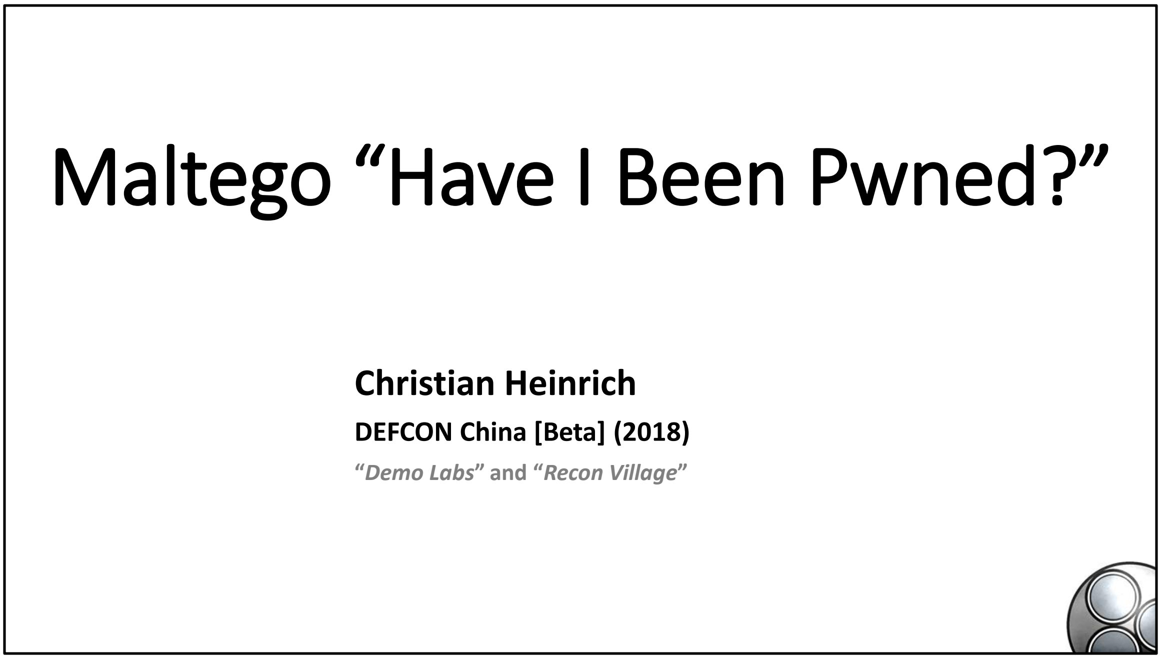
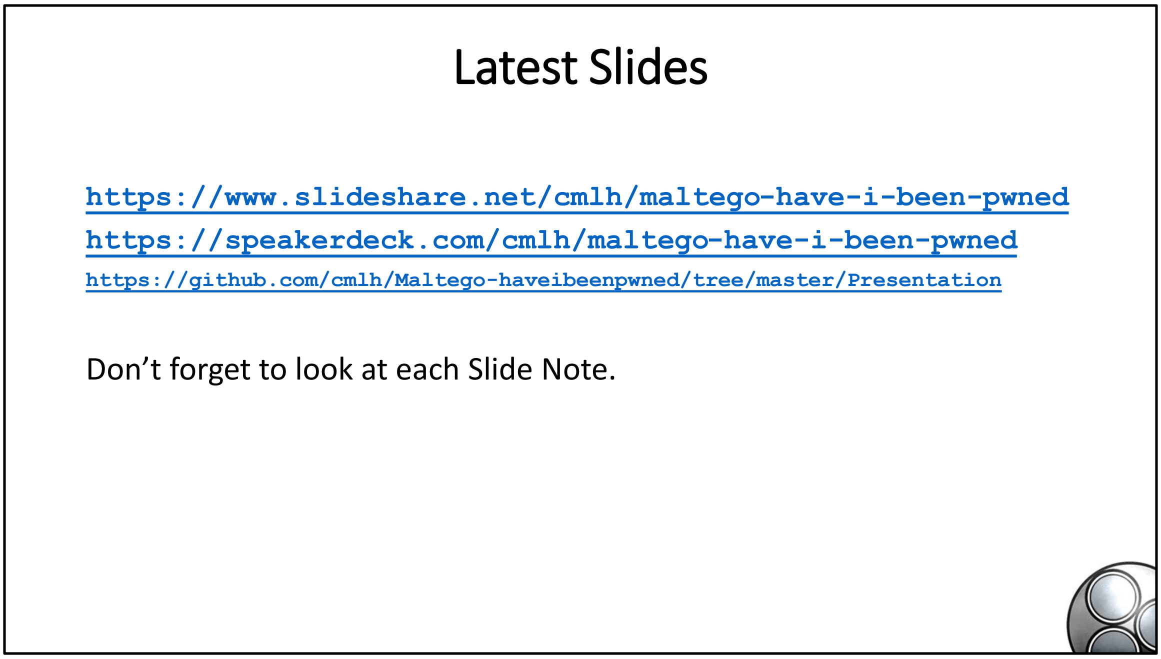


# Maltego “Have I Been Pwned?”

**Christian Heinrich**

**DEFCON China [Beta] (2018)**

“***Demo Labs***” **and** “***Recon Village***”



# Latest Slides

https://www.slideshare.net/cmlh/maltego-have-i-been-pwned
https://speakerdeck.com/cmlh/maltego-have-i-been-pwned
https://github.com/cmlh/Maltego-haveibeenpwned/tree/master/Presentation

Don’t forget to look at each Slide Note.

# $ whoami

https://www.linkedin.com/in/ChristianHeinrich

Developer of Local and Remote Maltego Transforms for:

- @Facebook
- @Instagram
- @Gravatar
- @RecordedFuture
- @TAIA Global REDACT™
- @VirusTotal
- @FullContact

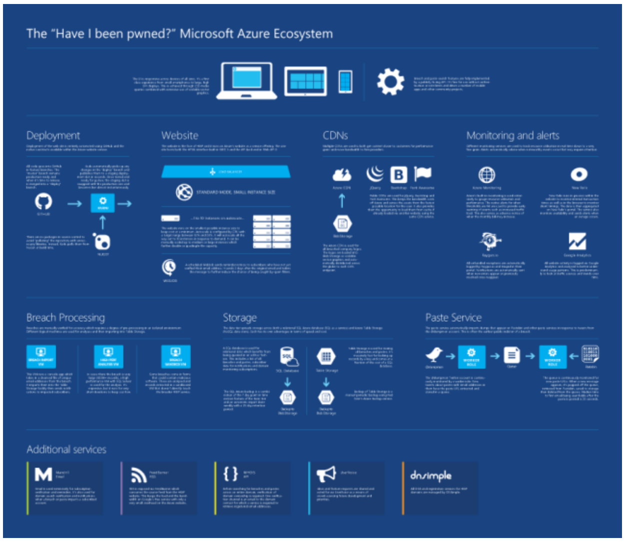
Python Modules from @CanariProject and @Paterva

https://github.com/search?q=user%3Acmlh+Maltego

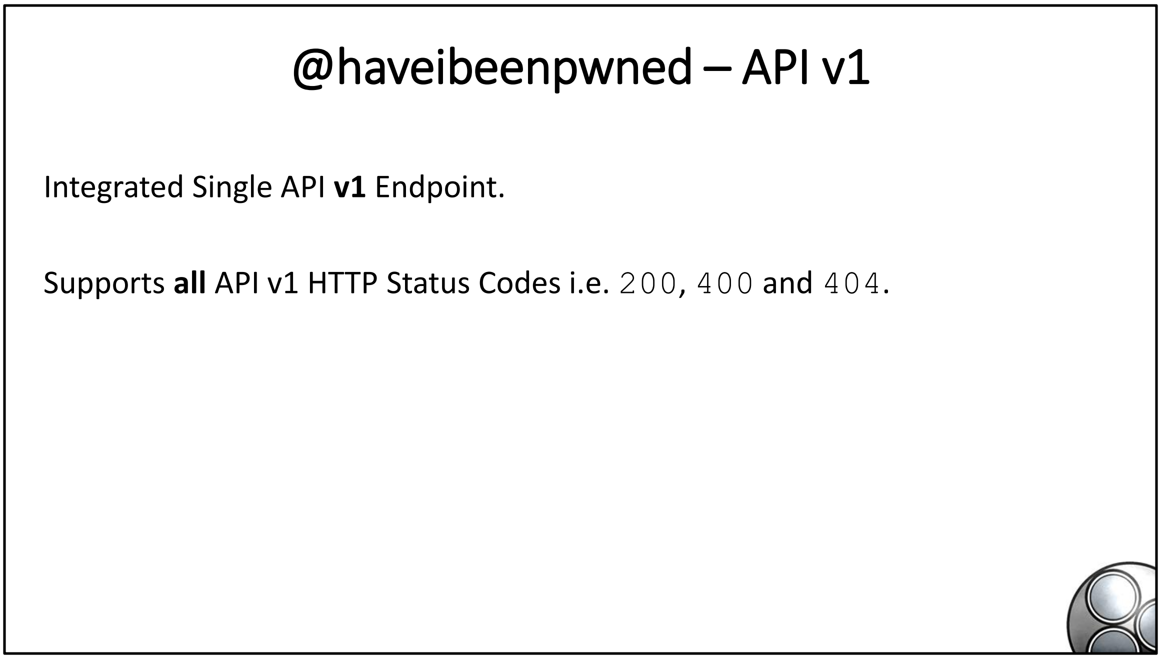
# Agenda

1. Integration of the API [v1 and v2], including “*Pwned Passwords*”
2. Configuration of Maltego:
   - ~~Import configuration file~~
   - “*Transform Hub*”
3. Case Studies
   - Penetration Tester
   - Incident Responder

# “Have I Been Pwned?”



https://haveibeenpwned.com/ecosystem.pdf



# @haveibeenpwned – API v1

Integrated Single API **v1** Endpoint.

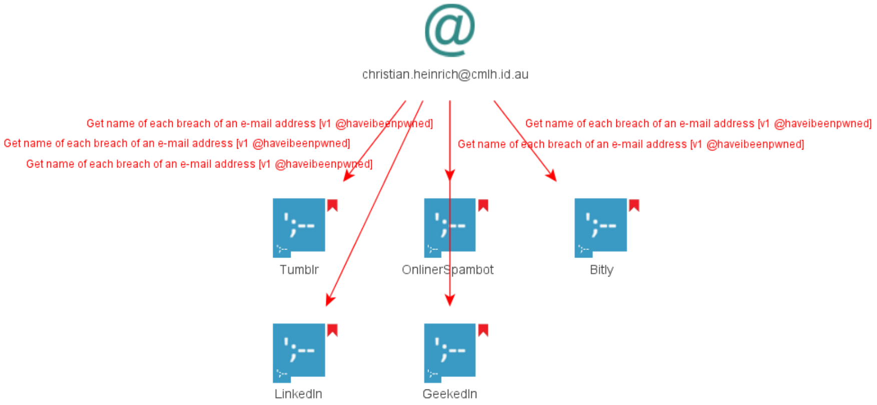
Supports **all** API v1 HTTP Status Codes i.e. `200`, `400` and `404`.

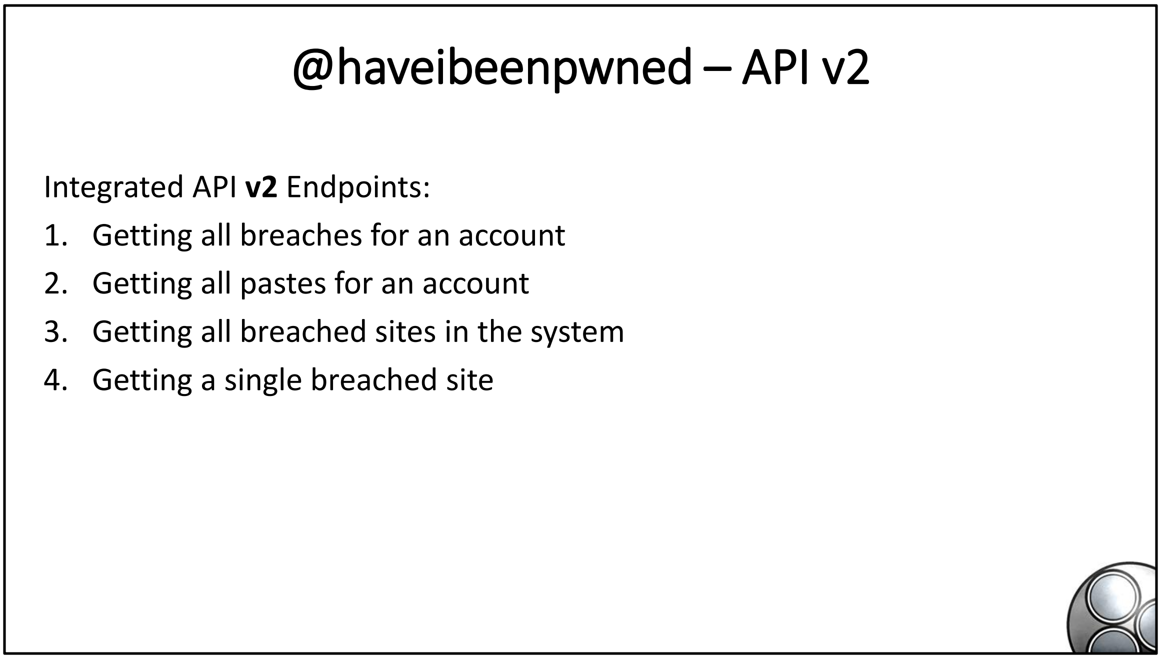
https://haveibeenpwned.com/API/v1

HTTP Status Codes

| | |
|---|---|
| 200 | Ok — everything worked and there's a string array of pwned sites for the account |
| 400 | Bad request — the account does not comply with an acceptable format (i.e. it's an empty string) |
| 404 | Not found — the account could not be found and has therefore not been pwned |

# @haveibeenpwned – API v1


christian.heinrich@cmlh.id.au
Get name of each breach of an e-mail address [v1 @haveibeenpwned]
Get name of each breach of an e-mail address [v1 @haveibeenpwned]
Get name of each breach of an e-mail address [v1 @haveibeenpwned]
Get name of each breach of an e-mail address [v1 @haveibeenpwned]
Get name of each breach of an e-mail address [v1 @haveibeenpwned]
Tumblr
OnlinerSpambot
Bitly
LinkedIn
GeekedIn

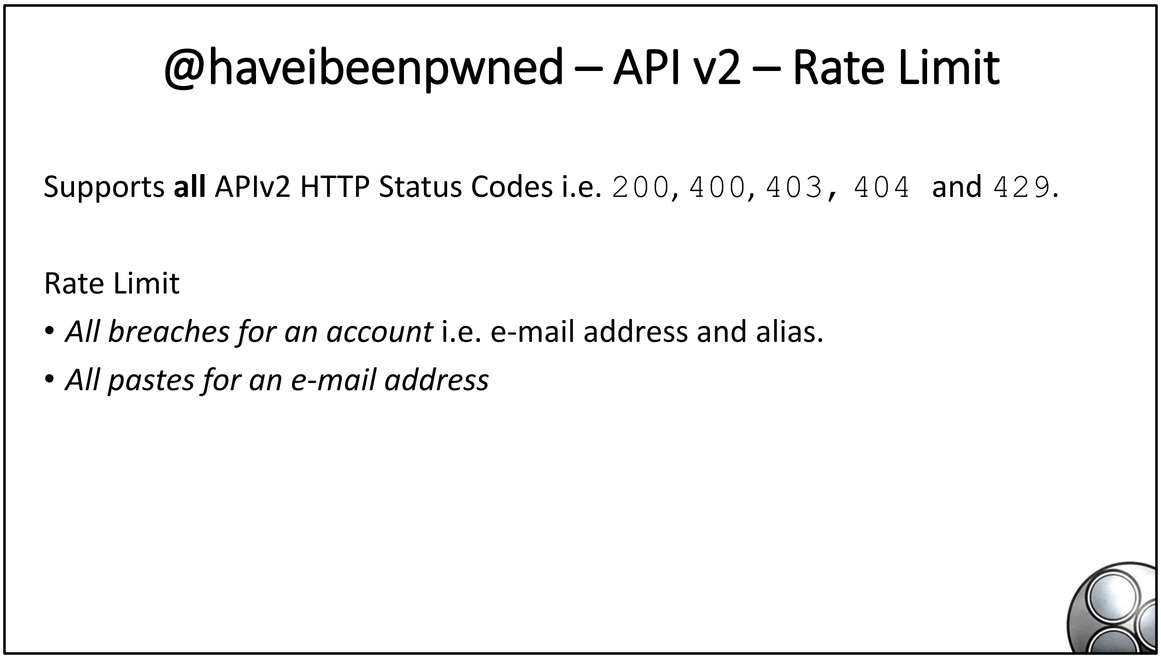


# @haveibeenpwned – API v2

Integrated API **v2** Endpoints:

1. Getting all breaches for an account
2. Getting all pastes for an account
3. Getting all breached sites in the system
4. Getting a single breached site

https://haveibeenpwned.com/API/v2



# @haveibeenpwned – API v2 – Rate Limit

Supports **all** APIv2 HTTP Status Codes i.e. `200`, `400`, `403`, `404` and `429`.

Rate Limit

- *All breaches for an account* i.e. e-mail address and alias.
- *All pastes for an e-mail address*

https://haveibeenpwned.com/API/v2#RateLimiting

HTTP Status Codes

200 Ok — everything worked and there's a string array of pwned sites for the account

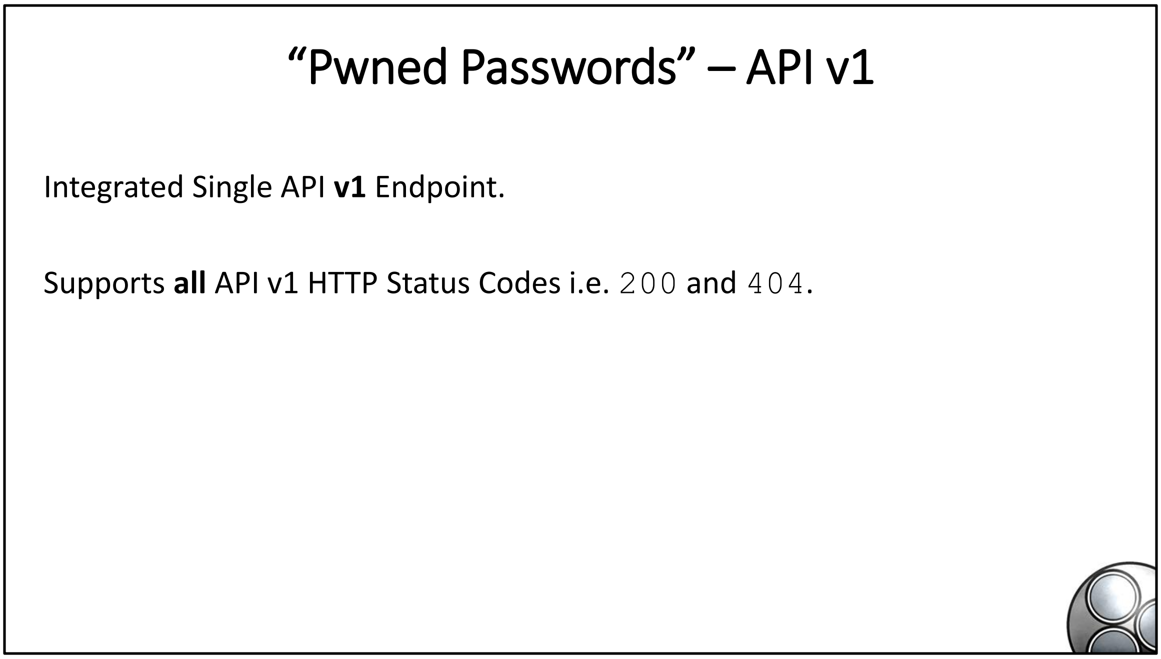
400 Bad request — the account does not comply with an acceptable format (i.e. it's an empty string)

403 Forbidden — no user agent has been specified in the request

404 Not found — the account could not be found and has therefore not been pwned

429 Too many requests — the rate limit has been exceeded

https://github.com/cmlh/Maltego-haveibeenpwned/wiki#rate-limit



# “Pwned Passwords” – API v1

Integrated Single API **v1** Endpoint.

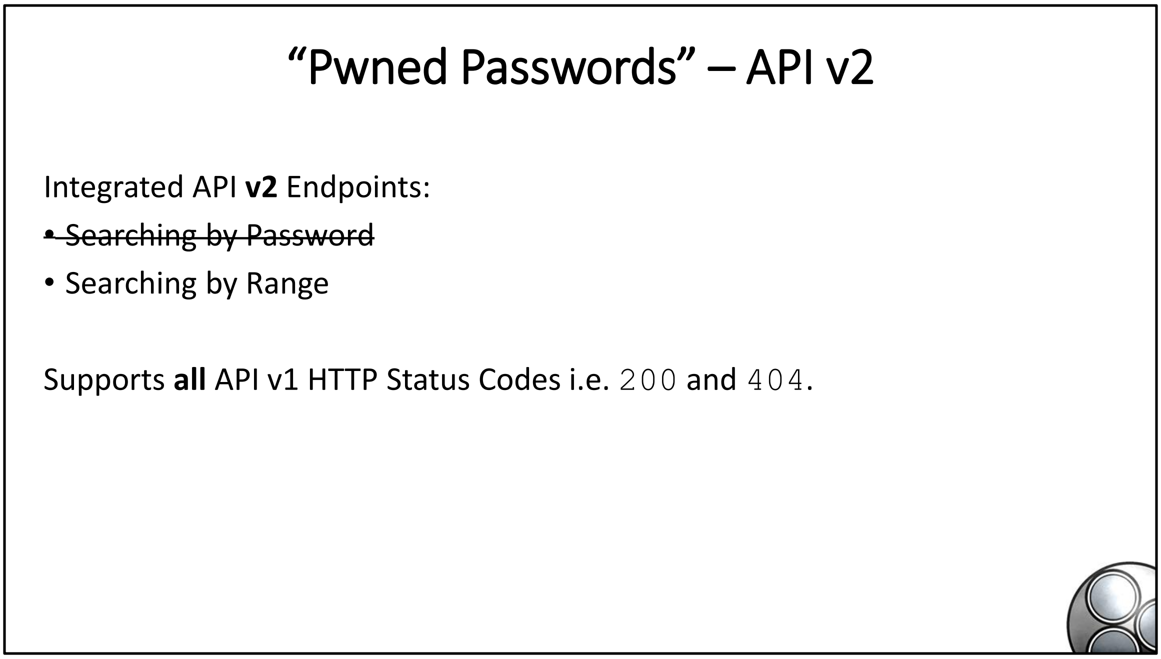
Supports **all** API v1 HTTP Status Codes i.e. `200` and `404`.

https://github.com/cmlh/Maltego-haveibeenpwned/wiki#api-v1-1

HTTP Status Codes

200 Ok — the password was found in the Pwned Passwords repository

404 Not found — the password was not found in the Pwned Passwords repository



# “Pwned Passwords” – API v2

Integrated API **v2** Endpoints:

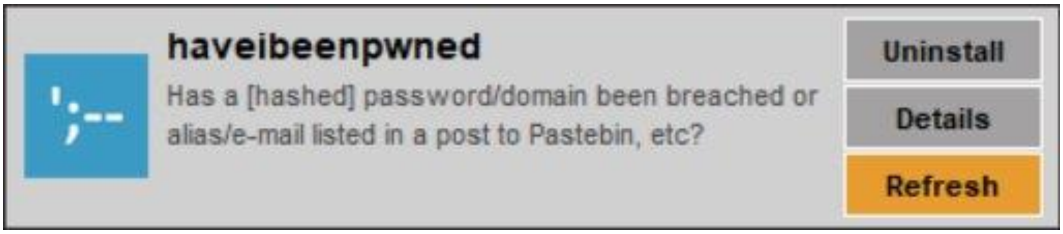
- ~~Searching by Password~~
- Searching by Range

Supports **all** API v1 HTTP Status Codes i.e. `200` and `404`.

https://haveibeenpwned.com/API/v2#SearchingPwnedPasswordsByPassword

HTTP Status Codes
200 Ok — the password was found in the Pwned Passwords repository
404 Not found — the password was not found in the Pwned Passwords repository

# Installation



haveibeenpwned

Has a [hashed] password/domain been breached or alias/e-mail listed in a post to Pastebin, etc?

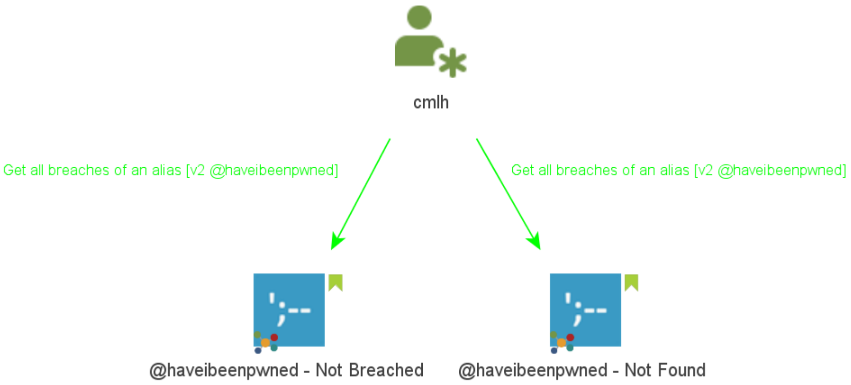
https://github.com/cmlh/Maltego-haveibeenpwned/wiki

# @haveibeenpwned – Maltego Input Entities

1. *“Account”*
   1. **`maltego.EmailAddress`**
   2. **`maltego.Alias`**

2. *“Site”*
   1. **`maltego.Domain`**
   2. **`Maltego.Phrase`**

# @haveibeenpwned – `maltego.Alias` Entity



cmlh

Get all breaches of an alias [v2 @haveibeenpwned]

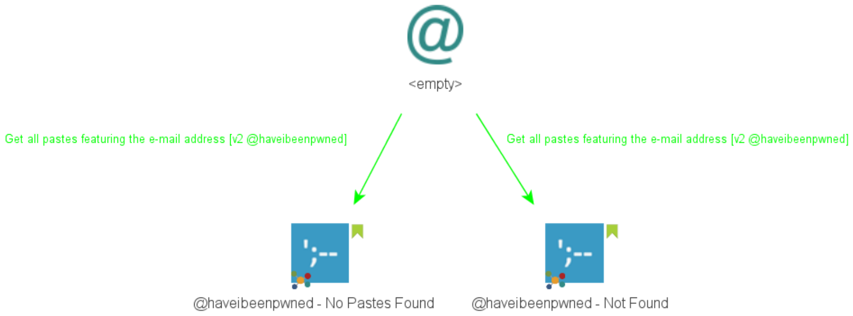
Get all breaches of an alias [v2 @haveibeenpwned]

@haveibeenpwned - Not Breached

@haveibeenpwned - Not Found

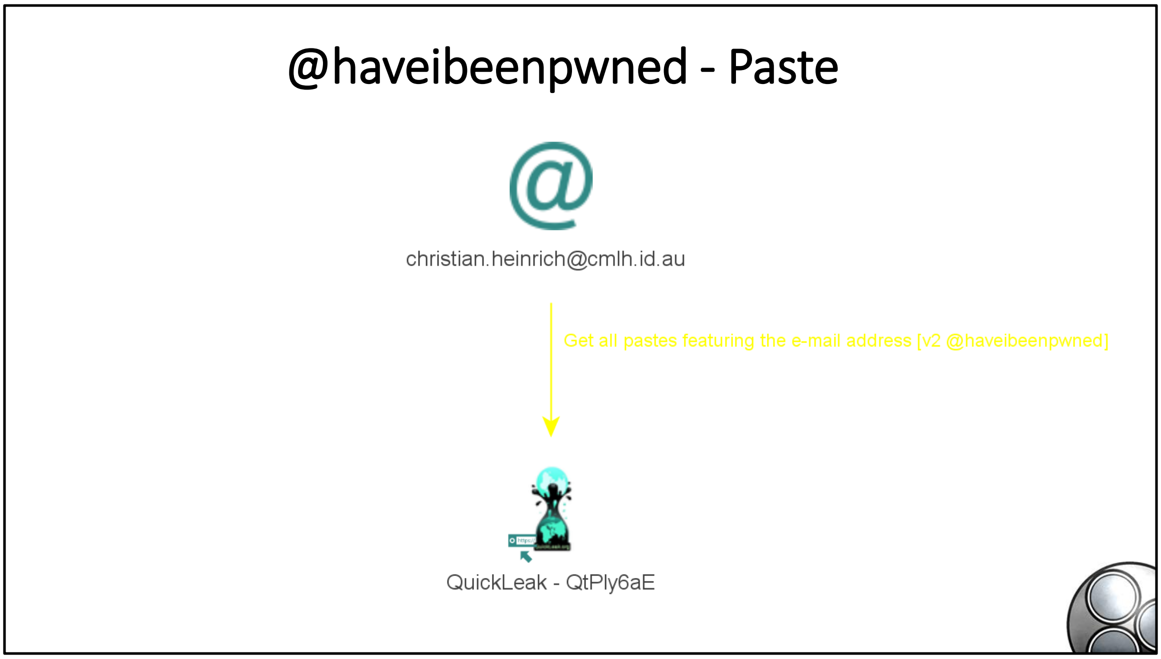
Green Bookmark

# @haveibeenpwned - Paste


<empty>
Get all pastes featuring the e-mail address [v2 @haveibeenpwned]
Get all pastes featuring the e-mail address [v2 @haveibeenpwned]
@haveibeenpwned - No Pastes Found
@haveibeenpwned - Not Found

Green Bookmark

# @haveibeenpwned - Paste



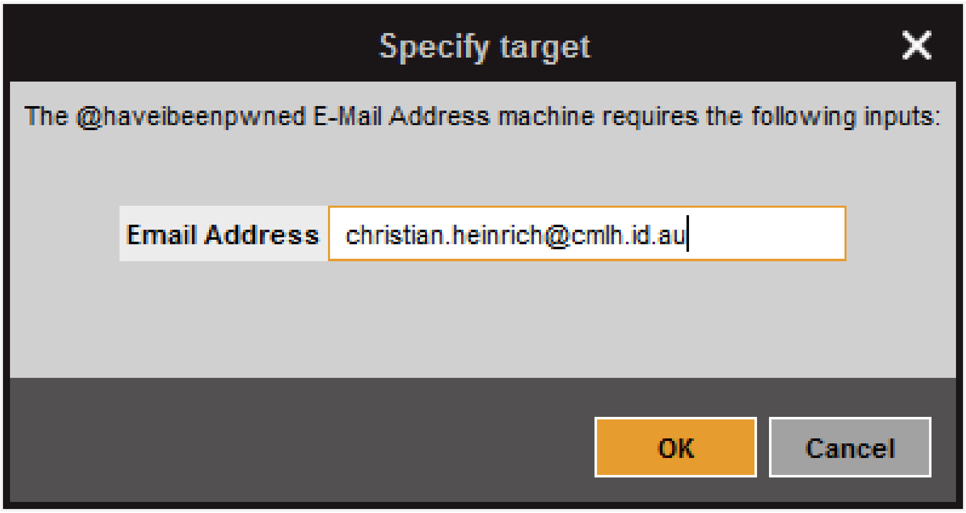
christian.heinrich@cmlh.id.au

Get all pastes featuring the e-mail address [v2 @haveibeenpwned]

QuickLeak - QtPly6aE

Yellow Link

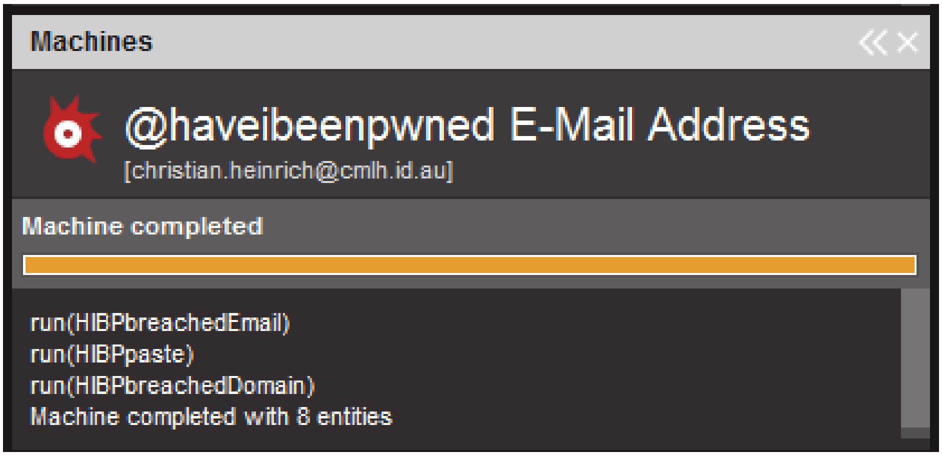
# @haveibeenpwned – Maltego Machines



The @haveibeenpwned E-Mail Address machine requires the following inputs:

Email Address: christian.heinrich@cmlh.id.au

# @haveibeenpwned – Maltego Machines

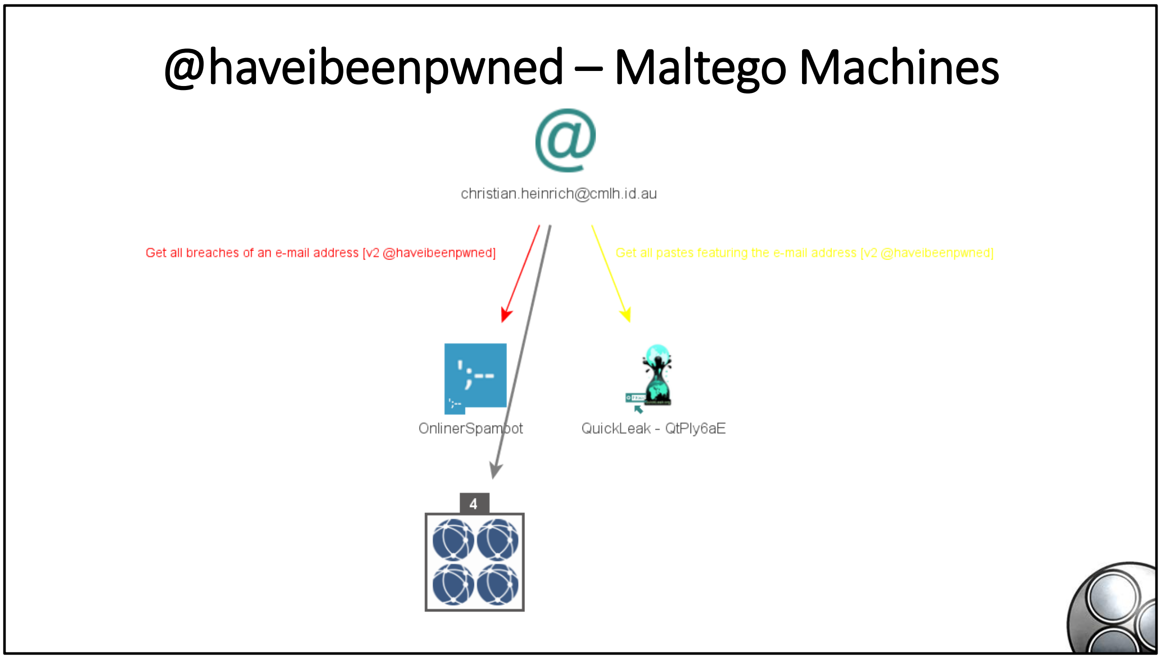


@haveibeenpwned E-Mail Address

[christian.heinrich@cmlh.id.au]

Machine completed

```
run(HIBPbreachedEmail)
run(HIBPpaste)
run(HIBPbreachedDomain)
Machine completed with 8 entities
```

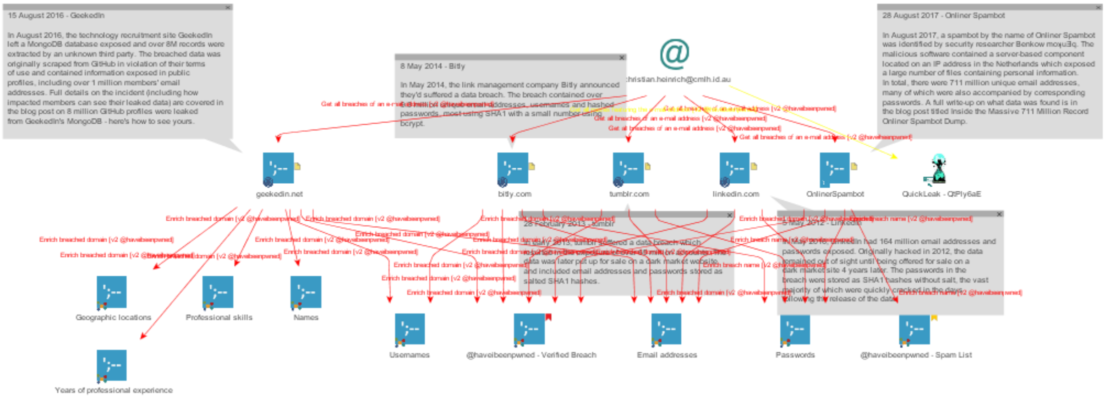


# @haveibeenpwned – Maltego Machines

christian.heinrich@cmlh.id.au
Get all breaches of an e-mail address [v2 @haveibeenpwned]
Get all pastes featuring the e-mail address [v2 @haveibeenpwned]
OnlinerSpambot
QuickLeak - QtPly6aE
4

Collections

# @haveibeenpwned – Maltego Machines



15 August 2016 - GeekedIn

In August 2016, the technology recruitment site GeekedIn left a MongoDB database exposed and over 8M records were extracted by an unknown third party. The breached data was originally scraped from GitHub in violation of their terms of use and contained information exposed in public profiles, including over 1 million members' email addresses. Full details on the incident (including how impacted members can see their leaked data) are covered in the blog post on 8 million GitHub profiles were leaked from GeekedIn's MongoDB - here's how to see yours.

8 May 2014 - Bitly

In May 2014, the link management company Bitly announced they'd suffered a data breach. The breach contained over 9.3 million unique email addresses, usernames and hashed passwords, most using SHA1 with a small number using bcrypt.

28 August 2017 - Onliner Spambot

In August 2017, a spambot by the name of Onliner Spambot was identified by security researcher Benkow moʞuƎq. The malicious software contained a server-based component located on an IP address in the Netherlands which exposed a large number of files containing personal information. In total, there were 711 million unique email addresses, many of which were also accompanied by corresponding passwords. A full write-up on what data was found is in the blog post titled Inside the Massive 711 Million Record Onliner Spambot Dump.

28 February 2013 - tumblr

In early 2013, tumblr suffered a data breach which resulted in the exposure of over 65 million accounts. The data was later put up for sale on a dark market website and included email addresses and passwords stored as salted SHA1 hashes.

5 May 2012 - LinkedIn

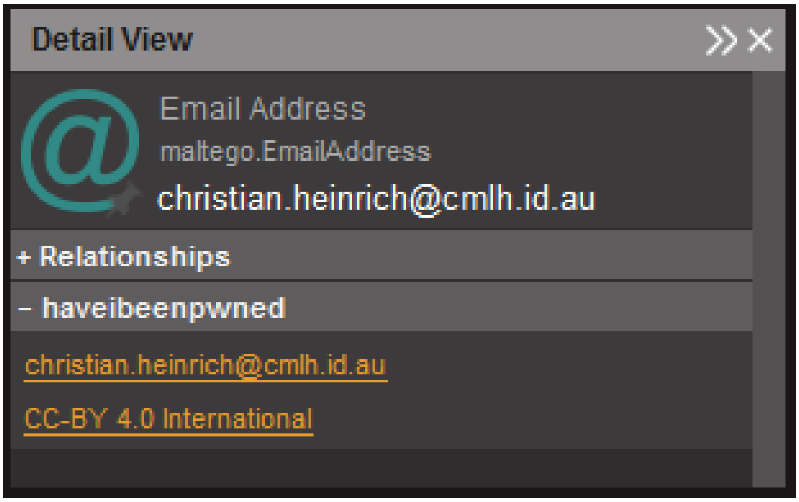
In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

christian.heinrich@cmlh.id.au
Get all breaches of an e-mail address [v2 @haveibeenpwned]
Get all pastes featuring the e-mail address
geekedin.net
bitly.com
tumblr.com
linkedin.com
OnlinerSpambot
QuickLeak - QtPly6aE
Enrich breached domain [v2 @haveibeenpwned]
Enrich breach name [v2 @haveibeenpwned]
Geographic locations
Professional skills
Names
Years of professional experience
Usernames
@haveibeenpwned - Verified Breach
Email addresses
Passwords
@haveibeenpwned - Spam List

Collections Disabled

Domains and Breach Names Link colour changed to red

# @haveibeenpwned – `<DisplayInformation>`



Detail View

Email Address

maltego.EmailAddress

christian.heinrich@cmlh.id.au

+ Relationships

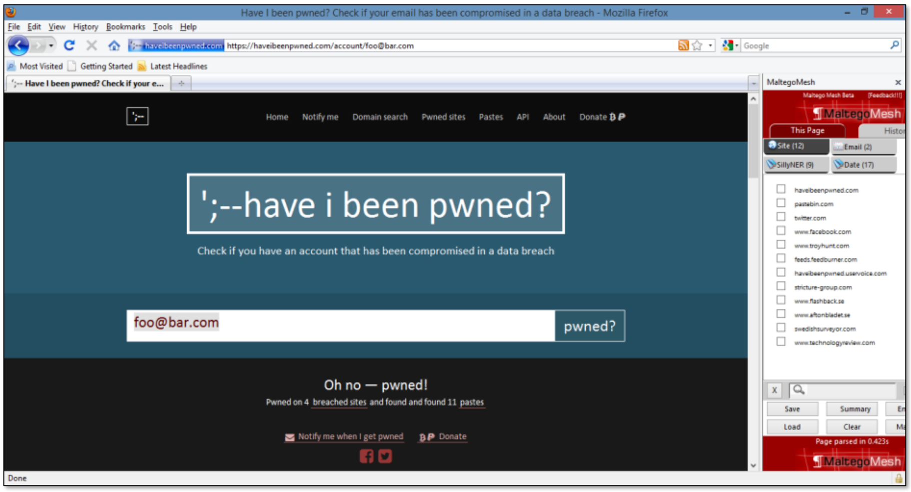
– haveibeenpwned

christian.heinrich@cmlh.id.au

CC-BY 4.0 International

https://haveibeenpwned.com/account/christian.heinrich@cmlh.id.au

# @haveibeenpwned – `<DisplayInformation>`



Have I been pwned? Check if your email has been compromised in a data breach - Mozilla Firefox

https://haveibeenpwned.com/account/foo@bar.com

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

foo@bar.com

Oh no — pwned!

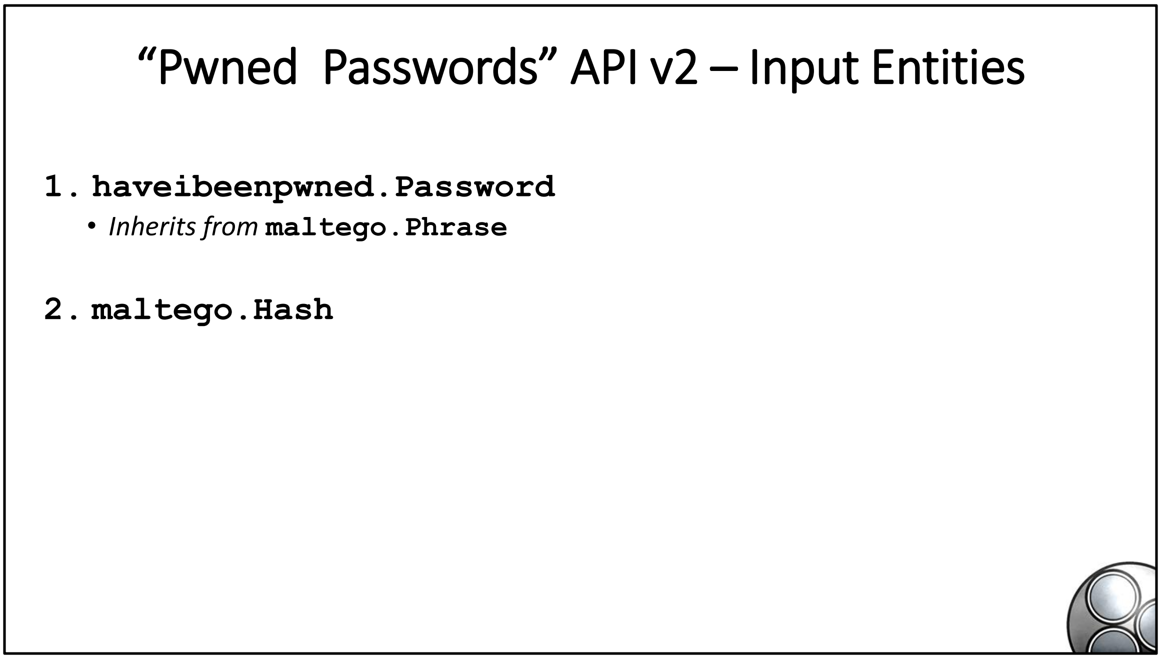
Pwned on 4 breached sites and found 11 pastes

Page parsed in 0.423s

- □ haveibeenpwned.com
- □ pastebin.com
- □ twitter.com
- □ www.facebook.com
- □ www.troyhunt.com
- □ feeds.feedburner.com
- □ haveibeenpwned.uservoice.com
- □ stricture-group.com
- □ www.flashback.se
- □ www.aftonbladet.se
- □ swedishsurveyor.com
- □ www.technologyreview.com

foo@bar.com from https://haveibeenpwned.com/API/v2#BreachesForAccount

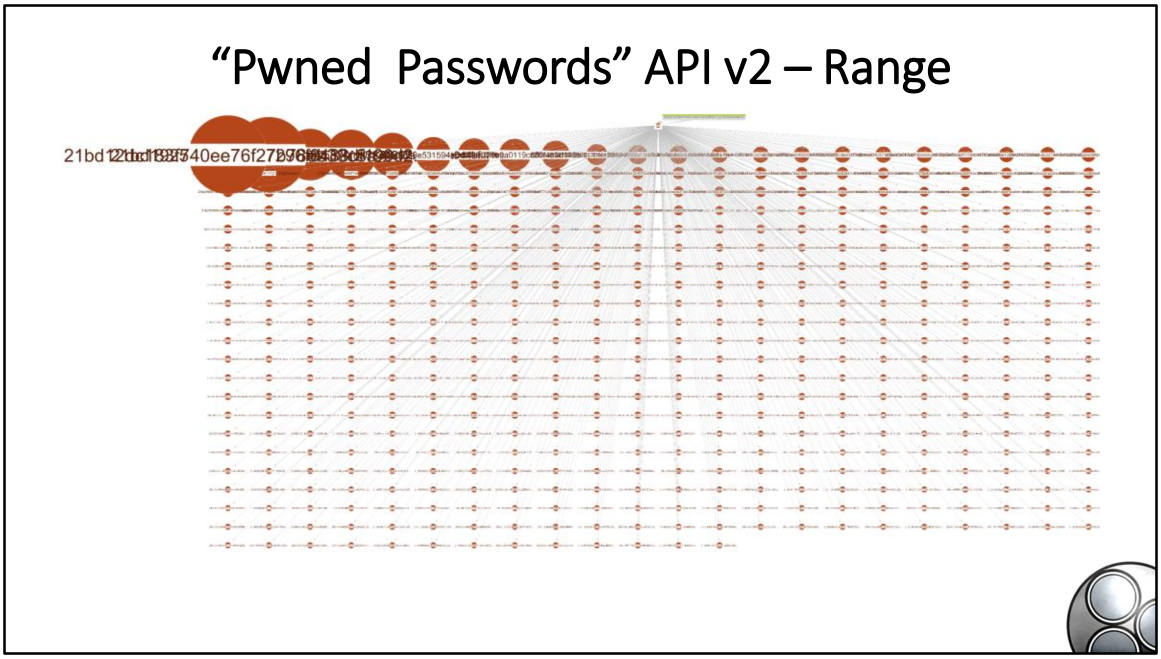
https://haveibeenpwned.com/account/foo@bar.com



# “Pwned  Passwords” API v2 – Input Entities

1. **`haveibeenpwned.Password`**
   - *Inherits from* **`maltego.Phrase`**

2. **`maltego.Hash`**



# “Pwned  Passwords” API v2 – Range

Weighting

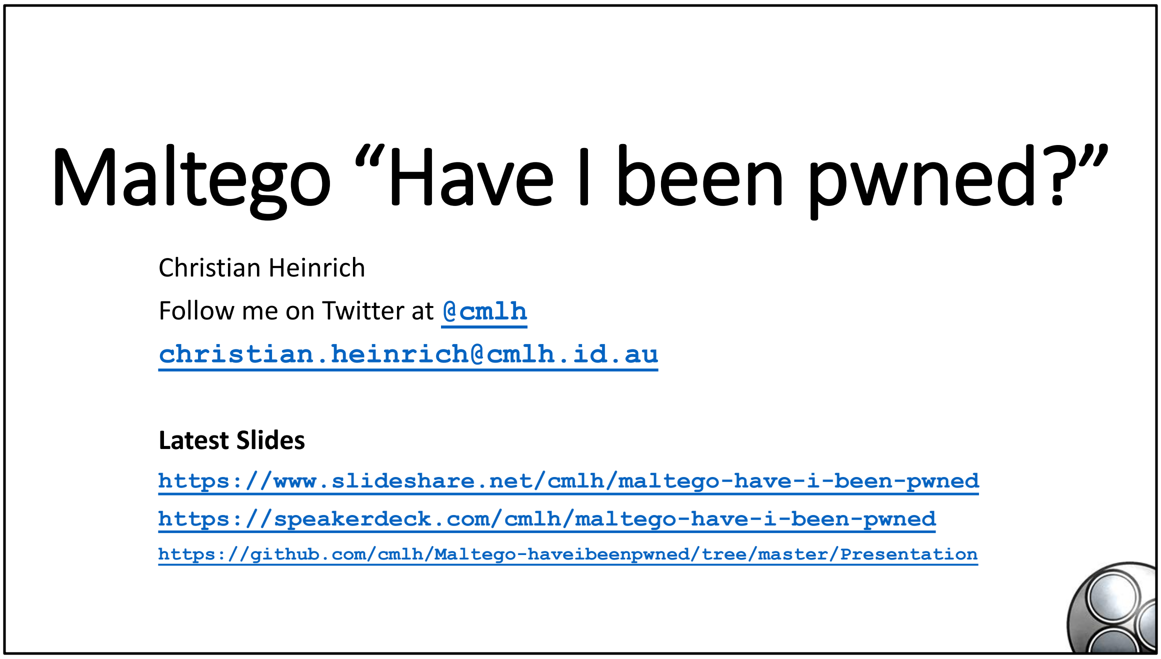
# Thanks

@troyhunt of @haveibeenpwned

@SudhanshuC of the forked Maltego local transforms

~~@RoelofTemmingh,~~ @AndrewMohawk and @paulRchds of @Paterva
@NoobieDog, @glennzw and @charlvdwalt of @SensePost
@dcuthbert

http://maltego.blogspot.com.au/2017/12/time-to-say-goodbye.html



# Maltego “Have I been pwned?”

Christian Heinrich

Follow me on Twitter at @cmlh

christian.heinrich@cmlh.id.au

**Latest Slides**

https://www.slideshare.net/cmlh/maltego-have-i-been-pwned

https://speakerdeck.com/cmlh/maltego-have-i-been-pwned

https://github.com/cmlh/Maltego-haveibeenpwned/tree/master/Presentation

https://twitter.com/cmlh