

BreachedEgo

Christian Heinrich

BlackHat USA

August 2015



Latest Slides

<https://www.slideshare.net/cmlh/maltego-breached>

<https://speakerdeck.com/cmlh/maltego-breached>

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™

Python Modules from @CanariProject and @Paterva

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



Agenda

1. Integration of the API from @haveibeenpwned, @Breach Alarm and @Abusix
2. Configuration for “*Chlorine*”, “*Carbon*” and “*Tungsten*” (Kali Linux)
3. Case Studies
 1. End User (Penetration Tester, Incident Responder, etc)
 2. Vendor (Quality Assurance)



@haveibeenpwned - API

Integrated API **v2** Endpoints:

1. Getting all breaches for an account
2. Getting all pastes for an account
3. Getting a single breached site

Supports **all** API HTTP Status Codes i.e. 200, 400, 403 and 404.



@haveibeenpwned – Maltego Configuration

Seed: <https://cetas.paterva.com/TDS/runner/showseed/haveibeenpwned>

Configuration: <https://raw.githubusercontent.com/cmlh/Maltego-haveibeenpwned/master/Maltego-Configuration-haveibeenpwned.mtz>

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

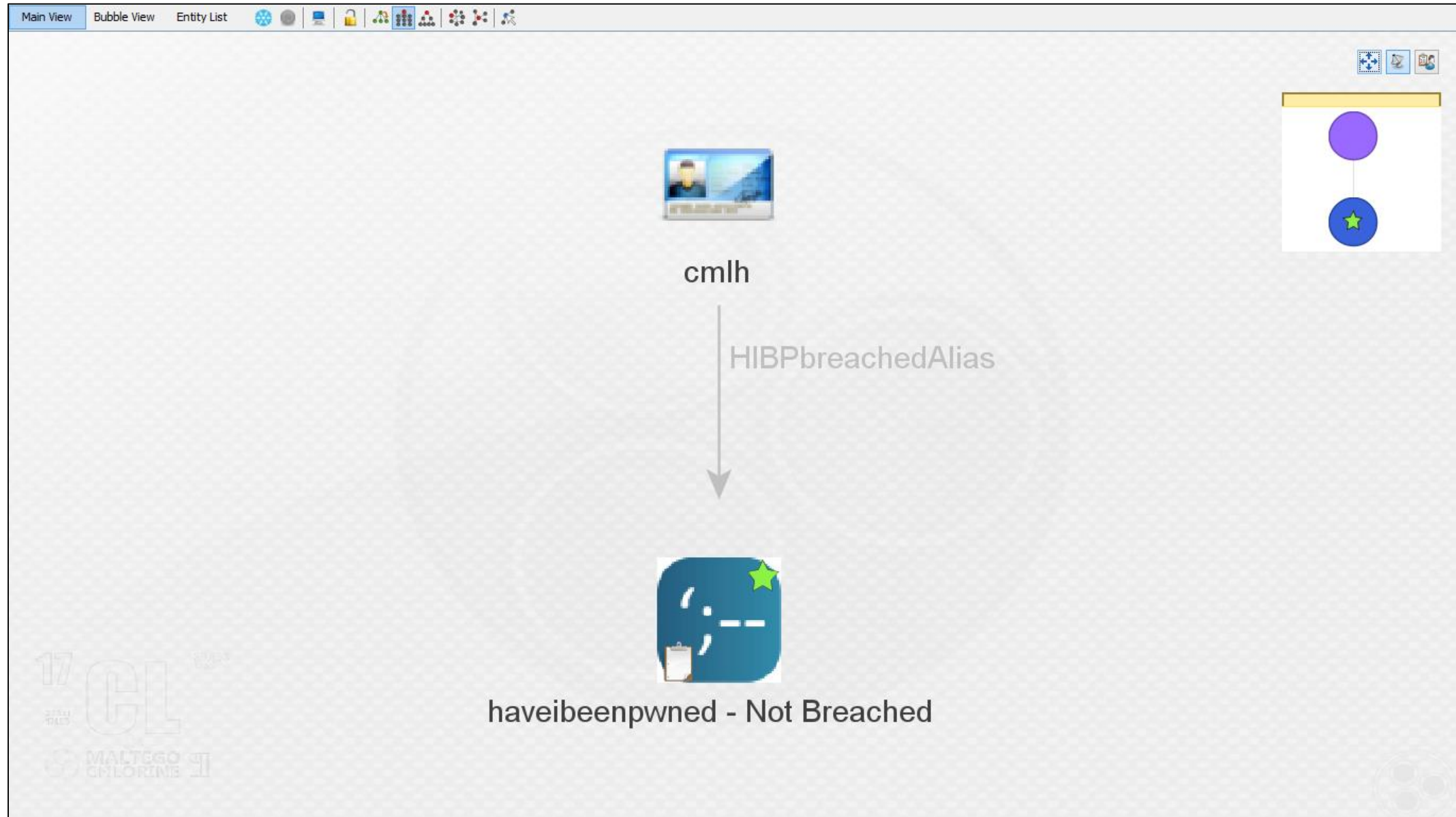


@haveibeenpwned – Maltego Input Entities

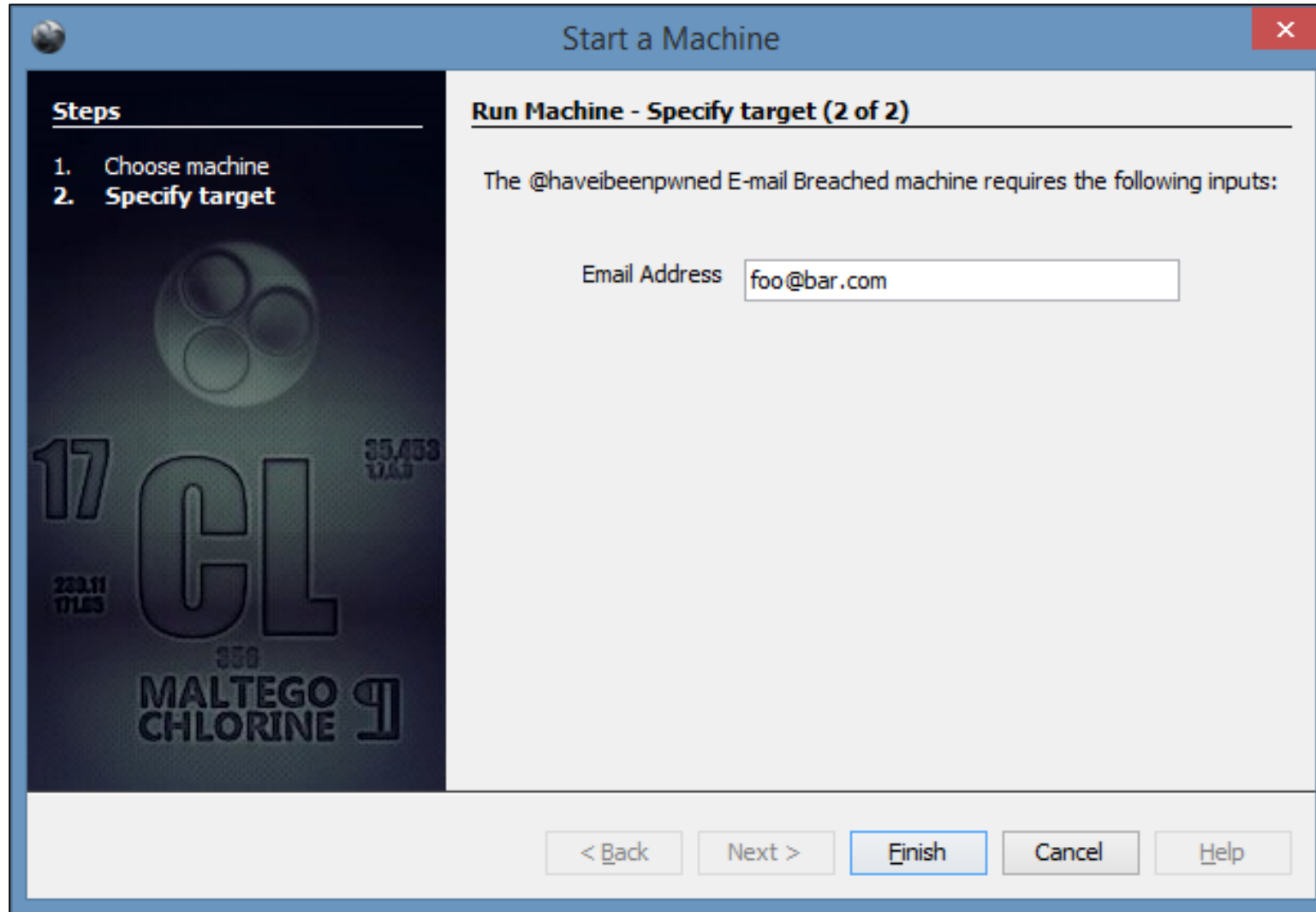
1. *“Account”*
 1. `maltego.EmailAddress`
 2. `maltego.Alias`
2. *“Site”*
 1. `maltego.Domain`



@haveibeenpwned – maltego .Alias Entity



@haveibeenpwned – Maltego Machines



The image shows a screenshot of the 'Start a Machine' dialog box in the Maltego application. The dialog has a blue title bar with the text 'Start a Machine' and a red close button. It is divided into two main sections. The left section, titled 'Steps', contains a list of two steps: '1. Choose machine' and '2. Specify target'. Below the list is a dark blue graphic with the text '17 CL 35,433 17.63' and 'MALTEGO CHLORINE 9'. The right section, titled 'Run Machine - Specify target (2 of 2)', contains the text 'The @haveibeenpwned E-mail Breached machine requires the following inputs:'. Below this text is a label 'Email Address' followed by a text input field containing the value 'foo@bar.com'. At the bottom of the dialog, there are five buttons: '< Back', 'Next >', 'Finish' (which is highlighted with a blue border), 'Cancel', and 'Help'.

Start a Machine

Steps

1. Choose machine
2. **Specify target**

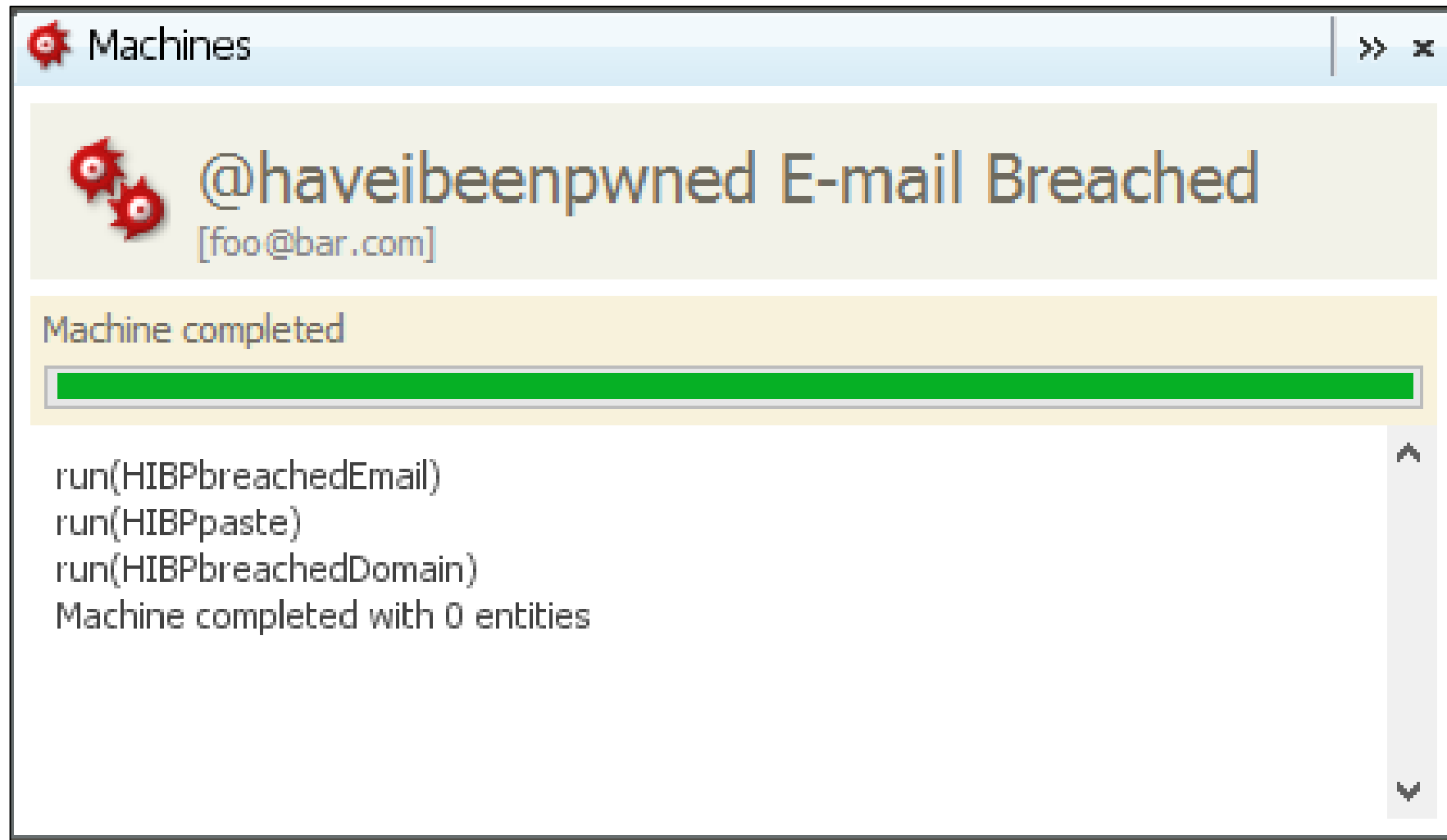
Run Machine - Specify target (2 of 2)

The @haveibeenpwned E-mail Breached machine requires the following inputs:

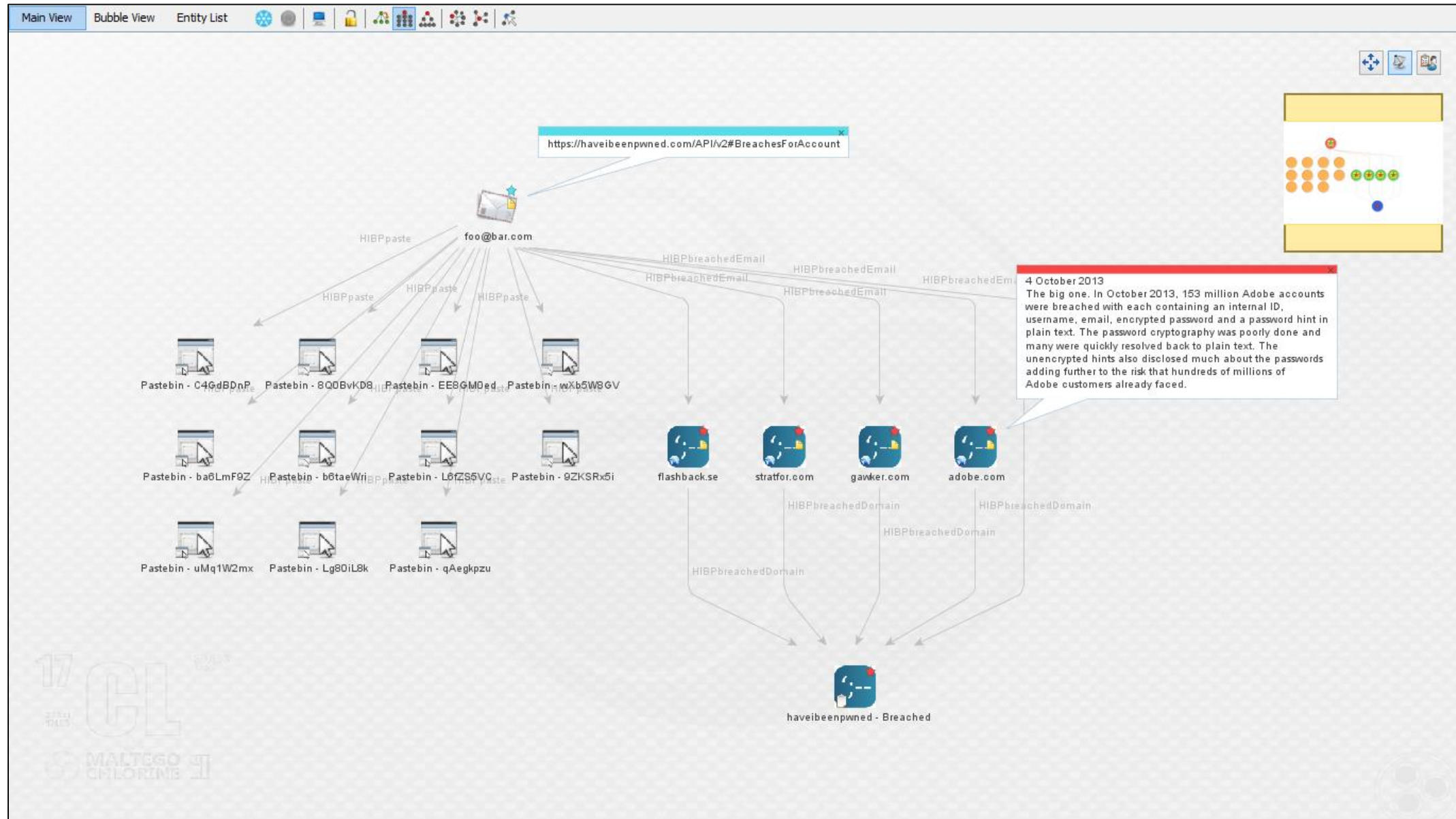
Email Address

< Back Next > Finish Cancel Help

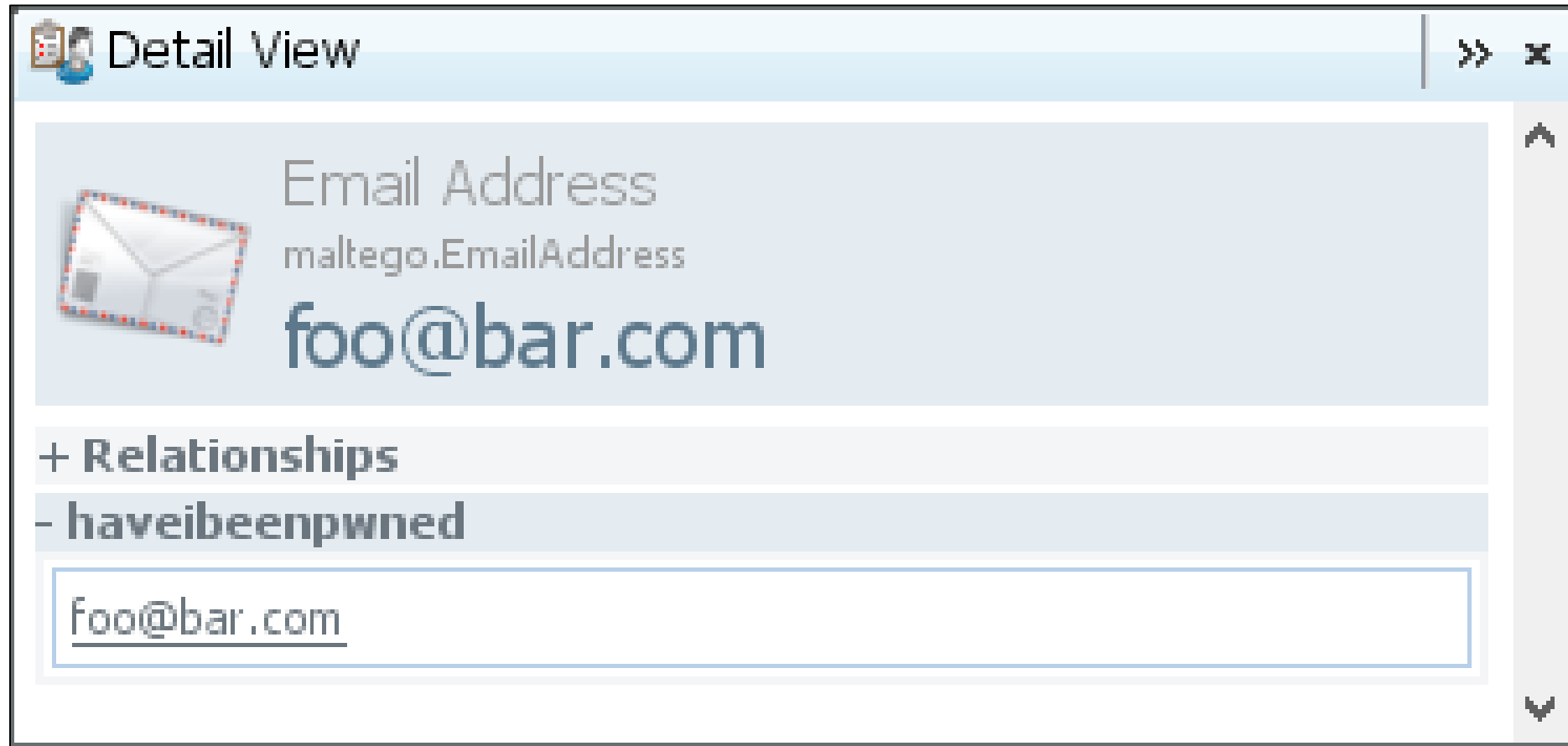
@haveibeenpwned – Maltego Machines



@haveibeenpwned – Maltego Machines



@haveibeenpwned – <DisplayInformation>



@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

@Breach Alarm - API

Integrated “Breached E-mails” API v1 Endpoint Only.

- “Avalanche Technology Group” provided @BreachAlarm API Key at no cost to @cmlh.

Unsupported [Paid] API v1 Endpoints:

1. “Breached E-mails (with History)”
2. “Breached Domains”
 - A. With History
 - B. Without History

Upon the paid API v1 endpoints being integrated then **paterva.v2.BreachAlarm** namespace will change



@Breach Alarm - API

Supports **all** API HTTP Status Codes:

- 200
- 400, 401, 403 and 404
- 500 and 501



@Breach Alarm – Maltego Configuration

Seed: <https://cetas.paterva.com/TDS/runner/showseed/breachalarm>

Configuration: <https://raw.githubusercontent.com/cmlh/Maltego-BreachAlarm/master/Maltego-Configuration-BreachAlarm.mtz>

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



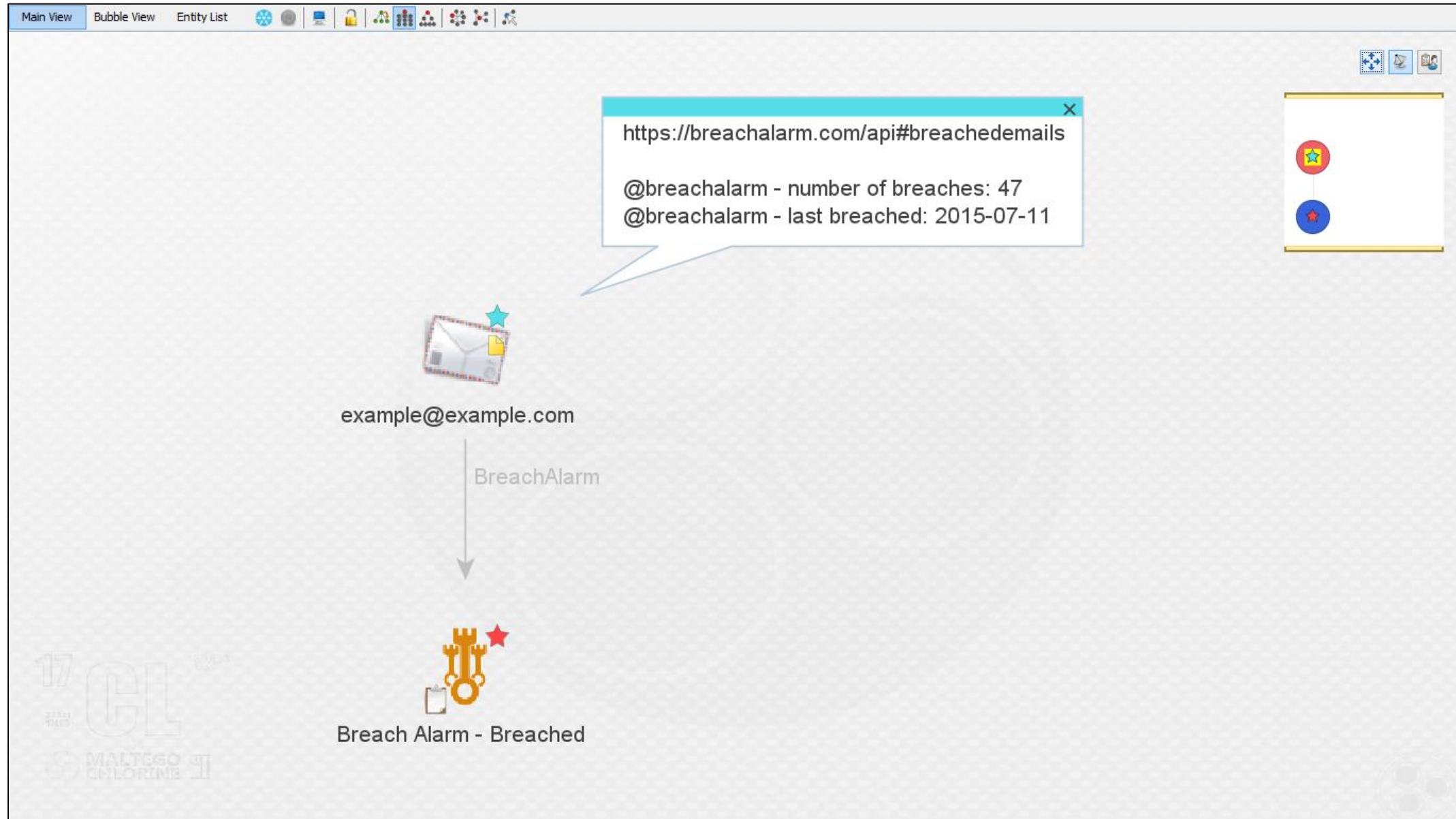
@Breach Alarm – SHA1 Hash



```
Output - Transform Output
Running transform BreachAlarm on 1 entities (from entity "example@example.com")
SHA1 of example@example.com is 914fec35ce8bfala067581032f26b053591ee38a (from entity "example@example.com")
Transform BreachAlarm returned with 2 entities (from entity "example@example.com")
Transform BreachAlarm done (from entity "example@example.com")
```



@Breach Alarm – Maltego Graph



@Abusix - API

LeakDB

- *“E-mail Address”* `maltego.EmailAddress`
- *“Password”* `maltego.Phrase`



@Abusix – Maltego Configuration

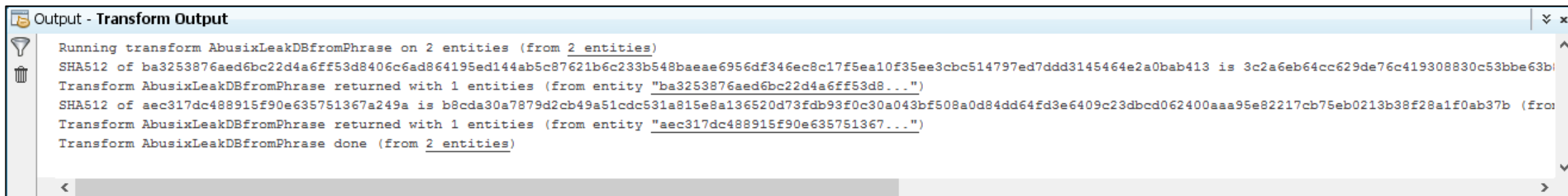
Seed: <https://cetas.paterva.com/TDS/runner/showseed/abusix>

Configuration: <https://raw.githubusercontent.com/cmlh/Maltego-Abusix/master/Maltego-Configuration-Abusix.mtz>

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

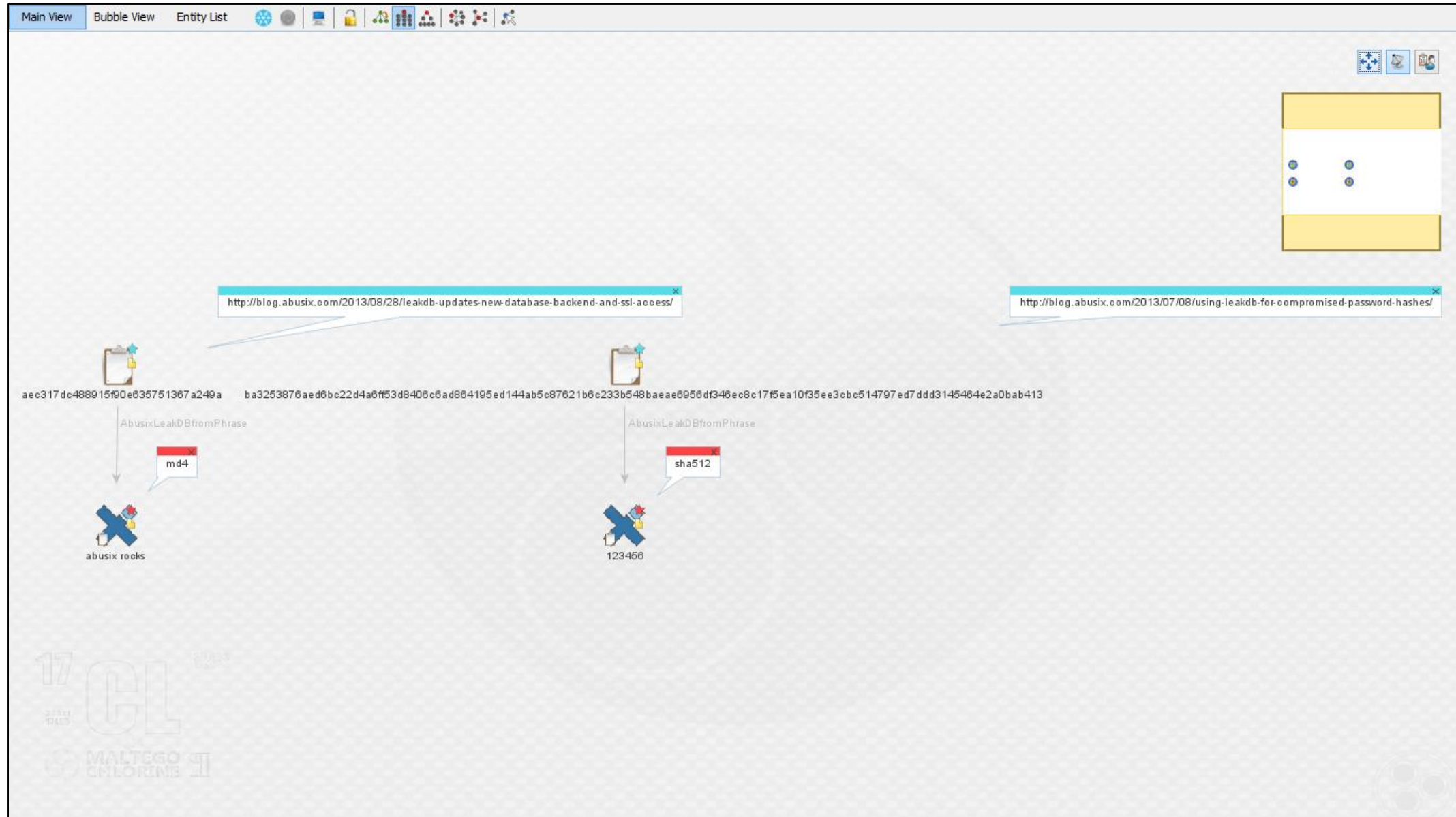


@Abusix – SHA512 Hash



```
Output - Transform Output
Running transform AbusixLeakDBfromPhrase on 2 entities (from 2 entities)
SHA512 of ba3253876aed6bc22d4a6ff53d8406c6ad864195ed144ab5c87621b6c233b548baeae6956df346ec8c17f5ea10f35ee3cbc514797ed7ddd3145464e2a0bab413 is 3c2a6eb64cc629de76c419308830c53bbe63b
Transform AbusixLeakDBfromPhrase returned with 1 entities (from entity "ba3253876aed6bc22d4a6ff53d8...")
SHA512 of aec317dc488915f90e635751367a249a is b8cda30a7879d2cb49a51cdc531a815e8a136520d73fdb93f0c30a043bf508a0d84dd64fd3e6409c23dbcd062400aaa95e82217cb75eb0213b38f28a1f0ab37b (fro
Transform AbusixLeakDBfromPhrase returned with 1 entities (from entity "aec317dc488915f90e635751367...")
Transform AbusixLeakDBfromPhrase done (from 2 entities)
```

@Abusix – maltego . Phrase/Password



Breached – Maltego Configuration

Seed: <https://cetas.paterva.com/TDS/runner/showseed/breached>

Configuration: <https://raw.githubusercontent.com/cmlh/Maltego-Breach/master/Maltego-Configuration-Breached.mtz>

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



Thanks

Alpha:

@troyhunt of @haveibeenpwned

@Abusix

@BreachAlarm

Beta:

@RoelofTemmingh, @AndrewMohawk and @paulRchds of @Paterva

@dcuthbert, @glennzw and @charlvdwalt of @SensePost

Release Candidate:

@bostonlink, @catalyst256, @tactical_intel, @digital4rensics and any1 I forgot (sorry)



Thanks

@toolswatch

@BlackHatEvents

- Jessica Hoffman at UBM



BreachEgo

Christian Heinrich

Follow me on Twitter at **@cmlh**

christian.heinrich@cmlh.id.au

Latest Slides

<https://www.slideshare.net/cmlh/maltego-breached>

<https://speakerdeck.com/cmlh/maltego-breached>

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

