Maltego “Have I been pwned?”

Christian Heinrich

DEFCON 25 (2017)

Demo Labs

Latest Slides

https://www.slideshare.net/cmlh/maltego-haveibeenpwned

https://speakerdeck.com/cmlh/maltego-haveibeenpwned

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

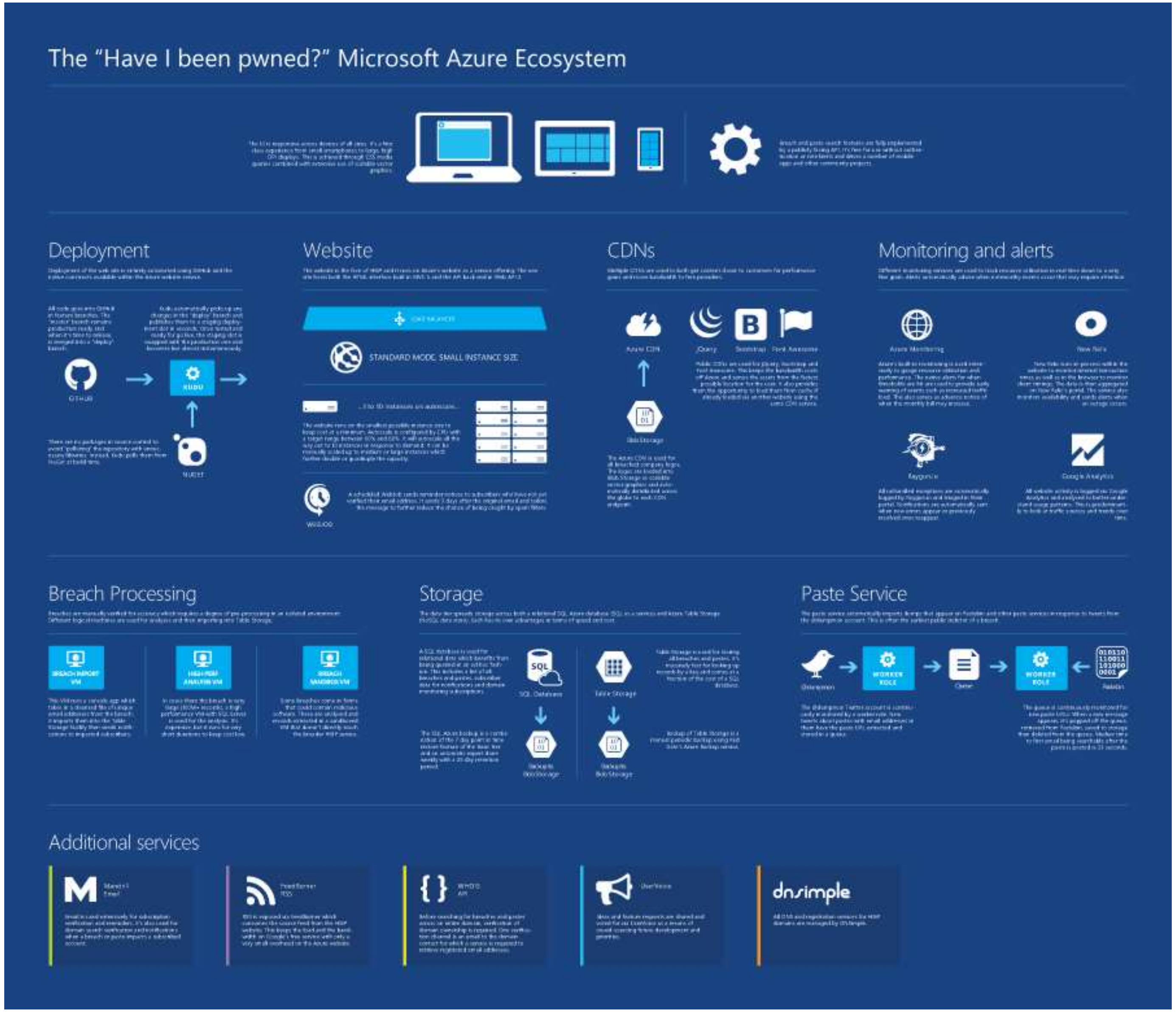
Python Modules from @CanariProject and @Paterva

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

Agenda

1. Integration of the API [v1 and v2] from @haveibeenpwned
2. Configuration of Maltego:
   - Import Maltego Configuration File.
   - Transform Hub
3. Case Studies
   - End User (Penetration Tester, Incident Responder, etc)

"Have I been pwned?"

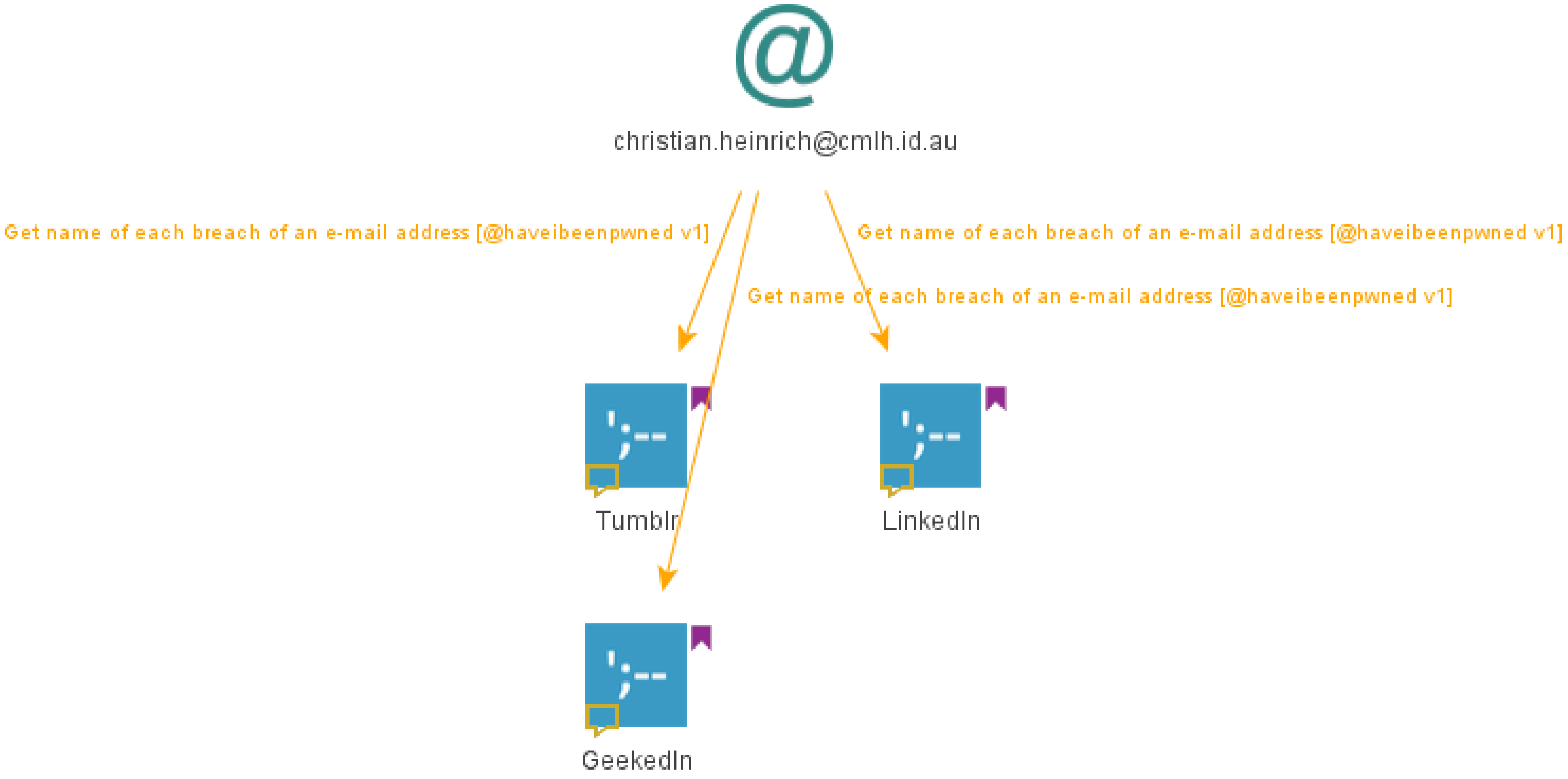


@haveibeenpwned – API v1

Integrated Single API **v1** Endpoint.

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

@haveibeenpwned – API v1



christian.heinrich@cmlh.id.au

Get name of each breach of an e-mail address [@haveibeenpwned v1]

Get name of each breach of an e-mail address [@haveibeenpwned v1]

Get name of each breach of an e-mail address [@haveibeenpwned v1]

Tumblr

LinkedIn

GeekedIn

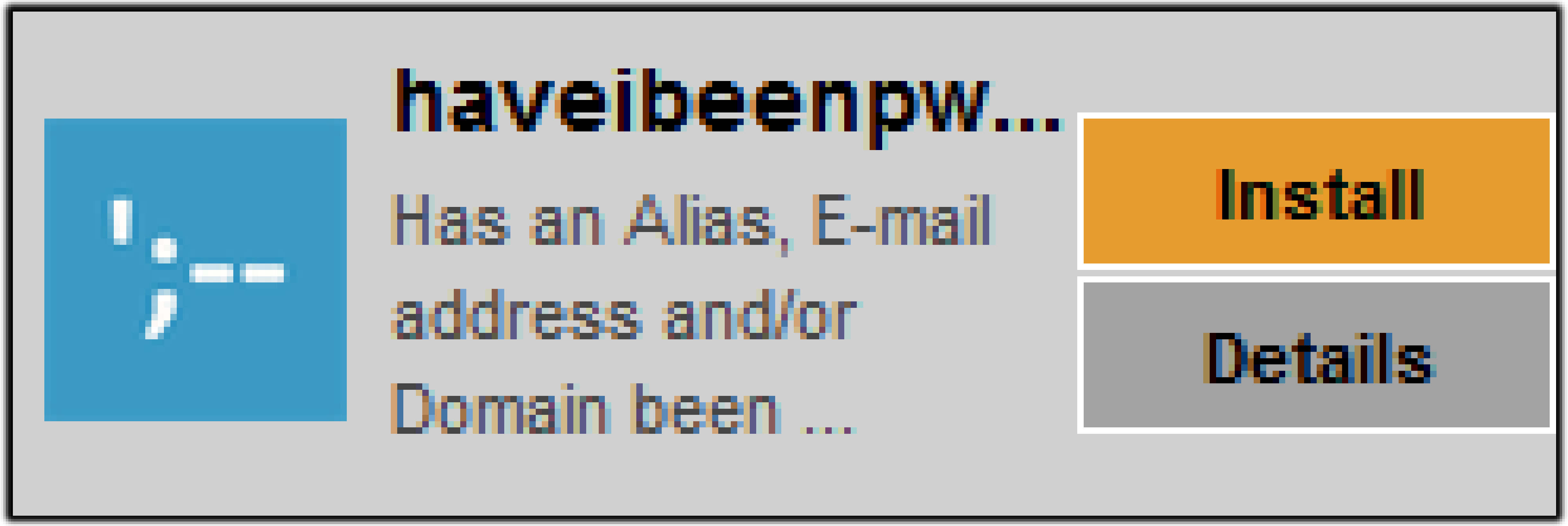
@haveibeenpwned – API v2

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

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

Installation



haveibeenpw...

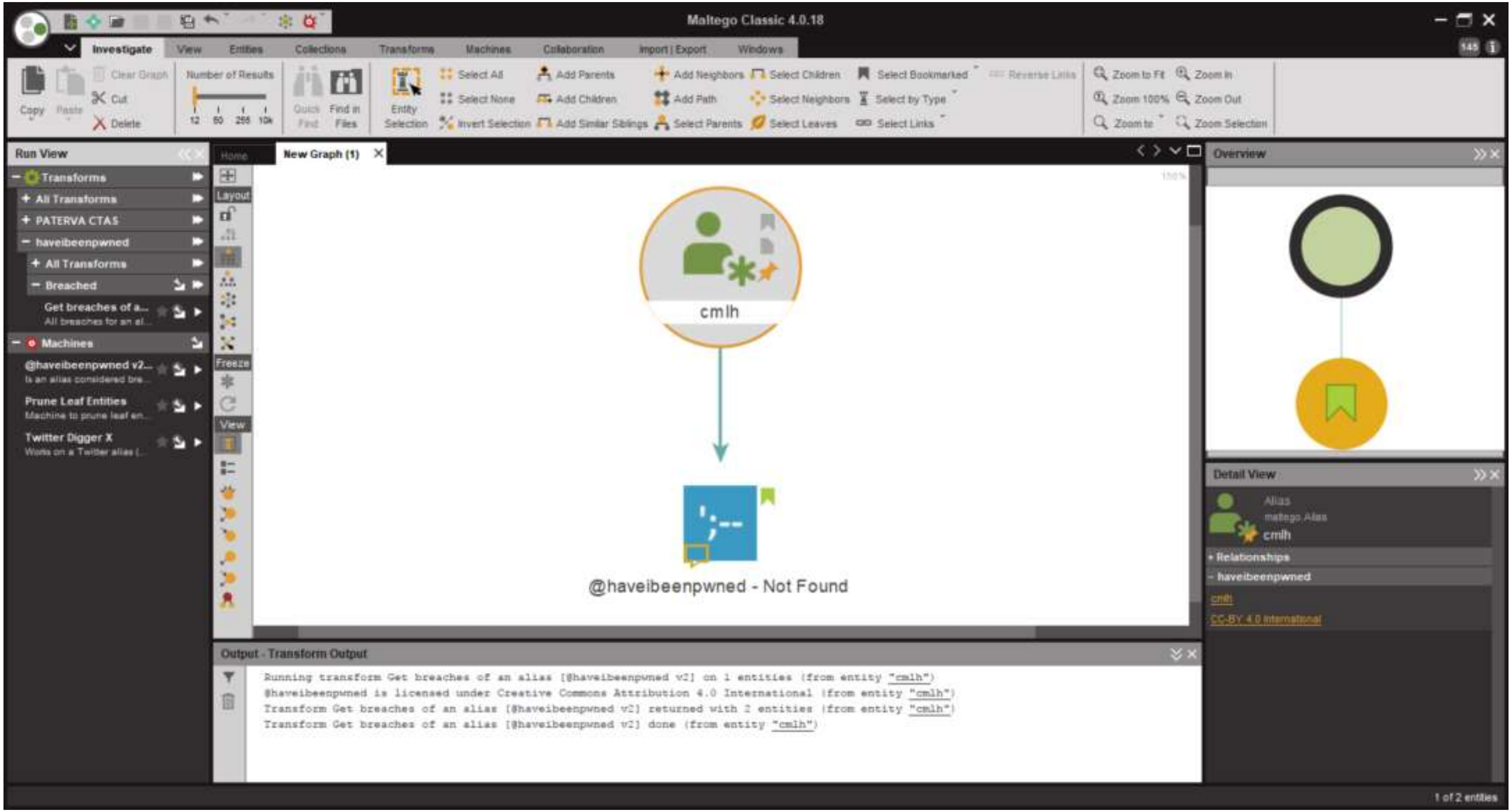
Has an Alias, E-mail address and/or Domain been ...

@haveibeenpwned – Maltego Input Entities

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

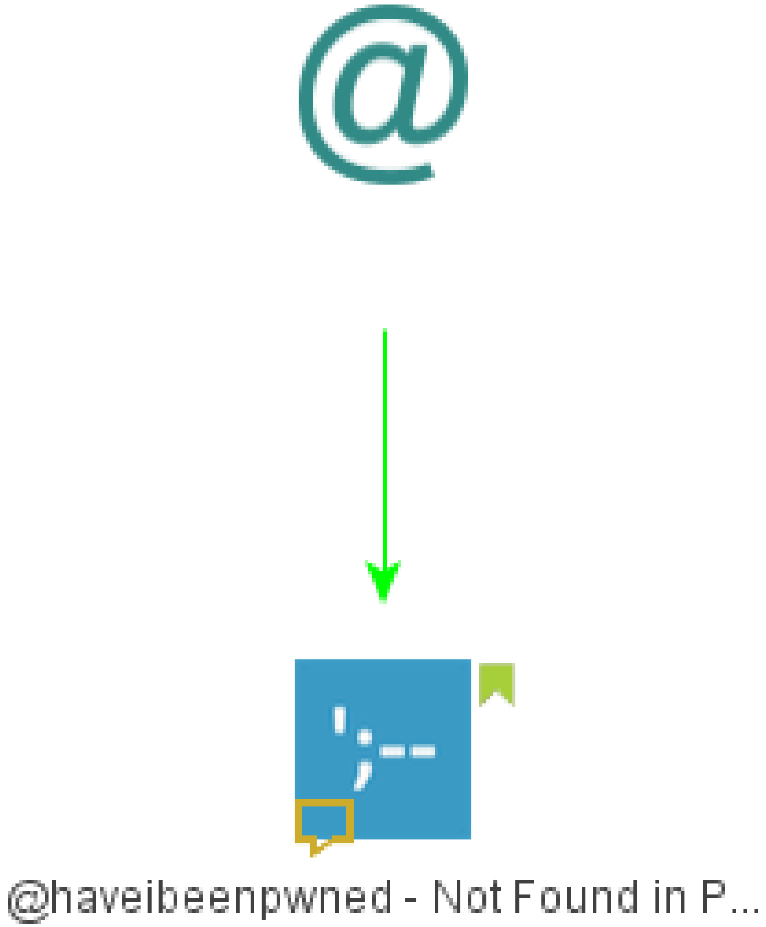
2. *“Site”*
    1. **`maltego.Domain`**
    2. **`Maltego.Phrase`**

@haveibeenpwned – `maltego.Alias` Entity

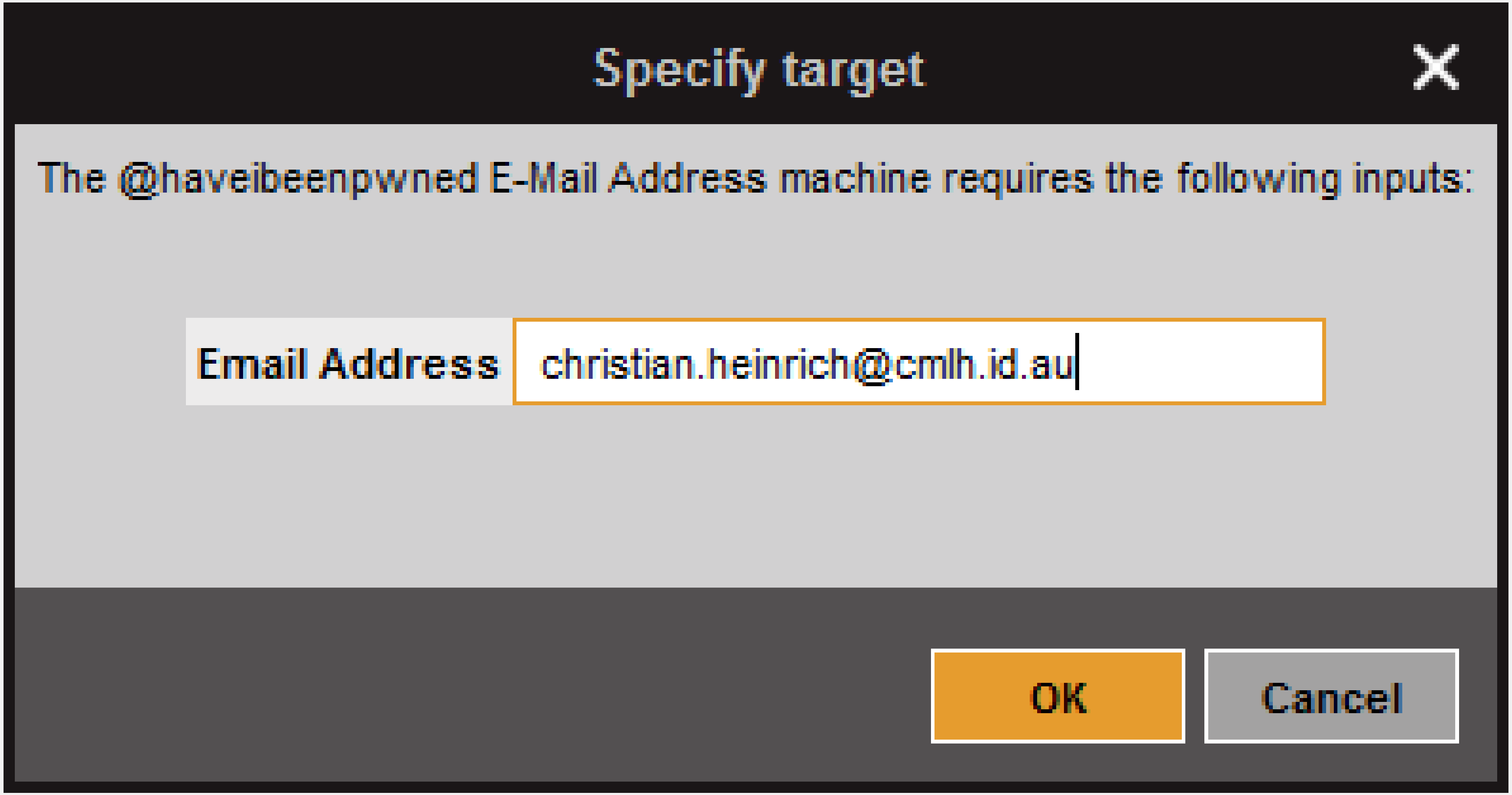


```
Running transform Get breaches of an alias [@haveibeenpwned v2] on 1 entities (from entity "cmlh")
@haveibeenpwned is licensed under Creative Commons Attribution 4.0 International (from entity "cmlh")
Transform Get breaches of an alias [@haveibeenpwned v2] returned with 2 entities (from entity "cmlh")
Transform Get breaches of an alias [@haveibeenpwned v2] done (from entity "cmlh")
```

@haveibeenpwned - Paste



@haveibeenpwned – Maltego Machines

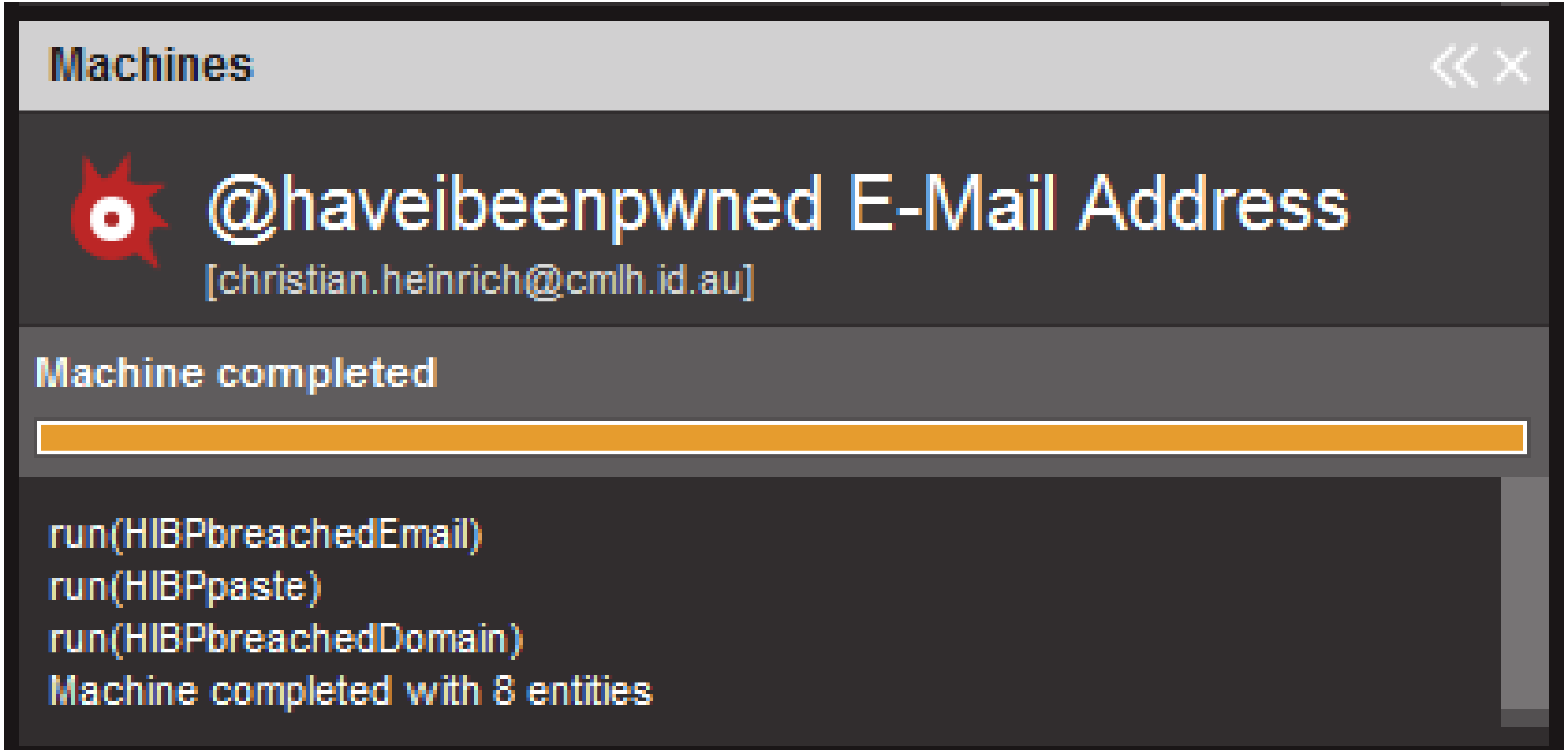


Specify target

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

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

@haveibeenpwned – Maltego Machines



Machines

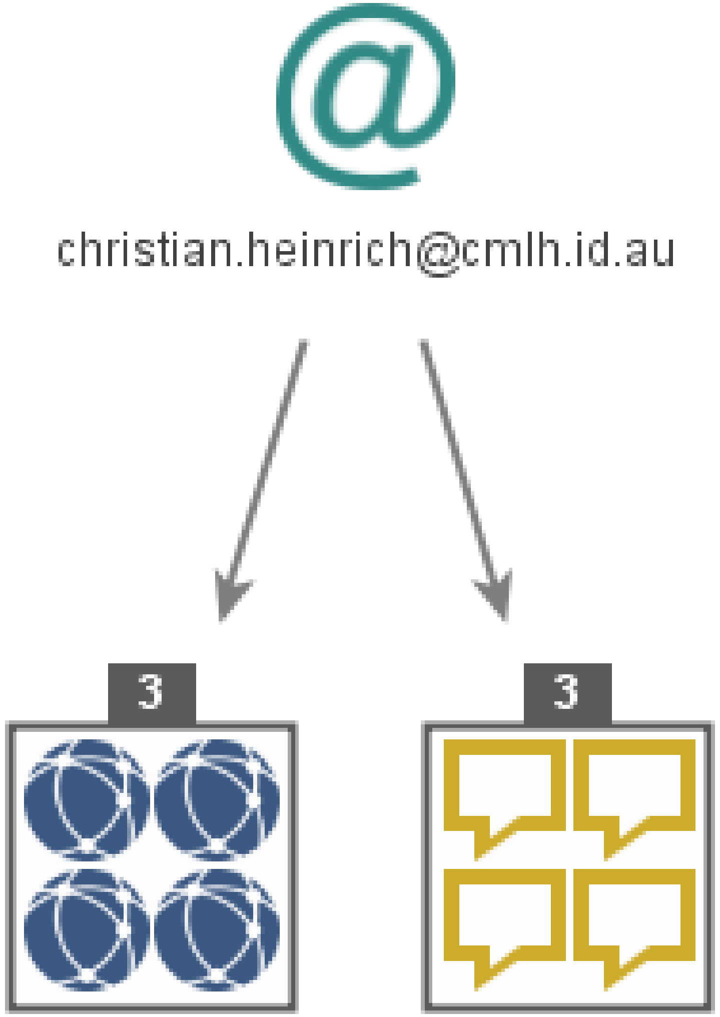
@haveibeenpwned E-Mail Address

[christian.heinrich@cmlh.id.au]

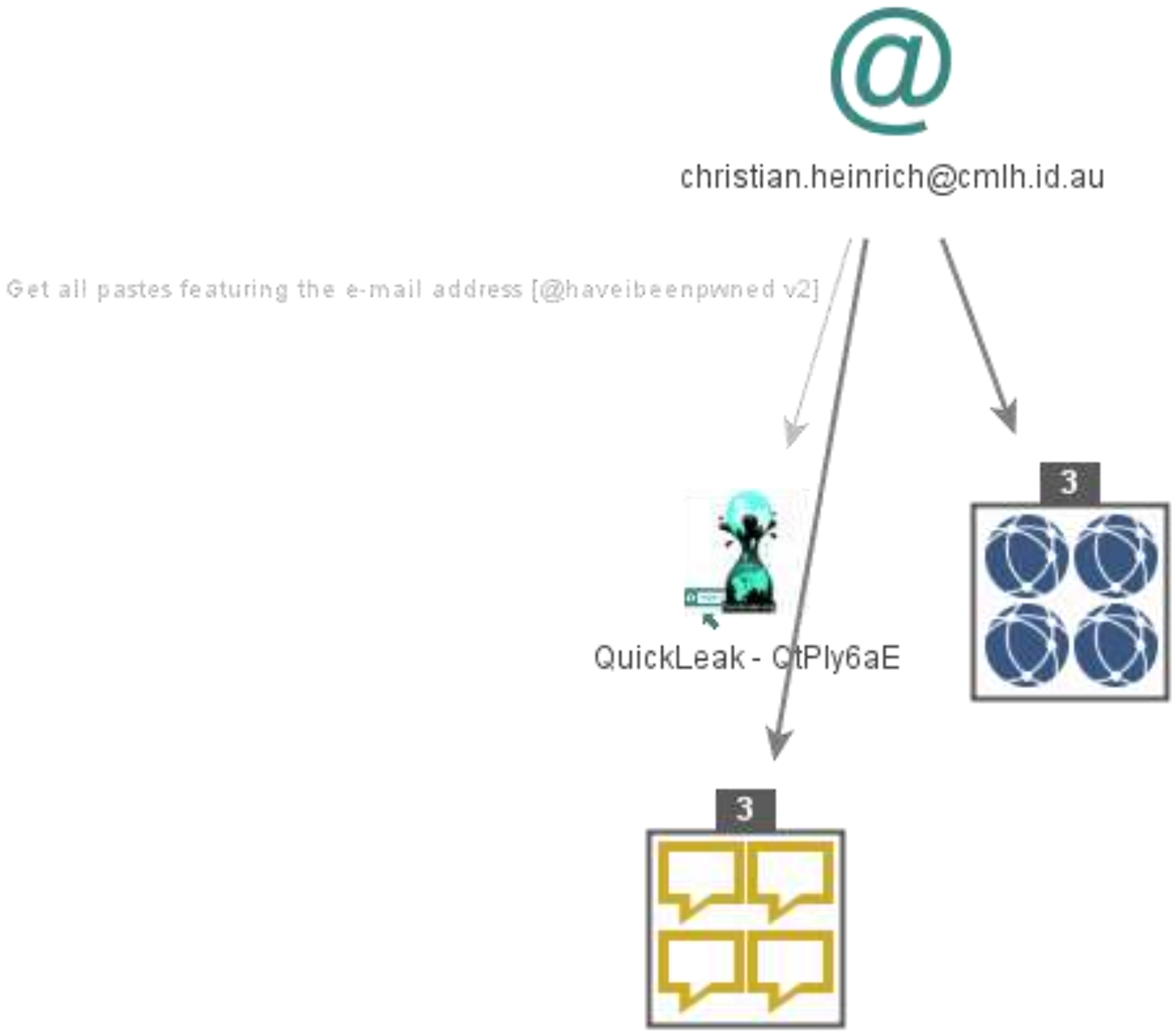
Machine completed

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

@haveibeenpwned – Maltego Machines

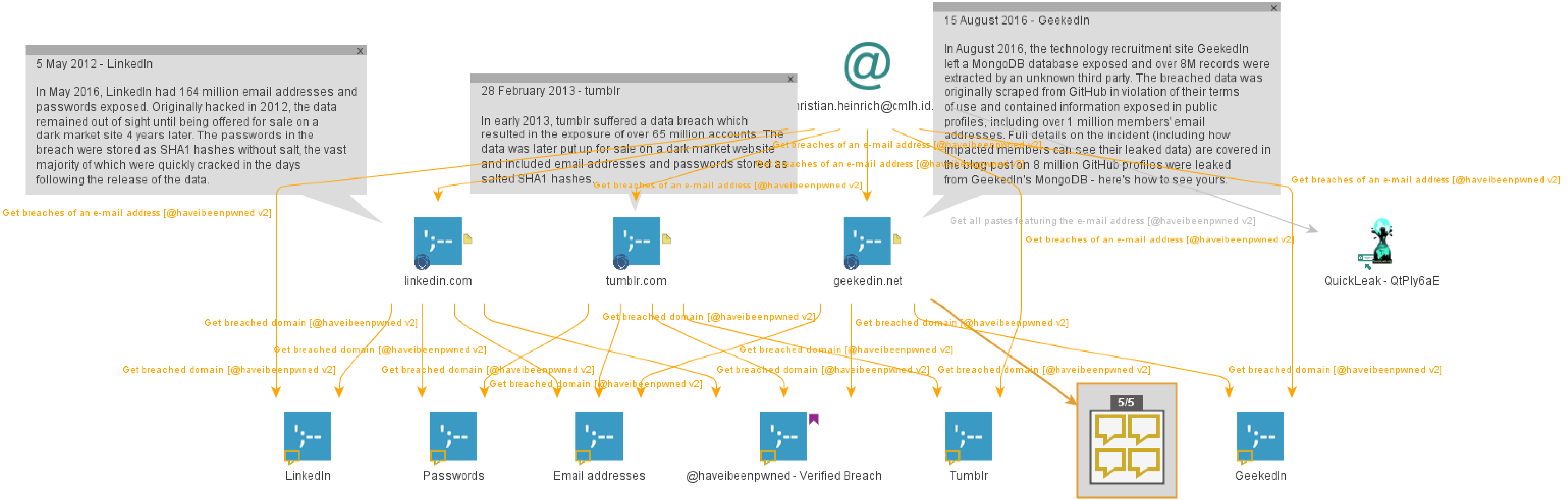


@haveibeenpwned – Maltego Machines



christian.heinrich@cmlh.id.au
Get all pastes featuring the e-mail address [@haveibeenpwned v2]
QuickLeak - QtPly6aE
3
3

@haveibeenpwned – Maltego Machines



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.

28 February 2013 - tumblr

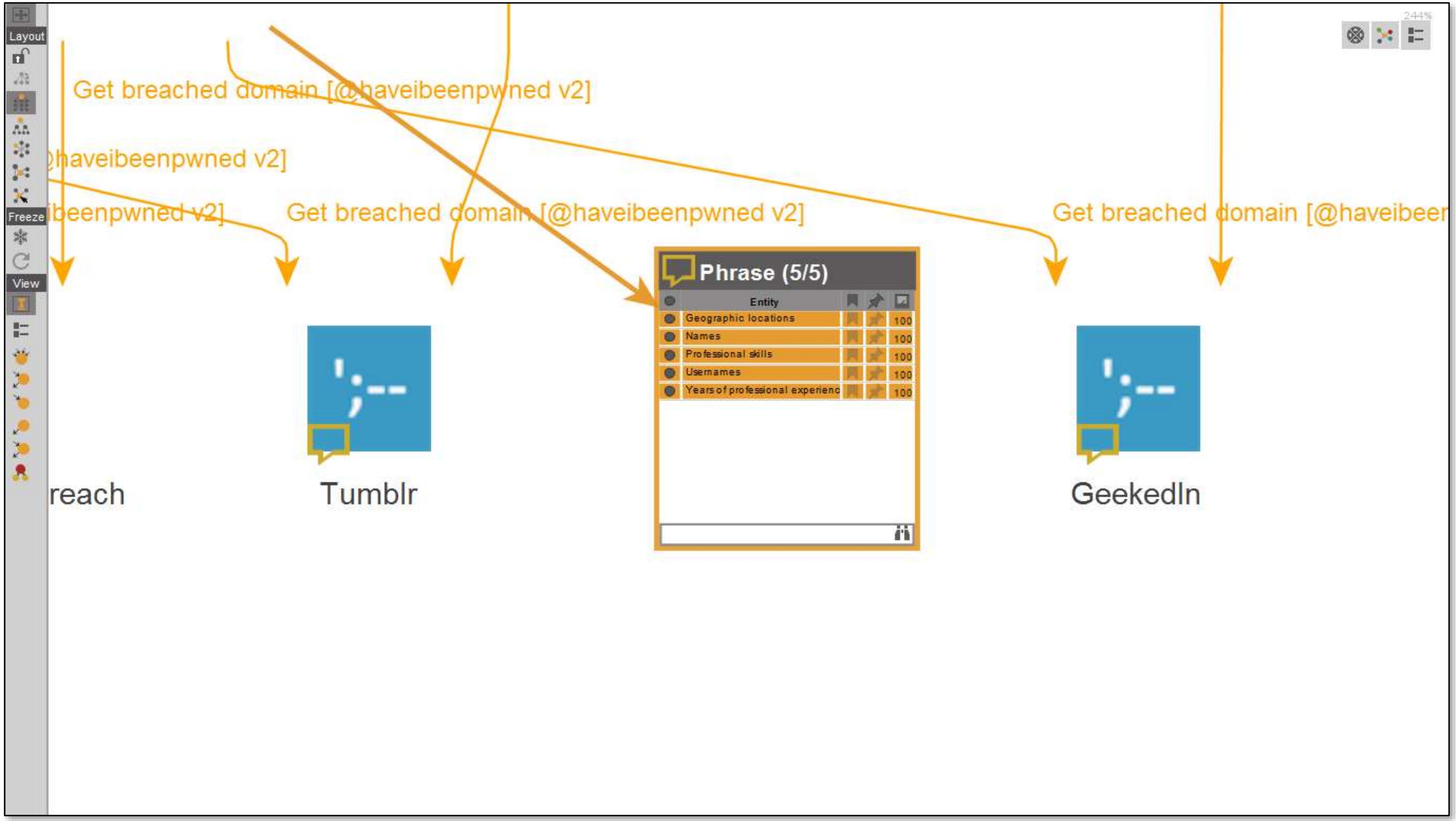
In early 2013, tumblr suffered a data breach which resulted in the exposure of over 65 million accounts. The data was later put up for sale on a dark market website and included email addresses and passwords stored as salted SHA1 hashes.

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.

hristian.heinrich@cmlh.id.
Get breaches of an e-mail address [@haveibeenpwned v2]
Get all pastes featuring the e-mail address [@haveibeenpwned v2]
linkedin.com
tumblr.com
geekedin.net
QuickLeak - QtPly6aE
Get breached domain [@haveibeenpwned v2]
LinkedIn
Passwords
Email addresses
@haveibeenpwned - Verified Breach
Tumblr
5/5
GeekedIn

@haveibeenpwned – Maltego Machines

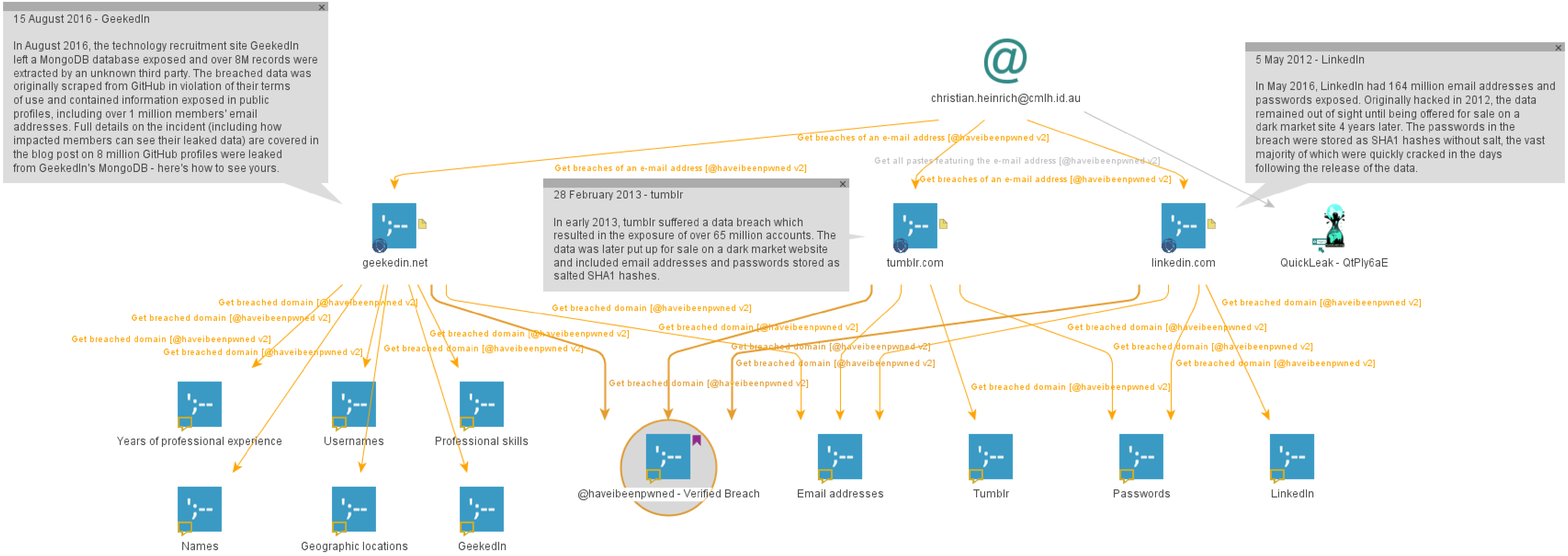


Layout
Freeze
View
Get breached domain [@haveibeenpwned v2]
@haveibeenpwned v2]
ibeenpwned v2]
Get breached domain [@haveibeenpwned v2]
Get breached domain [@haveibeer
reach
Tumblr
GeekedIn
244%

Phrase (5/5)

	Entity			
●	Geographic locations			100
●	Names			100
●	Professional skills			100
●	Usernames			100
●	Years of professional experienc			100

@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.

28 February 2013 - tumblr

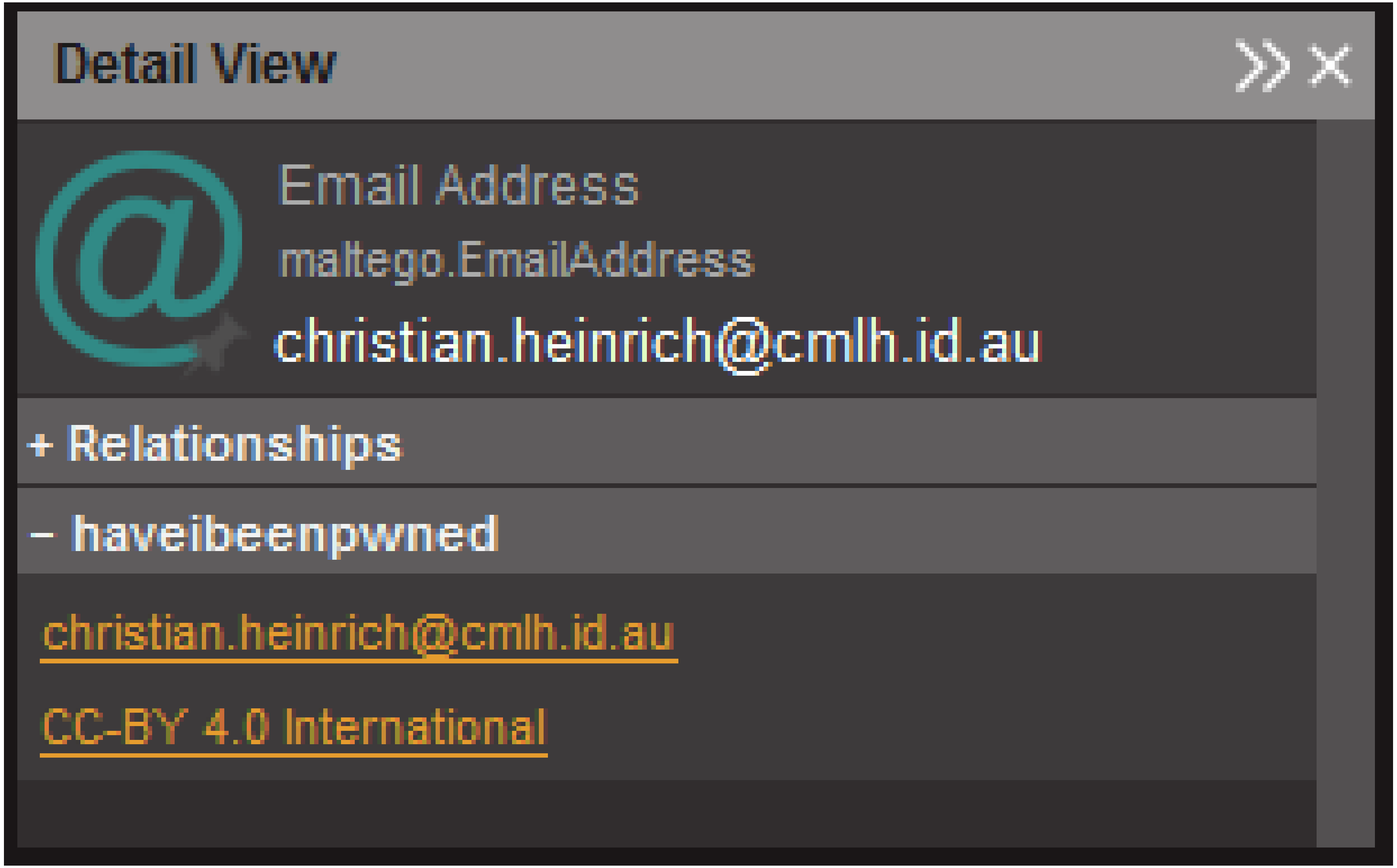
In early 2013, tumblr suffered a data breach which resulted in the exposure of over 65 million accounts. The data was later put up for sale on a dark market website and included email addresses and passwords stored as salted SHA1 hashes.

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 breaches of an e-mail address [@haveibeenpwned v2]
Get breaches of an e-mail address [@haveibeenpwned v2]
Get all pastes featuring the e-mail address [@haveibeenpwned v2]
Get breaches of an e-mail address [@haveibeenpwned v2]
geekedin.net
tumblr.com
linkedin.com
QuickLeak - QtPly6aE
Get breached domain [@haveibeenpwned v2]
Years of professional experience
Usernames
Professional skills
Names
Geographic locations
GeekedIn
@haveibeenpwned - Verified Breach
Email addresses
Tumblr
Passwords
LinkedIn

@haveibeenpwned – <DisplayInformation>



Detail View

Email Address

maltego.EmailAddress

christian.heinrich@cmlh.id.au

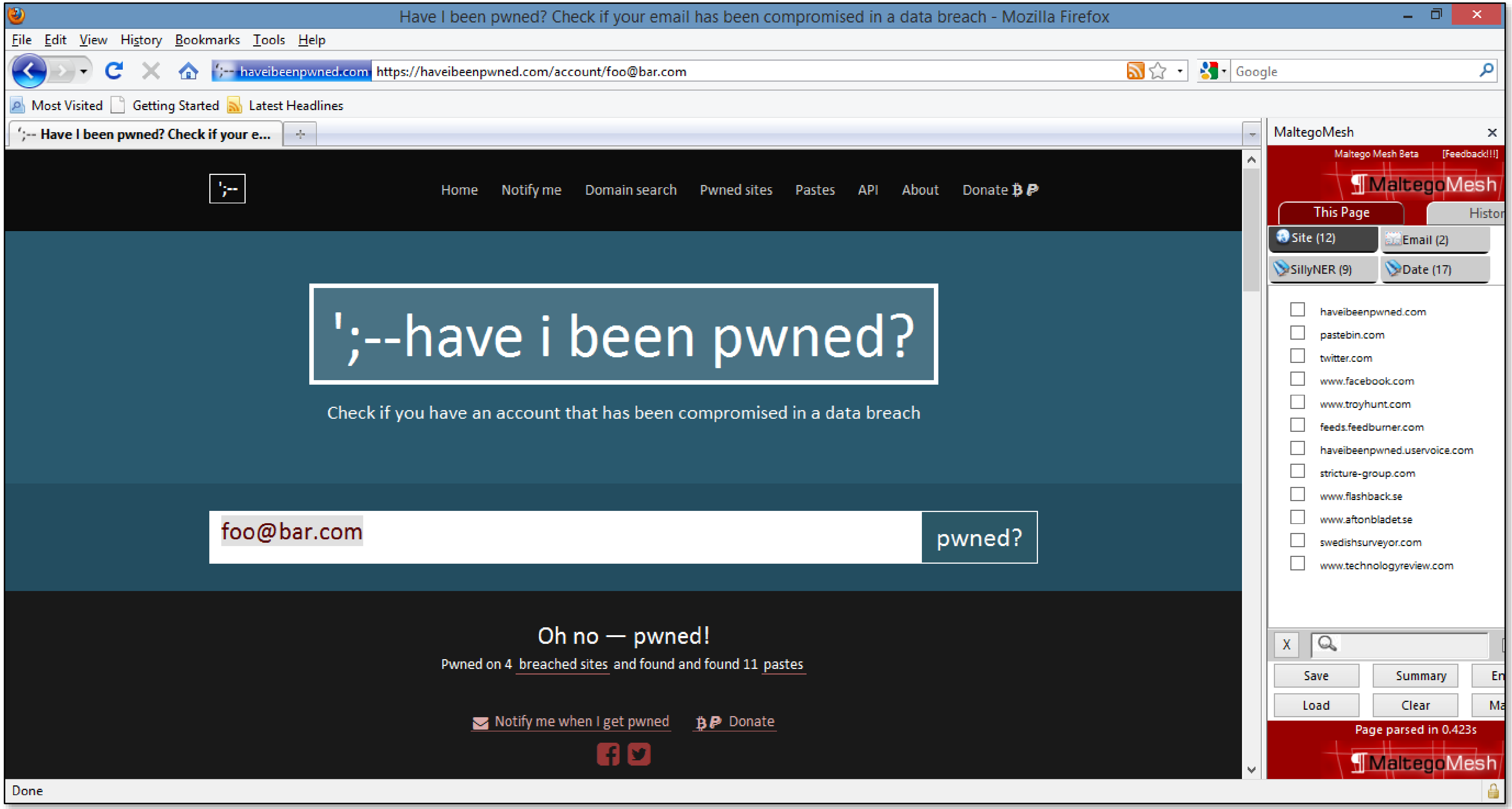
+ Relationships

– haveibeenpwned

christian.heinrich@cmlh.id.au

CC-BY 4.0 International

@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 and found 11 pastes

Notify me when I get pwned

Donate

MaltegoMesh

Site (12)

Email (2)

SillyNER (9)

Date (17)

- □ 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

Page parsed in 0.423s

Done

Thanks

@troyhunt of @haveibeenpwned

@SudhanshuC of the forked Maltego local transforms

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

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-haveibeenpwned

https://speakerdeck.com/cmlh/maltego-haveibeenpwned

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