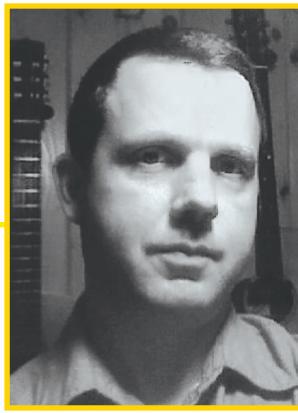
Connect

Maltego: Transform & Correlate



By Russ McRee – ISSA member, Puget Sound (Seattle), USA Chapter

Prerequisites

Windows, Linux, or Mac with Java runtime
Python and Nmap for local Nmap transforms

Similar Projects

I2[1]

toolsmith is officially three years old. Last month's column on Watcher was the 36th toolsmith, and I believe we've established "a good thing." As we enter the fourth year it struck me as important to discuss a tool that brings together so many of the things *toolsmith* stands for: usability, successful results that help information security practitioners do their jobs well, excellent features, and a strength of commitment from the development team. As I contemplated topics I was reminded that so often I'd heard of Maltego, especially in security visualization circles, but passed it by as a topic. When, over the past couple of months, I observed my primary incident handler, Bryan Casper, use Maltego to conduct reconnaissance and gather intel on both attackers and victims, I told myself "enough already, time to give Maltego its due." Thus, we start year four of *toolsmith* with a bang.

Paterva's Maltego is an open source intelligence and forensics application that offers extraordinary data mining and intelligence gathering capabilities. Results are well represented in a variety of easy to understand views. In concert with its graphing libraries, Maltego identifies key relationships between data sets and identifies previously unknown relationships between them.[2]

In a conversation with Andrew MacPherson, project lead, I learned that Paterva is currently working on version 3 of Maltego, including so many new features that the code difference between version 2 and 3 is greater than the entire 2.0 code base. However, Andrew is keeping the roadmap and list of new features confidential until the release date (Q1 2010) draws near. It was disclosed that the new version will allow for better usage with large graphs, as well as further customization of transforms and available tools to support specific end user requirements. The pending version will also allow for better analysis of entity relationships and improved visualization. Paterva offers a user guide,[3] examples[4] including various videos, screenshots, and presentations that highlight many Maltego uses. There is also a support forum[5] which hosts sample transforms and Maltego discussions.

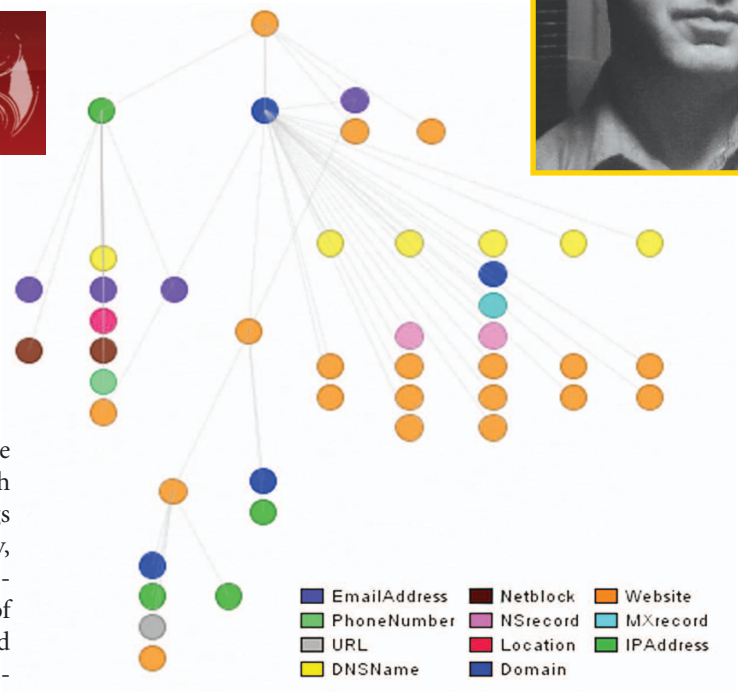


Figure 1 – Maltego color coded mining view

Paterva offers a commercial edition as well as a free community edition (CE) limited to 75 transforms a day with some functionality inhibited.[6] Paterva also offers a Transform Application Server (TAS). Maltego is available for Windows and Linux. I tested both the commercial and community versions on Windows and Linux.

Installing and running Maltego

Maltego installation is point and click; following the steps in the user guide will get you underway almost immediately.

You'll find the user interface (UI) simple:

- Palette offers all the transform types
- Mutiple graphs can be created/opened in tabs, including mining, centrality, and edge weighted views:
  - If all transforms are run, the mining view will color-code email addresses, netblocks, websites, phrases, NS

1 http://www.i2.co.uk.

2 http://www.paterva.com/web4/index.php/maltego.

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

4 http://www.paterva.com/web4/index.php/media.

5 http://www.paterva.com/forum.

6 http://www.paterva.com/web4/index.php/client/community-edition.

records, MX records, URLs, locations, DNS names, domains, IP addresses, phone numbers, and documents discovered (see Figure 1)

- Additional Satellite, Property, and Detail view allow you to drill into:
  - Transform details such as To Document (per our first example)
  - Entity type, weight, and value with URL-to-Document mappings
  - A zoomed satellite view per area of UI focus

A simple spin of your mouse wheel, while focused in a Maltego workspace, will zoom you right in. To create a graph, choose an entity, drag it to an empty workspace, then right-click on the entity to choose a transform.

Keep two very important bits of information in mind as you begin to work with Maltego. First, the Slider is very powerful and lives up to its name. The further to the right you slide it, the more results will be returned by the transform(s); keep it to the left and your transforms will run quickly with fewer results. Thus, the prospect for self-DOS is pretty high. ;-) Wield the slider carefully. Second, the decision to run *All Transforms* is hard refuse, but it too will demand serious system resources.

As part of UI features, you can opt to enable the memory view (View → Toolbars → Memory) which will show you how quickly you can bury your system if you're not careful. The lower right corner of the UI will show you a transform progress bar. If you go for All Transforms with *Results* cranked up, plan to wait awhile, but trust me, sometimes it's worth it. Other times, the results are too convoluted to be of use; you'll find your happy place, I'm sure of it.

Maltego local transforms - Nmap

For an appropriate introductory graph, consider the inherently useful concept of local transforms, specific to Nmap for this scenario. Rather than call home to a Transform Application Server (TAS) Maltego can make use of local resources such as Nmap. You'll need to grab the Nmap transforms,[7] and read the forum post[8] from May 2009.

To install the local transforms you have a bit of work to do first. Given the dependency on Python, I chose to perform these transforms on an Ubuntu server wherein Python is native.

For each of the local transforms mentioned in the Maltego forum post you'll have to do the following:

1. Click *Tools*, then *Manage Transforms*
2. Click *New Local Transforms*
3. Define the Display name as the name of the local transform. Example: nmapVersion
4. Each transform must map to an entity. Do so as follows for each transform as you create it.
   - nmapPorts.py to IP Address
   - nmapPorts-ask.py to IP Address
   - nmapPortsNetblock.py to Netblock
   - nmapVersion.py to IP Address
   - nmapDumpPort.py to Service
   - nmapDumpBanner.py to Service
5. Click *Next*
6. The *Command* field should point to Python (/usr/bin/python on Ubuntu 9.10)
7. The *Parameters* field should refer only to the transform name. Example: nmapVersion.py
8. *Work Directory* should be the complete path to the directory where you keep the Nmap local transform Python scripts
9. *Finish*, then *Save*

Andrew recommended this concept as an excellent introduction and suggested the following.

1. With a netblock in mind, drag and populate a Netblock entity to the workspace, and run the *nmapPortsNetblock* transform to produce all the IP addresses with open ports.
2. Then run the *nmapVersion* transform against all the resulting IP addresses from step 1, which will produce all running services.
3. The *nmapDumpPort* and *nmapDumpBanner* transforms can then be ran against the service entities discovered in step 2.

I chose an *Edge Weighted View* to produce Figure 2, which clearly weighs the most heavily offered service and shows all the IPs running said service.

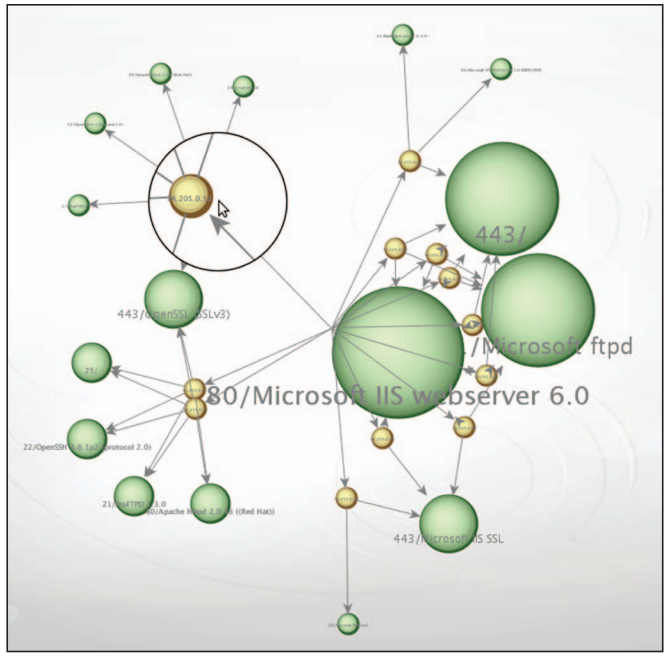


Figure 2 – Maltego Nmap local transforms

7 http://www.paterva.com/forum//index.php?action=dlattach;topic=134.0;attach=52.

8 http://www.paterva.com/forum//index.php/topic,134.0.html.

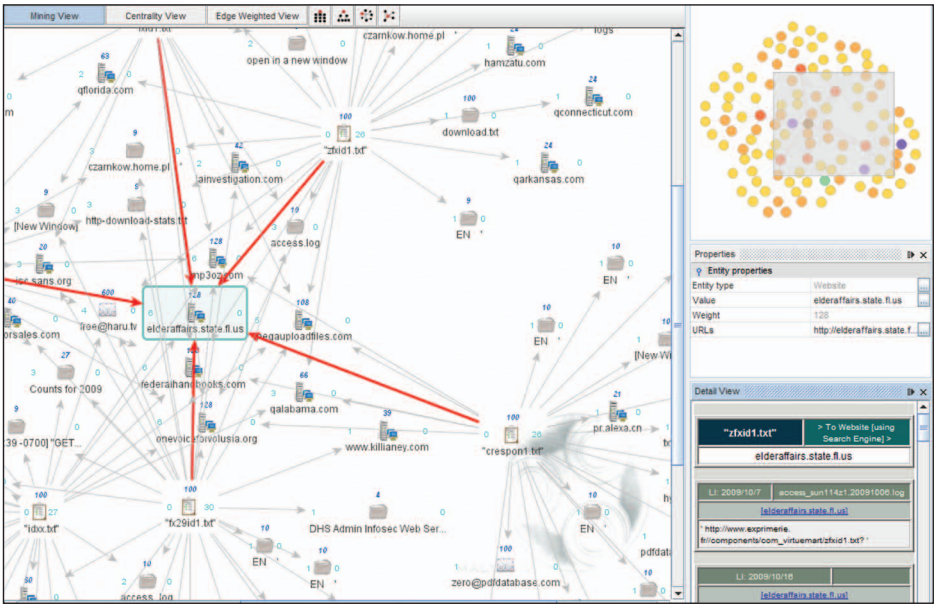


Figure 3 – Maltego mining view transformed RFI scripts

You can see how, when scanning a netblock through multiple iterations of Maltego transforms, "various ports/banners will start linking,"[9] helping you identify vulnerable services per IP during patch cycles and weigh them accordingly.

Maltego transforms remote file includes (RFI) attacks

Maltego shines when it comes to correlating badness conducted by Intarweb evildoers, including pattern matching remote file include (RFI) miscreants. I monitor my weblogs for RFI attacks, using a regex-driven Perl script to grep for specific attacker strings and URLs. A recent log review produced an ideal opportunity for Maltego to show off. RFI attack URL strings often end with a common script name with a .txt or .gif extension. I grabbed five such file names as most often seen in my logs from October:

```
"zfxid1.txt" "id1.txt" "fx29id1.txt"
"idxx.txt" "crespon1.txt" "fxid1.txt"
```

Maltego tightens transform results when enclosed in quotes for the very same reason a search engine does (it leverages search engines). I simply copied the above list to a Maltego work space with the phrase transform enabled, kept the slider far left (speed/accuracy), selected all six entities, and chose All Transforms. Figure 3 exhibits the immediately evident commonalities specific to all the victim sites that have suffered from successful RFI attacks, including the script names above. The center of Figure 3's focus is a predominant and common hub because the webserver exposes its weblogs, which in turn reveal all the same attacks I'm seeing in my weblogs.

This is most often the case for connections made between transform results in this case, but can we find an actual attacker rather than just the trails left in publicly available weblogs? I do believe we can! One of the transform matches from `"fxid1.txt"` was a website reference for `dnsbl.abuse.ch`. With that entity selected, I clicked on the *URLS* button in *Entity* properties in the *Properties* window. Figure 4 is the result.

One of the URLS revealed[10] showed results for a U.S. IP address, showing

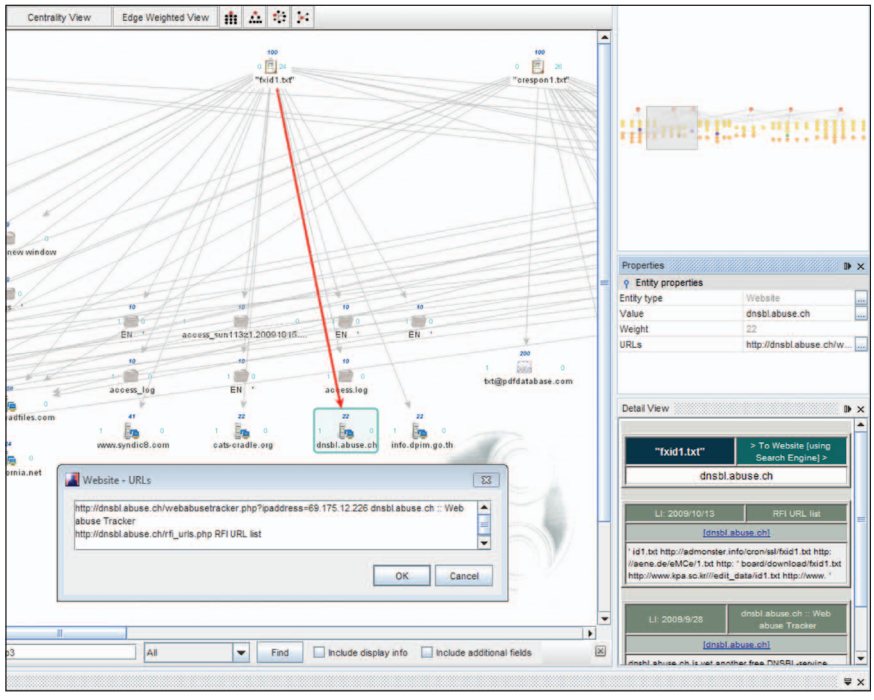


Figure 4 – Maltego website URL findings

that it had been flagged seven times for RFI attacks. "This IP address has been identified as hijacked host/automated scanning drone due to the fact, that the host at this IP address has tried to injected a malicious script (RFI attack): http://www.ciasoftwares.com/fxid1.txt [show script]." Clicking the show script link then revealed[11] that the script has a hash of `a05dfd7cca7771a7565a154d65f05ea2` with all the attack details including script locations (RFI URLs), related IPs, and RFI script details as seen in Figure 5.

9 Ibid.

10 http://dnsbl.abuse.ch/webabusetracker.php?ipaddress=69.175.12.226.

11 http://dnsbl.abuse.ch/webabusetracker.php?script=a05dfd7cca7771a7565a154d65f05ea2.

Figure 5 – dnsbl.abuse.ch results as discovered by Maltego

RFI script

Firstseen: 2009-05-24 22:10:55
Lastseen: 2009-11-10 18:40:28
Script size: 75 Bytes

```
<?php /* Fx29ID */ echo("FeeL"."CoMz"); die("FeeL"."CoMz"); /* Fx29ID */ ?>
```

As you can see, pattern matching and correlation is made exponentially easier thanks to Maltego.

Maltego transforms rogue AV

Above mentioned incident handler Bryan recently discussed the idea of researching rogue antivirus attackers with Maltego. I thought this was a grand idea and will offer results here.

We recently received a report about *www.malwareprofessional.com* as an abusive advertiser, in addition to the fact that Internet Explorer was flagging it as malicious. I dropped www.malwareprofessional.com in a website transform, chose All Transforms but received only a few results. One transform produced, of course, was the parent domain, malwareprofessional.com, so I selected that entity and chose All Transforms again. This time I was treated many more useful results, including an excellent *Tech Herald* story[12] from September, providing detail about a similar scam emanating from the netblock attributed to this domain in Maltego. Drilling into the email address *support@malwareprofessional.com* immediately revealed other scareware domains such as *anti-malware-2010.com*. Most interesting of all was the click revenue/promotion scheme in use by this rogue AV campaign, specifically noted via *clickbank.net*. The complete URL will click through right to the malicious binary, so I won't show it here; but Figure 6 will show you how the revenue/promotion campaign appears in an Edge Weighted View with the *Zoom Lense* (available on the toolbar or in the View menu).

12 http://www.thetechherald.com/article.php/200939/4499/TTH-Labs-Not-all-Rogue-anti-Virus-software-is-created-equal?page=1.

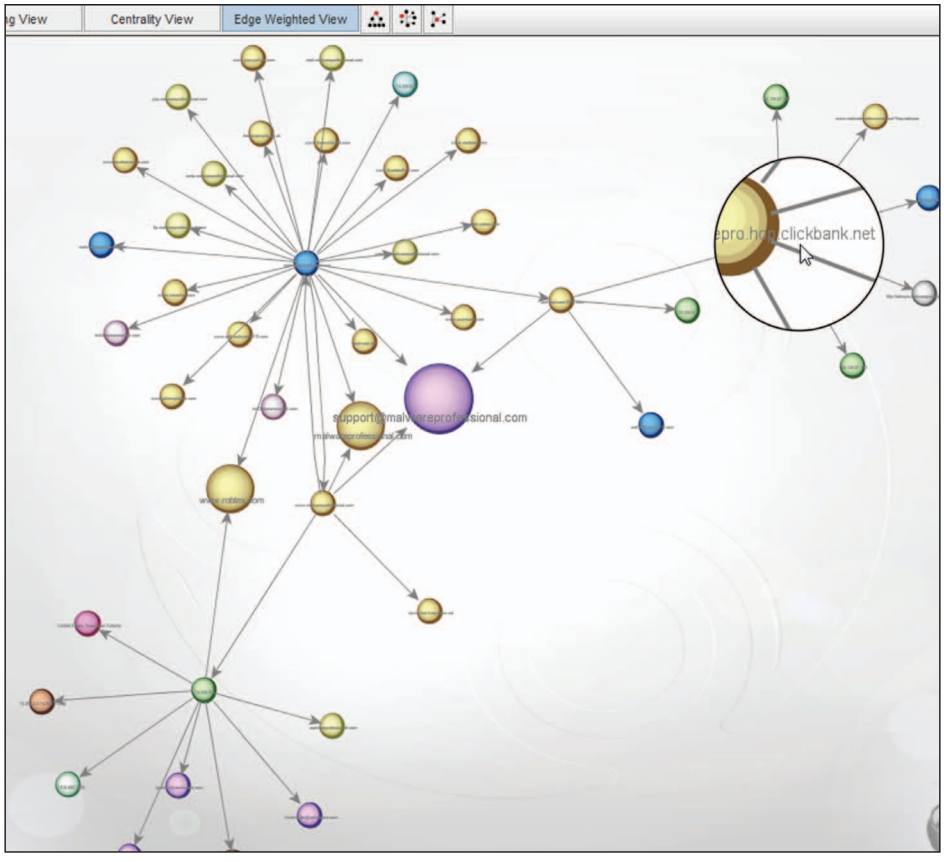


Figure 6 – Maltego analysis of a rogue AV campaign

Feel the power?

In conclusion

I simply love this tool. Can't say enough. The transform graphs discussed here are posted to my website[13] for you to play with. Download Maltego CE for your preferred operating system and make swift use of this excellent offering. Look forward to the release of version 3 as well.

I can say with certainty that you can't help but conduct successful research, analysis, and reconnaissance efforts with Maltego; I look forward to hearing about your findings. Feel free to share your graphs via email or as comments to my related blog post.

Cheers…until next month.

Acknowledgments

—Andrew MacPherson, project lead

—Bryan Casper, incident handler

About the Author

Russ McRee, GCIH, GCFA, GPEN, CISSP, is team leader and senior security analyst for Microsoft's Online Services Security Incident Management team. As an advocate of a holistic approach to information security, Russ' website is holisticinfosec.org. Contact him at russ@holisticinfosec.org.

13 http://holisticinfosec.org/toolsmith/files/maltego.