
PATERVA
Integrating with Maltego

Introduction

Who are we?

Roelof Temmingh
Paterva (http://www.paterva.com)
roelof@paterva.com

Chris Böhme
Pinkmatter (http://www.pinkmatter.com)
chris@pinkmatter.com

Last year we did a presentation on Maltego at BH Amsterdam

Where is the paper?

We spent most of our time building this cool new tech
Writing code is more fun than writing papers

Therefore – lots of demos – not a lot of talking
Don't blink or you'll miss something – no seriously

Disclaimer: doing a live demo is never a good idea….

… showing alpha version software, is neither…

Also – this is a brand new talk – we're not sure about the timing ☺

Agenda

- Introduction – what is Maltego again?
- New features for 2.5 we can show today
- Some demos

- Data collection with Maltego
  - Nmap
  - Nessus
  - Forum DBs

- Pre-emptive internal investigations
  - Squid

- Many demos – a picture is worth a 1000 words..

Maltego recap

… if you have been living under a rock

What is it?

- Visual tool for dealing with information
- Entities and relationships
- Platform for information integration & correlation

Power of Maltego lies in:

Small, easy to understand transforms or plugins

Run transform (and repeat…)

Really quick demo of Maltego
(demo of DNS_SE on defense.gouv.fr)

New features we want to show you

Since BlackHat Amsterdam 2008 we've been busy…

2.0.1 Copy & paste (to & from text)
Entity import

2.0.2 Mac support (beta)
Local transforms

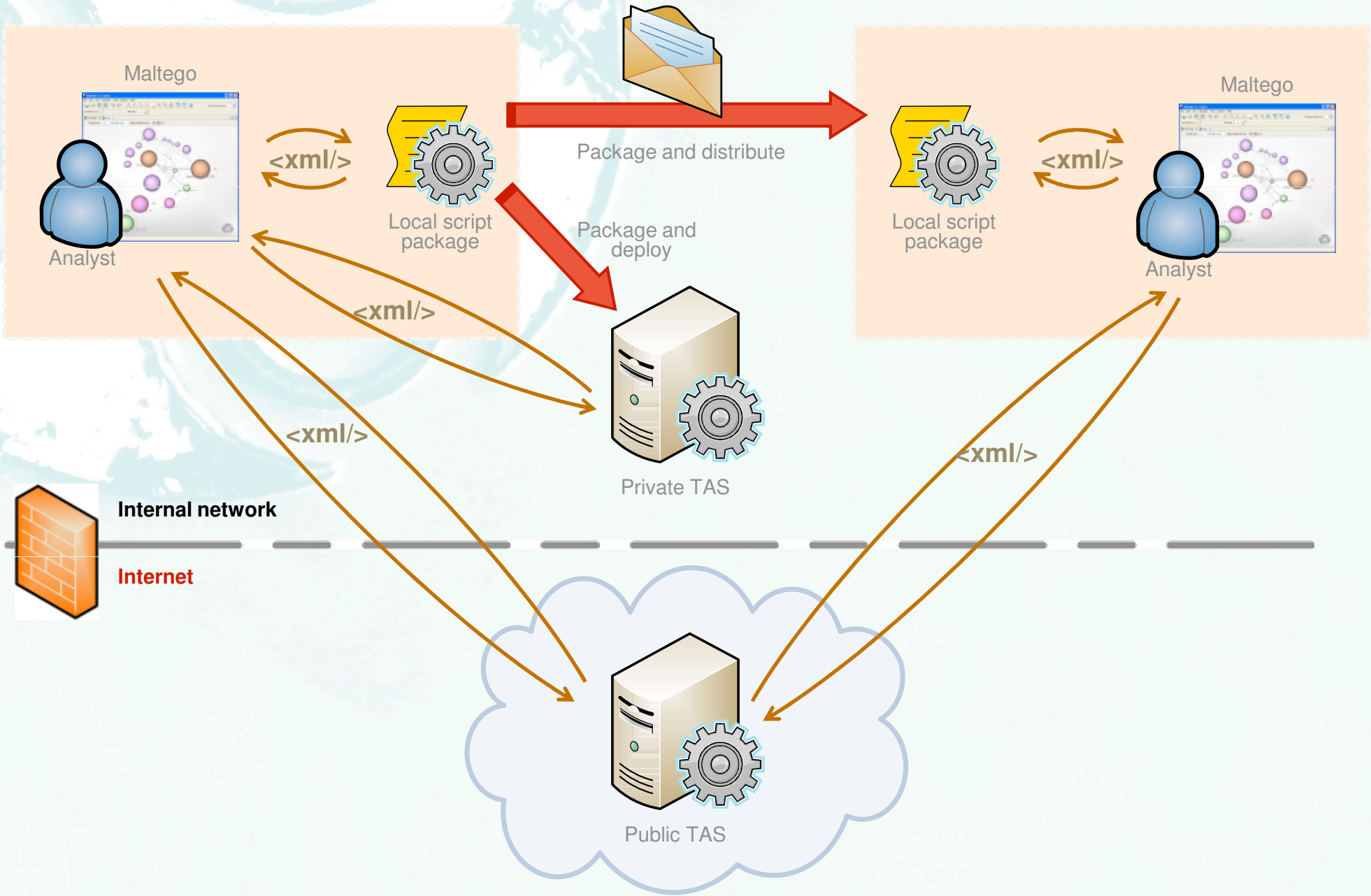
2.1 *internal release*
Group nodes
Navigation enhancements

2.5 *sometime soon*
Custom entities (2.5)
Sharing of transforms (2.5)

Community and BackTrack(3 & 4) releases

Maltego Transform Versions

2.0.2



Local transforms

Let's see how easy it is to integrate with Maltego

- any platform
- via stdin/stdout
- any external process that can do xml

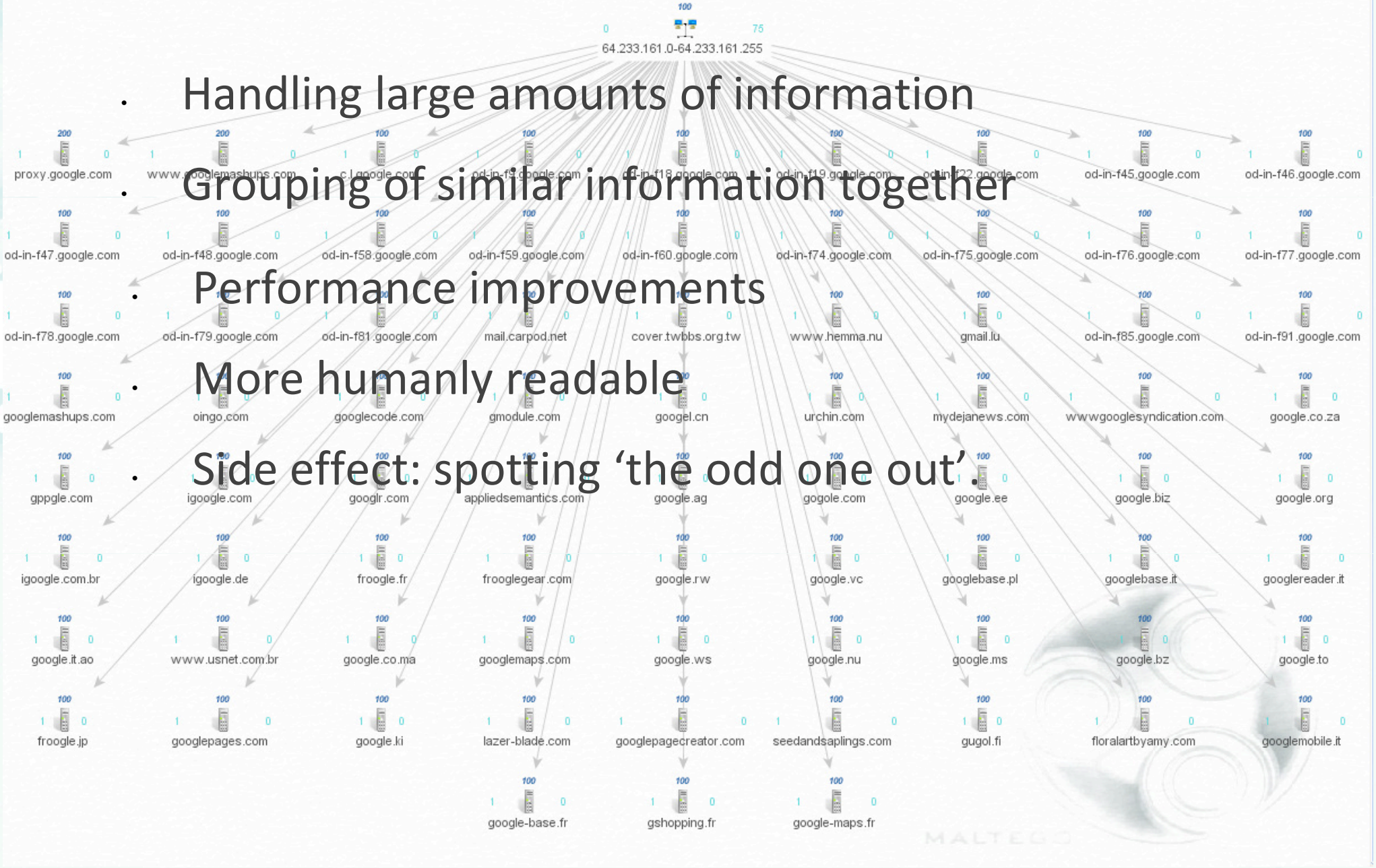
Local transforms specification at:

http://ctas.paterva.com/view/Local_Transforms

Demo of Maltego Local Transforms (Set website icon)

Group nodes

- Handling large amounts of information
- Grouping of similar information together
- Performance improvements
- More humanly readable
- Side effect: spotting ‘the odd one out’.



Demo of Maltego Collection nodes (Google network)


PATERVA
Integrating with Maltego

Integrating with Nmap

Real easy – use the local transform specification

Not a lot more to be said…

Couple of transforms:

- Scan IP for services
- Scan network for services
- Service to port
- Service to banner
- Using standard –sT and a port list

Integrating with Nessus

Real easy – use the local transform specification

Use the *nessuscmd* command as it will also load the dependencies.

Using list of nessus plugin IDs inside script

Both run from our Windows machine.

Demo of nmap/nessus integration

Integrating using SQL

Use the SQLTAS to query the SQL database

Late last year the forum website for B&H was hacked and put on PirateBay. Let's look at the forum DB.

Demo of using SQL TAS (Forum DB)


PATERVA
Integrating with Maltego

Integrating with Squid

Some history around this:

Rewind to 2006/6 – playing with Gmail cookies

Reaction then:

"exposure does represent a limited security problem."

2007 – Blackhat Las Vegas – Ferret scared lots of people.

Some changes to application – more later…

Integrating with Squid

Real world scenario:

Chasing Mr X who was speaking with an internal leak

Wanted something that could pro actively look for possible information leakage points.

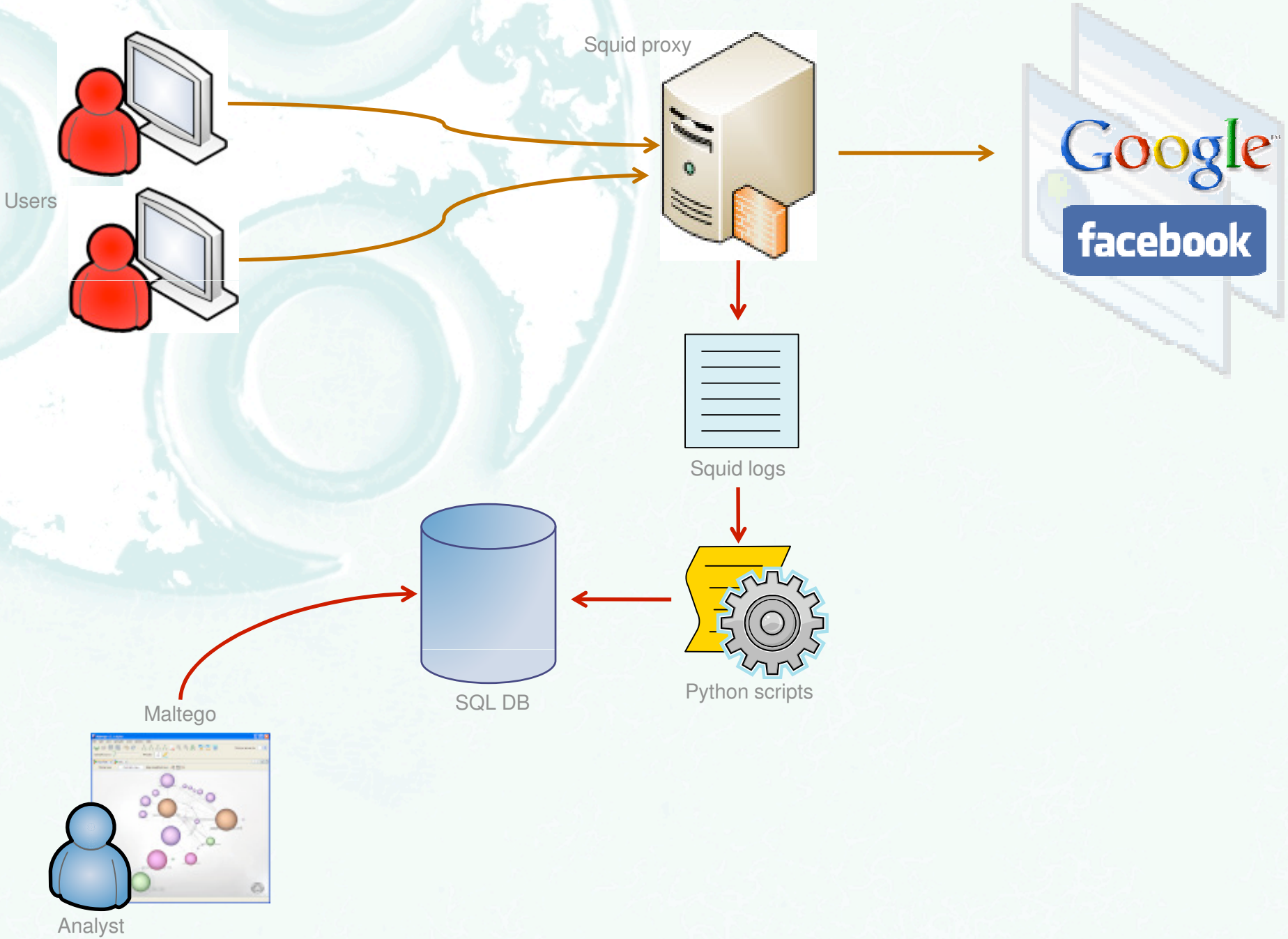
Integrating with Squid

Disclaimer:
Don’t try this at home or at the office. Total disregard for privacy.

This is NOT a commercial solution/product/whatever – so don’t ask.

Also known as ‘how bad does it get when your company/ISP/government want to spy on you’.

Squid setup and environment



Squid configuration

Two changes to standard squid configuration:

strip_query_terms off

log_mime_hdrs on

This gives you the cookies and the query terms.

Silly things to do:

Logs sites, questions to Google, large picture downloads☺, EXEs to DB

Become the user

With the session cookies we can become the user and automated some functions on behalf of the user – such as:

- View address book (Gmail)
- View friends (Facebook)

You cannot hide:

As soon as session cookie is seen and even before the user's app is even properly rendered we extract and store these.

Become the user part II

We can even search the user's mailbox for interesting things that might lurk there – as long as the cookies are valid we're good to go…

And – just for fun - set the user's Facebook status to his/her last Google search.

Different way to integrate different web applications.

Scenario for demo

"Any technology sophisticated enough is virtually indistinguishable from a rigged demo"

2 users – 'Chris' & 'Roelof'

Roelof == chief scientist at defense contractor

Chris == low life tech at same company

Information about secret project ("Inhaca") has been leaked to someone at Pentagon.

Here is what happened…

Squid demo (server side)
Setting the scene

Squid demo (investigation with Maltego):

1. Search terms
   (search search terms, other search terms,
   common search terms)

2. Pictures viewed
   (IconURL, who shares pictures)

3. Getting address book / friends
   (who are using GM/FB, who shares contacts, reverse sharing)

4. Real time searching Gmail for content

5. Gmail / Facebook login
   (taking over a session in style)

6. (Setting FB status to last search)

Panic

Grabbing the cookie is easier than grabbing the creds

Can be applied to *any* application that's not using SSL.

Idle time-out / logout and the death of a cookie
    Google address book app is not killed upon logout

Transparent proxies
    Testing for transparent proxies
Rogue APs
Open proxies / 'Anonymous' proxies
TOR nodes

Social virus??

Don’t Panic

Solutions to the problem:

- SSL
  - Setting it up in Gmail (Settings)
- Default state of applications should force SSL
- Idle timeout / logout should destroy cookies

We’ve known about this for ages ?

Conclusion

We've looked at many different tools and how to integrate them with Maltego.

Maltego becomes the framework where this data becomes information.

Some 'vulnerabilities' have been known for a long while, but it really becomes useful when you can visualize the data.