Maltego: Intelligent Information

by Washington Almeida

Many powerful tools are available for capturing, mining and processing information from the Internet environment, sometimes referred to as public network, but one in particular draws my attention: Maltego. Why? Maltego is a proprietary multi platform software tool developed by Paterva, used to gather information from public sources and display it in a graphic framework. This is a sophisticated tool that provides a set of transforms that can be done over entities, both infrastructures and people.

In this article, I will work on Maltego for network intelligence gathering and explore some of its functionalities.

In order to understand how hackers have success in their attacks, it is critical to understand how they think, how they plan and how they act. A product of extreme importance to the hacker is the information, and the more valuable the information, the better.

The traditional Internet is unsafe against a common form of public network surveillance known as traffic analysis. Traffic analysis can be used to infer who is talking to whom over a public network. Knowing the source and destination of the Internet traffic allows others to capture the data traveling between them.

One of the main hackers' objectives is to perform penetration tests in order to check whether the system under study is secure or not, looking for vulnerabilities on the target system that can be exploited in order to gain control of it. In order to check it, some tests need to be performed using several tools. They frequently make use of the deep web to keep themselves anonymous.

However, many powerful tools are available for capturing, mining and processing information from the Internet environment, sometimes referred to as public network, but one in particular draws my attention: Maltego.

Why Maltego?

Maltego is a proprietary multi platform software tool developed by Paterva (www.paterva.com), used to gather information from public sources and display it in a graphic framework. This is a sophisticated tool that provides a set of transforms that can be done over entities, both infrastructures and people.

In this article, I will work on Maltego for network intelligence gathering and explore some of its functionalities.

Legal note:

Maltego is a computer program developed by Paterva (Pty) Ltd., protected by copyright law and international treaties. Unauthorized reproduction or distribution of Maltego, or any portion of its resources, may result in severe civil and criminal penalties.

The citations of the resources belonging to the Paterva's domains www.paterva.com and the figure 5 used in this article were previously submitted for Paterva's review and approval, so that its publication could be authorized in this article.

Acknowledgment note:

I would like to reserve special thanks to the dedicated Paterva staff, who have made themselves available to provide all the necessary support and assistance in the preparation of this article since my first contact with them. Paterva has a great staff!

Also, I extend thanks to my professional colleague Paulo Cesar Breim, one of Brazil's largest Forensic Experts with extensive experience in Digital Forensics involving intellectual property infringement, bank fraud, and systems invasion, among others. Paulo has a great legacy as one of the first IP addresses in Brazil, creation of the first BBS's and developed security devices for banking systems.

What is Maltego used for?

Maltego is a sophisticated tool that can perform Internet based research which can be used for, but not limited to:

1. Reconnaissance on the understructure of web presences and technologies used;

2. Mapping URLs and networks;

3. Extractions of data from social networks such as Twitter;

4. Geo-localization of on-line contents;

5. Deepweb resource analysis capability;

6. Much more…

Working with Maltego:

In a first contact with Maltego, the user should probably ask himself: How and where to start? Of course, it is expected that the user has read all the product documentation, but in practice this is not what often occurs.

So at first glance, it may seem a bit tricky working with Maltego, but as we present the product, the Pentest Magazine reader will be able to certify that it is indeed an extremely simple tool, the result of the excellent work of Paterva's development team.

And as part of the excellent job done by Paterva's team the steps to install Maltego are very well documented at URI https://docs.paterva.com/en/user-guide/introduction/ for Windows, Mac OS and Linux.

Thus, we can go ahead and get start working on Maltego.

When you launch Maltego for the first time, the user see a screen similar to the exhibited in Figure 1.

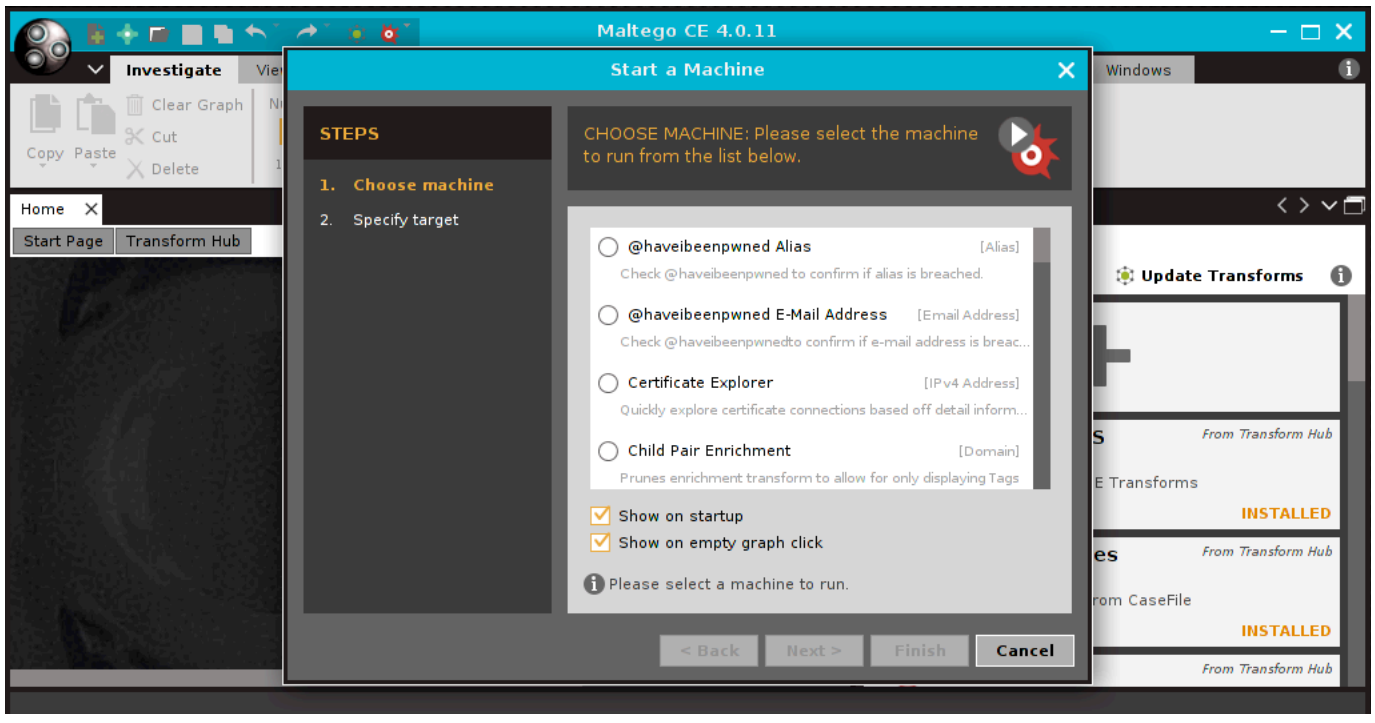


Figure 1: First contact with Maltego

There are many concepts involved within the Maltego environment, so I strongly recommend that the Pentest reader consult the excellent and detailed documentation of this powerful tool on Paterva's website.

Moving forward in the article, I will introduce some of these concepts, for to write in detail about Maltego would make this article a book.

So according to Figure 1, it is important to understand conceptually what is a machine in the Maltego context.

Actually, Maltego integrates two categories of searches that are known as Machines and Transforms. Machines refer to a sequence of codes that enable targeted data extractions from the public network, commonly referred as the Internet. Transforms are sequences of code that literally transform one type of entity to other types.

To better understand these concepts, let us move forward on a practical exercise.

At this point, I just cancel this initial options suggested in Figure 1 and I will be redirected to Maltego main panel.

Before starting working on Maltego it is important to remember the user must register the Maltego license.

Taking into consideration that all steps required for registration have been done and the user is in the main panel of Maltego, we start the exercise clicking in the Maltego icon followed by "New" option as shown in Figure 2.

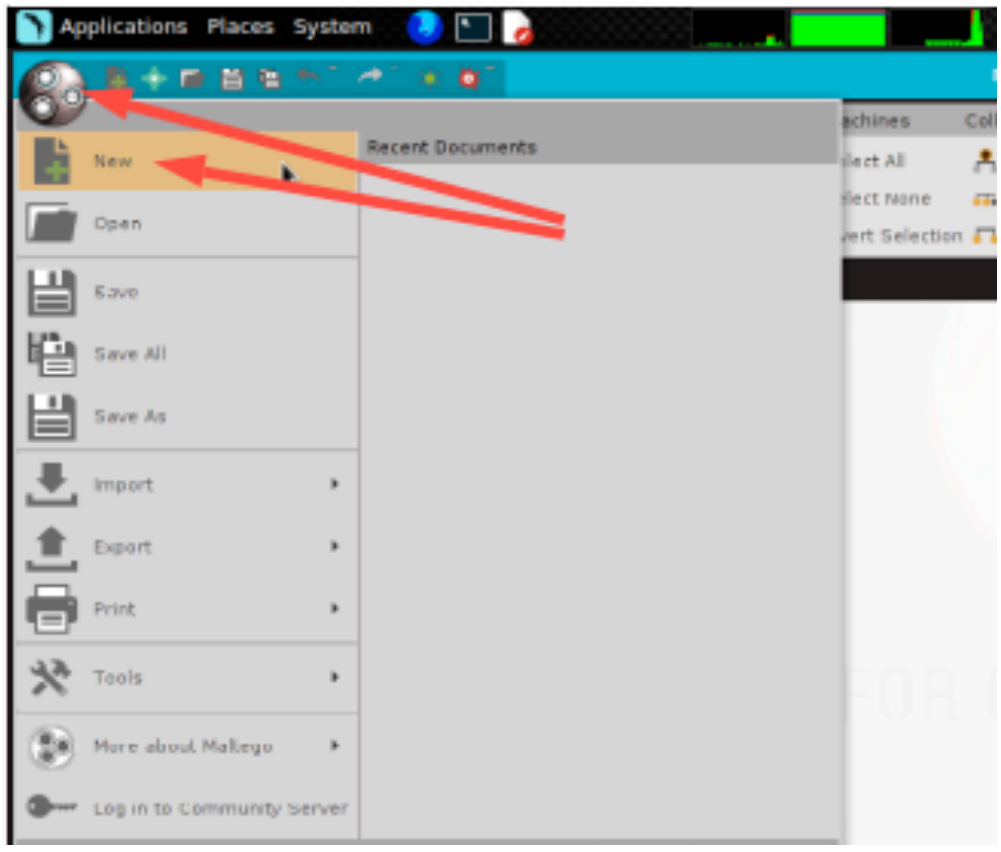


Figure 2: Starting a new graph

After clicking in the "New" option, a new graph named "New Graph(1)" is opened inside the Maltego framework. In the left side menu, there are lots of options and under Infrastructure, we can see all the entities belonging to Infrastructure group.

In this exercise, I will use the Entity named "URL", so I click in URL, holding down the left mouse button and dragging it to the graphical environment as shown in Figure 3.

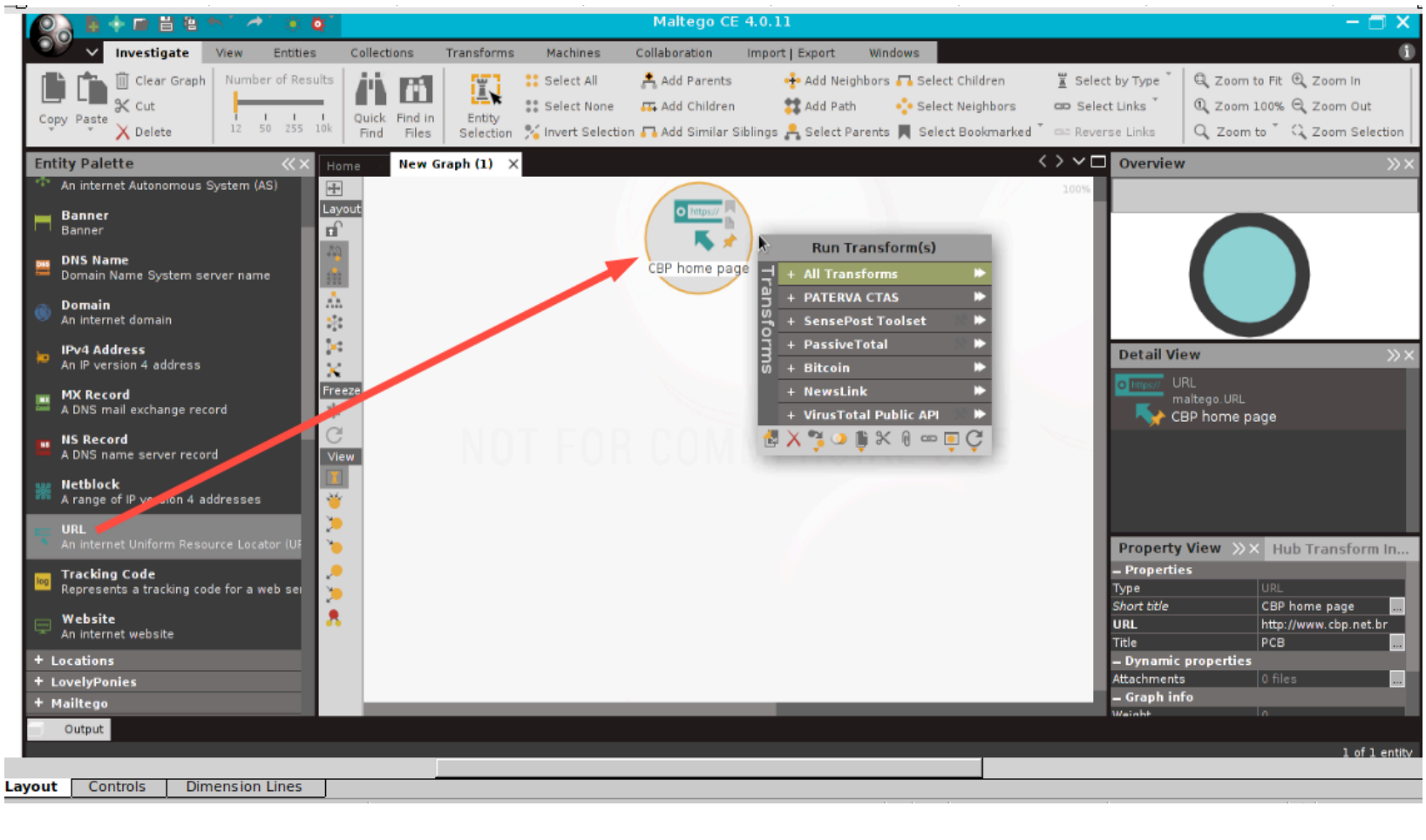


Figure 3: Creating a new transform

After having the object inside the graph area, I double click on it to set the object according to my interest.

In this case, I will perform research in the Paulo Cesar Breim company (thanks, Paulo, again, for the authorization). Thus I need to set the object up according to the targeted URL, which is shown in Figure

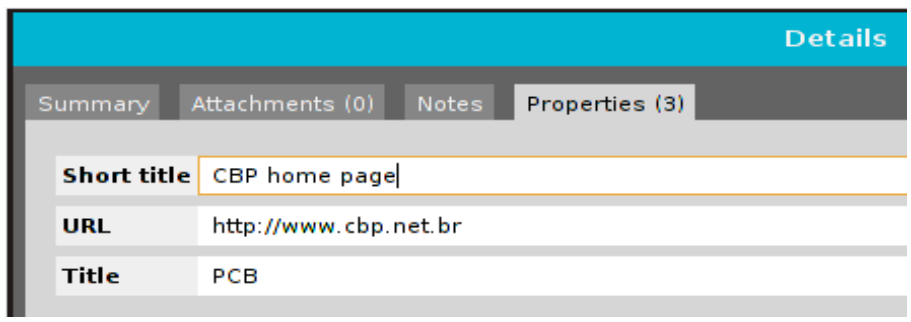


Figure 4: Setting the Maltego object

Note: URL entity is actually a special case. The display and edit information is the title and the URL itself is a entity field. The best way to get a URL into Maltego is to open the page in a browser and copy and paste the URL into Maltego.

Having the URL correctly set, I just right-click on the URL object and a series of options will be shown as exemplified in figure 5.

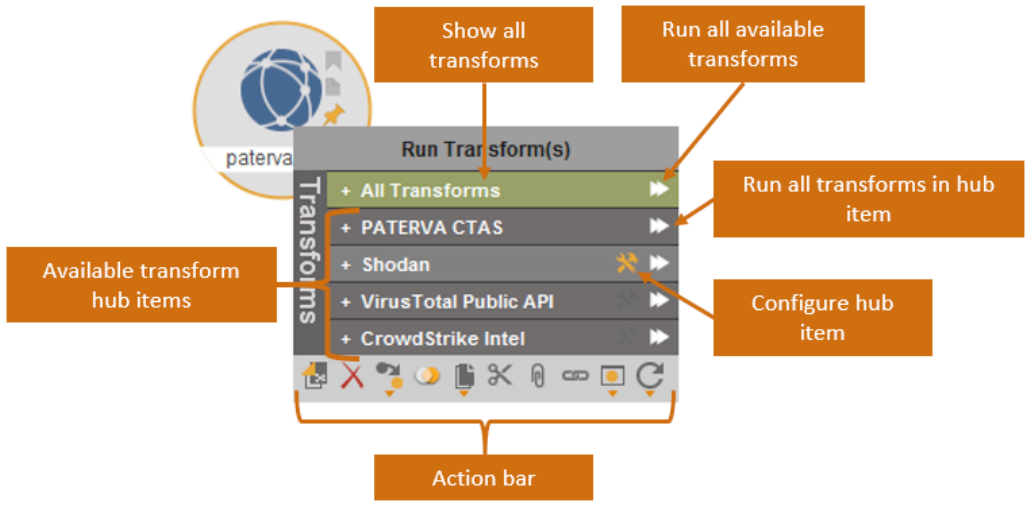


Figure 5: Top level context menu

Copyright notice: Figure 5 has been copied under Paterva authorization from the Paterva web site in the URI https://docs.paterva.com/en/user-guide/getting-started exclusively for the purposes of this article. All rights reserved to Paterva (Pty) Ltd.

Figure 5, created by Paterva's team, is very explanatory and also much better than I could do. Therefore, respecting the exclusive copyrights of Paterva, I just click on the arrows in the end of the "All Transforms" option identified as "Run all available transforms" by Paterva.

According to Paterva's documentation, "this option is almost always a bad idea as it is important to know what we are running and where the transform is getting the information from".

Paterva's recommendation makes sense because it makes no sense to seek information that I do not know where it comes from and what it is used for.

For the purpose of this article, the idea is to bring as much information as I can research from the resource in order to comment about some concepts.

Remember I wrote that "Transforms are sequences of code which literally transforms one type of entity to other types."

This is what happened when having a look at figure 6, where we can see other types of data that has been generated by the first one. Also, we can realize that the type of data generated are different from the first.

This was my only motivation to perform "All Transforms" at this point, since I completely agree with Paterva's recommendations.

So remembering what I always write in my articles, the Forensic Specialist is solely responsible for the information obtained, not the tool.

Thus, although I trust all the information that Maltego brought, I decided to verify the information gathered, checking the outputs from other tools, and I start using nikto to check what it brings as output (some outputs removed).

```
┌─[wash@parrot]─[~]

└──╼ $nikto -h http://www.cbp.net.br

- Nikto v2.1.6

---------------------------------------------------------------------------

+ Target IP:          (***REMOVED***)

+ Target Hostname:   (***REMOVED***)

+ Target Port:     80

+ Start Time:      2017-03-15 13:37:29 (GMT-3)

---------------------------------------------------------------------------

+ Server: nginx/1.4.6 (Ubuntu)
```

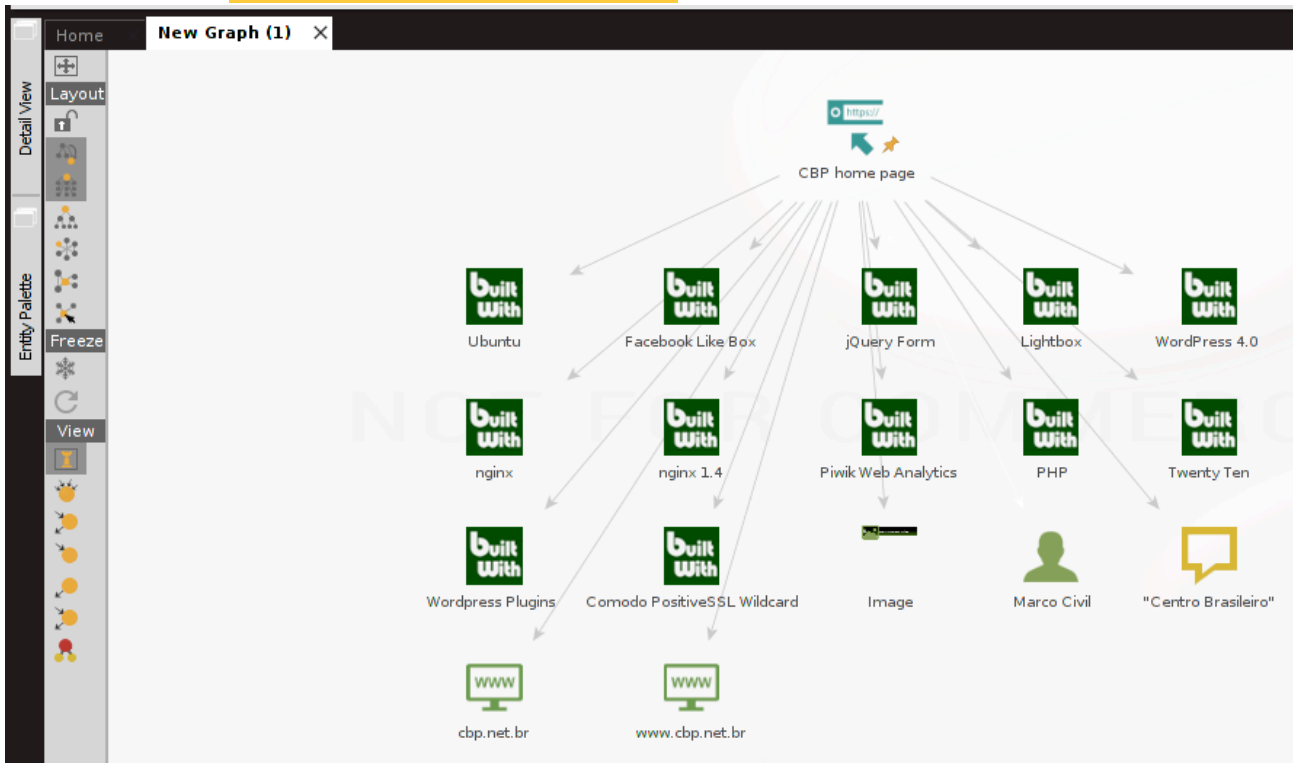


Figure 6: Maltego Transforms in action

As we could verify with nikto, the CBP's website was built with ngix/ngix 1.4 under Ubuntu as reported by Maltego. But there is more information to verify.

Also, we can see the “Comodo PassiveSSL Wildcard” as a result in Figure 6.

Let us perform an sslscan against CBP’s website to check its outputs (some information removed).

```
┌─[root@parrot]─[/home/wash]
└──╼ #sslscan www.cbp.net.br
Version: 1.11.8-static
OpenSSL 1.0.2k-dev xx XXX xxxx
Testing SSL server www.cbp.net.br on port 443
TLS Fallback SCSV:
Server supports TLS Fallback SCSV
TLS renegotiation:
Secure session renegotiation supported
SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:  2048
Subject: *.cbp.net.br
Altnames: DNS:*.cbp.net.br, DNS:cbp.net.br
Issuer:  COMODO RSA Domain Validation Secure Server CA
```

Once again, we were able to certify that the information collected by Maltego is correct.

But not all elements listed by Maltego could be verified yet, so I'll use another scanner to try to make sure there is more content that can be validated in the Maltego results.

So I will use WordPress Security Scanner as follows (some outputs removed):

```
┌─[root@parrot]─[/home/wash]
└──╼ #wpscan --url www.cbp.net.br
[i] The remote host tried to redirect to: https://cbp.net.br/
[?] Do you want follow the redirection ? [Y]es [N]o [A]bort, default: [N]y
[+] URL: https://cbp.net.br/
```

```
[+] Started: Wed Mar 15 19:12:43 2017

[+] Interesting header: SERVER: nginx/1.4.6 (Ubuntu)

[+] Interesting header: X-POWERED-BY: PHP/5.5.9-1ubuntu4.20

[+] WordPress version 4.0.16 (Released on 2017-03-06) identified from meta
generator, rss generator, rdf generator, atom generator

[+] WordPress theme in use: twentyten

[+] Finished: Wed Mar 15 19:13:28 2017

[+] Requests Done: 87
```

Once more, we could see the PHP and WordPress was reported by Maltego. We also could observe the Website objects named www.cbp.net.br and cbp.net.br. This is shown because the host on remote site www.cbp.net.br redirects to the http secure at UTI https://cbp.net.br. And the Twenty Ten is the theme in use by WordPress.

Maltego also has taken an image from CBP's website. Let us check it in figures 7 and 8.

Figure 7: Centro Brasileiro de Perícia's website

Again, we can certify that Maltego was very assertive on its results, bringing correctly the image taken from CBP's main page. Compare figures 7 and 8.

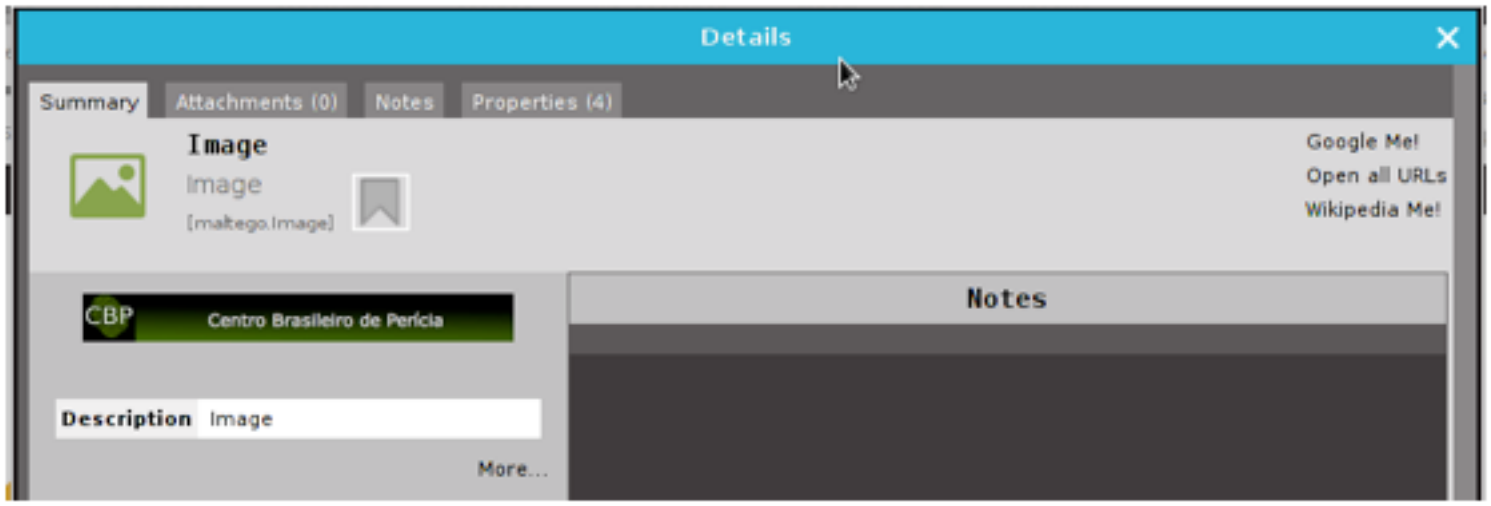


Figure 8: Image taken by Maltego

There are still some items to check: jQuery Form, LightBox, Piwik Web Analytics and Facebook Like Box.

Analyzing CBP's main page source code, I can find the following lines (some outputs removed):

- jQuery Form:
- <script type='text/javascript' src='https://cbp.net.br/wordpress/wp-content/plugins/ contact-form-7/ includes/js/jquery.form.min.js?ver=3.51.0-2014.06.20'></script><script type='text/javascript'>
- LightBox and Facebook Like Box:
- <p> <iframe src="//www.facebook.com/plugins/likebox.php?href=https
- Piwik Web Analytics:

```
<!-- Piwik -->
<script type="text/javascript">
 var _paq = _paq || [];
 (content ommited)
(...)
 s.parentNode.insertBefore(g,s);
 })();
</script>
<!-- End Piwik Code -->
```

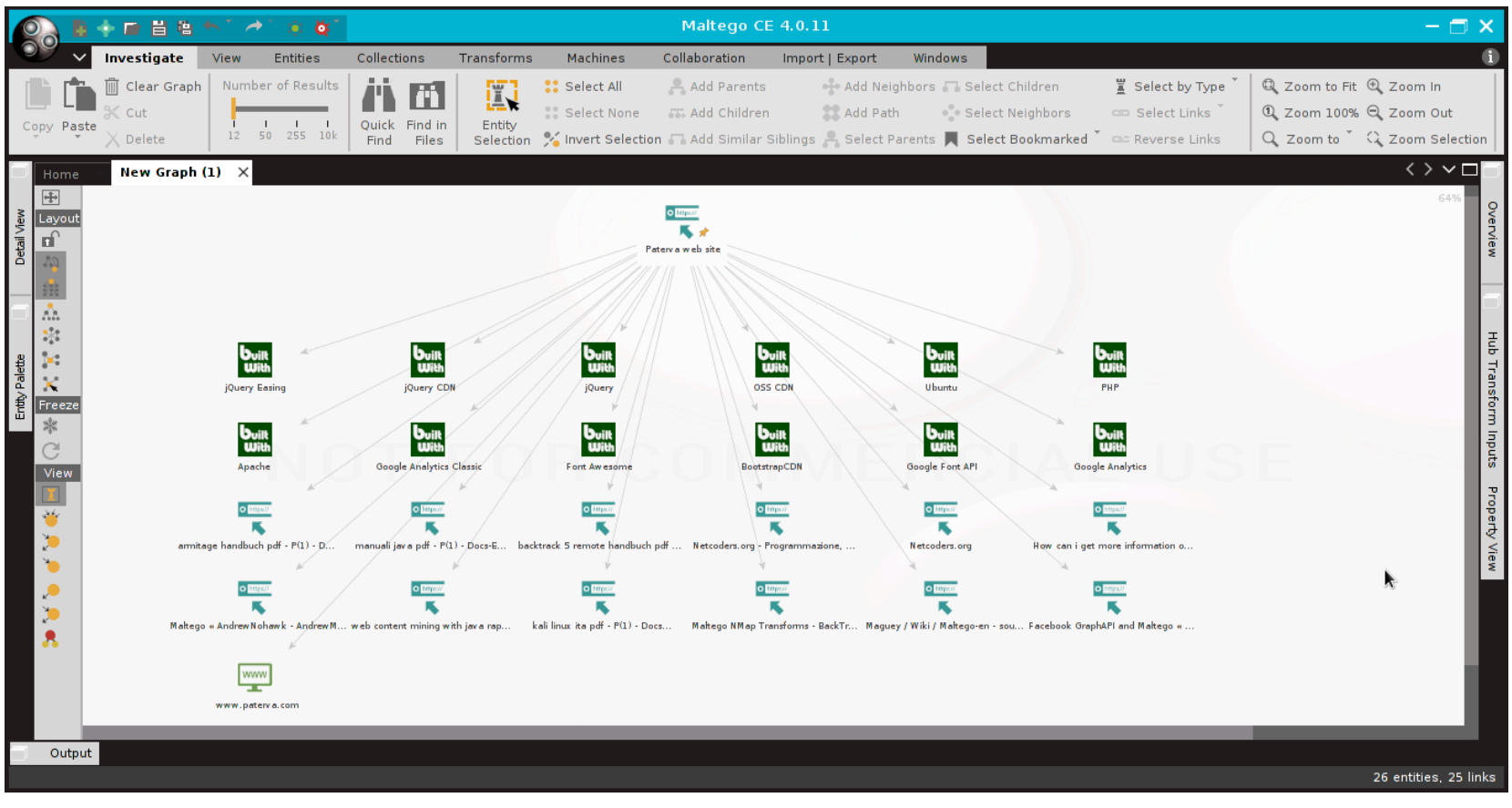
Thus, we could certify that all results presented by Maltego could be verified by a range of others tools. And what does this mean?

It is simple: the Pentest Magazine reader must realize that I had to make use of lots of tools in order to have the information that Maltego brought to me in its first research. Maltego is a very powerful research tool.

Now let us explore more functionalities of Maltego that can help us. Let us suppose, in a fictitious way, the following scenario: Paterva hired me to perform a research work in his web environment, in order to know what public resource may have an incoming link to the Paterva's website. So in the same way we explored CBP's website, we will explore some other possibilities having only Paterva's domain paterva.com as starting point.

Under Paterva environment I would like to look for "incoming links" to the site www.paterva.com represented by the entity "www".

In figure 9, we can see the same first exercise done to CBP's website. As a result, we can visualize the entity website represented by www.paterva.com.



Figue 9: Paterva's data collected

In this exercise, I will follow Paterva's recommendations and get specific information regarding incoming links. In order to find out the incoming links to site www.paterva.com, I have to right-click in website entity and do two stages of action:

1. Click in the option “Links in and out of site” to expand this menu option (do not click the rightmost arrow, it will perform all Transforms) shown in figure 10;

2. Click the rightmost arrow in the option “Links in and out of site” as shown in figure 11.

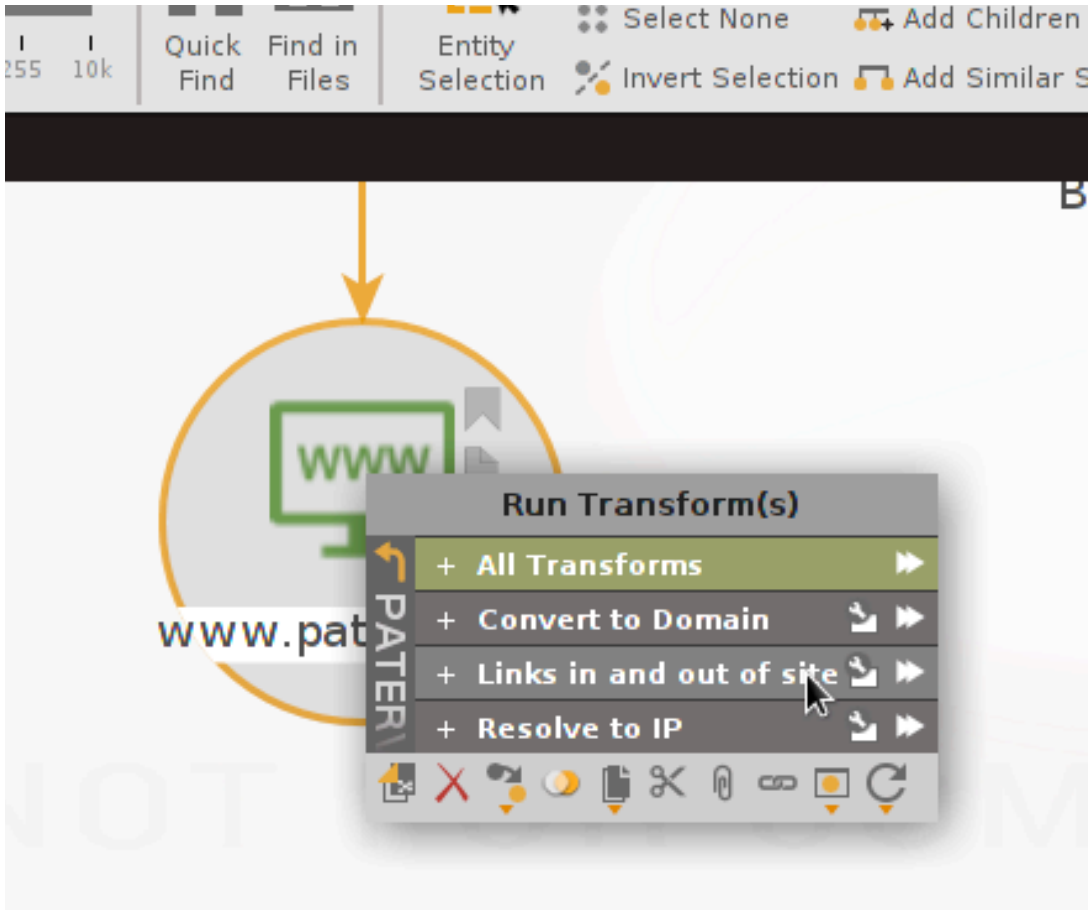


Figure 10: Expanding menu options

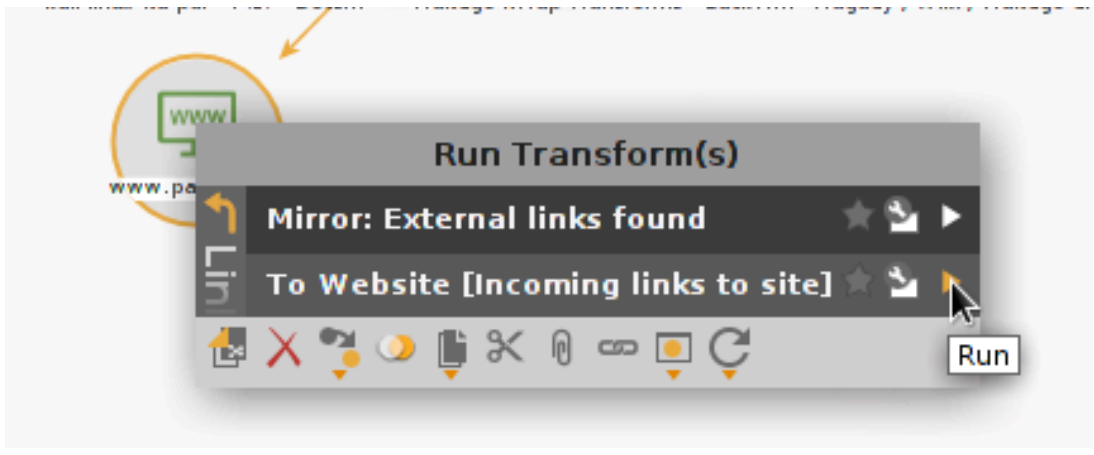


Figure 11: Running a specific Transform

In this action, the transform queries the search engines to determine what sites link to the supplied website. Reading the Paterva documentation, we see this is useful in combination with To websites using mirror, which will give the analyst an idea of what goes into a site (e.g. links to the site) and what comes out of a site (e.g. links from the site).

As a result, I can see a new website entity revealing a site from where the link is referred to. This link in question could be both a simple reference as well as something potentially malicious. Therefore, with

the exception that the Paterva company is aware of this, it is important to mention that we must have mutual respect of our actions in the Internet environment.

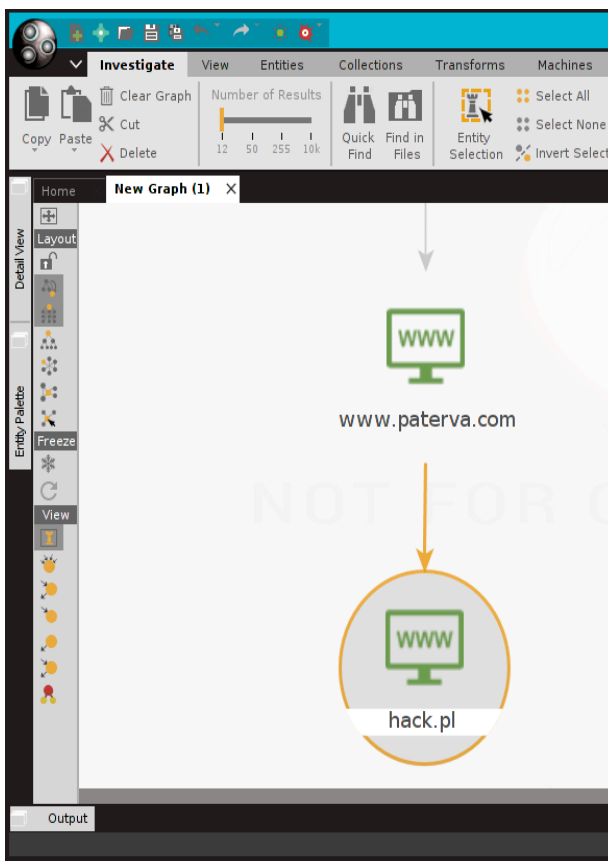


Figure 12: To Website [Incoming links to site] revealing hack.pl

The site hack.pl seems to be specialized in hacking subjects.

Based in a incoming link to www.paterva.com, we found the site hack.pl and I had my attention turned to this site. This aroused interest because I expected this site to be more cautious with its own environment by the subject they treat.

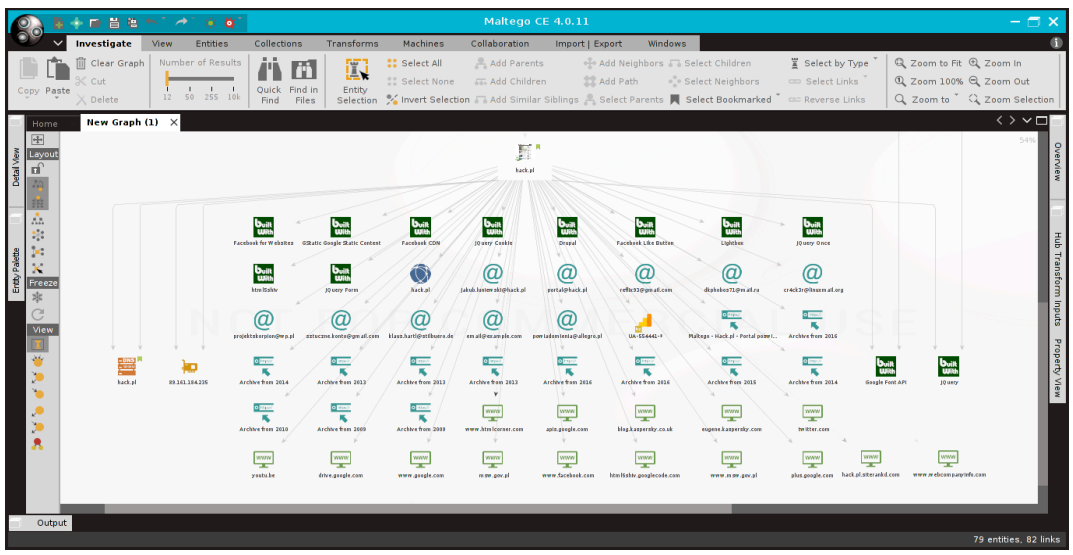


Figure 13: Data collected about hack.pl website

Based on the information Maltego brought to me, it was possible to identify in hack.pl website:

1. The X-XSS-Protection header is not defined;

2. `/user/password/` is in non-forbidden status;

3. ASP config file is accessible;

4. `/sitemap.xml` gives a listing of the site content;

5. `/etc/passwd` file is available via the web site and allows directory traversal;

6. Cookies were created without the httponly flag;

7. The worst: phpMyAdmin is using the default UserId and Password.

What does it mean? It means that Maltego is not only a sophisticated research tool, but it is also an excellent tool that can be used for reconnaissance.

Maltego research inside Deepweb:

In the issue 04/2017 of Pentest Magazine, we addressed a real case of ransomware from the forensic analysis point of view. In this exercise, I will use Maltego to collect more information about the criminal's web resources.

So I create a resource based on website entity as shown in figure 13.

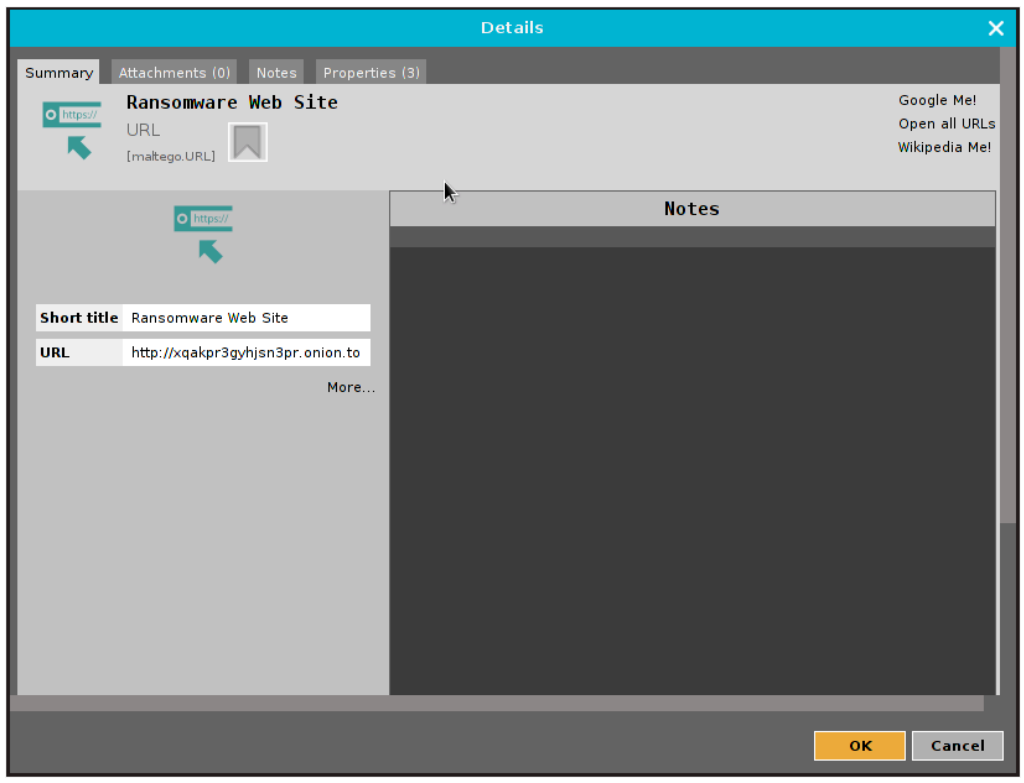


Figure 14: Researching deep web based site

Following the same steps given in the examples with the web sites CBP and Paterva, we have as a result the resources presented in figure 14. The Pentest reader can verify the same IPV4 addresses in the Pentest Magazine issued in 04/2017 about ransomware.

We will now focus our efforts on the interface feature that is identified by the IPV6 address shown in Figure 15.

Why our focus on IPv6? Some research tools do not work with IPv6 by default, thus the Engineer uses the outputs for IPv4 instead. But there are some interesting differences between the IPV4 and IPV6 addresses. Let us remember some of them before moving forward on our approach, limiting our points to what is important for the purpose of this analysis.

1. IPv4 addresses are 32 bit length, IPv6 addresses are 128 bit length;

2. IPv4 addresses are binary numbers represented in decimals, IPv6 addresses are binary numbers represented in hexadecimals.

3. IPv4 fragmentation is done by sender and forwarding routers, IPv6 fragmentation is done only by sender.

4. IPv4 has no packet flow identification, IPv6 packet flow identification is available within the IPv6 header using the Flow Label field (See this specification in the URI https://tools.ietf.org/html/rfc6437).

5. Address Resolution Protocol (ARP) is available to map IPv4 addresses to MAC addresses, in IPv6 Address Resolution Protocol (ARP) is replaced with a function known as Neighbor Discovery Protocol (NDP).

6. Internet Group Management Protocol (IGMP) is used to manage multicast group membership in IPv4, in IPv6 the IGMP protocol is replaced with Multicast Listener Discovery (MLD) messages.

7. Broadcast messages are available in IPv4, in IPv6 broadcast messages are not available, instead a link-local scope "All nodes" multicast IPv6 address (FF02::1) is used for broadcast similar functionality.

Technically, these differences bring extra possibilities that we would not consider while working only with the IPV4 interfaces. But Maltego is a great tool and also provides support for IPv6, so let us explore them.

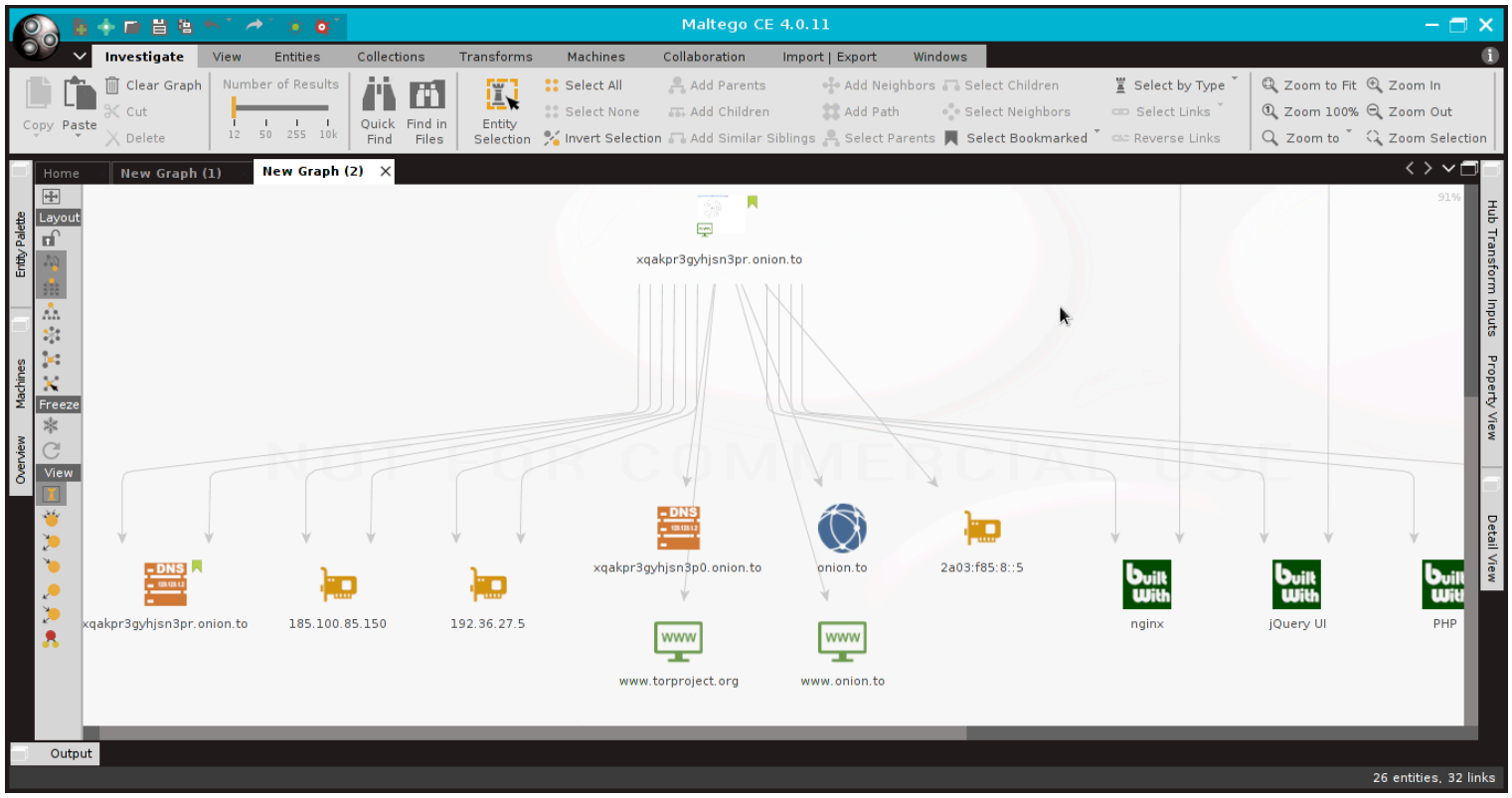


Figure 15: Researching criminal's web site inside Deepweb

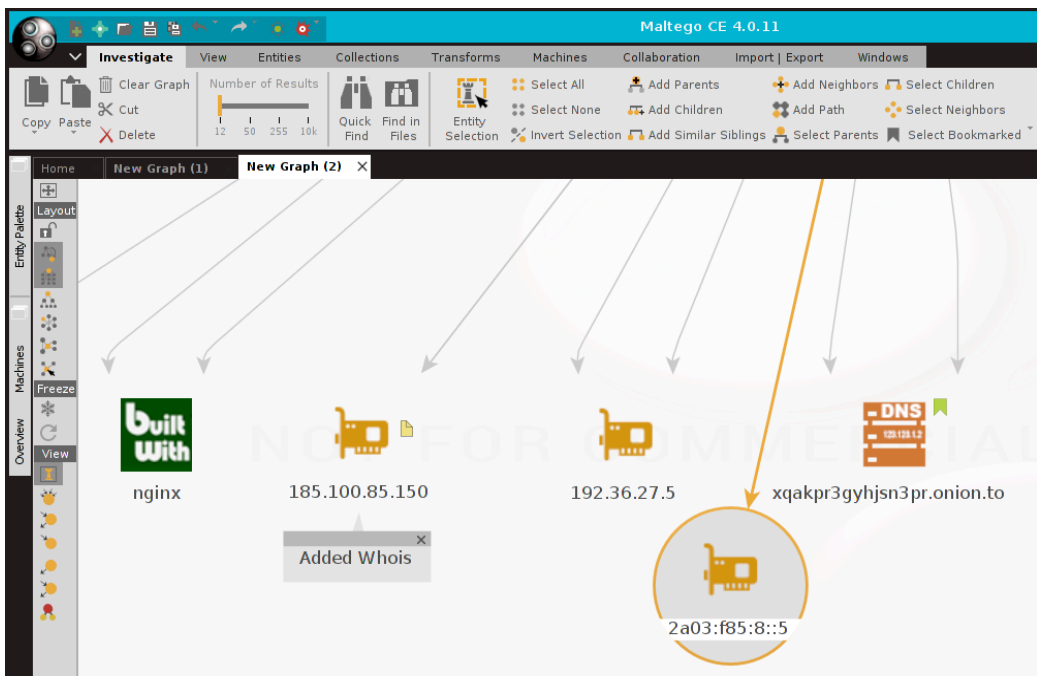


Figure 16: Using Maltego to inspect IPv6 interface

From the IPv6 interface Maltego Transforms brings as a results the resources shown in figure 16.

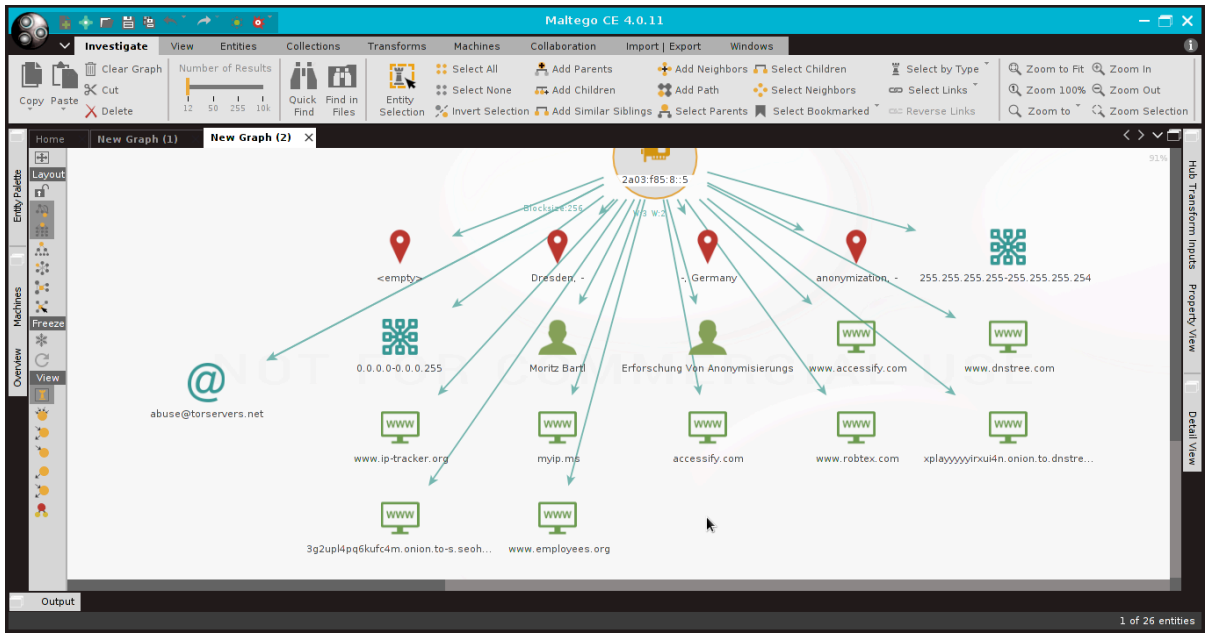


Figure 17: Transforms generated from interface IPV6 address 2a03:f85:8::5

The whois against all addresses brings the fake locations provided by TOR tunnels, being informed as Iceland and Germany.

It is important to mention at this point there are multiple approaches with the Maltego results. I have only chosen one of them. So Maltego brought an additional interesting from-to resource named myip.ms. Let us explore it.

Exploring the myip.ms I can verify in more detailed information regarding the real location of the IPv6 address 2a03:f85:8::5.

The service brings the information shown in figure 17 which differs from the results taken by traditional WhoIs.

The information needed to be delivered to a law firm specializing in Digital Law is listed in this figure 17.

```
IP Location : Austria

IP Owner : Germany (TOR tunnel) – listed in WhoIs
```

Now we know (thanks, Maltego) the real location of the criminal's web site is in Austria.

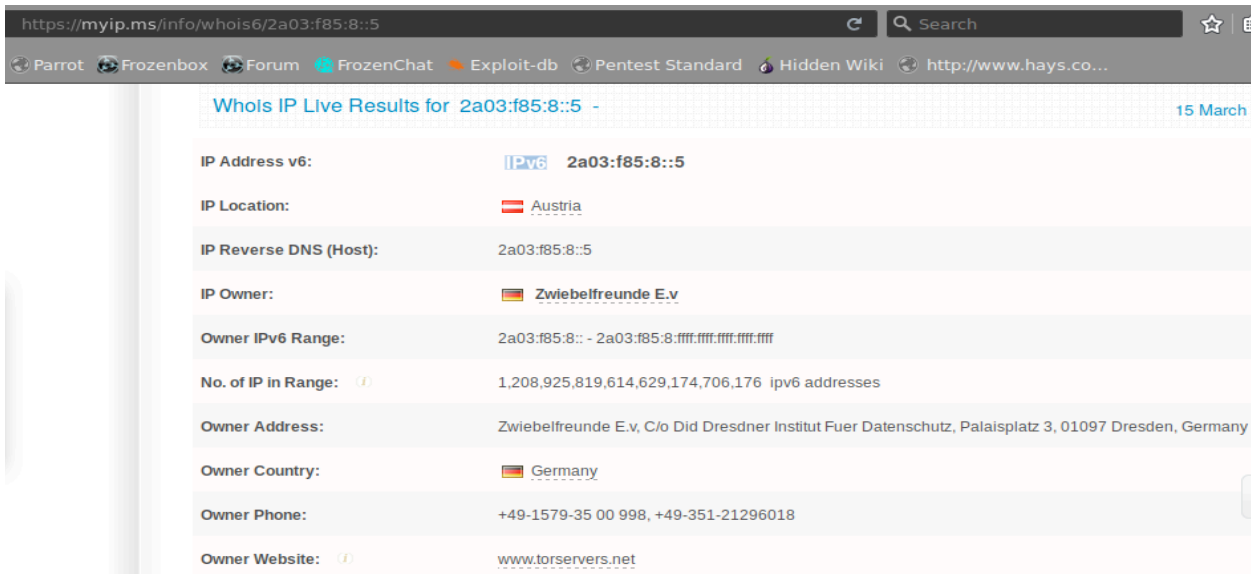


Figure 18: Real IP location revealed

Following our exercise we can see the name "Moritz Bartl" in the group of Transforms generated from the IPv6 interface, shown in figure 18. But who is this guy and why his name emerged in the results?

Figure 19: Finding people with Maltego

Exploring the Entity object under the Maltego environment, we can see lots of other relationships shown in figure 20. And using Maltego we can get more, and more, and more information of the entities and its relationships.

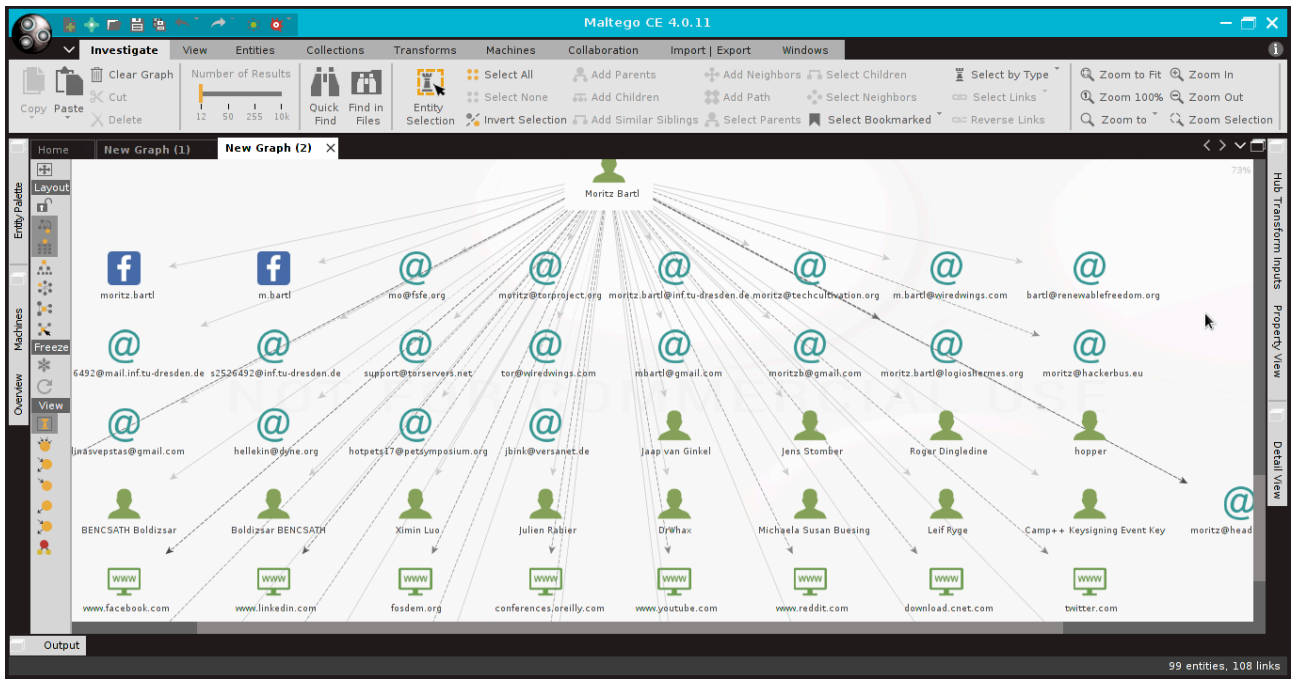


Figure 20: Taking more details about people with Maltego

This person is the point of contact for the range of IP addresses the address 2a03:f85:8::5 belongs to. See the whois results below.

```
┌─[wash@parrot]─[~]

└──╼ $whois 2a03:f85:8::5 (some outputs removed)

% Abuse contact for '2a03:f85:8::/48' is 'abuse@torservers.net'

inet6num:    2a03:f85:8::/48

netname:     ZWIEBELFREUNDE-v6

descr:      Zwiebelfreunde e.V.

person:      Moritz Bartl

address:     **** Dresden

address:     Germany

phone:      (*** REMOVED ****)

fax-no:      (*** REMOVED ****)

abuse-mailbox: abuse@torservers.net

remarks:     ---------------------------------

remarks:     This network is used for research

remarks:     in anonymization services and

remarks:     provides Tor exit nodes to end
```

```
remarks:    users.
remarks:    ---------------------------------
remarks:    Dieser Netzblock wird zur
remarks:    Erforschung von Anonymisierungs-
remarks:    techniken genutzt und stellt
remarks:    Endnutzern Tor zur Verfuegung.
remarks:    ---------------------------------
remarks:    http://www.torservers.net/abuse.html
remarks:    ---------------------------------
% Information related to '2a03:f85:8::/48AS60729'
route6:     2a03:f85:8::/48
origin:     AS60729
mnt-by:     ZWIEBELFREUNDE
```

Let us double check this information using another Maltego Entity named AS to verify if its outputs are quite the same.

Just for concept, AS stands for Autonomous System, which is a group of IP networks operated by one or more network operator(s) that has a single and a clearly defined external routing policy. Exterior routing protocols are used to exchange routing information between Autonomous Systems. The complete Autonomous System specification can be consulted by RFC1930 in the URI https://www.ietf.org/rfc/rfc1930.txt.

As we can see in figure 21, the person who is the point of contact for the AS60729 is the same. Actually, I did this last Transform exercise just to make use of another Maltego resource.

If you have a look at figure 21, you can see the IPv4 address 192.36.27.5 shown in Figure 15 which is under this AS60729 management.

Also notice that I toggle the mode for showing the Maltego's interface in figure 20, that is different from the other screenshots I have taken, since this tool is very flexible to work with.

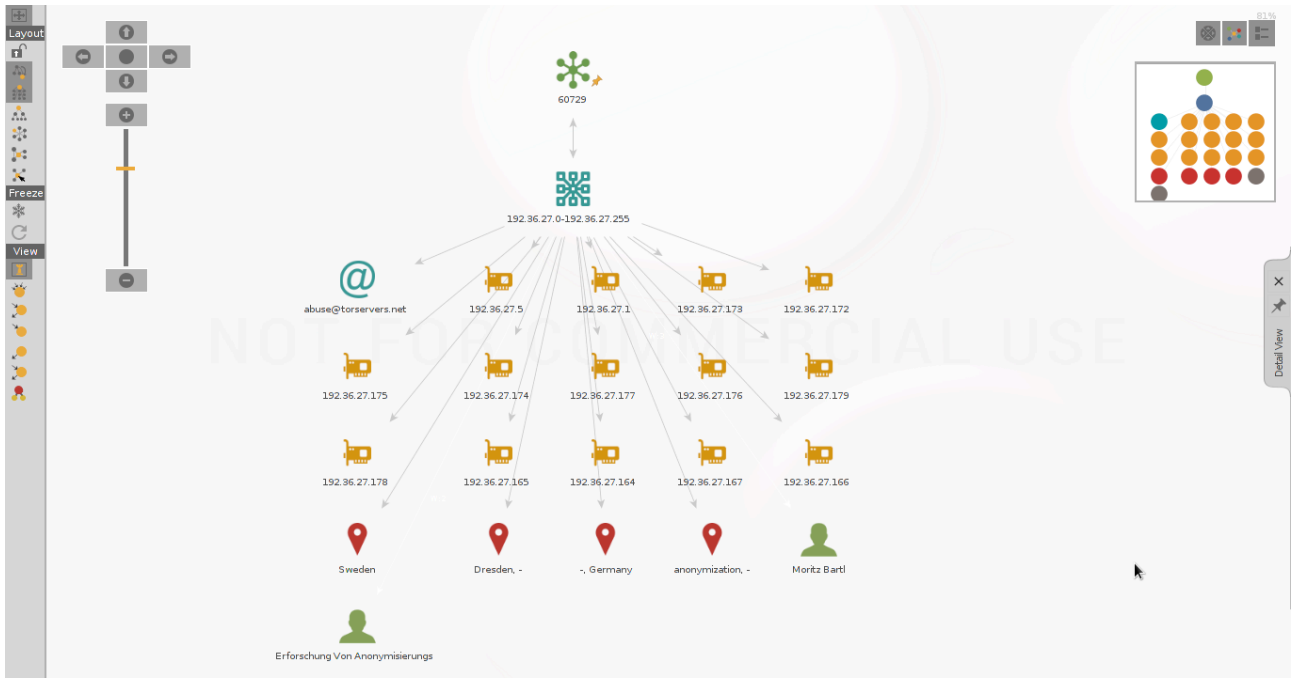


Figure 21: Outputs from AS60729

From now on, I can prepare my report to hand it to the law firm that I would follow with the necessary measures for this case.

Summary

In this article, we could see how powerful Maltego is, using a few simple examples. It is important to mention that the exercises performed in this article are the simplest ones. Imagine what can be done if developing sophisticated research methods to run on this powerful tool.

In my professional activities, I recommend the use of the Commercial Edition version of Maltego (Maltego XL or Maltego Classic) to my clients, medium and large companies, depending on their needs. Why let Maltego show itself important to my professional activity?

The same way hackers can compromise systems for their criminal actions thinking they can be hidden under deep web, we can find them, in an intelligent way, with very powerful research tools such as Maltego.

Hacker criminals are becoming increasingly sophisticated in their methods of compromising systems, so tools like Maltego are of extreme importance to assist the justice in hunting down these kind of criminals.

References:

https://docs.paterva.com/en/user-guide/getting-started/. Access in March 18, 2017.

Author: Washington Almeida

Washington is an Electronic Engineer specialized in Digital Forensics and Cyber Security with more than 25 years of experience in the Information Technology and Engineering areas, working for large companies in sectors such as Engineering, Information Technology, Consulting, Chemical and Mining. Professional certified by players such as Cisco and Microsoft, acts as Digital Forensics with in-depth knowledge of computer hardware, network technologies, telephony, programming, data communication protocols and a vast knowledge of information security with a set of skills known by ethical hackers, where this knowledge base is fundamental to assist the justice.

Wash Web page: www.washingtonalmeida.com.br

Washington Almeida e-mail: wualmeida@washingtonalmeida.com.br