Maltego Part I - Intro and Personal Recon

By Chris Gates, CISSP, GCIH, C|EH, CPTS

According to their web site, "Paterva invents and sells unique data manipulation software. Paterva is headed by Roelof Temmingh who is leading a light and lethal team of talented software developers." On May 6 2008, they released a new version of a very kewl tool named Maltego.

"Maltego, is an open source intelligence and forensics application. It allows for the mining and gathering of information as well as the representation of this information in a meaningful way. Coupled with its graphing libraries, Maltego, allows you to identify key relationships between information and identify previously unknown relationships between them. It is a must-have tool in the forensics.security and intelligence fields!"

Chris Gates' talk at ChicagoCon 2008s entitled "New School Information Gathering" touched on many tools and techniques. One of the tools he introduced to the audience is Maltego v2. This first in a two part series expands on this new tool with a basic introduction to Maltego followed by step-by-step personal recon tutorials. Part II will focus on infrastructure enumeration with Maltego.

The Facts

Where to get it?http://www.paterva.com/maltego

There is a Free Version and a Commercial Version

Maltego User's Guide (You'll want to read this first to get Maltego installed -- I'm not covering installation)

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

Who made it?

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

What is Maltego?

Maltego is an information gathering tool that allows you to visually see relationships. Maltego allows you to enumerate network and domain information like:

- Domain Names
- Whois Information
- DNS Names
- Netblocks
- IP Addresses

Maltego also allows you to enumerate People information like:

- Email addresses associated with a person's name
- Web sites associated with a person's name
- Phone numbers associated with a person's name
- Social groups that are associated with a person's name
- Companies and organizations associated with a person's name

Maltego also allows you to:

- Do simple verification of email addresses
- Search blogs for tags and phrases
- Identify incoming links for websites
- Extract metadata from files from target domains

More information: http://ctas.paterva.com/view/What_is_Maltego

What can Maltego do for you?

From the Maltego wiki:

Maltego can be used for the information gathering phase of all security related work. It will save you time and will allow you to work more accurately and smarter. Maltego aids you in your thinking process by visually demonstrating interconnected links between searched items.

Maltego provide you with a much more powerful search, giving you smarter results. If access to "hidden" information determines your success, Maltego can help you discover it.

Maltego Practical Example

Let's use Maltego to find information about a person, we'll then use maltego for network information, and finally blog and file information. We will use the Community Edition (free) of Maltego.

Fire up Maltego CE v2.0 and click on the Personal/Person icon.

Let's get oriented. On the left side we have our searchable options sorted by Infrastructure and Personal.

At the top in the middle we have our different "views" including Mining, Centrality and Edge Weighted.

Maltego supports 4 types of layout algorithms:

Block layout. This is the default layout and is also used during mining. This layout is discussed in more depth later.
Hierarchical layout. Think of this a tree based layout â€“ like a file manager.
Centrality layout. Nodes that are most central to the graph (e.g. most incoming links) appear in the middle with the other nodes scattered around it.
Organic layout. Nodes are packed tight together in such a way that the distance between each node and all the other nodes are minimized.

**Check the users guide for more information on the views and layouts. http://ctas.paterva.com/view/Userguide

Above that is our Speed/Accuracy versus #Results tab. This should be fairly self explanatory. If you slide the bar toward #Results the more results you get. Slide it to the other side, and you get fewer results which will increase the speed of your search but also sacrifice your accuracy. So if you don't like the results or don't get any results with the Speed/Accuracy slider to the left, slide it to the right to change the weights of the search.

On the far right is your Satellite View, and detailed transform output:

And finally at the bottom is our Transform Log/Output:

Before we get started, there's one last piece of background on Maltego. All the information gathering "processes" that Maltego does are called "Transforms," and unfortunately not all of them are documented. But different transforms query different types of information. The full list is here.

Here is an example of a transform (DomainToMXrecord_DNS):
"This transform determines if an MX record exists for the given Domain. The MX record is the mail exchanger record and is returned as a MXrecord. The IPAddress of this record gives a good indication of the network location of the target as most organizations keep their mail close to their network. This is normally used in the infrastructure footprinting of an organization."

Personal Recon Tutorials

Let's get started enumerating information on Don :-)

We start with taking a name, in this case Don Donzal, and use Maltego to enumerate possible email addresses. The first thing we have to do is input our search terms. First Name: Don, Surname: Donzal. You can also use additional search terms like Country Code and Additional Search Term.

Maltego gives us three options for email address enumeration. PersonToEmail_SamePGP, PersonToEmail_Common, PersonToEmail_SE (Search Engine)

It appears Don hasn't registered an email address tied to a PGP key, so nothing there. Email to common gave us one email address, of most benefit was using PersonToEmail_SE or Search Engine which gave us 16 results. You can see this in the Output-Transform Execution. I ran this transform without any additional search terms or country code.

Here is the output using "ethicalhacker" as a search term.

It wouldn't take much background about Don to know that immediately two email addresses are good, don at digitalconstructionco.com and don at ethicalhacker.net.

Let's select the digitalconstruction email and dig from there.

In the Transform Detail View we can see what Search Engine links that fed us the don at digitalconstuctionco email.

Using the EmailAddressToEmailAddress_Verify Transform we can also verify the email address.

Using the Person To Phone Number Search Engine Transform, we can gather possible phone numbers based on Don's Name. We got eleven phone numbers. It wouldn't take that long to call them all, or we could use some of the Infrastructure Transforms (later) to get a geographical location to help us narrow down which area codes might correspond to Don's location. Or we can use our powers of deduction to say that there is a high probability that The Digital Construction Company, which produces ChicagoCon, just might be in Chicago :-)

Using the PersonToAff_Spock Transform, we can see if Don has a Spock profile that will (hopefully) give us any Social Network sites Don is a part of.

We use the AffSpockToAff_Others Transform from the Spock output to see other social networks Don is a part of, or at least don at digitalconstructionco.com is.

We can see that Don also has a LinkedIn profile, and we are given a link to it.

The AffSpockToWebSite_List Transform also leads us back to The Digital Construction Company. At this point we could start some Network Infrastructure Enumeration on The Digital Construction Company's website and IP Space, but we'll leave that for Part II.

The EmailAddressToAff_Rapleaf Transform shows us there is a myspace profile as well. Keep in mind that if the person you are querying hasn't been queried before by rapleaf (either through Maltego or the website), you'll have to try to run the transform again after a few hours. This is because rapleaf needs time to do its querying.

In addition to our Spock results we can run a Website Search Transform on Don Donzal to see what web sites are associated with that name. Notice the results are weighted, and we get the associated URLs when we click on a web site.

As you can see we have found a lot of information just based on a little bit of prior knowledge and Maltego. We have email addresses, phone numbers, social networking profiles, and a list of web sites for further investigation or enumeration, and Maltego has even "weighted" them for us to help us along. In Part II we'll cover Infrastructure Enumeration with Maltego.