

Forum:[Hack Forums](#)

Thread: [Malcom - Malware Communications Analyzer](#)

Angelis - December 28, 2018, 10:18 am

Malcom is a Malware Communication Analyzer designed to analyze a system's network communication using graphical representations of network traffic, and cross-reference them with known malware sources.

This comes handy when analyzing how certain malware species try to communicate with the outside world.

Malcom Malware Communication Analyzer Features
Malcom can help you:

- Detect central command and control (C&C) servers
- Understand peer-to-peer networks
- Observe DNS fast-flux infrastructures
- Quickly determine if a network artifact is 'known-bad'

The aim of Malcom is to make malware analysis and intel gathering faster by providing a human-readable version of network traffic originating from a given host or network. Convert network traffic information to actionable intelligence faster.

Installing Malcom Malware Communication Analyzer

Malcom is written in Python. Provided you have the necessary libraries, you should be able to run it on any platform. It's recommended to use Python virtual environments (virtualenv) so as not to mess up your system libraries.

Install git, python and libevent libs, mongodb, redis, and other dependencies:

```
sudo apt-get install build-essential git python-dev libevent-dev mongodb libxml2-dev libxslt-dev  
zlib1g-dev redis-server libffi-dev libssl-dev python-virtualenv
```

1

```
sudo apt-get install build-essential git python-dev libevent-dev mongodb libxml2-dev libxslt-dev  
zlib1g-dev redis-server libffi-dev libssl-dev python-virtualenv
```

Environment for Malware Communication Analyzer

If you're used to doing malware analysis, you probably already have tons of virtual machines running on a host OS. Just install Malcom on a new VM, and route your other VM's connections through Malcom. Use `enable_routing.sh` to activate routing / NATing on the VM Malcom is running on. You'll need to add an extra network card to the guest OS.

As long as it's getting layer-3 network data, Malcom can be deployed anywhere. Although it's not recommended to use it on high-availability networks (it wasn't designed to be fast), you can have it running at the end of your switch's mirror port or on your gateway.

You can download Malcom here:

<https://github.com/tomchop/malcom/archive/v1.3a.zip>

Mr. Robot - *January 10, 2019, 12:13 pm*

Actually a very good thread.