

Maltego “Have I been pwned?”

Christian Heinrich

DEFCON 25 (2017)

Demo Labs



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] from @haveibeenpwned
2. Configuration of Maltego:
 - Import Maltego Configuration File.
 - Transform Hub
3. Case Studies
 - End User (Penetration Tester, Incident Responder, etc)



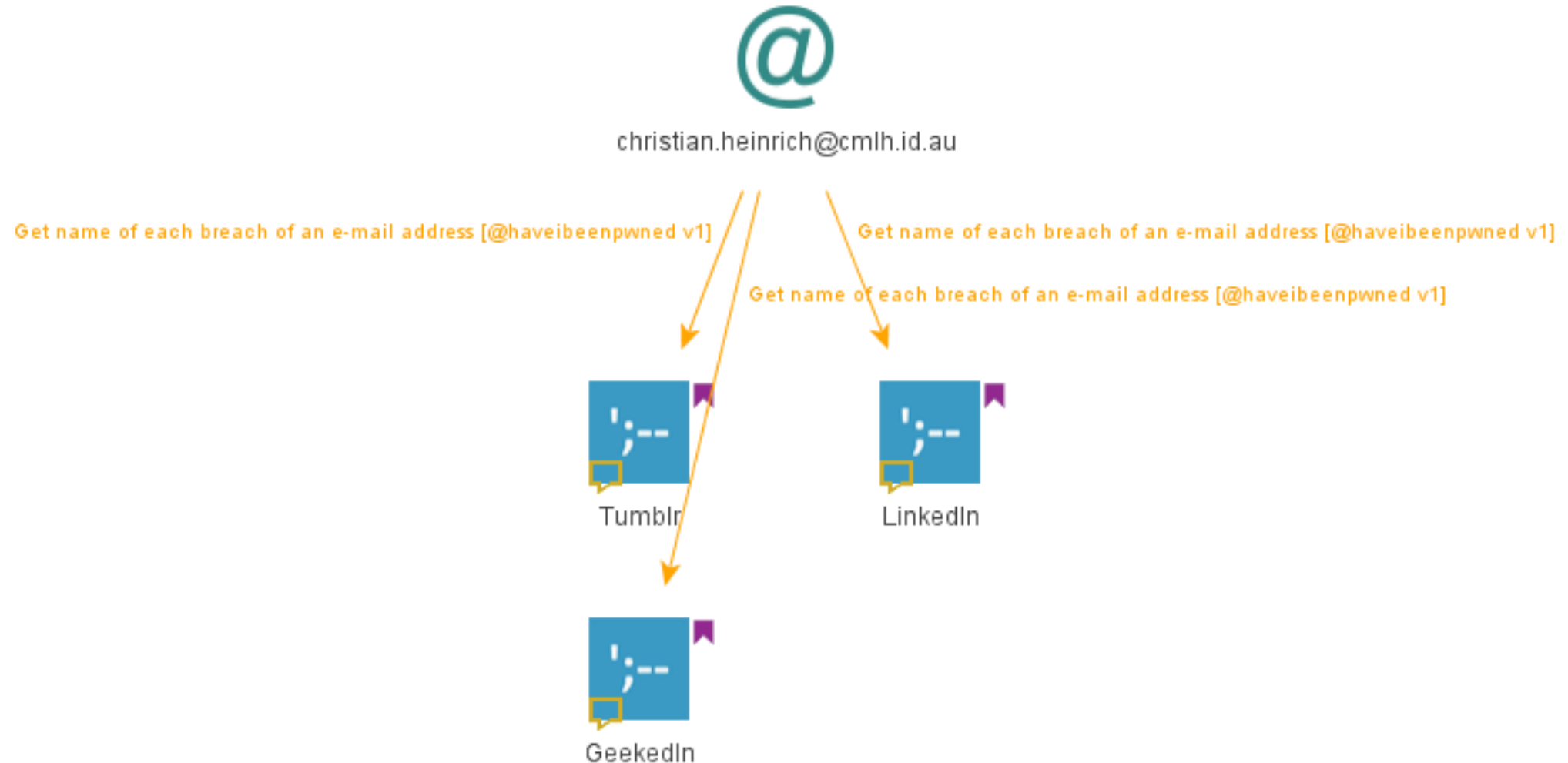
@haveibeenpwned – API v1

Integrated Single API **v1** Endpoint.

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



@haveibeenpwned – API v1



@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



have been pw...

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

Install

Details



@haveibeenpwned – Maltego Input Entities

1. *“Account”*

- 1. `maltego.EmailAddress`
- 2. `maltego.Alias`

2. *“Site”*

- 1. `maltego.Domain`
- 2. `Maltego.Phrase`



@haveibeenpwned – maltego .Alias Entity

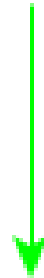
The screenshot displays the Maltego Classic 4.0.18 interface. The main workspace shows a graph with two entities: a green circular entity labeled 'cmih' and a blue square entity labeled '@haveibeenpwned - Not Found'. A green arrow points from 'cmih' to '@haveibeenpwned - Not Found'. The left sidebar contains a 'Run View' panel with a tree structure showing 'Transforms' and 'Machines'. The 'Machines' section is expanded, showing '@haveibeenpwned v2...' and 'Twitter Digger X'. The bottom panel shows the 'Output - Transform Output' for the '@haveibeenpwned v2' transform, displaying the following text:

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

The right sidebar shows the 'Overview' and 'Detail View' panels. The 'Detail View' panel displays the 'Alias' entity 'cmih' and its relationships, including a link to '@haveibeenpwned' and a license link 'CC-BY 4.0 International'.

@haveibeenpwned - Paste

@



@haveibeenpwned - Not Found in P...



@haveibeenpwned – Maltego Machines

Specify target X


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

Email Address	<input type="text" value="christian.heinrich@cmlh.id.au"/>
---------------	--



@haveibeenpwned – Maltego Machines

Machines << x

 **@haveibeenpwned E-Mail Address**
[christian.heinrich@cmlh.id.au]

Machine completed

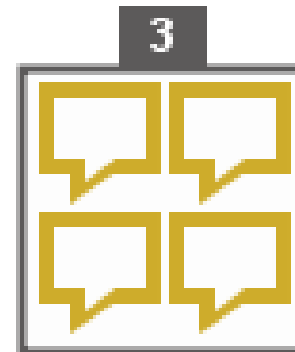
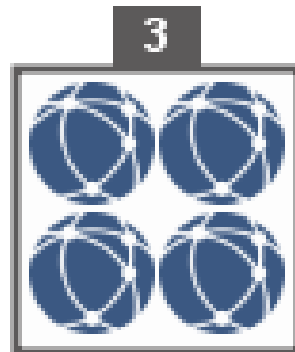
```
run(HIBPbreachedEmail)
run(HIBPpaste)
run(HIBPbreachedDomain)
Machine completed with 8 entities
```



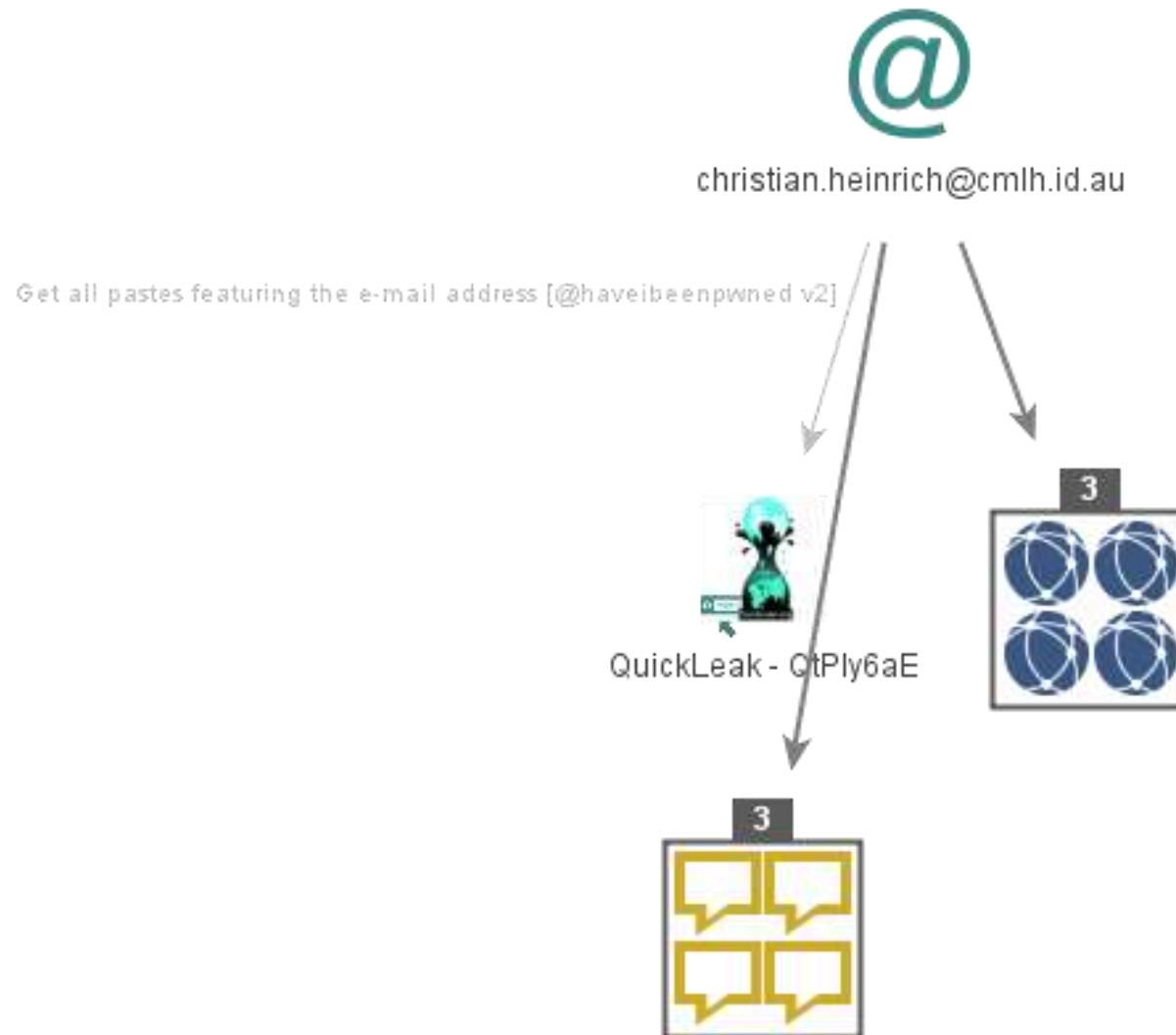
@haveibeenpwned – Maltego Machines



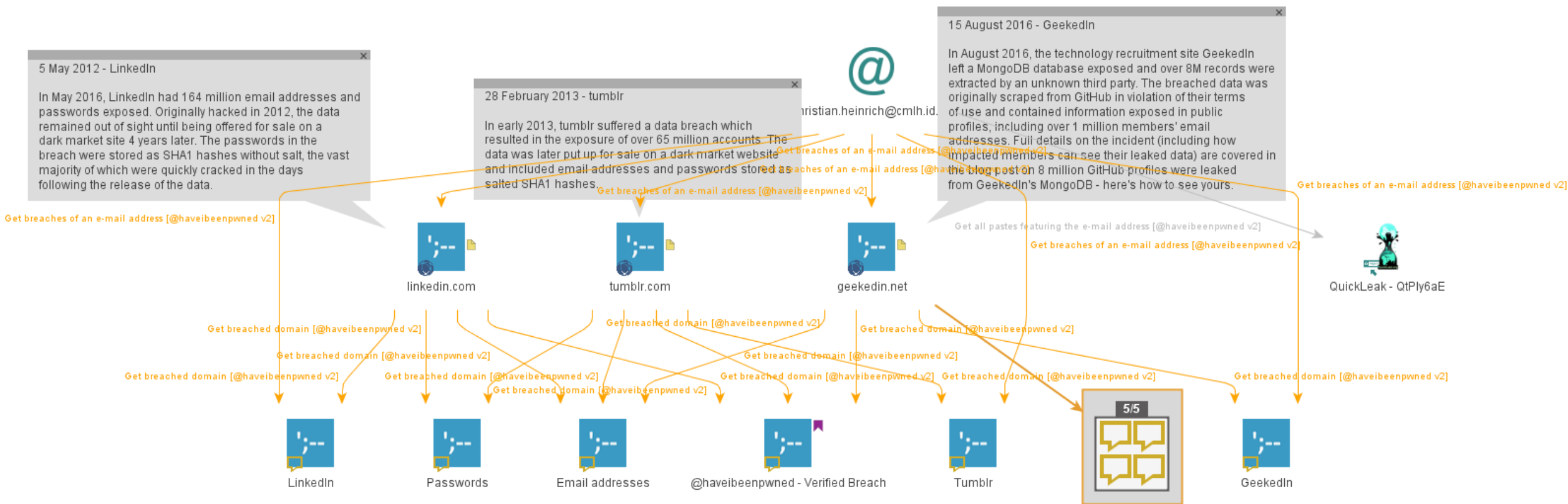
christian.heinrich@cmlh.id.au



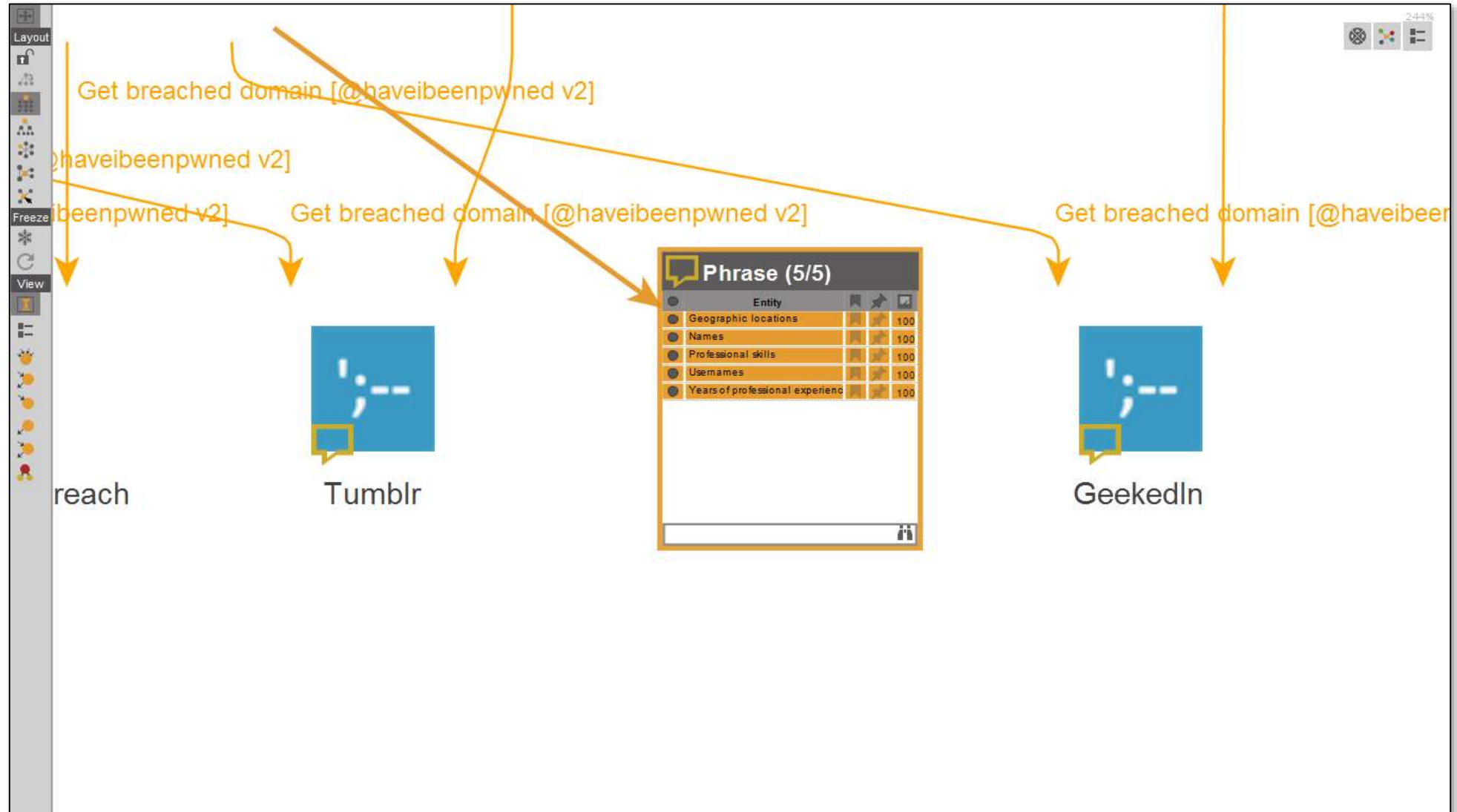
@haveibeenpwned – Maltego Machines

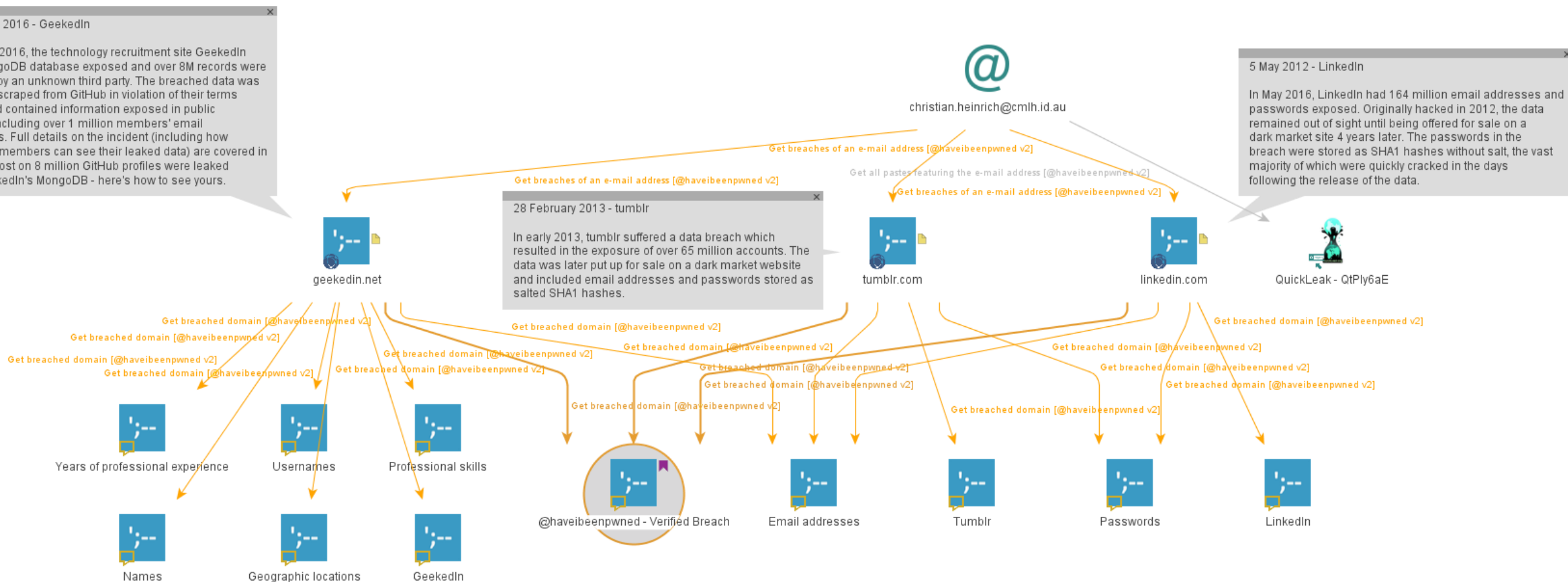


@haveibeenpwned – Maltego Machines



@haveibeenpwned – Maltego Machines






@haveibeenpwned – <DisplayInformation>

Detail View

>> X



Email Address
maltego.EmailAddress
christian.heinrich@cmlh.id.au

+ Relationships

- haveibeenpwned

[christian.heinrich@cmlh.id.au](#)

[CC-BY 4.0 International](#)



@haveibeenpwned – <DisplayInformation>

The screenshot shows a Mozilla Firefox browser window with the title "Have I been pwned? Check if your email has been compromised in a data breach - Mozilla Firefox". The address bar shows the URL "https://haveibeenpwned.com/account/foo@bar.com". The website's navigation bar includes links for Home, Notify me, Domain search, Pwned sites, Pastes, API, About, and Donate. The main content area features a large text input field containing "foo@bar.com" and a "pwned?" button. Below the input field, the message "Oh no — pwned!" is displayed, followed by "Pwned on 4 breached sites and found and found 11 pastes". At the bottom, there are links for "Notify me when I get pwned" and "Donate", along with social media icons for Facebook and Twitter. A MaltegoMesh sidebar is visible on the right, showing a list of domains and a search bar.

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

File Edit View History Bookmarks Tools Help

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

Most Visited Getting Started Latest Headlines

Have I been pwned? Check if your e...

Home Notify me Domain search Pwned sites Pastes API About Donate

';--have i been pwned?

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

foo@bar.com pwned?

Oh no — pwned!

Pwned on 4 breached sites and found and found 11 pastes

Notify me when I get pwned Donate

Facebook Twitter

Done

MaltegoMesh

Maltego Mesh Beta [Feedback!!!]

This Page

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

X

Save Summary

Load Clear

Page parsed in 0.423s

MaltegoMesh

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](https://twitter.com/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>

