OWASP WrongSecrets @ NLUUG 2024

How to (not) Use Secrets with OWASP WrongSecrets

Jeroen Willemsen



Ben de Haan


Token
QR code
2FA code
Urltoken
HMAC key
TLS private key
Private key
JWTs
MFA backup code
API-token
Credentials
Activation link
OTP
GPG key
IAM access keys
Encryption key
API key
Signing key
Password
SSH key

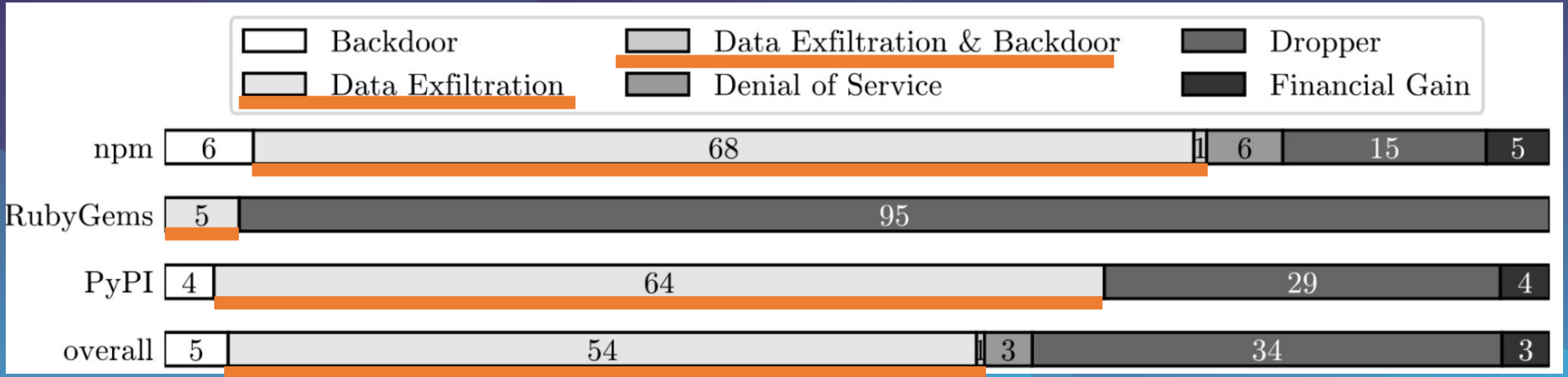
NPM DELIVERY



What if one of these packages is bad news?

Backstabber's Knife Collection: A Review of Open Source Software Supply Chain Attacks, *M. Ohm et al*, 2020

(arXiv:2005.09535 [cs.CR])



Massive GitHub analysis reveals 10 million secrets hidden in 1 billion commits

GitGuardian scanned 1.027 billion new Git
to 2021) and found 10,000,000 secrets oc
What is interesting beyond this ever-increa
of 10 exposed a secret in 2022.

How corporate data and secrets leak from GitHub repositories



hashicorp / vault-examples

Code | Issues 2 | Pull requests 1

Example can leak credentia

Open MirahImage opened this issue on Feb 6, 202

MirahImage commented on Feb 6, 2023

This example can leak the credentials to the lo
rabbitmq/messaging-topology-operator#545

vault-examples/examples/token-renewal/go/example.go
Line 75 in 45d7501

```
75      log.Printf("Successfully renewed: %#v", renewal)
```

Discover Dangerous ensitive Kubernetes

ention to the public exposure of Kubernetes configuration
ganizations are vulnerable to this “ticking supply chain

ets via

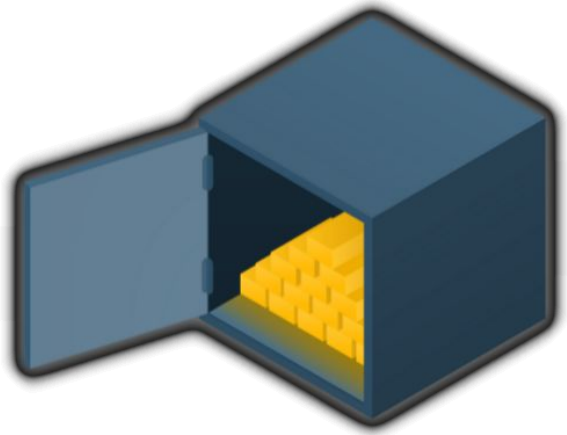
es of recent data breaches through leaked

h - January 2020
und in GitHub repository

- April 2020
onal GitHub account granted access to sensitive data for equifax customers

Uber Data Breach - October 2016
Poor password hygiene allowed intruders to access Uber's Amazon S3 Datastore using an AWS access key posted in a private GitHub repository.

Introducing…

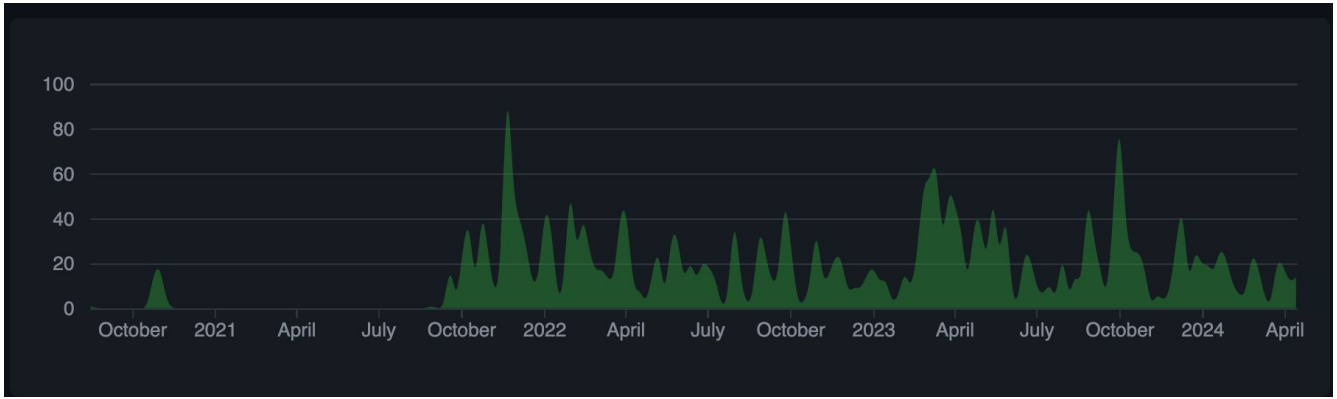


OWASP WrongSecrets

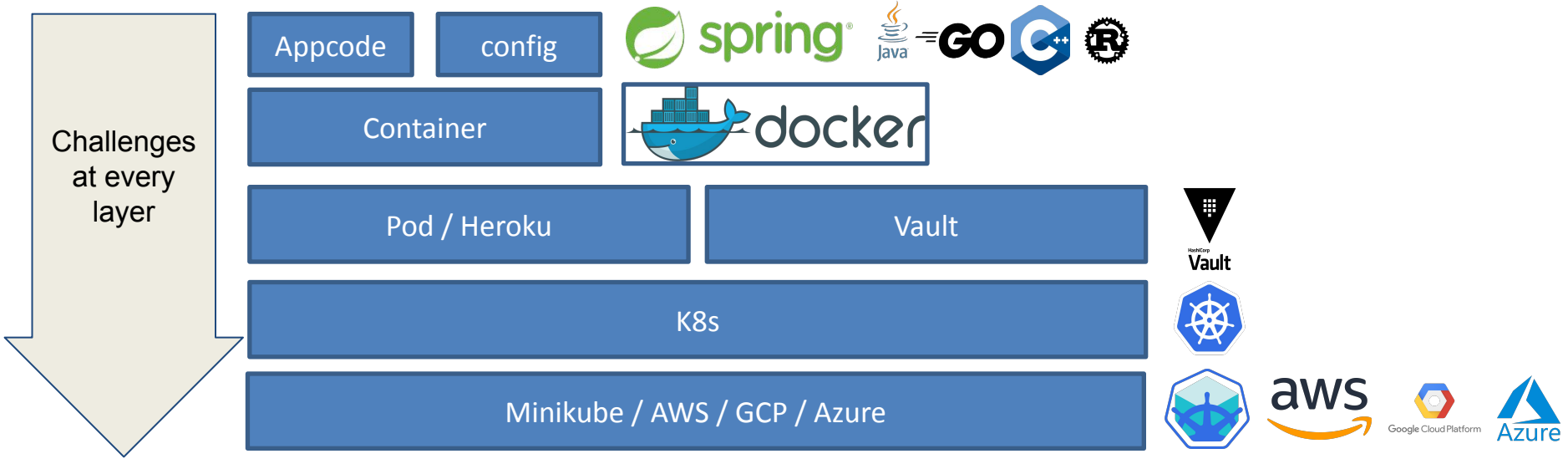
What is it?

Production Project

- Vulnerable app & secret detector testbed
- Goals:
  - Educate on secret management and its pitfalls
  - Help people reflect on their secrets management strategy
  - Promote secrets management as important facet of security



Overall architecture



Demo time!



https://wrongsecrets.herokuapp.com

A note on the binaries

Built by us

Source code: https://github.com/OWASP/wrongsecrets-binaries/



So what *should* you do?



Put them in a safe place



Reduce scope



Set a lifetime



Validate user origin



Audit usage

So what does this tell us?

Secrets Management is complex

So what does this tell us?

Secrets Management is complex

A secrets manager can help!

So what does this tell us?

Secrets Management is complex

A secrets manager can help!

Secrets management is an ever evolving spiral

Want to know more about doing it right?

Secrets Management - OWASP Cheat Sheet Series

OpenCRE on secrets management

Blog: 10 Pointers on Secrets Management

OWASP SAMM on Secret Management

The secret detection topic at Github

Special Thanks

OWASP Project Leaders:

- Ben de Haan @bendehaan
- Jeroen Willemsen @commjoen

Top Contributors:

- Jannik Hollenbach @J12934
- Puneeth Y @puneeth072003
- Joss Sparkes @RemakingEden

Contributors:

- Nanne Baars @nbaars
- Marcin Nowak @drnow4u
- Rodolfo Cabral Neves @roddas
- Osama Maggy @osamamaggy
- Divyanshu Dev @Novice-expert
- Tibor Hercz @tiborhercz
- Chris Elbring Jr. @neatzsche
- Diamond Rivero @diamant3
- Adarsh A @adarsh-a-tw
- Filip Chyla @fchyla
- Dmitry Litosh @Dlitosh
- Turjo Chowdhury @turjoc120
- Norbert Wolniak @nwolniak
- Josh Grossman @tghosth
- alphasec @alphasecio
- CaduRoriz @CaduRoriz
- Madhu Akula @madhuakula
- Mike Woudenberg @mikewoudenberg
- Spyros @northdpole
- Vineeth Jagadeesh @djvinnie
- RubenAtBinx @RubenAtBinx
- za @za
- Alex Bender @alex-bender
- Nicolas Humblot @nhumblot
- Rick M @kingthorin
- Shlomo Zalman Heigh @szh
- Fern @f3rn0s

Testers:

- Dave van Stein @davevs
- Marcin Nowak @drnow4u
- Marc Chang Sing Pang @mchangsp
- Vineeth Jagadeesh @djvinnie

Special mentions for helping out:

- Madhu Akula @madhuakula @madhuakula
- Nanne Baars @nbaars @nbaars
- Björn Kimminich @bkimminich
- Dan Gora @devsecops
- Xiaolu Dai @saragluna
- Jonathan Giles @jonathanGiles

Special Thanks

GitGuardian for their sponsorship which allows us to pay the bills for our cloud accounts.

Jetbrains for licensing an instance of Intellij IDEA Ultimate edition to the project leads. We could not have been this fast with the development without it!

Docker for granting us their Docker Open Source Sponsored program.

1Password for granting us an open source license to 1Password for the secret detection testbed.

AWS for granting us AWS Open Source credits which we use to test our project and the Wrongsecrets CTF Party setup on AWS.

We can really use your help!

⭐ **Promote https://github.com/OWASP/wrongsecrets:**

GitHub Stars & social media

💻 **Take the project for a spin**

💬 **Give feedback!**

File an issue or contact us on OWASP Slack in channel #project-wrongsecrets

🔧 **Improve the project: File PRs!**

Questions?



Twitter: @BJFdeHaan
Email: ben.dehaan@owasp.org

Twitter: @commjoenie
Email: jeroen.willemsen@owasp.org