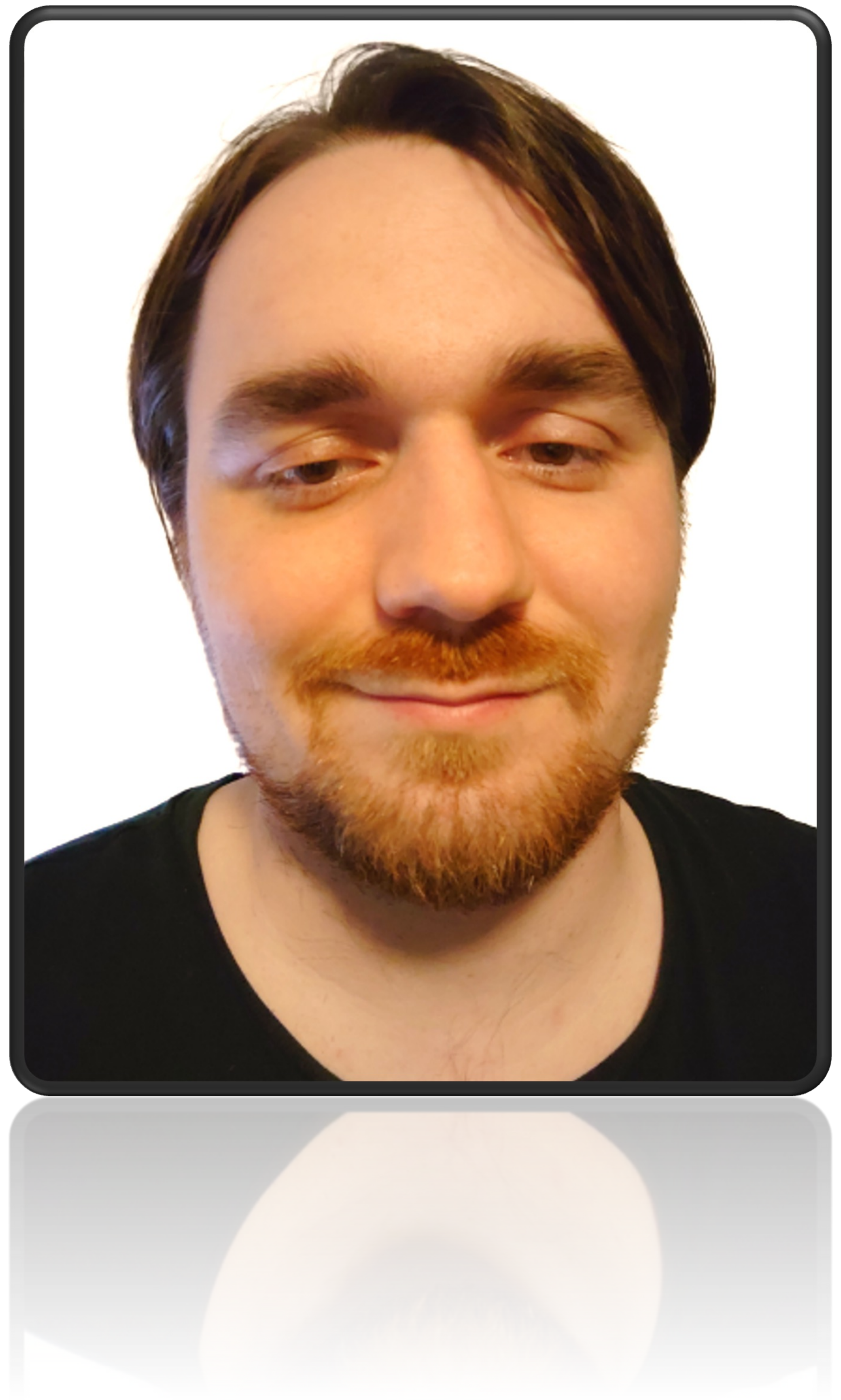
with your own PSGallery

Introduction

Who am I?

- Cloud Consultant @ OGD-ict diensten
  - IAC, CI/CD, Automation, Agile, DevOps

- Previous experiences:
  - Technical Lead SysOps Team
  - SysOps Engineer
  - Functional Application Specialist
  - PHP Backend Developer



AUTO-SYS-OPS

Twitter: @AutoSysOps
Blog: www.autosysops.com

Agenda

- What to be afraid of?
- How bad is it?
- What can we do?
- Demo time!
- Questions

What to be afraid of?

/ Common attacks

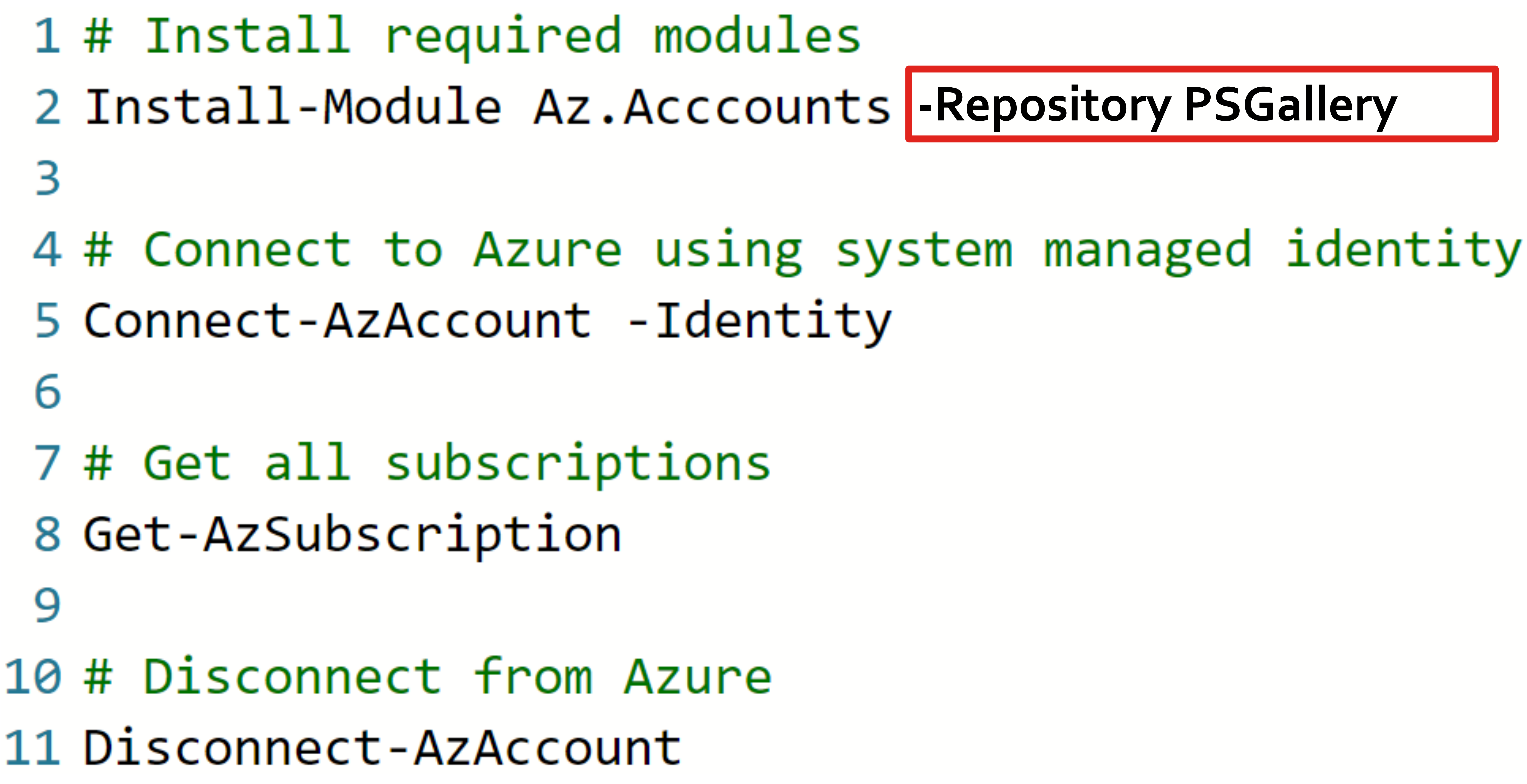
What to be afraid of

Can you spot the error?

```
# Install required modules
Install-Module Az.Acccounts

# Connect to Azure using system managed identity
Connect-AzAccount -Identity

# Get all subscriptions
Get-AzSubscription

# Disconnect from Azure
Disconnect-AzAccount
```

What to be afraid of

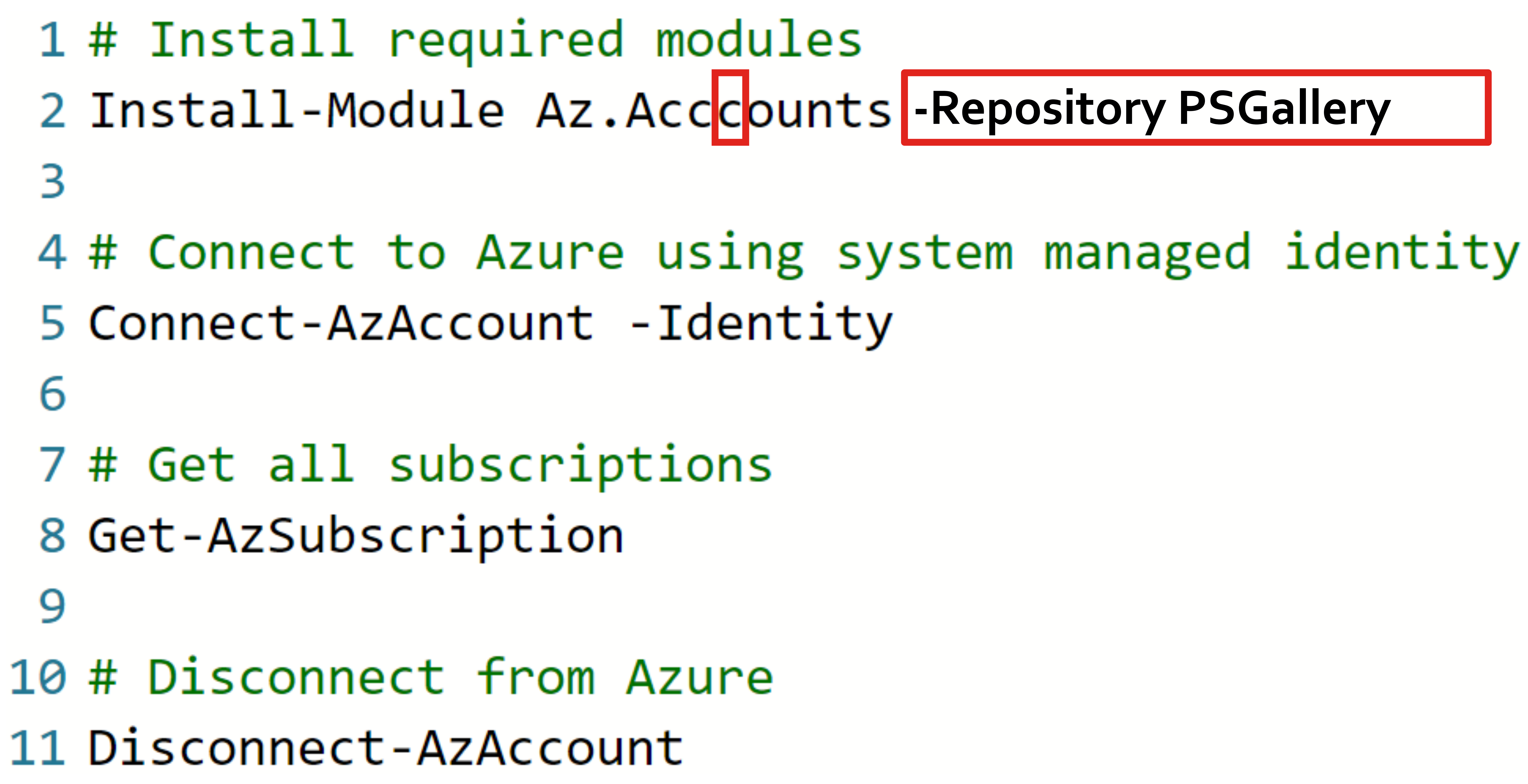
Can you spot the error?



```
# Install required modules
Install-Module Az.Acccounts -Repository PSGallery

# Connect to Azure using system managed identity
Connect-AzAccount -Identity

# Get all subscriptions
Get-AzSubscription

# Disconnect from Azure
Disconnect-AzAccount
```

What to be afraid of

Can you spot the error?



```
# Install required modules
Install-Module Az.Acccounts -Repository PSGallery

# Connect to Azure using system managed identity
Connect-AzAccount -Identity

# Get all subscriptions
Get-AzSubscription

# Disconnect from Azure
Disconnect-AzAccount
```

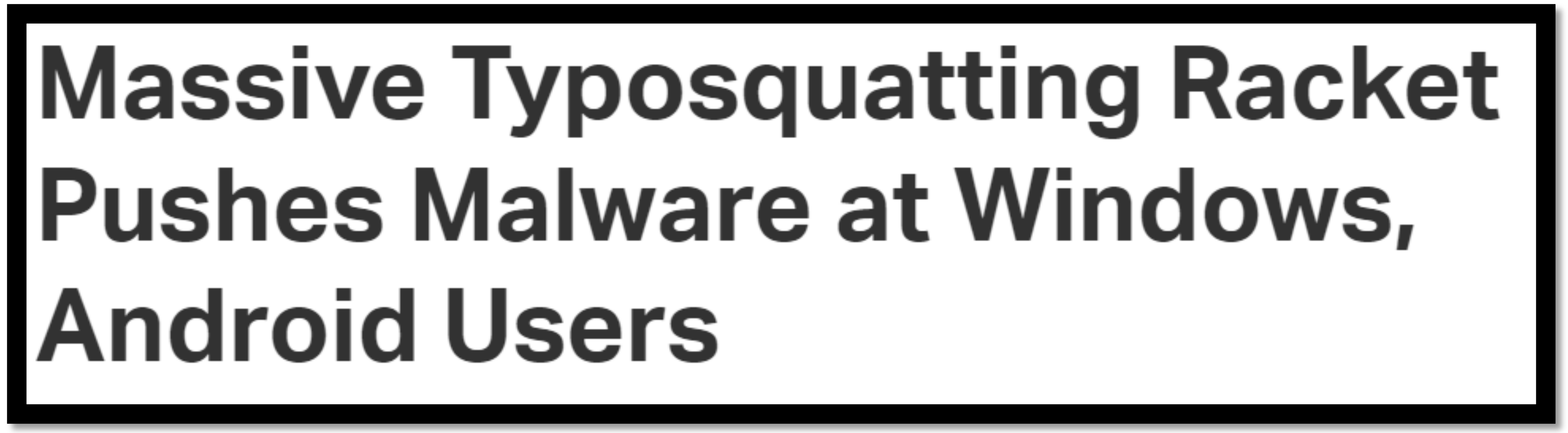
How bad is it?

/ Am I going to be fired?

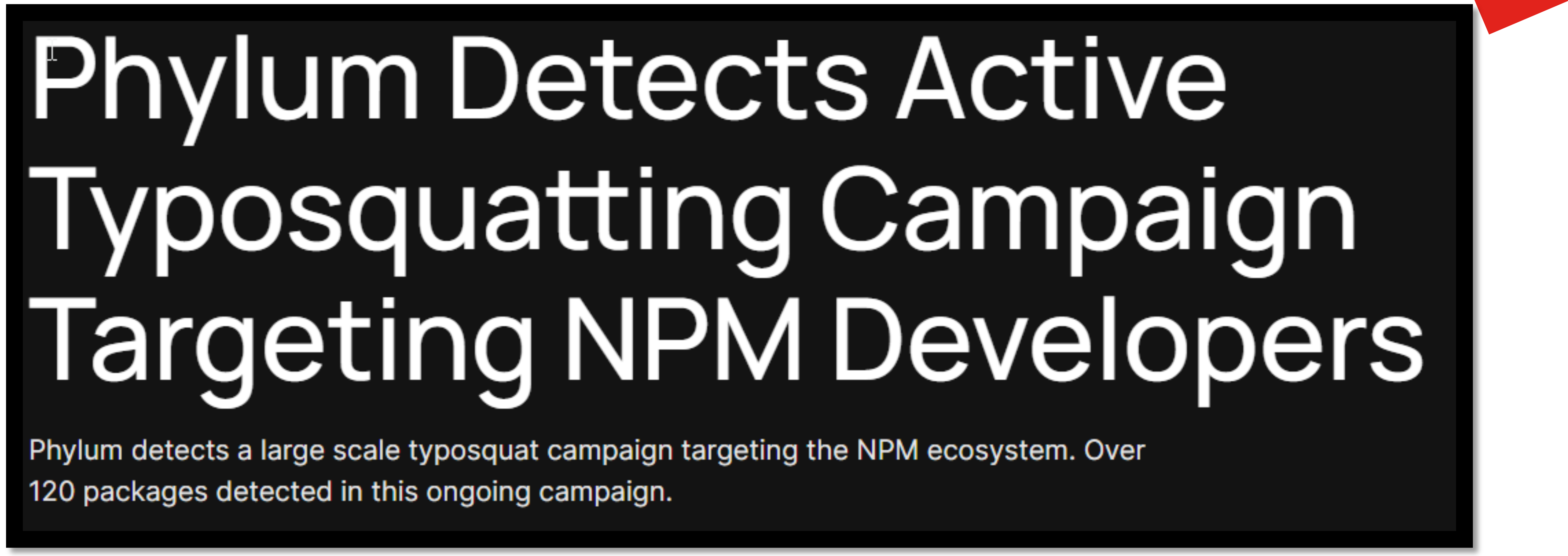
How bad is it?

Let's find out!

How bad is it?

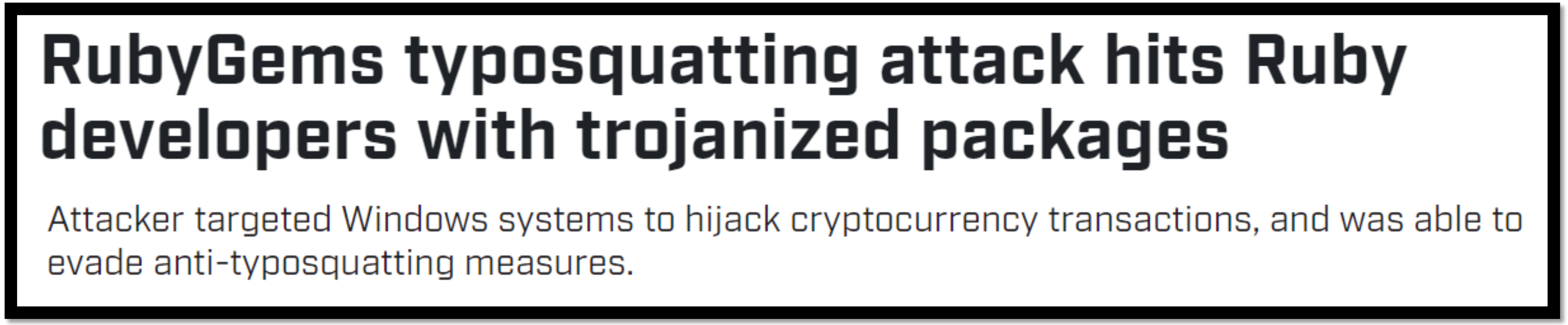


Massive Typosquatting Racket Pushes Malware at Windows, Android Users



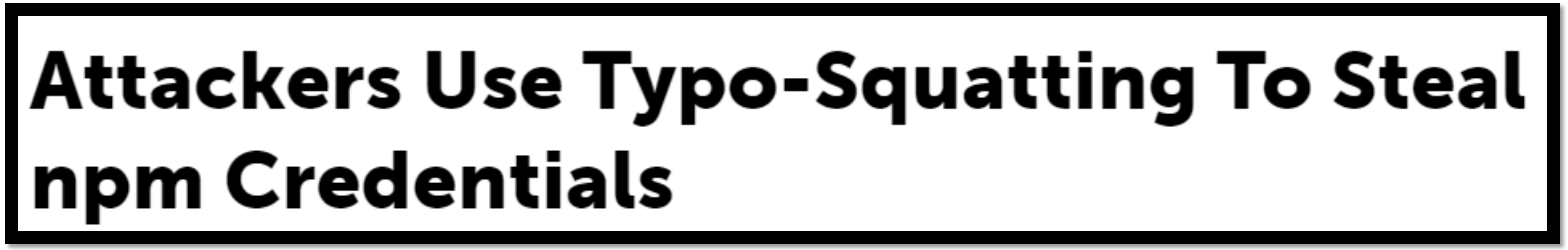
Phylum Detects Active Typosquatting Campaign Targeting NPM Developers

Phylum detects a large scale typosquat campaign targeting the NPM ecosystem. Over 120 packages detected in this ongoing campaign.



RubyGems typosquatting attack hits Ruby developers with trojanized packages

Attacker targeted Windows systems to hijack cryptocurrency transactions, and was able to evade anti-typosquatting measures.



Attackers Use Typo-Squatting To Steal npm Credentials

How bad is it?

Typosquatting?

- Uses public repositories
- Generators available
- Can go undetected easily

https://support.microsoft.com/en-us/topic/what-is-typosquatting-54a18872-8459-4d47-b3e3-d84d9a362eb0
https://blogs.microsoft.com/on-the-issues/2010/04/15/the-trouble-with-typosquatting/

How bad is it?

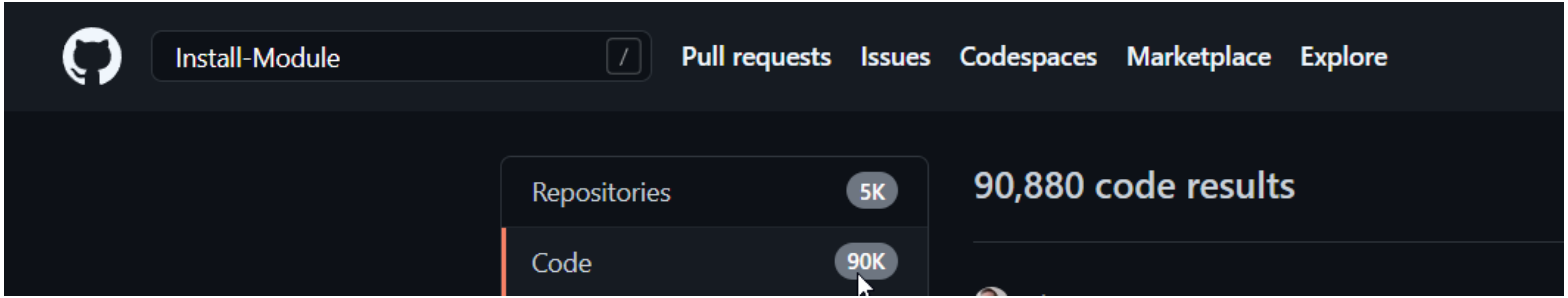
Is powershell vulnerable?

- Many modules are standalone

How bad is it?

Is powershell vulnerable?

- Many modules are standalone
- But ….



90,880 code results

- Many scripts have dependencies

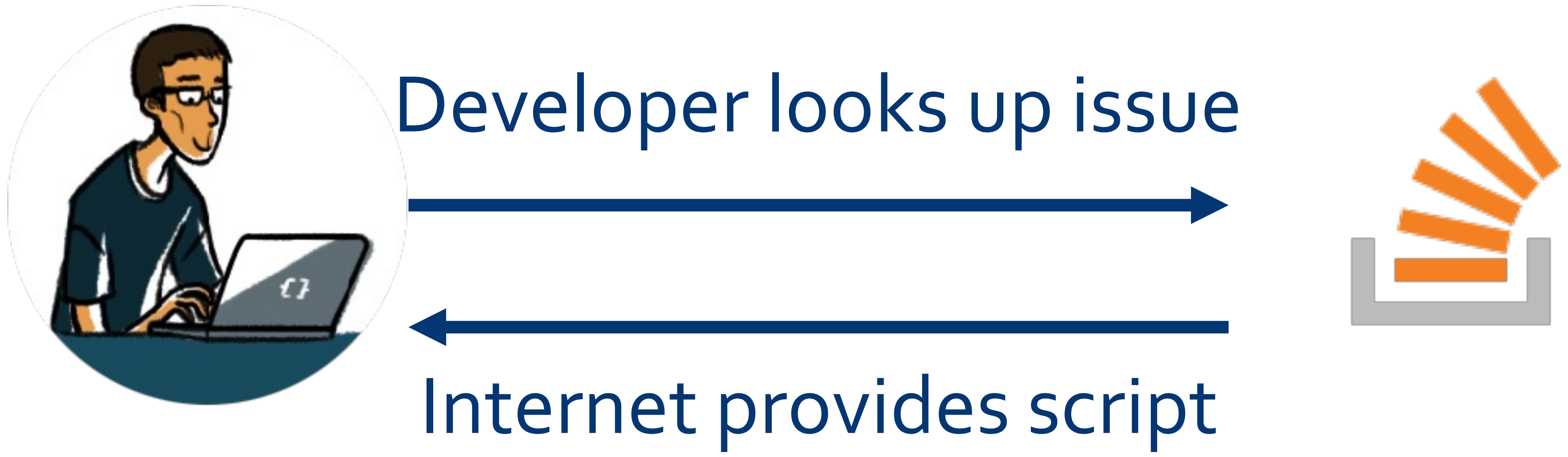
How bad is it?

Is powershell vulnerable?

Developer looks up issue

How bad is it?

Is powershell vulnerable?

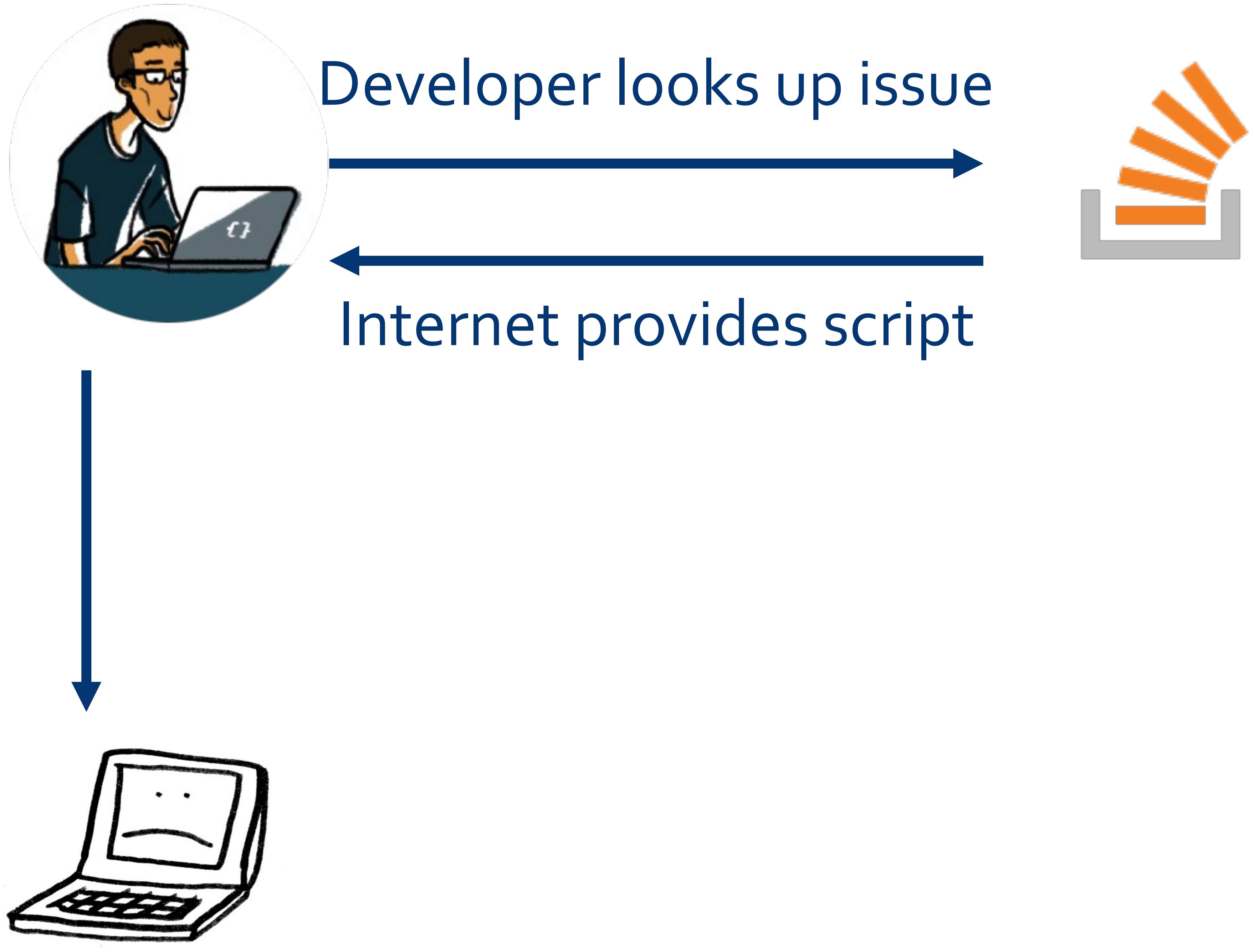


Developer looks up issue

Internet provides script

How bad is it?

Is powershell vulnerable?



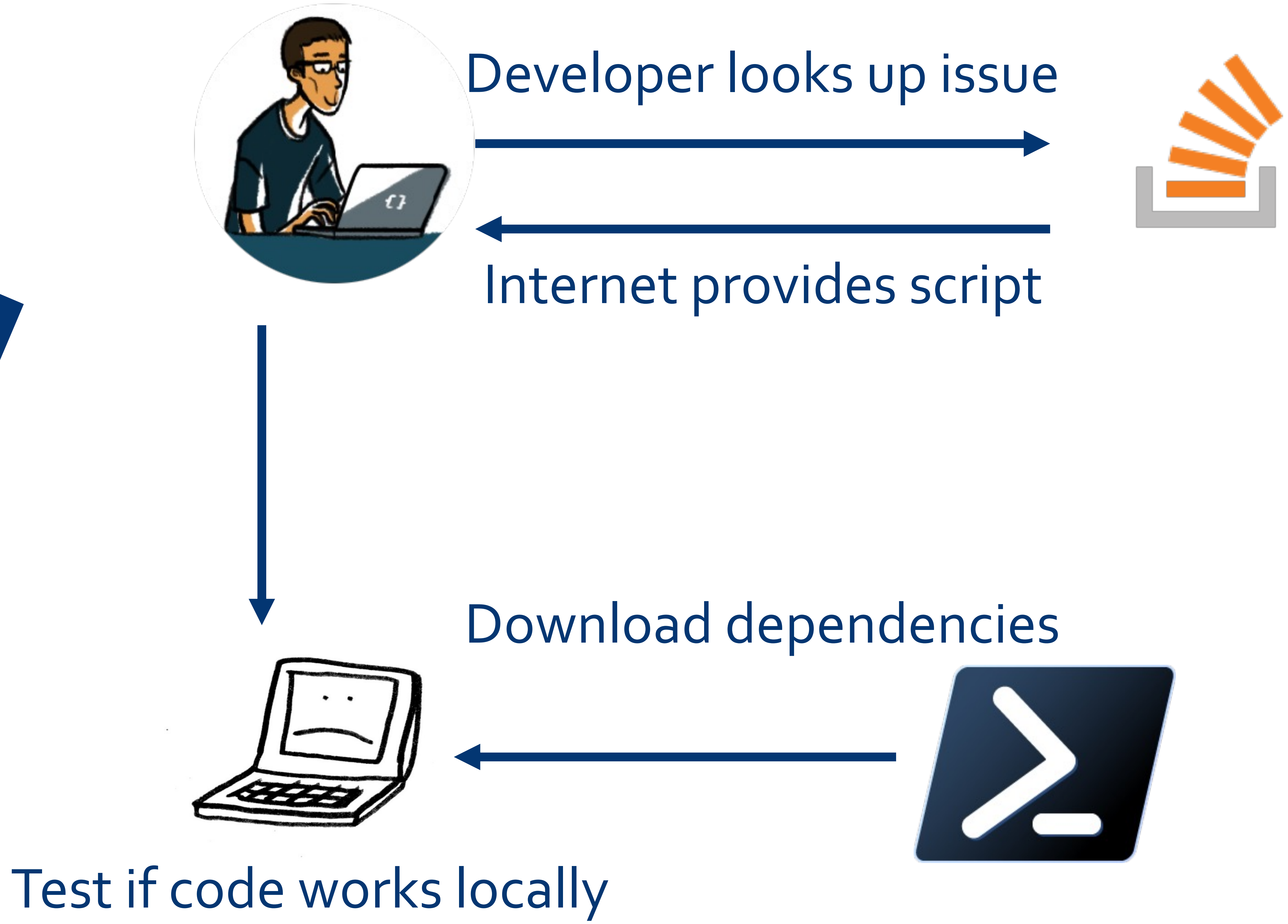
Developer looks up issue

Internet provides script

Test if code works locally

How bad is it?

Is powershell vulnerable?



Developer looks up issue

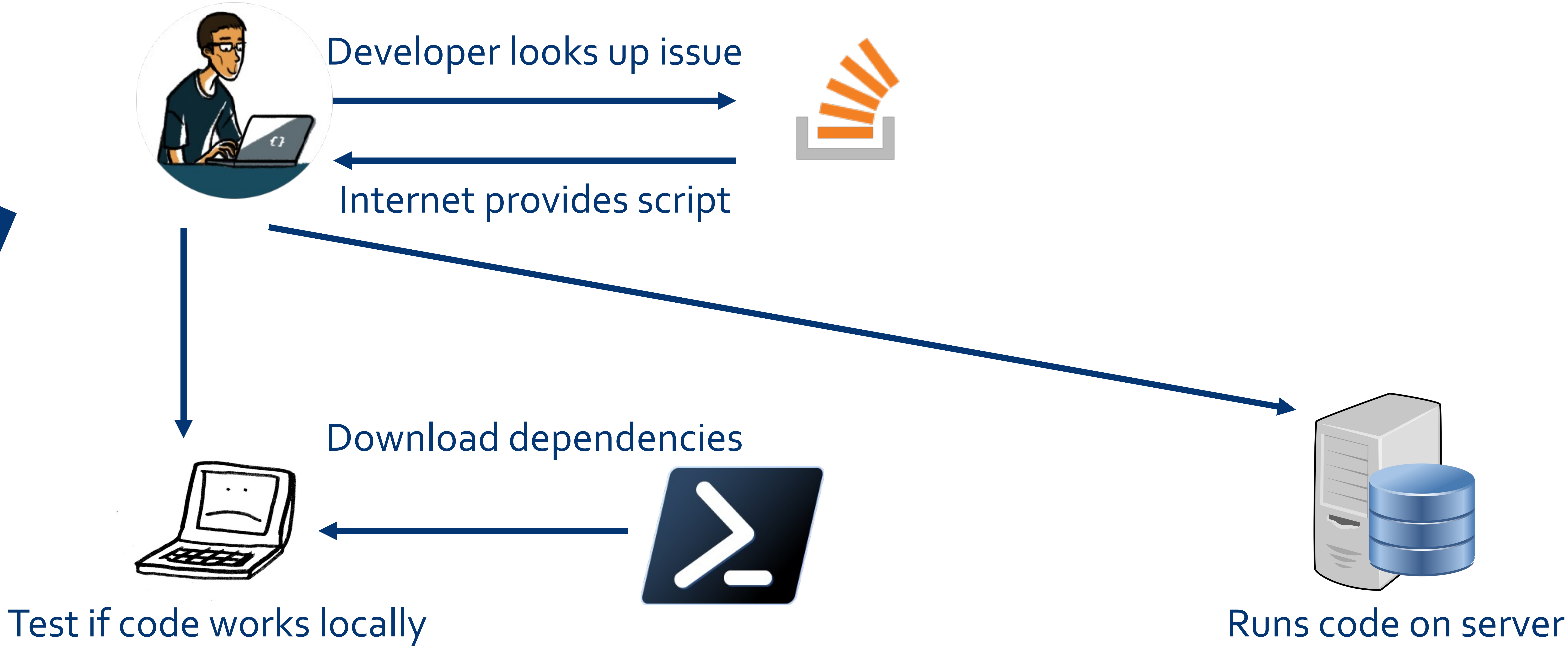
Internet provides script

Download dependencies

Test if code works locally

How bad is it?

Is powershell vulnerable?



Developer looks up issue

Internet provides script

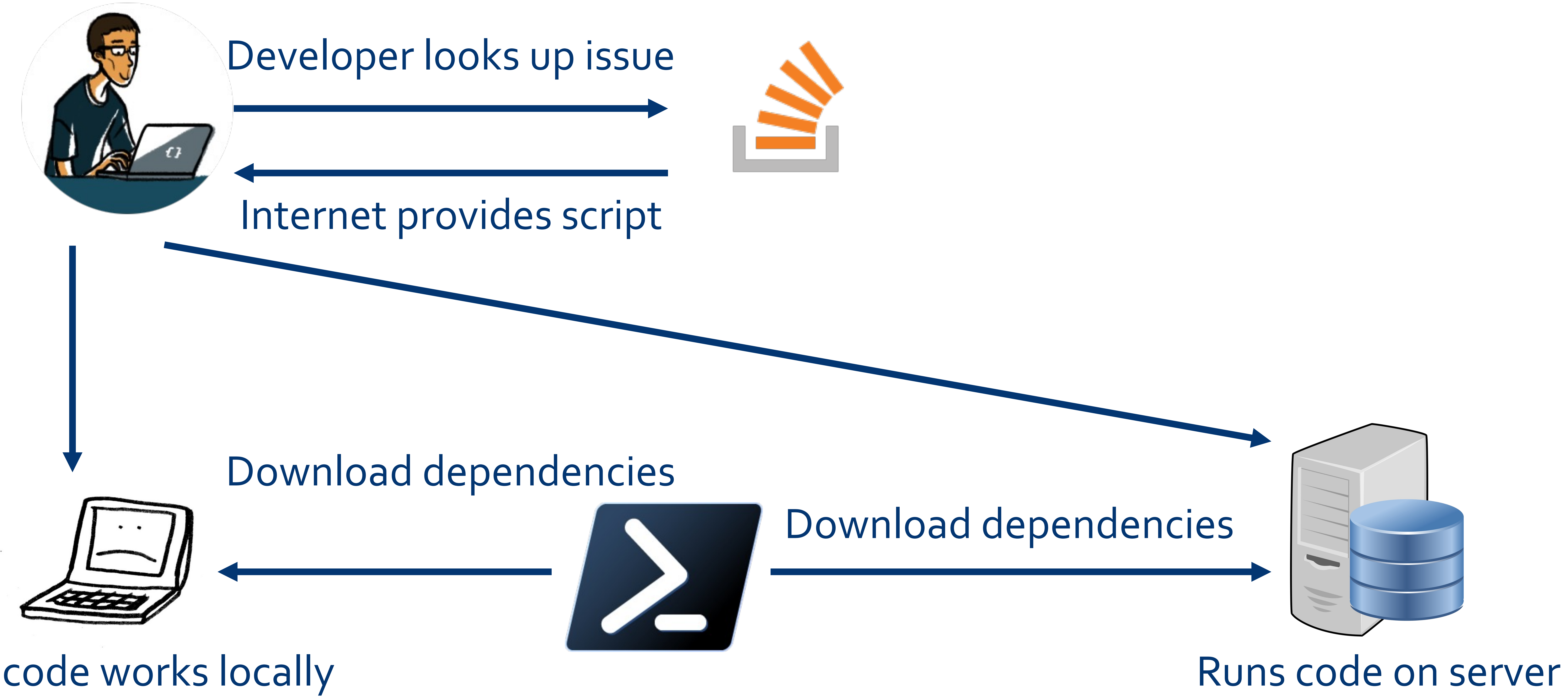
Download dependencies

Test if code works locally

Runs code on server

How bad is it?

Is powershell vulnerable?


Developer looks up issue

Internet provides script

Download dependencies

Download dependencies

Test if code works locally

Runs code on server

How bad is it?

Is powershell vulnerable?

- Typing mistakes are easy
- Malicious code is hard to spot
- One time can be enough to cause problems
- Once in automation, code isn’t checked

How bad is it?

Is powershell vulnerable?

- Other types of attack:
  - Inject malicious code in popular module
  - Have machine look at malicious feed
  - And many more ….

What can we do?

/ Has someone seen security?

What can we do?

Security

- Code scanning and testing

What can we do?

Security

- Code scanning and testing
  - Beware: Data in module manifest can be fake

What can we do?

Security

- Code scanning and testing
  - Beware: Data in module manifest can be fake
- Code signing

What can we do?

Security

- Code scanning and testing
  - Beware: Data in module manifest can be fake
- Code signing
  - No checks on claims in manifest or domains

What can we do?

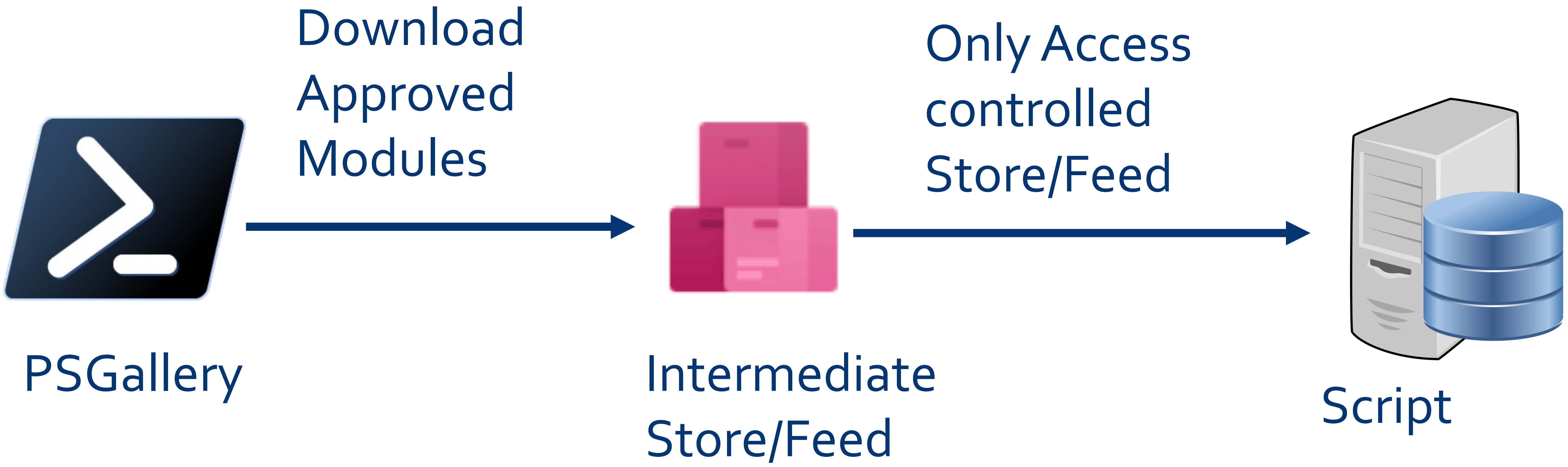
Security

- Code scanning and testing
  - Beware: Data in module manifest can be fake
- Code signing
  - No checks on claims in manifest or domains

- Protect and audit your supply chain!

What can we do?

Azure DevOps to the rescue



PSGallery

Download Approved Modules

Intermediate Store/Feed

Only Access controlled Store/Feed

Script

https://learn.microsoft.com/en-us/azure/devops/artifacts/tutorials/private-powershell-library
https://azure.microsoft.com/en-us/resources/3-ways-to-mitigate-risk-using-private-package-feeds/

Demo time

/ Azure DevOps private feeds

What can we do?

Disadvantages

- Usage of PAT Token
  - Automatic Renewal
  - Service Principal on roadmap for Q1 2023
- Maintenance required
- Updates less quick in production

https://autosysops.com/blog/automatic-pat-renewal-for-azure-devops
https://learn.microsoft.com/en-us/azure/devops/release-notes/roadmap/support-azure-managed-identities

What can we do?

Extra advantages

- Control versions of modules
- Multiple feeds for multiple environments
- Overview of dependencies used
- Usage statistics

Questions?

Leo Visser

- Twitter: @autosysops
- Blog: www.autosysops.com

AUTO - SYS - OPS

Thank you for listening!