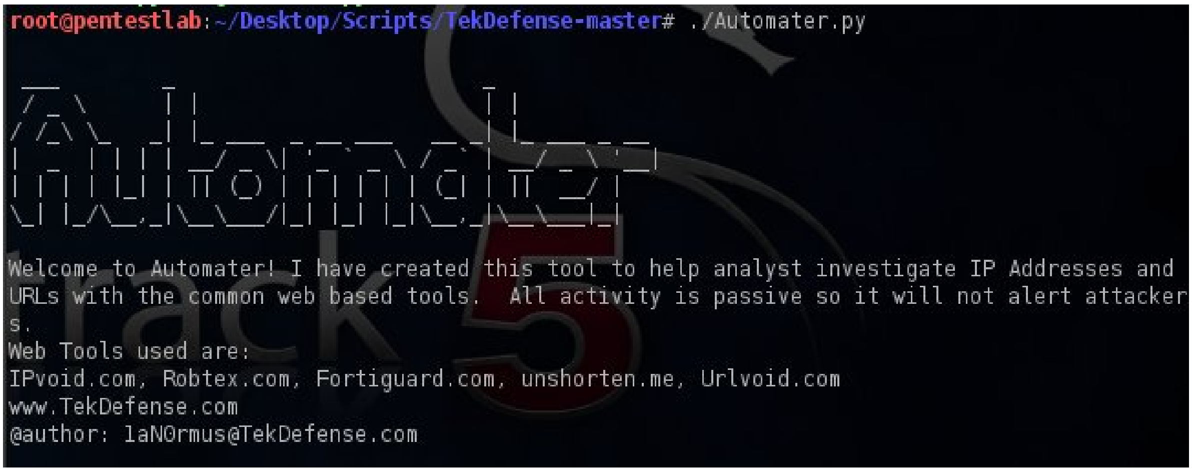
Automater

pentestlab.blog/category/tools/page/5

December 10, 2012



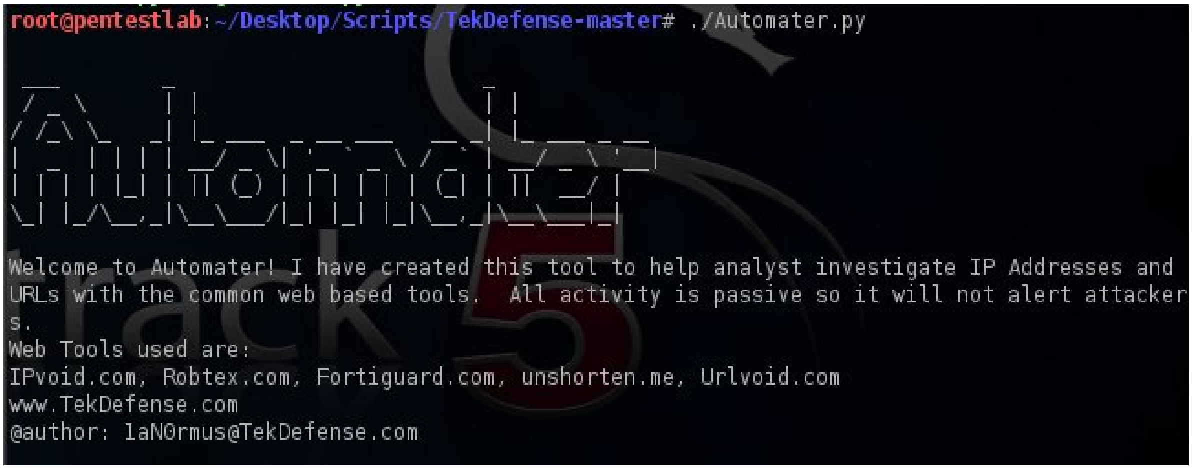
```
root@pentestlab:~/Desktop/Scripts/TekDefense-master# ./Automater.py

  ___        _                        _
 / _ \      | |                      | |
/ /_\ \_   _| |_ ___  _ __ ___   __ _| |_ ___ _ __
|  _  | | | | __/ _ \| '_ ` _ \ / _` | __/ _ \ '__|
| | | | |_| | || (_) | | | | | | (_| | ||  __/ |
\_| |_/\__,_|\__\___/|_| |_| |_|\__,_|\__\___|_|

Welcome to Automater! I have created this tool to help analyst investigate IP Addresses and
URLs with the common web based tools.  All activity is passive so it will not alert attacker
s.
Web Tools used are:
IPvoid.com, Robtex.com, Fortiguard.com, unshorten.me, Urlvoid.com
www.TekDefense.com
@author: 1aN0rmus@TekDefense.com
```

Automater is a tool that can analyze and investigate IP addresses and URL’s for malicious content.Specifically this tool is using some web-based tools in order to obtain information about the URL and it passes the output to the user.The tool is written in python and there are four options for the user so far:

- Query one IP address or URL for info
- Import a file that contains a list of IP addresses or URL’s
- Export the results to a file
- Expansion of a shortened URL

In order to run the following tool properly on backtrack we need to download and install the following two libraries:httplib2 and argparse.

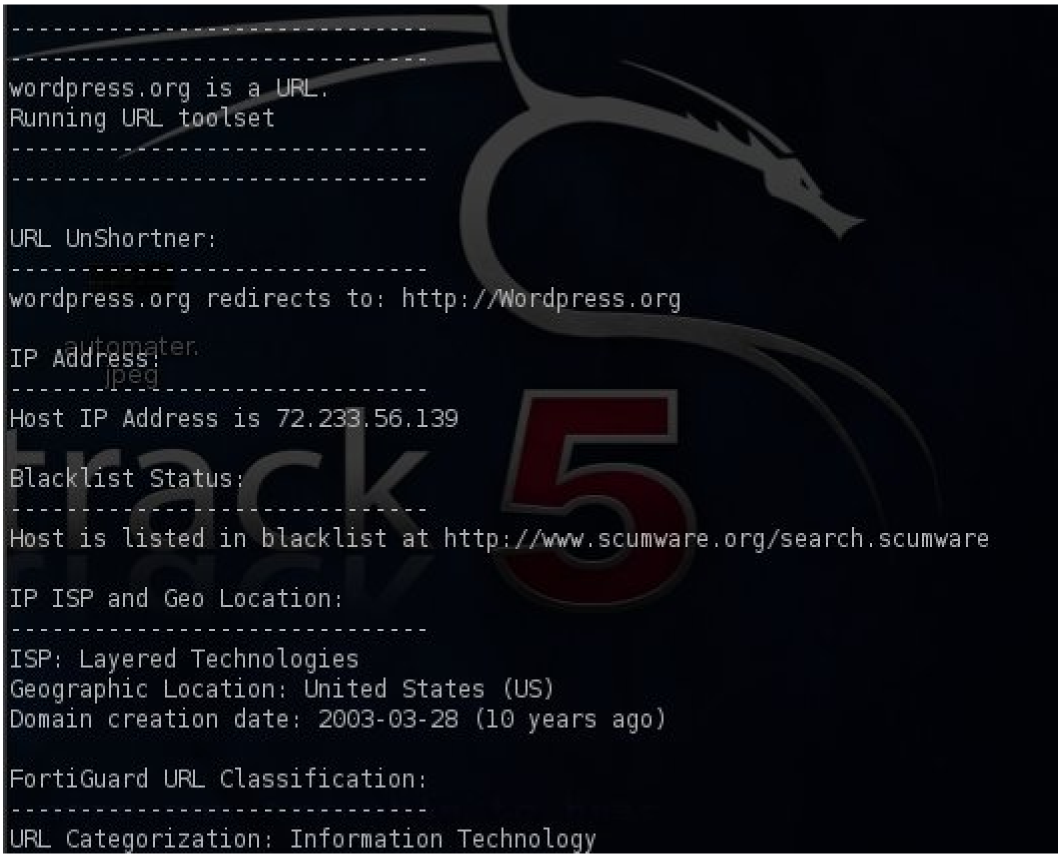
In the image below we can see a small description of the tool:



```
root@pentestlab:~/Desktop/Scripts/TekDefense-master# ./Automater.py

  ___        _                        _
 / _ \      | |                      | |
/ /_\ \_   _| |_ ___  _ __ ___   __ _| |_ ___ _ __
|  _  | | | | __/ _ \| '_ ` _ \ / _` | __/ _ \ '__|
| | | | |_| | || (_) | | | | | | (_| | ||  __/ |
\_| |_/\__,_|\__\___/|_| |_| |_|\__,_|\__\___|_|

Welcome to Automater! I have created this tool to help analyst investigate IP Addresses and
URLs with the common web based tools.  All activity is passive so it will not alert attacker
s.
Web Tools used are:
IPvoid.com, Robtex.com, Fortiguard.com, unshorten.me, Urlvoid.com
www.TekDefense.com
@author: 1aN0rmus@TekDefense.com
```

Description of Automater

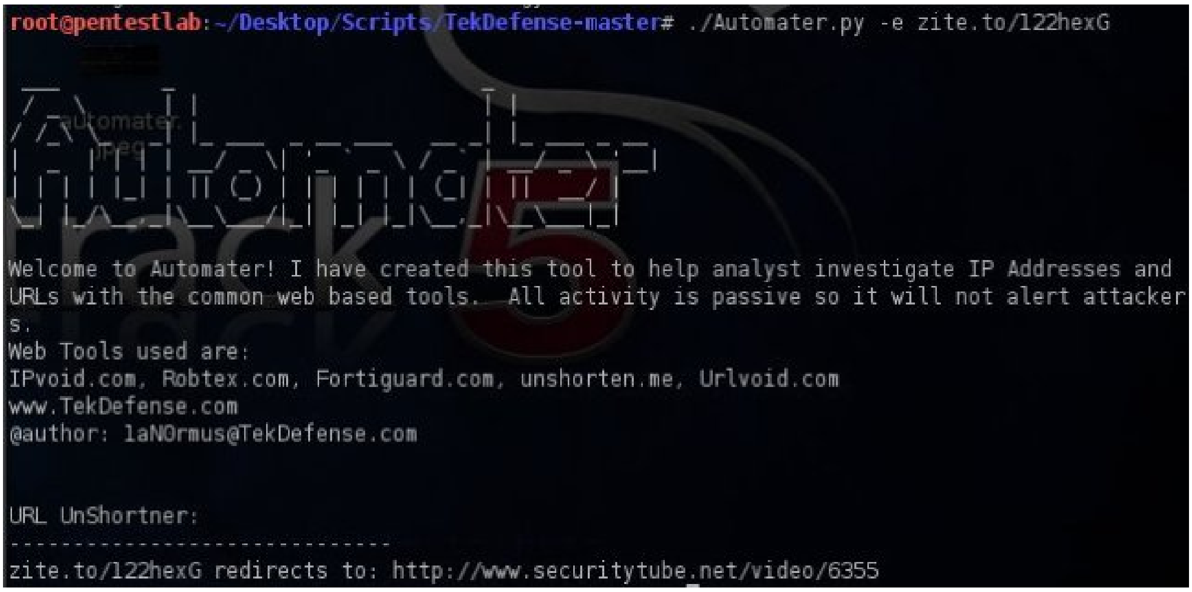
Now lets run the Automater with the command ./Automater.py -t URL against a website.



```
------------------------------
------------------------------
wordpress.org is a URL.
Running URL toolset
------------------------------
------------------------------

URL UnShortner:
------------------------------
wordpress.org redirects to: http://Wordpress.org

IP Address:
------------------------------
Host IP Address is 72.233.56.139

Blacklist Status:
------------------------------
Host is listed in blacklist at http://www.scumware.org/search.scumware

IP ISP and Geo Location:
------------------------------
ISP: Layered Technologies
Geographic Location: United States (US)
Domain creation date: 2003-03-28 (10 years ago)

FortiGuard URL Classification:
------------------------------
URL Categorization: Information Technology
```

Running Automater against a URL

We can also use the URL expansion option in order to expand a short URL with the -e option.



```
root@pentestlab:~/Desktop/Scripts/TekDefense-master# ./Automater.py -e zite.to/122hexG

Welcome to Automater! I have created this tool to help analyst investigate IP Addresses and
URLs with the common web based tools.  All activity is passive so it will not alert attacker
s.
Web Tools used are:
IPvoid.com, Robtex.com, Fortiguard.com, unshorten.me, Urlvoid.com
www.TekDefense.com
@author: 1aN0rmus@TekDefense.com


URL UnShortner:
------------------------------
zite.to/122hexG redirects to: http://www.securitytube.net/video/6355
```

URL Expansion

As we can see the usage of the tool is pretty simple and it can help us to avoid visiting websites with malicious content.According to the author this is the first stable release and more features are coming in the upcoming versions.

Tool Details

Author:1aN0rmus

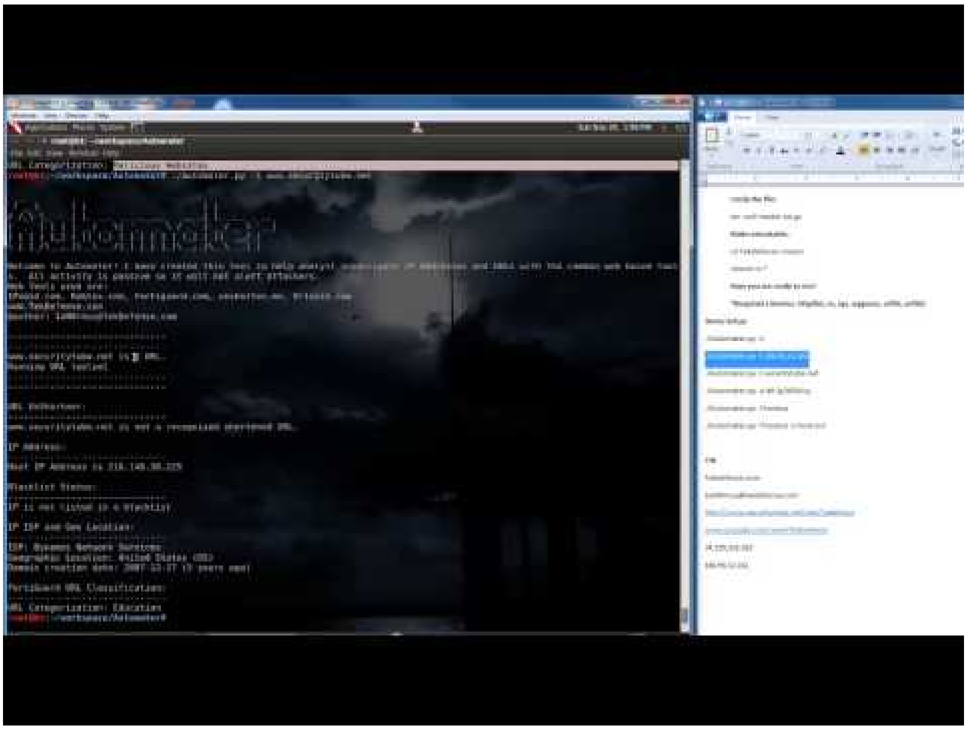
Email:1aN0rmus@tekdefense.com

Twitter Account: http://twitter.com/TekDefense

Download:https://github.com/1aN0rmus/TekDefense/blob/master/Automater.py

Official Tutorial: http://www.tekdefense.com/news/2012/11/25/automater-10-passive-ip-and-url-analysis.html

Video Demonstration



```
URL Categorization: Malicious Websites
[illegible]
Automater
[illegible]
www.securitytube.net is a URL.
Running URL toolset
------------------------------
URL UnShortener:
------------------------------
www.securitytube.net is not a recognized shortened URL.
IP Address:
------------------------------
Host IP Address is 216.146.38.125
Blacklist Status:
------------------------------
IP is not listed in a blacklist
IP ISP and Geo Location:
------------------------------
ISP: Dynamic Network Services
Geographic Location: United States (US)
Domain creation date: 2007-12-27 (5 years ago)
FortiGuard URL Classification:
------------------------------
URL Categorization: Education
```

Watch Video At: https://youtu.be/lbVmRfpvs7c