Maltego and its features

Rahul Tak

University of Applied Sciences Ulm

Bachelor of Computer Science

Date: 21.01.2019

Abstract

As we are in approaching towards an era of digital life, the importance of our data is more important than anything else. One of the biggest challenges is to store the sensitive data securely. As information gathering is an really important aspect in the process of Penetration testing, it is taken seriously into account by security professionals, hackers etc. An attacker will try to gather as much information as possible before even starting the attack and this is done by using many different tools. This paper discusses about the usage of a really powerful open source intelligence tool (OSINT) know as Maltego and its features. This tool is designed to fetch data on DNS and WHois, this tool offers search engine querying, SMTP queries etc.

1 Introduction

Maltego is a really powerful proprietary software which fetches and uses the data from open sources and visualizes that information in a graphical format. It puts a lot more emphasis on relationships between nodes in the graphs. It is used for open source intelligence and digital forensics and is developed by Paterva.

Maltego is using a client/server based architecture for purpose of collecting the data and determining the relationship and real world links between pieces of data. Analysis of the real world relationships social networks and computer node networks between people, domains, webpages, networks etc.

It generates a node graph in which nodes called entities are plotted and relationships are represented with arrows and this property let’s an attacker find relationships between pieces of data he has.

1.1 Types of forms

It offers two types of reconnaissance options “Infrastructural” and “Personal”. **Infrastructural Reconnaissance** covers information:

- DNS information
- Name server, mail exchangers
- Zone transfer tables
- DNS to IP mapping

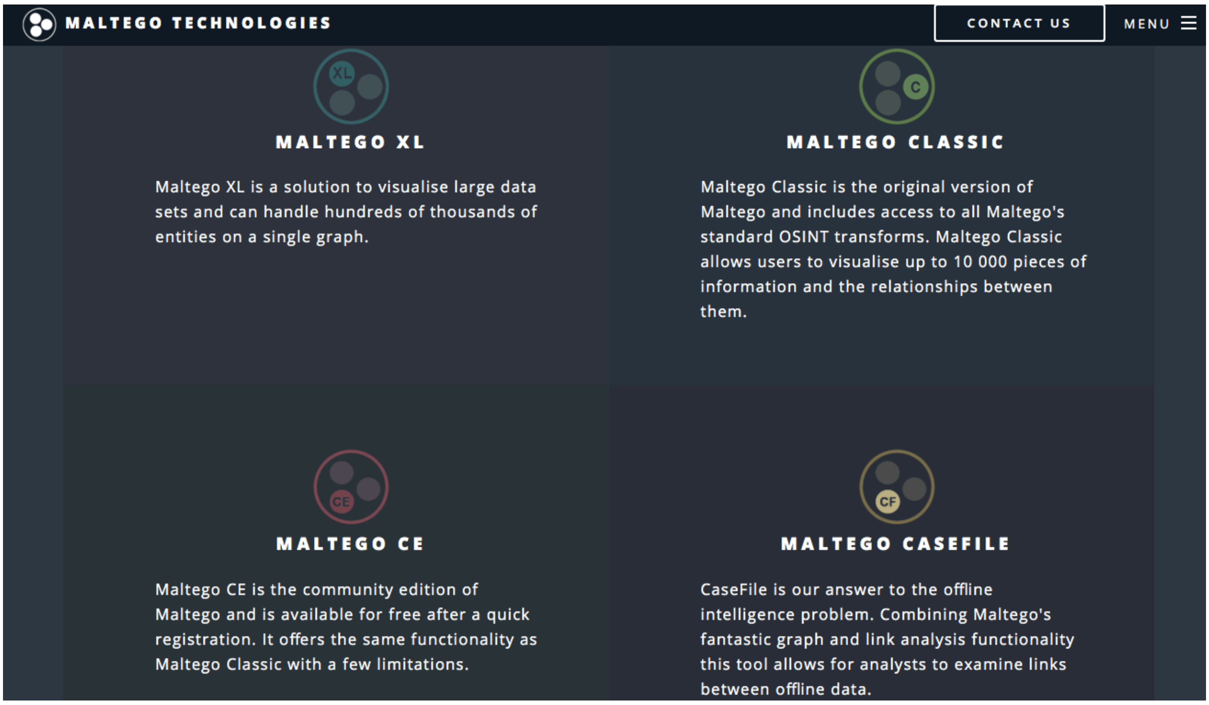
Personal Reconnaissance covers information:

- Personal information
- Email addresses
- Phone numbers
- Social networking profiles

1.2 Maltego Editions

Maltego is available in 4 different editions :

1. Maltego XL
2. Maltego Classic
3. Maltego CE
4. Maltego CaseFile



MALTEGO XL

Maltego XL is a solution to visualise large data sets and can handle hundreds of thousands of entities on a single graph.

MALTEGO CLASSIC

Maltego Classic is the original version of Maltego and includes access to all Maltego's standard OSINT transforms. Maltego Classic allows users to visualise up to 10 000 pieces of information and the relationships between them.

MALTEGO CE

Maltego CE is the community edition of Maltego and is available for free after a quick registration. It offers the same functionality as Maltego Classic with a few limitations.

MALTEGO CASEFILE

CaseFile is our answer to the offline intelligence problem. Combining Maltego's fantastic graph and link analysis functionality this tool allows for analysts to examine links between offline data.

Figure 1: Types of Maltego editions and their description

Maltego is a java based application which is supported on a large scale and on many operating systems. The key components of maltego framework are entities and transforms. Entities represent objects which transforms are run on. They are used represent a number of things ranging from telephone numbers to IP addresses v4 and v6. Transforms are pieces of code that take in an entity as input and perform some kind of alteration on this entity and returns a new entity.

Lately, in 2014, 80 million users data were stolen and the forensic expert used Maltego to find out that there servers were connected to the Chinese hacker groups.

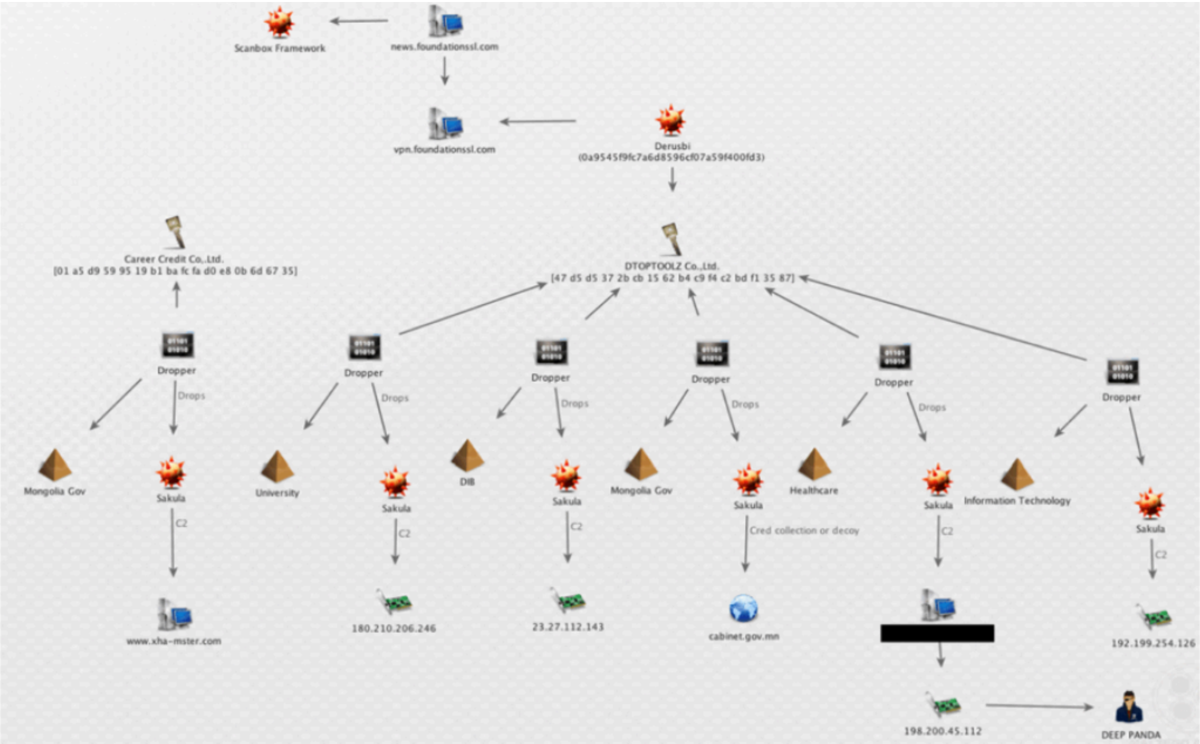
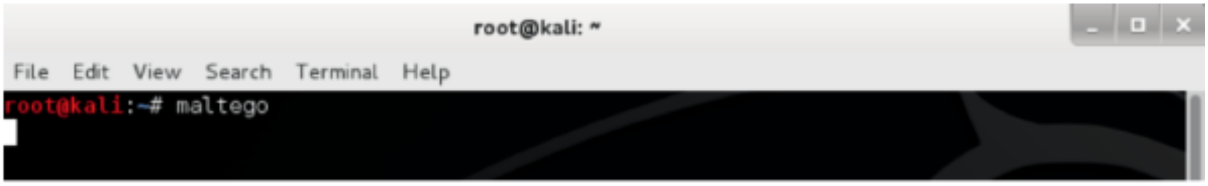


Figure 2: Example showing the use of Maltego in a graphical view

2 Use of maltego in an practical example

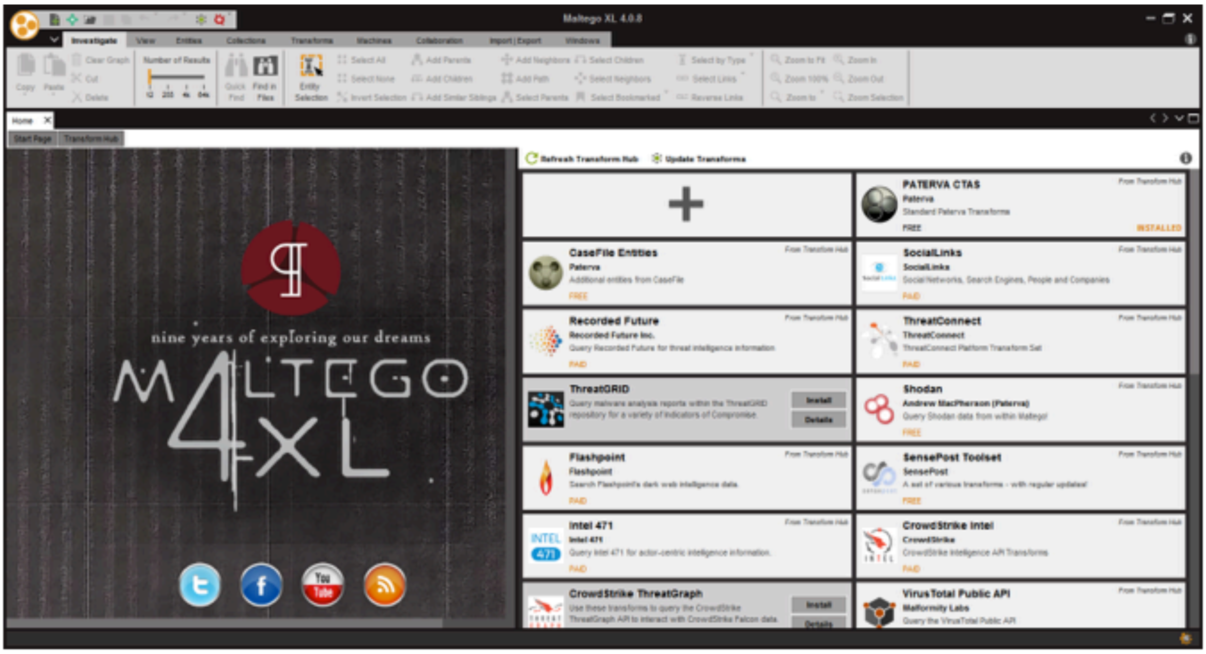
To start using the maltego, run the command **“maltego”** in kali linux terminal.



```
root@kali:~# maltego
```

Figure 3: command to open “maltego”

After booting up, it will ask for login credentials of the new user. The next process is to select from all the available options to create a visualised formation of the fetched data helps in more deep understand of the attacker/victim's situation.



PATERVA CTAS
Paterva
Standard Paterva Transforms
FREE
INSTALLED

CaseFile Entities
Paterva
Additional entities from CaseFile
FREE

SocialLinks
SocialLinks
Social Networks, Search Engines, People and Companies
PAID

Recorded Future
Recorded Future Inc.
Query Recorded Future for threat intelligence information
PAID

ThreatConnect
ThreatConnect
ThreatConnect Platform Transform Set
PAID

ThreatGRID
Query malware analysis reports within the ThreatGRID repository for a variety of Indicators of Compromise.

Shodan
Andrew MacPherson (Paterva)
Query Shodan data from within Maltego!
FREE

Flashpoint
Flashpoint
Search Flashpoint's dark web intelligence data.
PAID

SensePost Toolset
SensePost
A set of various transforms - with regular updates!
FREE

Intel 471
Intel 471
Query Intel 471 for actor-centric intelligence information.
PAID

CrowdStrike Intel
CrowdStrike
CrowdStrike Intelligence API Transforms
PAID

CrowdStrike ThreatGraph
Use these transforms to query the CrowdStrike ThreatGraph API to interact with CrowdStrike Falcon data.

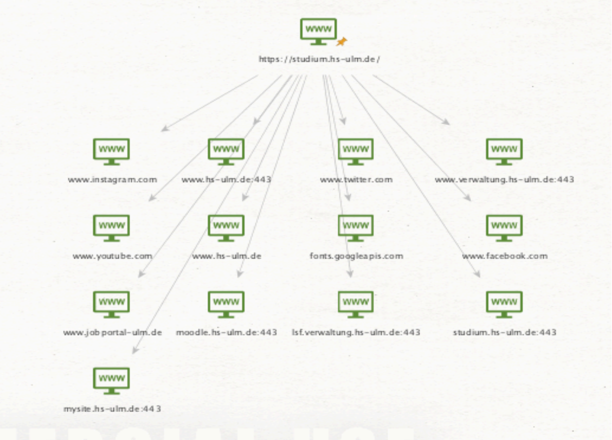
VirusTotal Public API
Malformity Labs
Query the VirusTotal Public API

Figure 4: The selection panel

As for example, just by using the website URL, an attacker gets all the related information about the whole organization available. The information displayed in a graphical format lets attacker to understand the whole IT infrastructure of the company.

2.1 Network information of an organization

In the below example, creating a new graph with new entities and using the address of the Hochschule website https://studium.hs-ulm.de/en, gavefollowing result in a visual paradigm.



Using the following, information and digging in further an attacker can find more information about DNS, Domains, Network Blocks, IP etc. Below are the results of different transforms used.

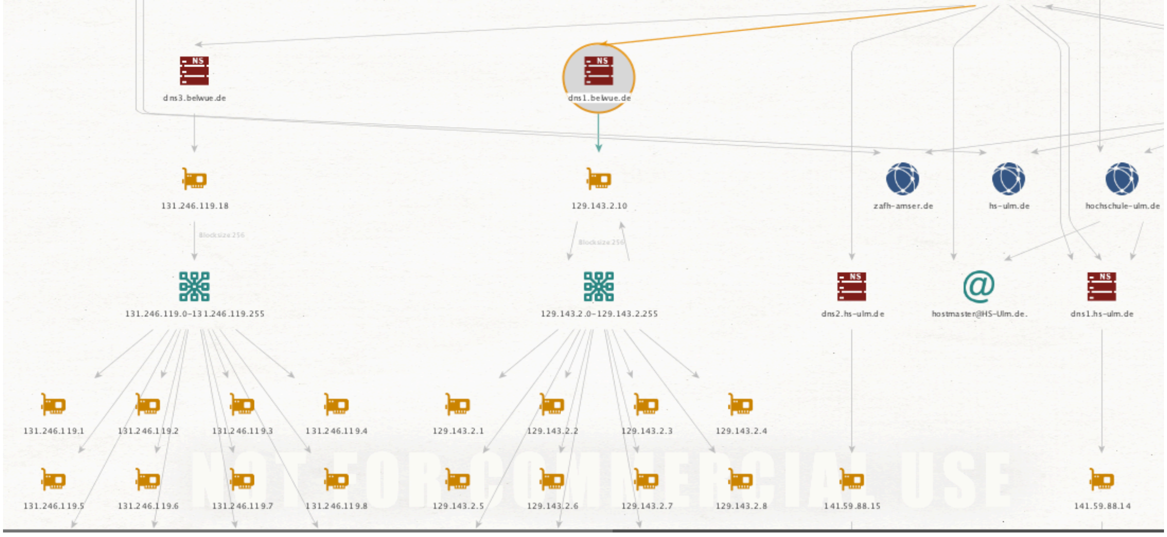


Figure 6: Connected network nodes

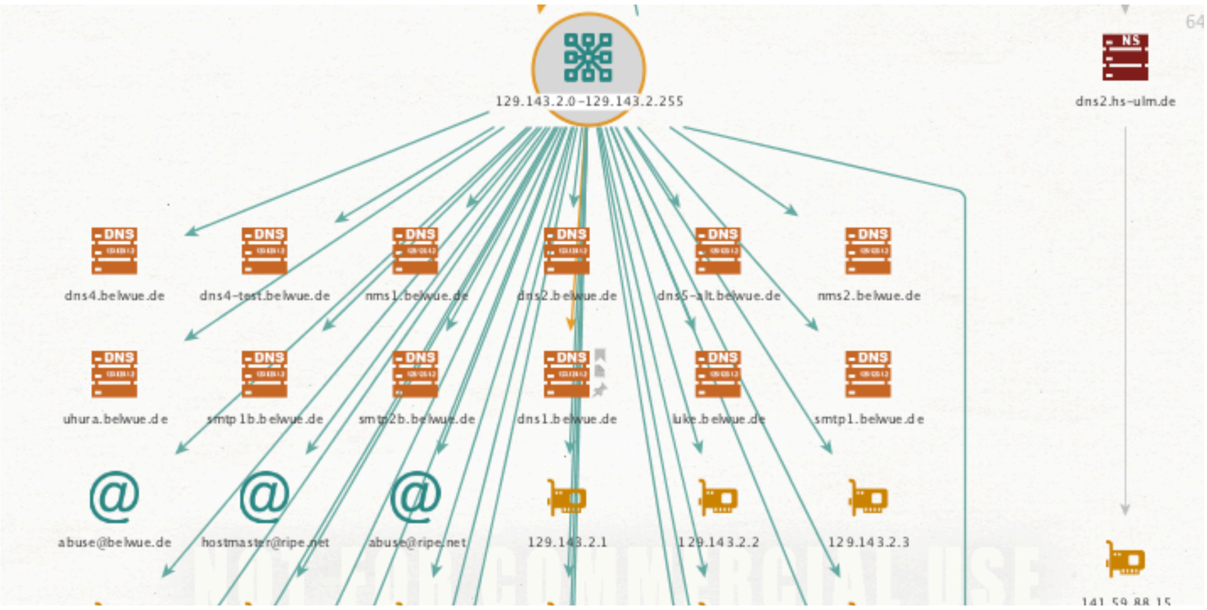


Figure 7: Transform—Domain to DNS and admin email

Just some clicks, gives a lot amount of information which is stored on the web.

2.2 Email information harvesting

- Select an email address from an organization. Run the email transformation. For eg “ tak@mail.hs-ulm.de.”

- Selecting the phone numbers, codes and location etc.

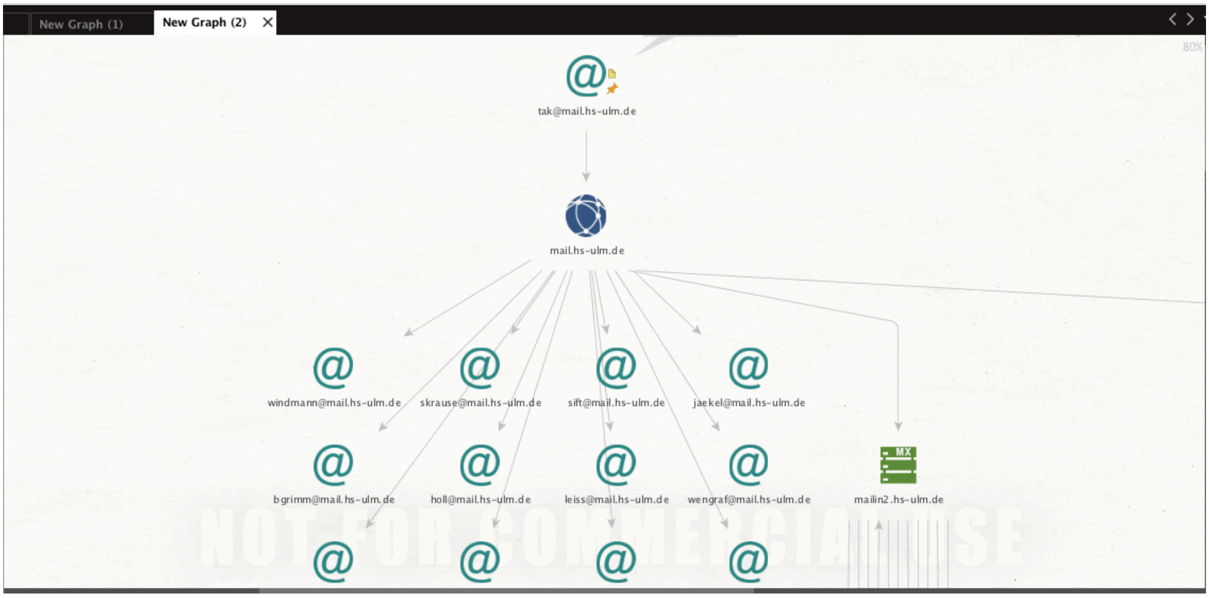


Figure 8: Email fetched

The free version of the Maltego CE edition gives the first 12 entities it maps from the information. In the above case, it tries to fetch all the related email address with the name “mail.hs-ulm.de”. Just like this attacker gets the email address of the employee on the web or website itself, runs through the transforms get’s the information like mail exchange server, location of the server etc. and does go on collecting bit of information which gives him a huge advantage to get his victim down. Every bit of information is being visualized and thus helps to map the whole organization.

2.3 Person search

Further, using the above founded email results to gather more information about an individual. Maltego provides an transfrom specifically designed for searching a person details based on his email in different search engines, social media etc.

Maltego gives three different options:

- PersonToEmail_SamePGP
- PersonToEmail_Common
- PersonToPhoneNumber_SE
- PersonToEmail_SE(search engine)

There are different transforms that are used by attackers to further dig in every small bit of information and reach his victim as soon as possible without spending much time.

2.4 Transforms

The process which are done in the background of the software which gathers all kinds of information are called “Transforms”. In Maltego “Transforms in the software are the piece of code which change one kind of information to another”. Each transform shows the pops up message with the both input and output requirements. Not all the transforms are documented.

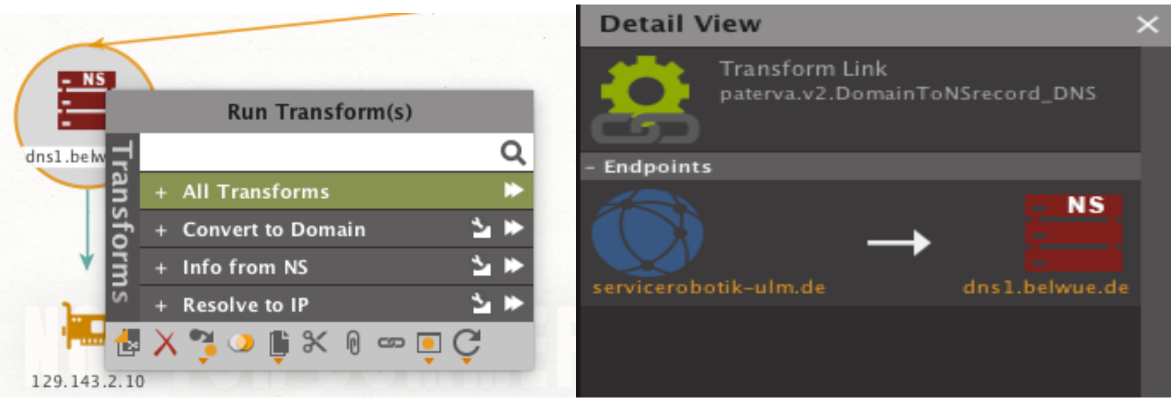


Figure 7: Transforms

Example: This transform determines if an NS record exists for the domain given. This is kind of transforms are used mostly for infrastructure foot printing of an organization.

There is a very special framework available for developing transforms called **Canari Web Framework**. It is known to be the world’s most famous rapid7 transform development framework for maltego. Attacker can make his own transforms locally and then can use them remotely by migrating to the remote transform package.

2.4 Fetched data in a visualized graph

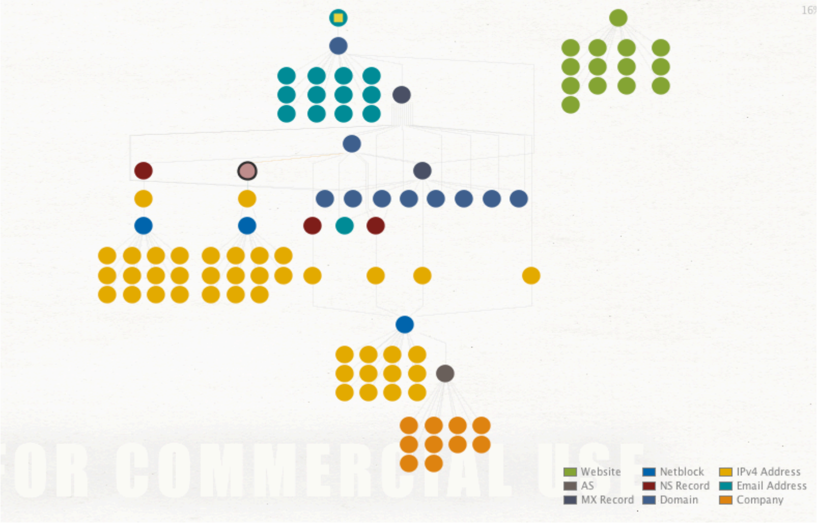


Figure 8: All kinds of data in graphical format

There are many options, transforms available to find hidden data on web or elsewhere. Below are some default transforms:

- Company Stalker: This option searches a company's email addresses and social media accounts linked to it based on just the domain.
- Footprint L1: It is a simple form of a domain search.
- Footprint L2: Takes more time, but gives more information which was hidden.
- Person to email address: It searches for a particular person based on the email address.
- URL to network and domain information

Maltego can be used with Metasploit biggest framework to develop and execute exploit code against remote machines and also many other tools.

Conclusion

Maltgeo is a tool which is best suited for footprinting and reconnaissance. It is an amazing tool which is being used by both attackers and defenders as their favourite tool. Many security firms also uses it and thus they look for pentesters who have knowledge about maltego. It does not require much experience for the using it. In a single sentence "Collects all distributed data into an visualized graph, easy to understand for brain."

References

- http://www.canariproject.com/en/latest/canari.quickstart.html#hello-world
- http://www.cs.ru.ac.za/research/g11m3847/downloads/thesis.pdf
- https://scholarspace.jccc.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1082&context=c2c_sidlit
- https://www.blackhat.com/presentations/bh-europe-08/Temmingh-Bohme/Presentation/bh-eu-08-temmingh-bohme.pdf
- https://en.wikipedia.org/wiki/Metasploit_Project
- https://www.maltego.com