

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?”

The “Have I been pwned?” Microsoft Azure Ecosystem

The .NET ecosystem across devices of all sizes. It's a first-class ecosystem from small microcontrollers to large IoT deployments. It's supported through .NET Core, .NET Standard, and .NET Framework, all of which are supported on a wide range of hardware and operating systems.



Mobile and game stack solutions are fully implemented. It's possible to run .NET on a wide range of hardware, from IoT devices to a wide range of mobile and other computing platforms.

Deployment

Deployment of the web site is entirely automated using GitHub Actions and the Azure DevOps ecosystem.

All code goes into GitHub or Azure DevOps. The repository branch contains production-ready code and when it's time to release, it's merged into a "staging" branch.



These are the packages in order: GitHub Actions, Kudu, NuGet, and Workflow.

Website

The website is the face of the .NET ecosystem. It's a .NET Core application built on ASP.NET Core and the ASP.NET Core framework.

...to 10 instances on auto-scale...

The website runs on the smallest possible instance size to keep cost at a minimum. Auto-scale is configured by Kudu with a target range between 10 and 100 instances. At the end of the day, the website is scaled to 10 instances. It can be manually scaled up to 100 instances or scaled down to 10 instances.

Instance Size	Instances	Cost (per hour)
10	10	\$0.0001
20	20	\$0.0002
30	30	\$0.0003
40	40	\$0.0004
50	50	\$0.0005
60	60	\$0.0006
70	70	\$0.0007
80	80	\$0.0008
90	90	\$0.0009
100	100	\$0.0010

A scheduled task runs every 15 minutes to check for updates to the website. It's a .NET Core application built on ASP.NET Core and the ASP.NET Core framework.

CDNs

Multiple CDNs are used to both get content closer to customers for performance and reduce bandwidth to the origin.

Public CDNs are used for static content, including images and CSS. The content is stored in the origin and served from the CDN. The content is served from the CDN to the customer. The content is served from the CDN to the customer.

The Azure CDN is used for all content. It's a .NET Core application built on ASP.NET Core and the ASP.NET Core framework.

The Azure CDN is used for all content. It's a .NET Core application built on ASP.NET Core and the ASP.NET Core framework.

Monitoring and alerts

Different monitoring services are used to track resource utilization in real-time and to alert on any issues. Alerts are sent to the Azure portal and to the email inbox.

Azure Monitor is used to track resource utilization. It's a .NET Core application built on ASP.NET Core and the ASP.NET Core framework.

Azure Monitor is used to track resource utilization. It's a .NET Core application built on ASP.NET Core and the ASP.NET Core framework.

Breach Processing

Breaches are manually verified for accuracy which now uses a degree of pre-processing in an isolated environment. Different logical machines are used for analysis and then importing into Table Storage.



The Breach Processing service is a .NET Core application built on ASP.NET Core and the ASP.NET Core framework.

Storage

The data is stored in a relational SQL database and in a non-relational NoSQL database. The data is stored in a relational SQL database and in a non-relational NoSQL database.



The data is stored in a relational SQL database and in a non-relational NoSQL database.

Paste Service

The paste service is a .NET Core application built on ASP.NET Core and the ASP.NET Core framework.



The paste service is a .NET Core application built on ASP.NET Core and the ASP.NET Core framework.

Additional services



Front-End is a .NET Core application built on ASP.NET Core and the ASP.NET Core framework.



Front-End is a .NET Core application built on ASP.NET Core and the ASP.NET Core framework.



Workflow is a .NET Core application built on ASP.NET Core and the ASP.NET Core framework.



Chat/Voice is a .NET Core application built on ASP.NET Core and the ASP.NET Core framework.



InSimple is a .NET Core application built on ASP.NET Core and the ASP.NET Core framework.

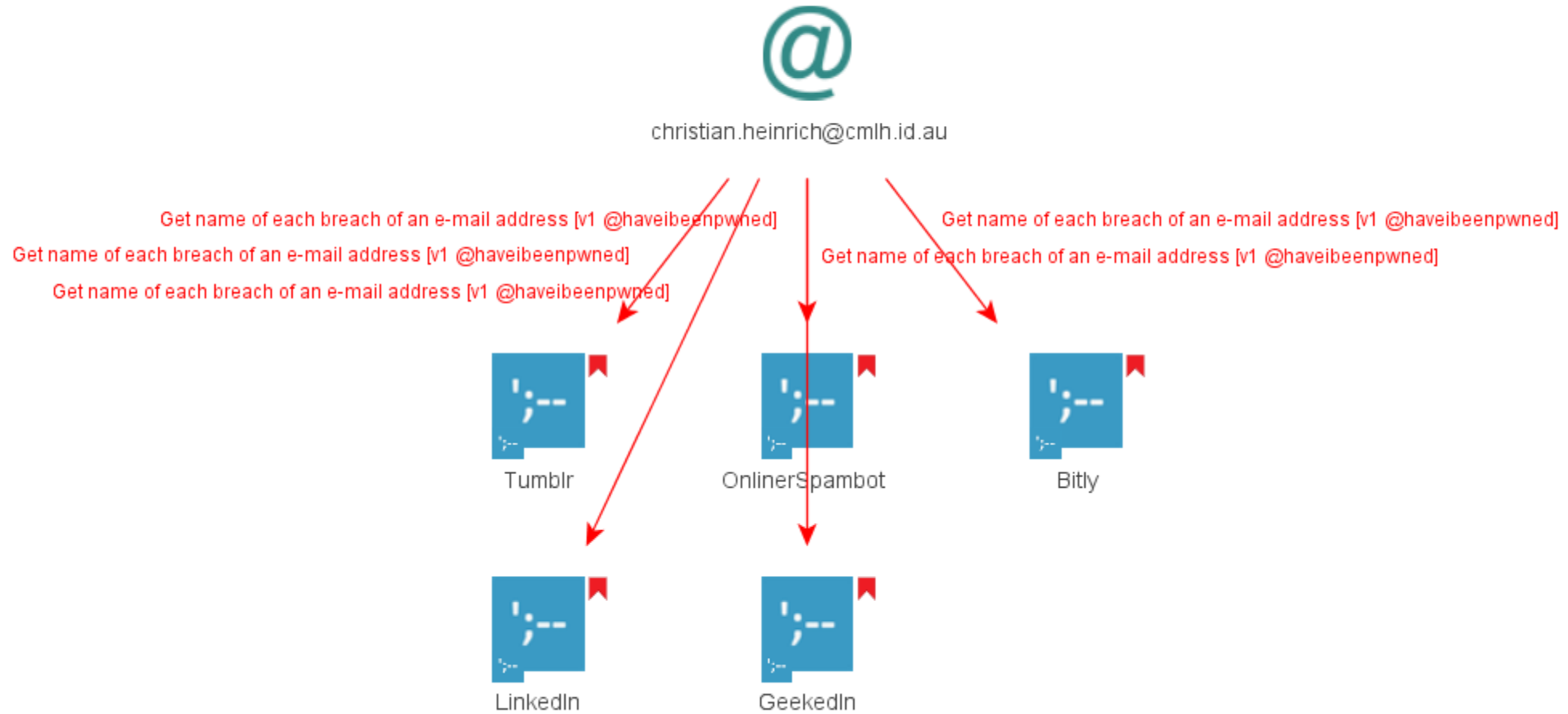
@haveibeenpwned – API v1

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



@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*



“Pwned Passwords” – API v1

Integrated Single API **v1** Endpoint.

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



“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.



Installation



haveibeenpwned

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

[Uninstall](#)
[Details](#)
[Refresh](#)



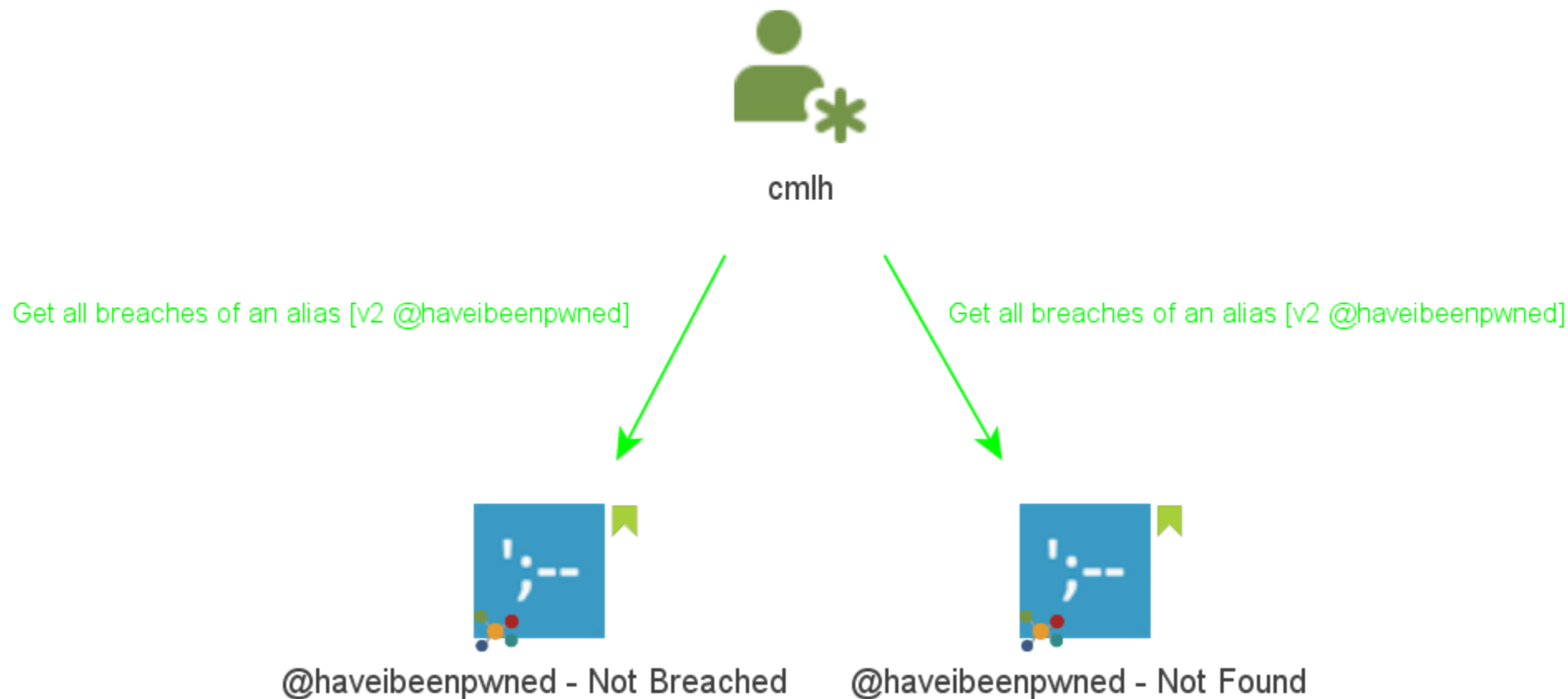
@haveibeenpwned – Maltego Input Entities

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

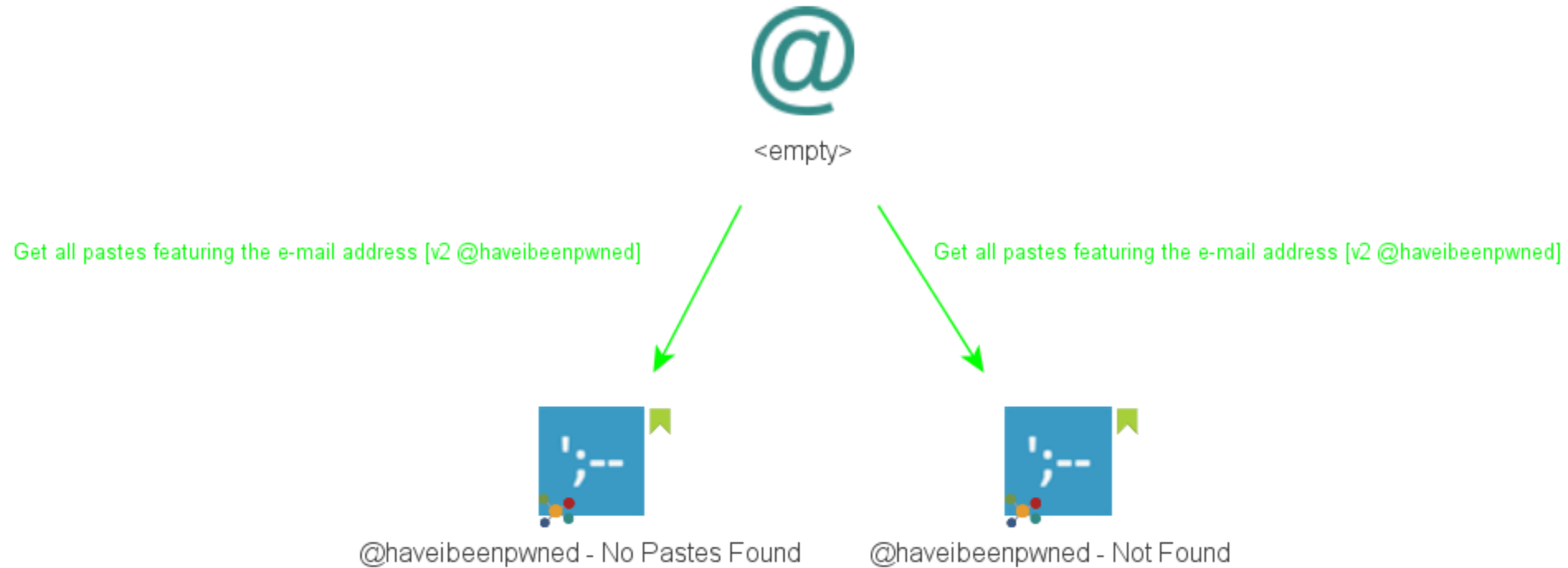
2. *“Site”*
 1. `maltego.Domain`
 2. `Maltego.Phrase`



@haveibeenpwned - maltego .Alias Entity



@haveibeenpwned - Paste



@haveibeenpwned - Paste



christian.heinrich@cmlh.id.au

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



QuickLeak - QtPly6aE



@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

Get all breaches of an e-mail address [v2 @haveibeenpwned]

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



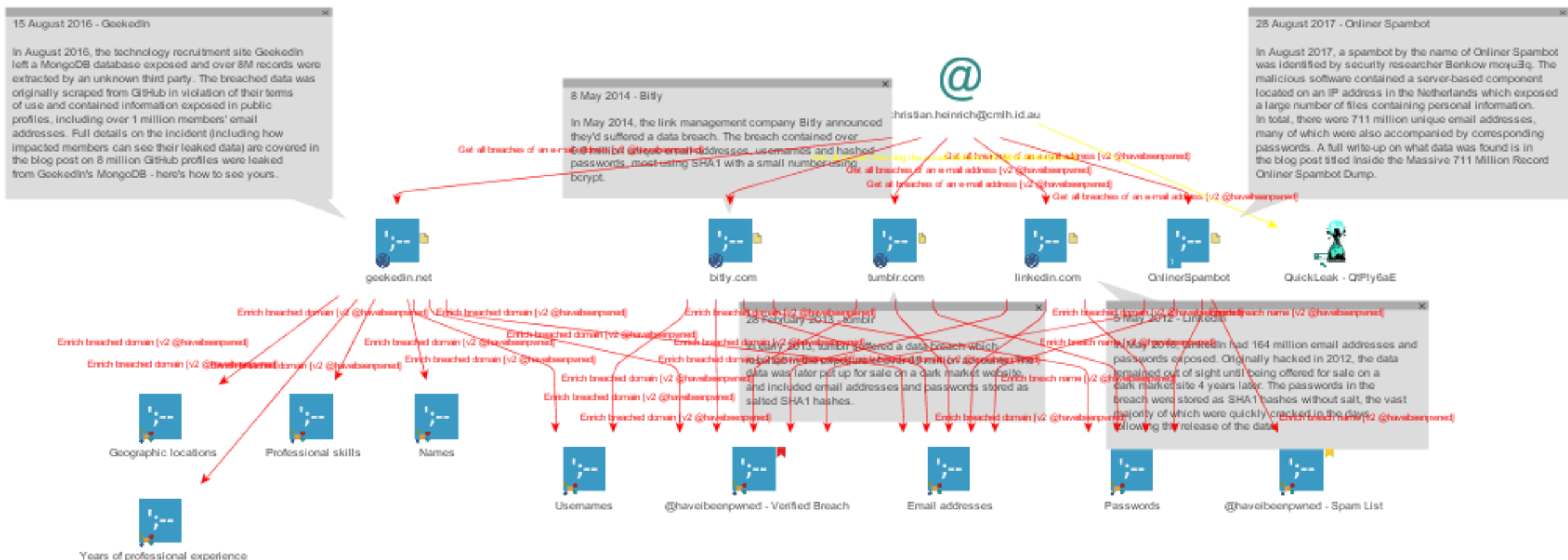
OnlinerSpamoot



QuickLeak - QtPly6aE

4






@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>

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

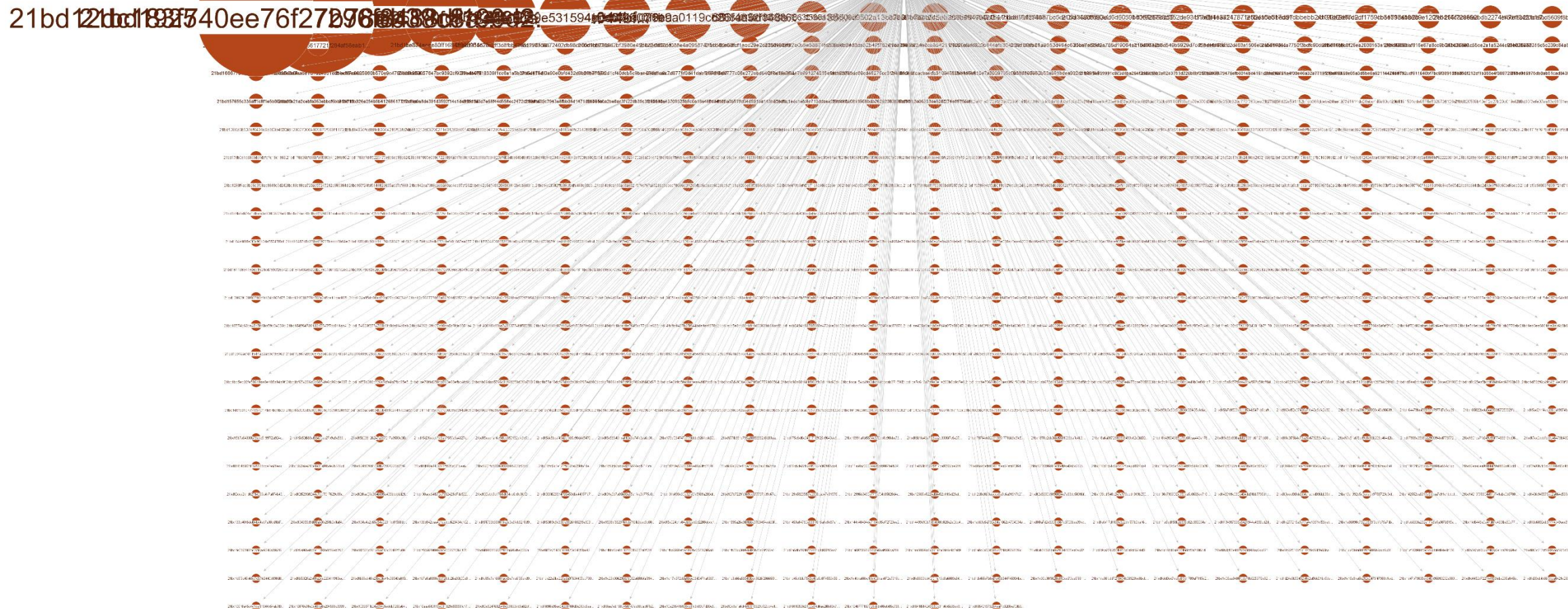
“Pwned Passwords” API v2 – Input Entities

1. `haveibeenpwned.Password`

- *Inherits from* `maltego.Phrase`

2. `maltego.Hash`





Thanks

@troyhunt of @haveibeenpwned

@SudhanshuC of the forked Maltego local transforms

~~@ReelofTemmingh~~, @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>

