

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>

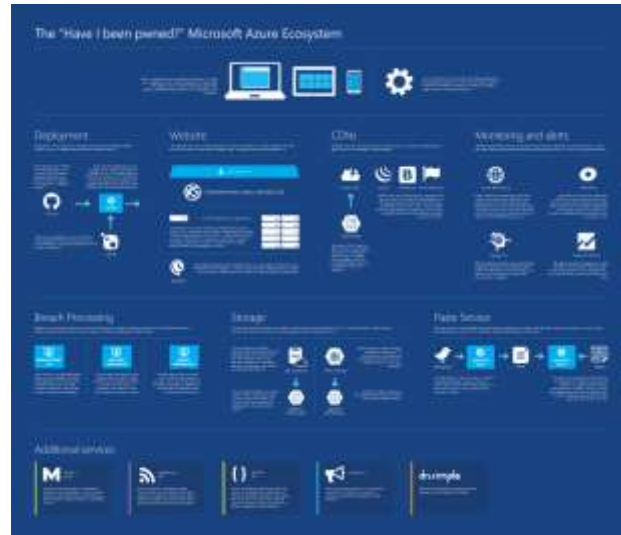


Agenda

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)



“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.

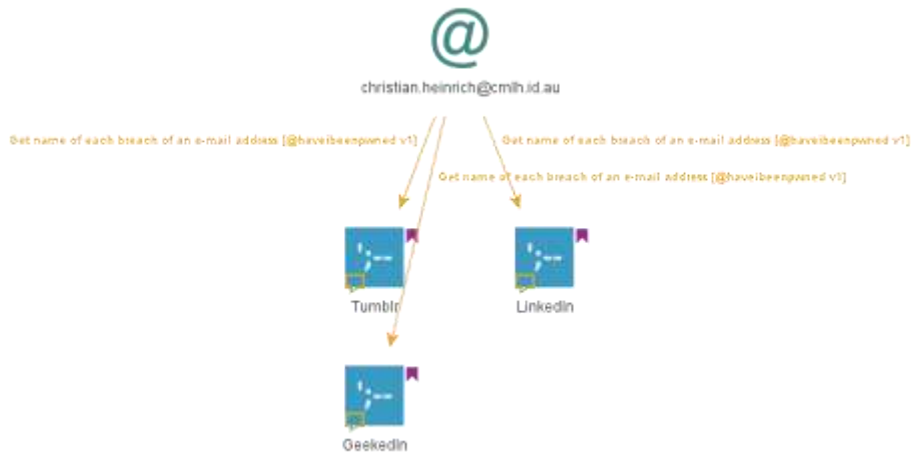


<https://haveibeenpwned.com/API/v1>

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



@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.



<https://haveibeenpwned.com/API/v2>

<https://haveibeenpwned.com/API/v2#ResponseCodes>

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

Installation



haveibeenpw...

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

[Install](#)
[Details](#)



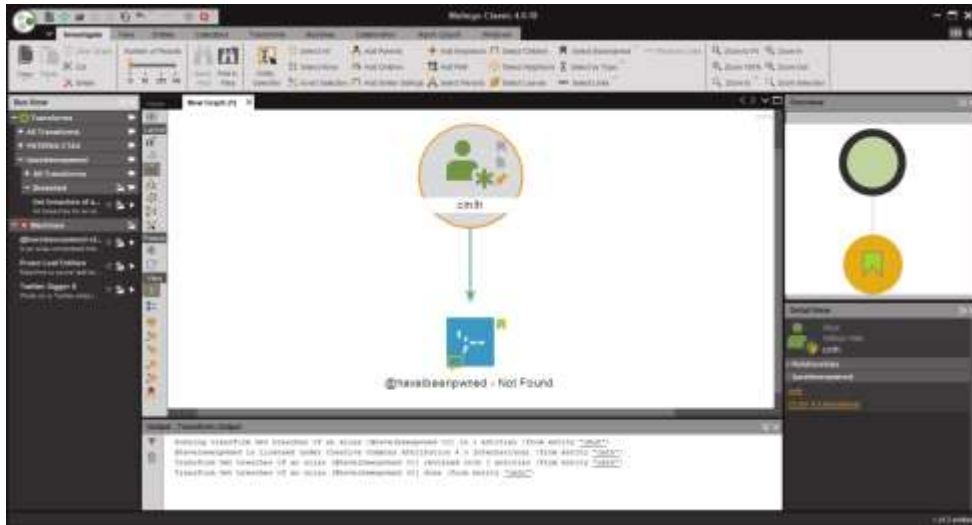
<https://github.com/cmlh/Maltego-haveibeenpwned/wiki>

@haveibeenpwned – Maltego Input Entities

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



@havebeenpwned – maltego.Alias Entity



Green Bookmark

@haveibeenpwned - Paste

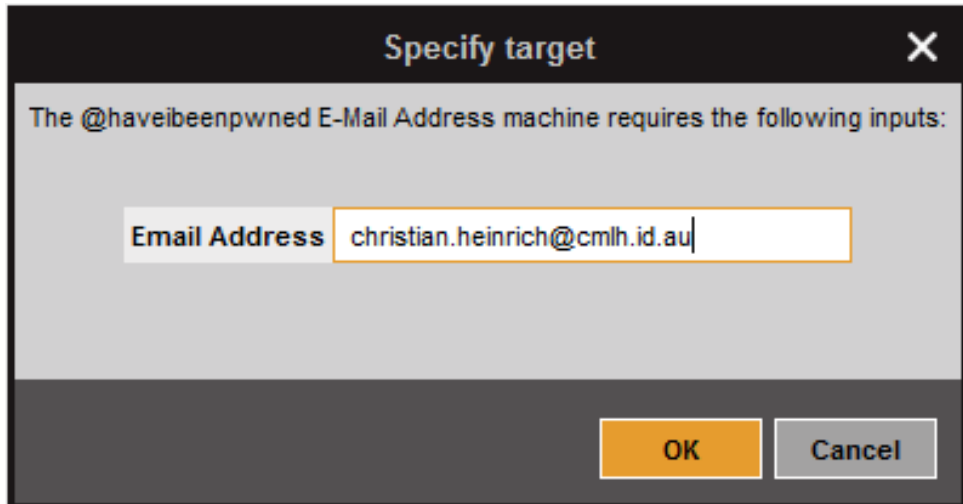


@haveibeenpwned - Not Found in P...



Green Bookmark

@haveibeenpwned – Maltego Machines



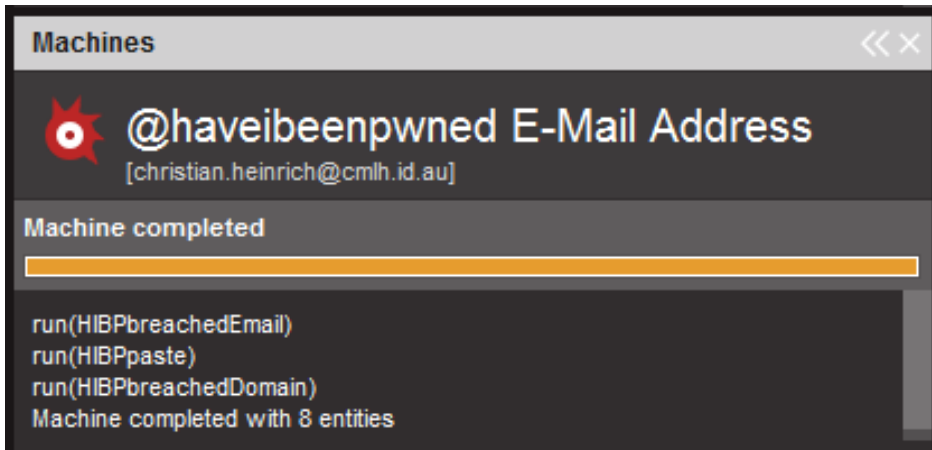
Specify target

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

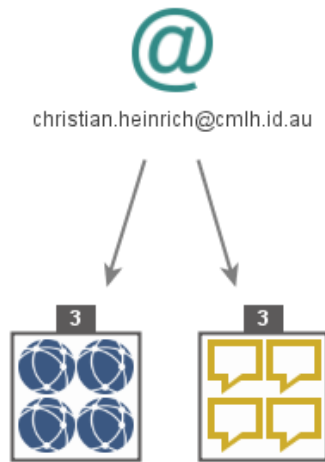
Email Address

OK Cancel

@haveibeenpwned – Maltego Machines

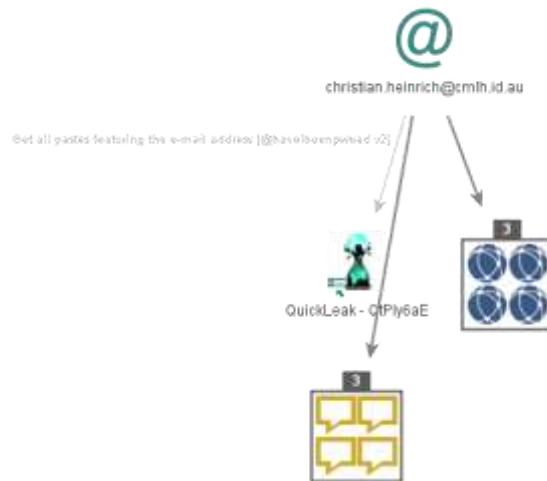


@haveibeenpwned – Maltego Machines



Collections

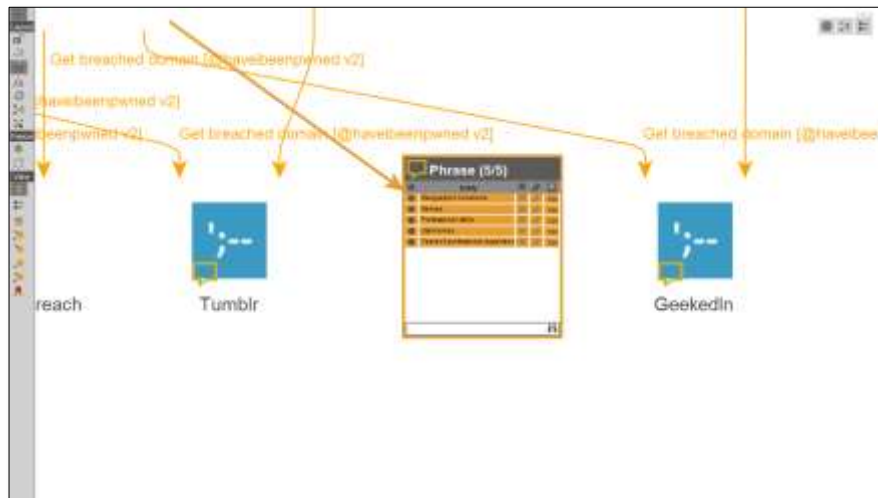
@haveibeenpwned – Maltego Machines



@haveibeenpwned – Maltego Machines

18

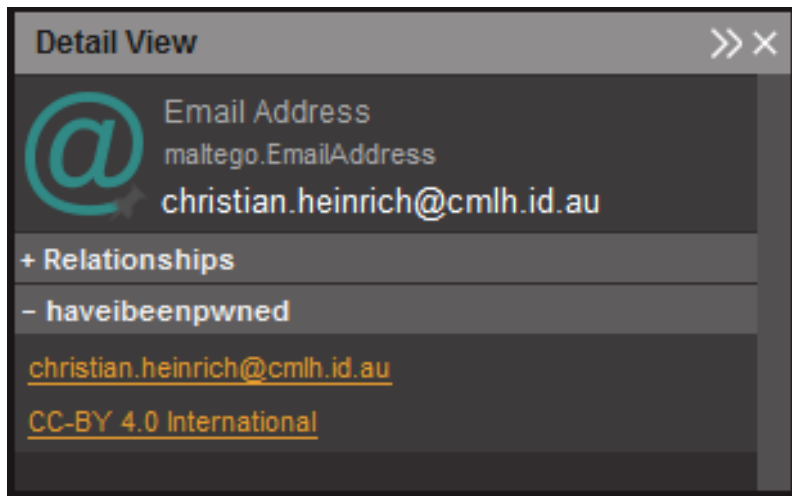
@haveibeenpwned – Maltego Machines



@haveibeenpwned – Maltego Machines

20

@haveibeenpwned – <DisplayInformation>



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

@haveibeenpwned – <DisplayInformation>



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

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

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>



<https://twitter.com/cmlh>