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

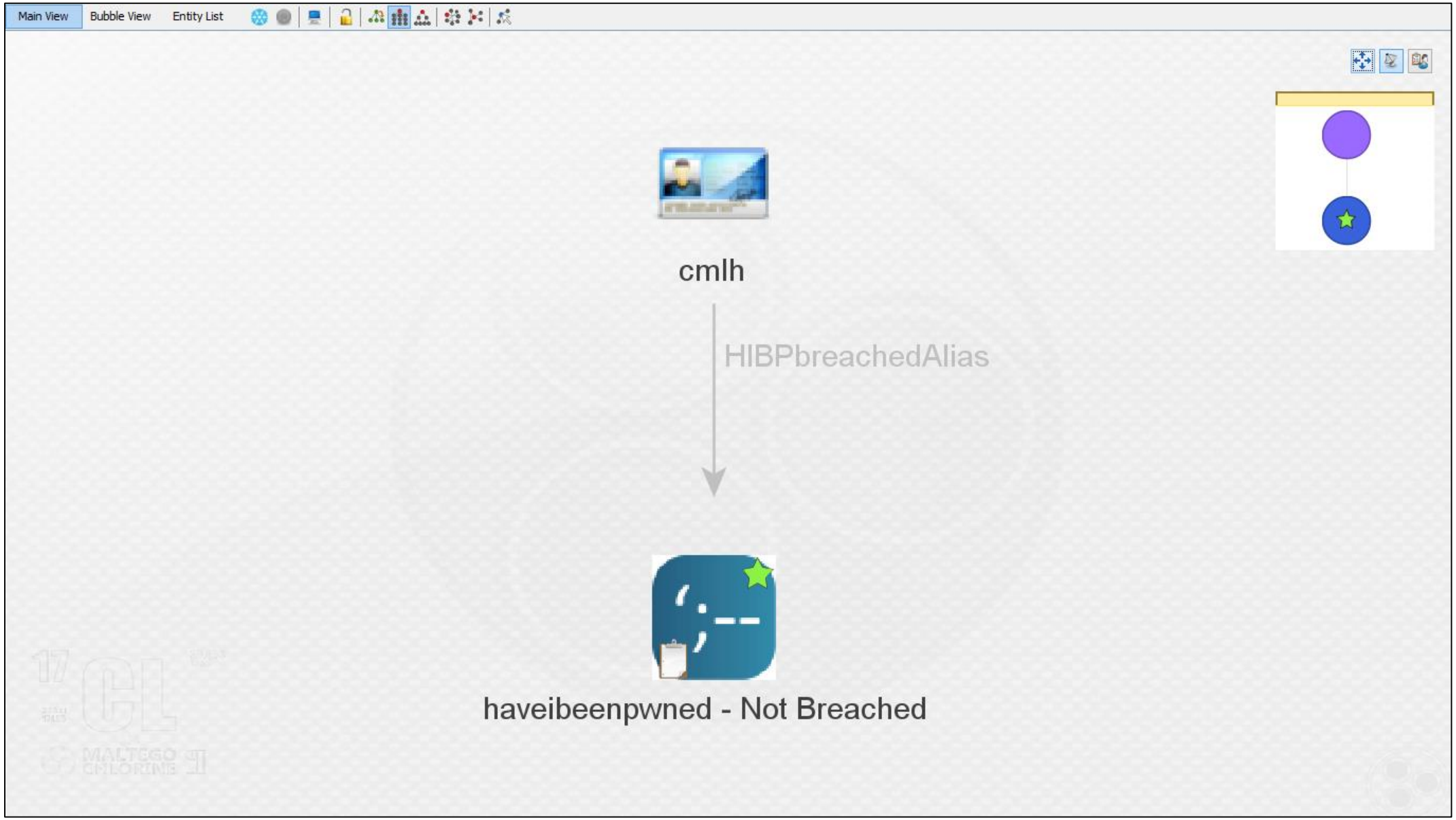
Documentation: https://github.com/cmlh/Maltego-haveibeenpwned/wiki

@haveibeenpwned – Maltego Input Entities

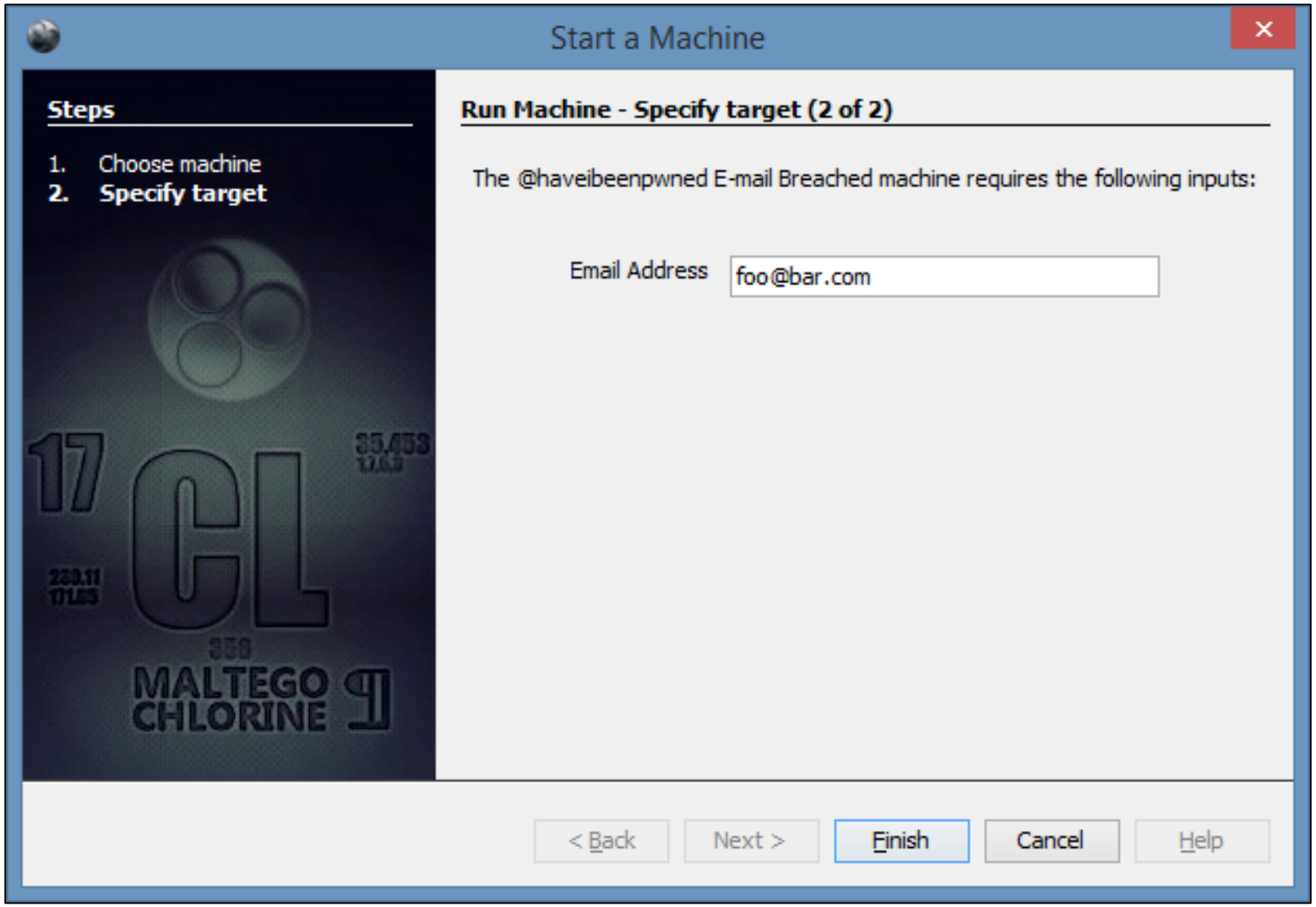
1. *"Account"*
    1. **`maltego.EmailAddress`**
    2. **`maltego.Alias`**

2. *"Site"*
    1. **`maltego.Domain`**

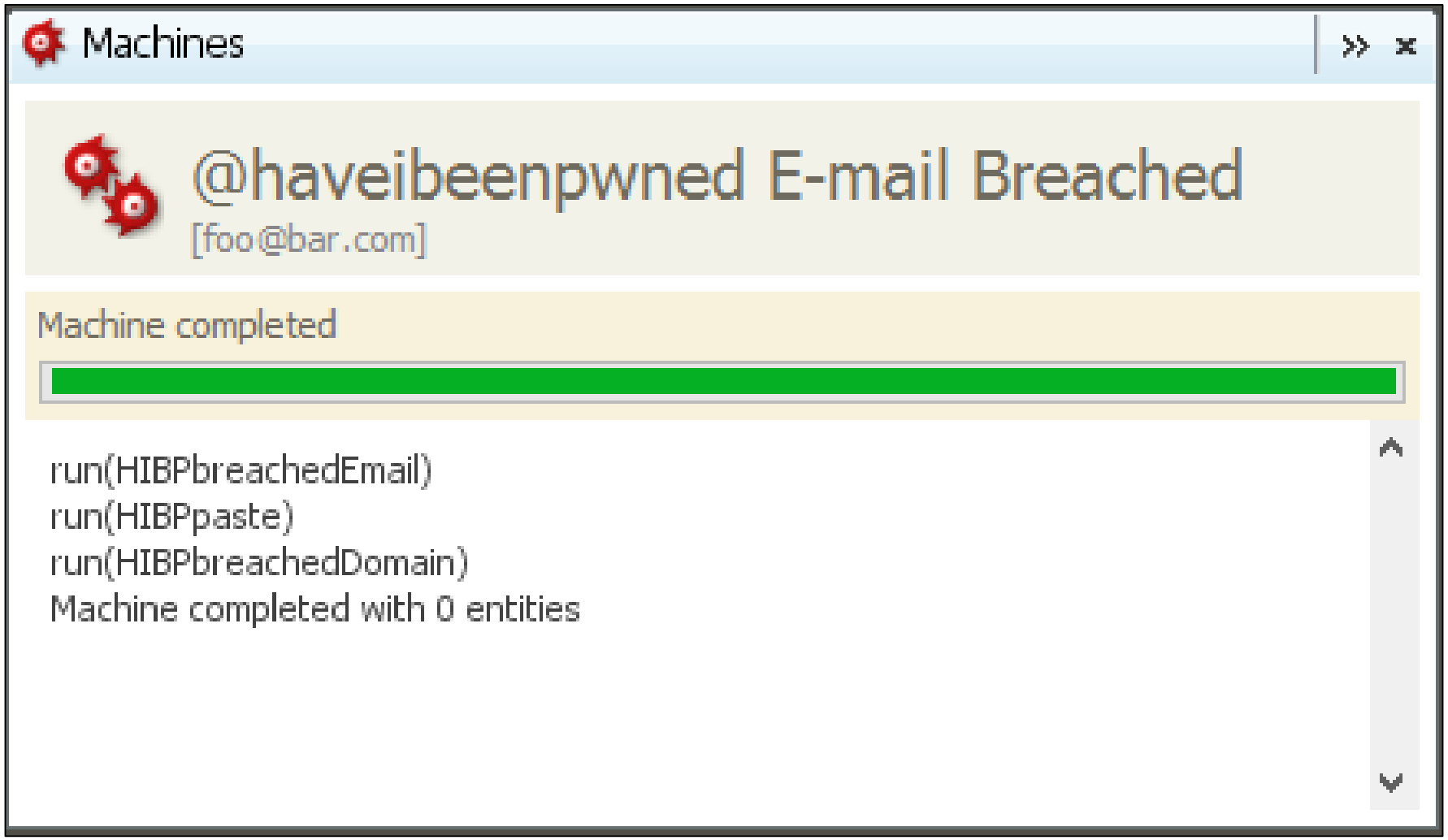
@haveibeenpwned – `maltego.Alias` Entity



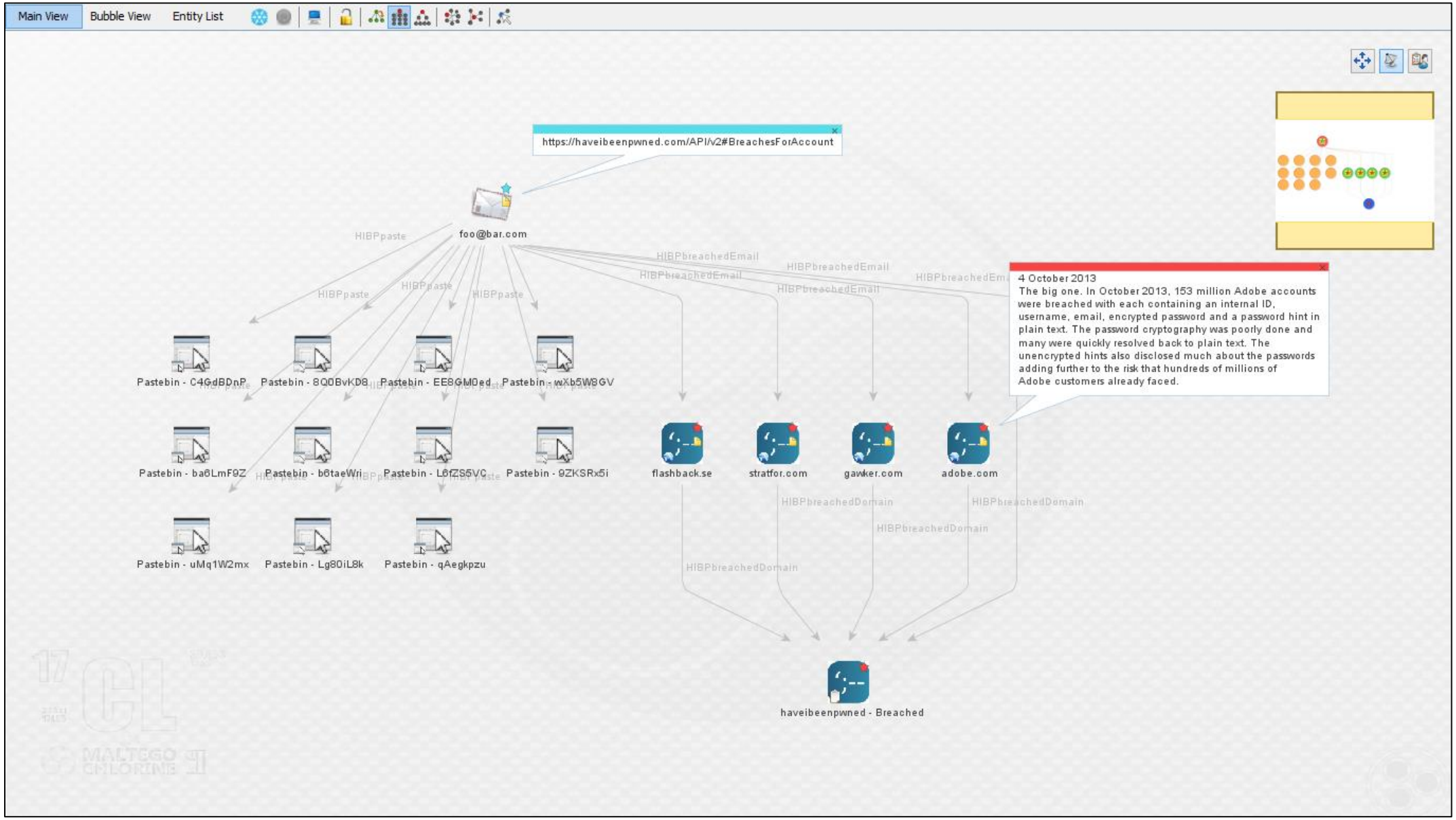
@haveibeenpwned – Maltego Machines



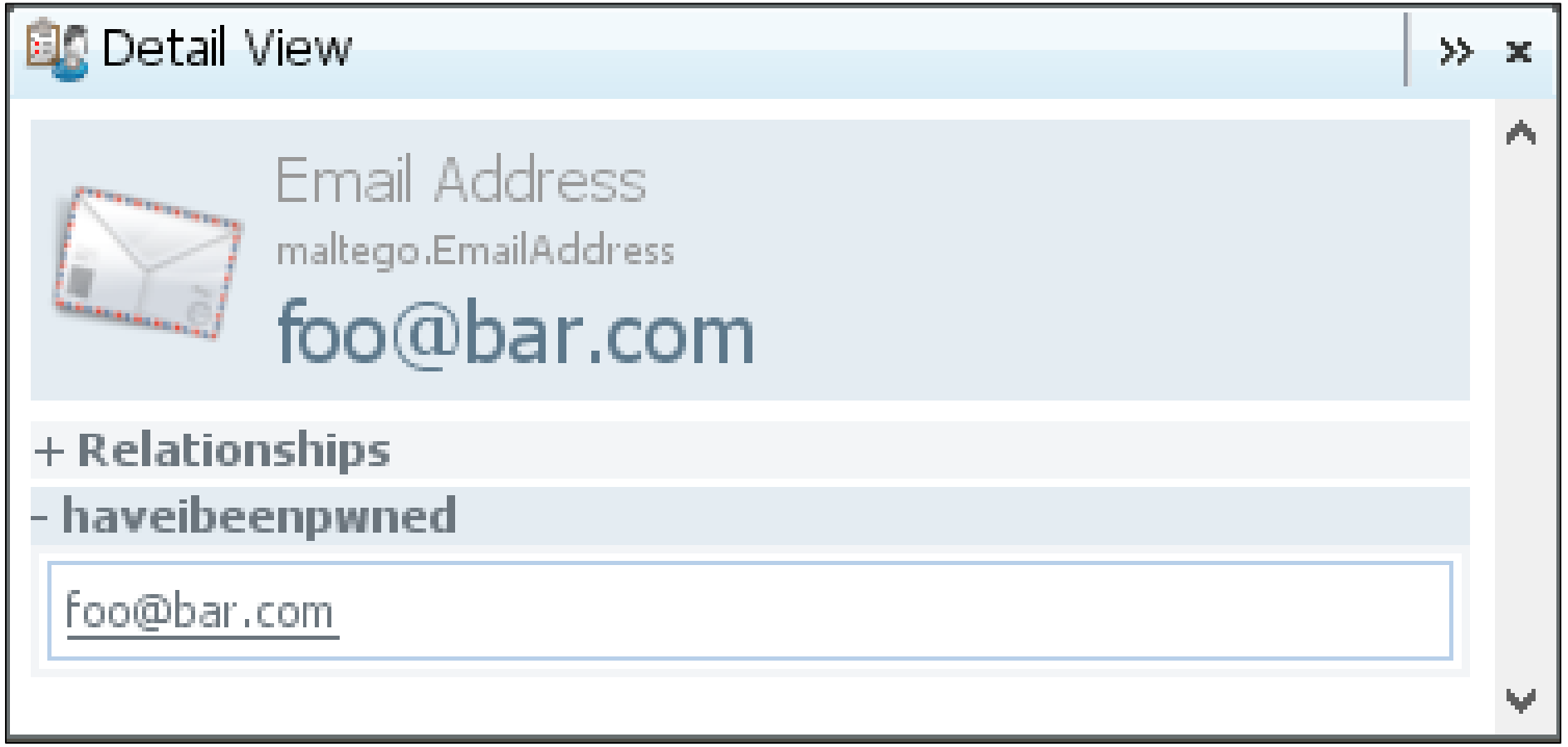
@haveibeenpwned – Maltego Machines



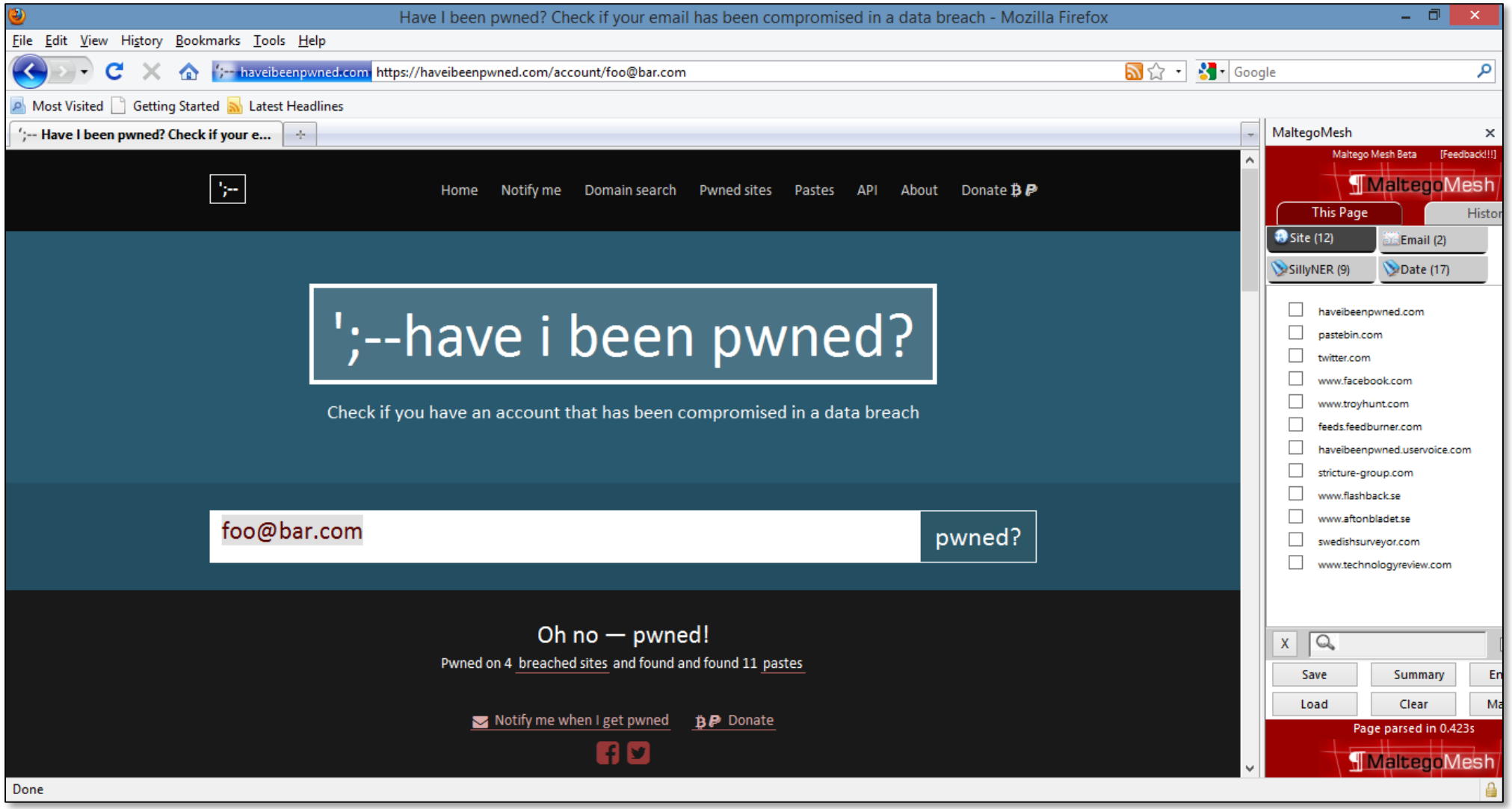
@haveibeenpwned – Maltego Machines



@haveibeenpwned – <DisplayInformation>



@haveibeenpwned – <DisplayInformation>



@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`

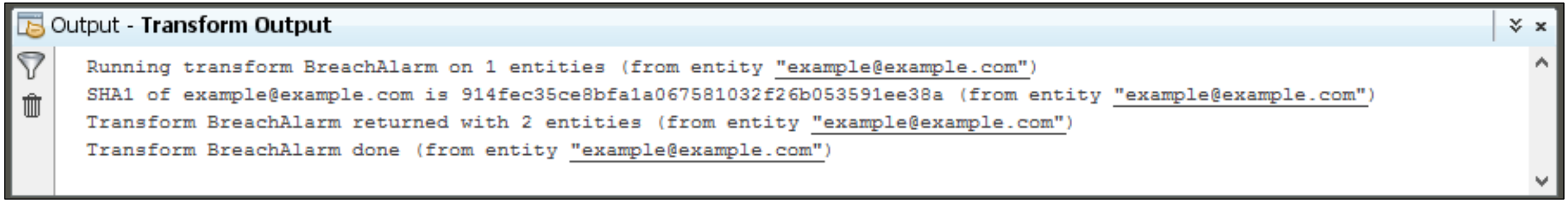
@Breach Alarm – Maltego Configuration

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

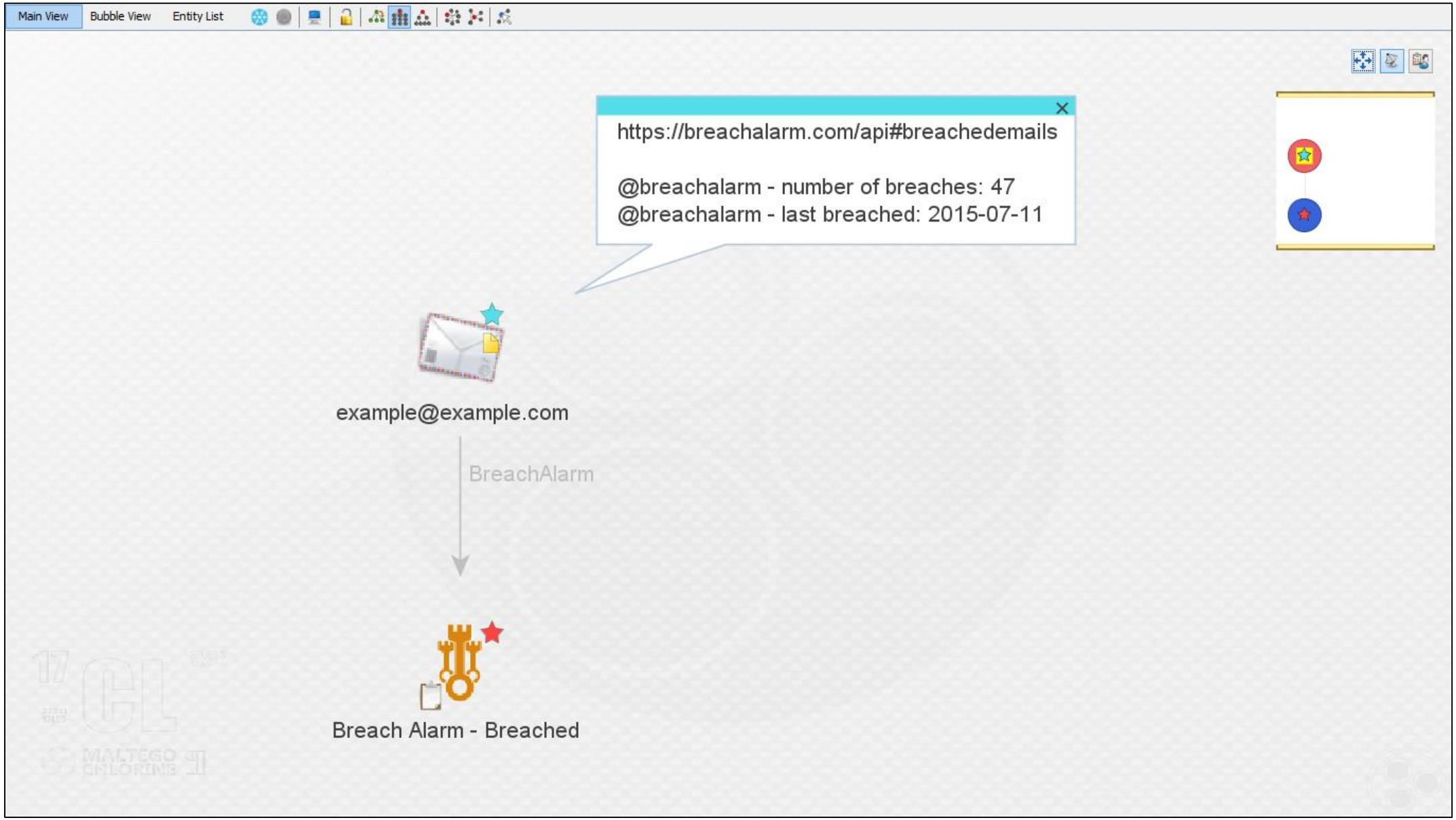
Configuration: https://raw.githubusercontent.com/cmlh/Maltego-BreachAlarm/master/Maltego-Configuration-BreachAlarm.mtz

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

@Breach Alarm – SHA1 Hash



@Breach Alarm – Maltego Graph



@Abusix - API

LeakDB

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

@Abusix – Maltego Configuration

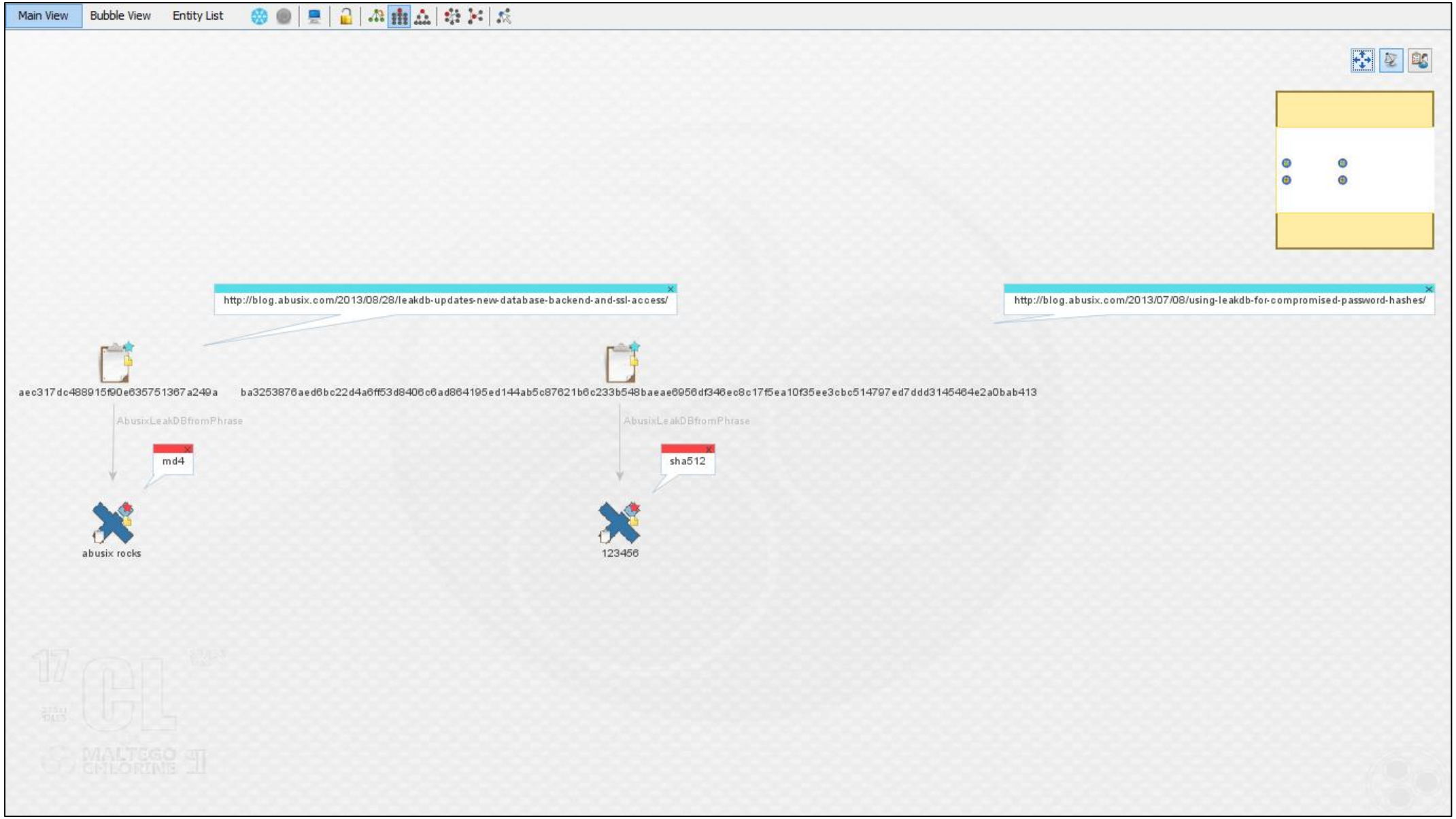
Seed: https://cetas.paterva.com/TDS/runner/showseed/abusix

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

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

@Abusix – SHA512 Hash

@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