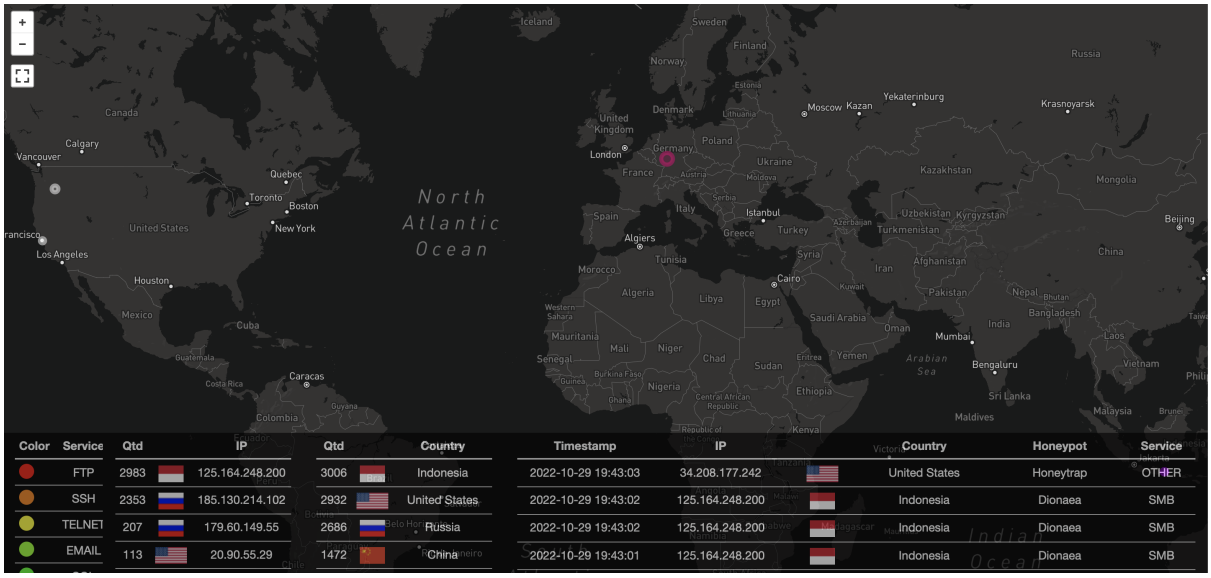
How To: Automatically Upload Dionaea Samples to Dropbox



The Tpot Honeypot provides an easy system to quickly set up a honeypot, analyze in-the-wild attacks and collect a variety of malware samples (although these are usually just versions of WannaCry).

However, I quickly became annoyed trying to transfer my collected samples to a remote database without needing to constantly SSH in and do it manually. That's what this guide solves.

Note: This setup is for Debian distributions .

Requirements:

- Rclone
- Dropbox account

Installing Rclone

While I originally tried to use the Dropbox-Uploader on github, I quickly ran into problems with syncing and it more or less just became a headache. I found Rclone to be a better solution.

Step 1:

```
#Use apt to install Rclone
sudo apt-get install rclone
```

Step 2:

With Rclone now installed, we just need to setup the config. I'm running on a headless server so I have a few extra steps I need to do in order to connect to dropbox.

```
rclone config
```

This will bring up a menu of options, type *n*:

```
n) New remote
d) Delete remote
q) Quit config
e/n/d/q> n
```

Give it whatever name you want, I used dropbox so that's what will be used in the rest of this setup:

```
name> dropbox
```

This will bring up all the different storage providers you can use, currently Dropbox is #9:

```
Storage> 9
```

After this, rclone will ask you for a client_id and a client_secret as well as whether or not you would like to edit the advanced config.

Just press enter for client_id and client_secret, then type "n" for advanced config:

```
OAuth Client Id
Leave blank normally.
Enter a string value. Press Enter for the default ("").
client_id>
OAuth Client Secret.
Leave a blank normally.
Enter a string value. Press Enter for the default ("").
client_secret>
Edit advanced config? (y/n)
y) Yes
n) No (default)
y/n>n
```

Next you will be asked if you want to use auto config. Since I'm on a headless server, I'm going to select no.

```
Use auto config?
 * Say Y if not sure
 * Say N if you are working on a remote or headless machine
y) Yes (default)
n) No
y/n> n
```

Step 3:

For this next part, you need to go onto your host system or whatever OS you have with access to a browser and where you can install Rclone. I did this from my kali box. There's OS dependent instructions for installation here: https://rclone.org/install/

For me, I'm just going to use the same install command as before:

```
sudo apt-get install rclone
```

Now, wait for it to install and once it's all finished run. Make sure that you are logged into your dropbox account before running:

```
rclone authorize "dropbox"
```

This will open up a browser window where dropbox will ask you to verify that you want to connect to rclone. Select allow, now there will be a section in the terminal titled

```
Paste the following into your remote machine --->
{"access_token":"XXXXXX","token_type":"bearer","refresh_token":"XXXXX","expiry":XXXX-XX-XXXXX:XXXXXX"}
<---End paste
```

Copy the text in-between the arrows and paste that back into your Tpot machine.

Step 4:

Now, your new config should be all setup and your dropbox will be connected to your system. Let's run the following command to check:

```
rclone lsd dropbox:
```

Note: Remember, change dropbox to whatever you named your config.

This should return your directories from your dropbox storage. Now, you can begin copying your Dionaea samples into your dropbox:

```
rclone copyto /data/dionaea/binaries dropbox:YourDirectory
```

Here I'm utilzing the rclone command copyto because it will skip those which have already been copied.

If all is well, these files should now be populating your dropbox storage.

Step 5:

While this already makes the process of moving samples a lot easier, I'd rather this be automated so I don't need to bother with it.

To do this, I'm just going to be utilizing a bash script and a cron task that will zip up the binaries, move them to a different folder, and then run rclone to automatically upload them to dropbox every hour. This script will also remove the binaries after they've been uploaded to dropbox.

First I'm just going to make a file named /temp/ in my home directory.

```
mkdir temp
```

Now, we're going to navigate to /etc/cron.hourly and create our bash script:

```
cd /etc/cron.hourly
nano autoupload.sh
```

Once we're in nano write out this bash script edited from sinkmanu on stack overflow (https://stackoverflow.com/questions/65836837/zip-name-and-move-files-to-another-director-using-bash-script):

```
#!/bin/bash

data=$(find /data/dionaea/binaries/)
archive=/home/tsec/temp

if [ -z "$data" ]; then
    echo "No data to archive"
elif [ -n "$data" ]
    then
    echo "Archiving data"
    for i in $data; do
    f=$(i//\//_)
    zip "$date +"%d-%m-$Y")_$f.zip" $i
    mv $(date +"%d-%m-%Y")_$f.zip $archive
    rclone copyto /home/tsec/temp dropbox:Dionaea
    rm -r /data/dionaea/binaries/*
    done
    echo "Archive complete"
```

```
else
    echo "Error"
fi
```

Now just press ctrl+x, saving the bash script in your cron.hourly directly and now you should be set up to automatically upload samples to your dropbox storage.