

Forum:[Hack Forums](#)

Thread: [\[Spreading\] How to infect your community or a company](#)

?pth?n - August 5, 2013, 10:44 am

Welcome

NOTE: This tutorial is for educational purpose only. Thinking about things in theory is fine, but don't use your knowledge to harm others. I am not reliable for any harm that is done with the information I cover in this tutorial.

Table of contents

- I. Introduction
- II. Community spreading
- III. Requirements
- IV. Creating an infected CD
- V. How to spread your CD
- VI. Conclusion
- VII. Spreading without a CD
- VIII. Compromising a big company
- IV. Final words

I. Introduction:

Welcome to my first tutorial on HF. You may wonder what this is about. Let me tell you - it's not just another spreading guide. I came up with this idea today and I thought "why not write a guide about this?!".

This is in fact, a very experimental and new spreading method. If you want to setup a botnet with thousands of slaves, this is not for you. This tutorial is for people that want to get some new ideas and try to spread a different way.

If you are simply searching on a good mass spreading guide, have a look into:

[Ultimate spreading guide](#)
[Omegle Spreading](#)

II. Community spreading:

What do I mean when talking about community spreading?

Most of you know, that you can SE your neighbours or friends into opening a RAT. If you are on their network, you can even redirect them to your JDB. However, I'm not talking about this.

We are exploiting the trust of your community in free giveaways and services. This method requires time and some money to start, and it's definately not for everybody.

In general, we are going to burn a CD with the RAT/Keylogger/Worm/whatever on autorun. Autorun

has been disabled for USB devices since Windows XP SP2, but autorun from CD is still working. I will give you a few ideas on how to get your infected CD "on the market", but the best ideas are coming from your own brain.

When I'm saying "CD", it can be a DVD aswell - common sense

III. Requirements:

You will need the following things:

- A file you want to spread
- Crypter
- Raw CD's and a burner
- Brain

IV. Creating an infected CD:

Step 1:

Set up your malicious file. If you don't know how to setup your RAT for example, please search for a tutorial and make sure it's working.

Step 2:

Crypt your server so the AV programs won't detect it. Make sure it is FUD on scantime and runtime. Don't use a free crypter, since they will get detected way faster. If you got some extra money to spare, invest in a private stub.

Step 3:

You need to have some legit file on the CD aswell. It will be obvious which file you can use if you read about the different methods later in this guide.

Step 4:

Burn a new CD with your RAT and the legit file.

It is important to make it run automatically when put in! Check out this guide if you don't know how to do this:

[Autorun CD tutorial](#)

Now you should have a CD with your crypted server and a legit looking file. When someone puts in the CD into his hard drive, he is going to be infected instantly because your RAT is starting automatically.

V. How to spread your CD:

Now we are coming to the interessting part.

There are multiple ways on how to spread your CD, each will result in different slaves. You will be able to get very specific slaves, because the slave you get depends on the way you spread.

These are a few methods you can consider using:

Library spreading:

You could install your server on the PC of your local library. However, this is obvious and you may thought about this already.

A lot of books are coming with a CD. The CD may features a e-book of the print, programmes or additional information.

You can lend any book and copy the files from the CD. Then you burn the CD with the original files and your RAT. If you are worried about the cover of the book: You can clone the original cover if you are willing to spend more time and money on making it more legit.

Put your fake CD back into the book and give it back. The next time someone lends the book and runs the CD, he will get infected.

You can also use this method with DVD's and games!

Grab new games and copy them! Games are high on demand and everyone is looking for them. If you do this method with games that require good hardware, you will get some good slaves if you are into bitcoin mining.

Rental services:

These are even better to spread with, because the most people only lend the games and DVD's for a short period of time. This means you will get more slaves when planting your material.

You better only use this method when you are able to make a good looking cover for the CD. Have in mind that if the rental service is finding out what you are doing, you will get in big trouble.

Using this, aswell as the library method gives you the chance to target very specific personalities. A few examples:

Infect love films = Couples, women, sentimental men

Infect shooter games = Teenagers (mostly boys), good hardware, facebook accounts, possible other game accounts

Infect programming e-book = Coders, programmers Spoiler ([Click to View](#)) Don't be an asshole and infect these people

Infect erotic movies = Perverts in your neighbourhood

Infect tax manager software = People who keep track of their money and probably aren't that poor

I don't support financial fraud in any way. The contrary is the case. Don't steal innocent peoples hard earn money, how would you feel?

This list can be continued, I just wanted to give a small example on what is possible with this method.

Free giveaways:

You can always get on the streets and make some giveaways.

Get a nice pretext who you are and why you are giving away the CD. Tell the people what's on it and why it's so awesome. This is the fastest community spreading method. But you should consider this:

Every act of communication is a huge security risk. Even if you travel to another state - if the people find out what you are doing and are able to tell the police about how you looked, you will get in serious trouble.

If you are a professional social engineer you should have a method on how to get a lot of money in mind already. You could target on rich, older people.

This method is very, again very illegal. Don't do this unless you want to spend some time in jail. This kind of scam and financial fraud isn't anything easy.

VI. Conclusion:

You should have an idea on how you can spread in real life now. There are so many methods on how to spread a CD, I can't cover them all. Use your brain and think in which situations you get in touch with a CD and you will find more ways.

The CD spreading method has one huge downside:

Your FUD rate. You can't simply reFUD the file once you gave it out. Because of this, it is very important to get a long FUD rate. Get a private stub or code your own crypter/stub. Don't expect the library or rental method to work that great when using a server which is FUD for 2 days only.

Since this is a community spreading guide, I will give you a few more ideas on where to spread a RAT without a CD.

The last chapter is about how to infect a big company. Note that the method is similar to the ones used before, so this is why I will cover it.

VII. Spreading without a CD:

So where to spread when you actually have access to the computer you want to infect? Let me give you a few ideas:

- School computers
- Library computers
- Internet coffee
- LAN partys
- Computer related events
- Your own idea here

VIII. Compromising a big company:

NOTE:

I said this a few times already: Deal with this information on your own risk.

The following idea is for professional social engineers and penetration testers who are recruited to infect a company.

I was talking about public librarys earlier. However, the most bigger companies got a own, internal library aswell. These libraries offer specific literature. Alot of these books feature CD's which are very related to the content of the book. The execution rate of these scientific CD's is rather high.

If you can manage to swap the original CD of the book with your infected one, you have high chances that some employee runs the CD on his PC at work.

If the library of the company isn't public, you have to see how to get into it. It's not impossible - but this is going much too far for this tutorial. Let me suggest you some books which can be very helpful for social engineers:

- [Human hacking](#)
- [Introducing NLP](#)
- [Guide to social engineering and dumpster diving](#)
- [Influence](#)
- [How to engage people doing sth.](#)
- [Hacking the human](#)
- [Art of Intrusion](#)

These are a few interesting books about social engineering and how to get into an internal library for example.

IV. Final words:

Thanks for reading my tutorial!

I'm not sure on how many people will actually use this method, but it was fun coming up with this idea. In fact, I like writing tutorials and guides but I'm lacking on ideas. If you got any suggestions for a tutorial which isn't written yet (or very LQ only), feel free to send me a PM.

If you found any bigger mistakes, let me know.

Have a nice day everyone.

ankitkhosya - August 5, 2013, 10:48 am

Man ! thats some HQ post after some few days . thankx for refreshing me dude.

want to +rep but cant .

Military_Shadow - August 5, 2013, 11:09 am

I really like this idea! Great way to mix your real life and your virtual one too :)

?pth?n - August 13, 2013, 12:06 pm

Thanks for your replies ;)

Hope it's useful for someone

pzelite - August 13, 2013, 12:18 pm

This is really awesome. Can't wait to read it again when I get home, so I can focus 100% on it :)

"Hack to learn. Don't learn to hack."

?pth?n - October 3, 2013, 1:22 am

Hope this helped one or another, if anyone got suggestions and improvements, please tell me about it :)

I'll probably add another "James Bond method" in the future (AR Drone, wlan hacking, dns spoofing to your site)

Kraken t3ch - October 3, 2013, 2:16 am

Nicely written tutorial. Thanks for your time and effort. Will surely come in handy

tkmremi - October 3, 2013, 2:28 am

thanks for this :D !!

[img]http://www.findandtry.com/landings/map/1/?filter_gender=man_or_woman&age_limits=18_25&filter_race=0&photo_rating=any&lang=auto&number_of_pins=10&aff=94561426-tsp[/img]

[img]http://www.findandtry.com/landings/map/2/?filter_gender=man_or_woman&age_limits=18_25&filter_race=0&photo_rating=any&lang=auto&number_of_pins=10&aff=94561426-tsp[/img]

del224 - October 3, 2013, 3:01 am

Only a total jerk would hack real life friends, I know that if you do everything well you wont get caught but I wouldnt take that risk as you would be pretty much fucked if you would get caught, no one would even talk to you anymore, lol. And if youre about to break into a companys network and you need to come to hackforums to search for info youre even bigger jerk, just saying

Great tut tho.

Tylerrrr™ - October 3, 2013, 9:49 am

after reading your thread I developed some very good ideas on spreading also. Thanks :D

darkflower - October 3, 2013, 10:35 am

You can spread it and from an udp server or rdp

?pth?n - October 6, 2013, 2:17 am

(Oct 3, 2013 03:01 AM)del224 Wrote: [\[CITE\]](#) Only a total jerk would hack real life friends, I know that if you do everything well you wont get caught but I wouldnt take that risk as you would be pretty much fucked if you would get caught, no one would even talk to you anymore, lol. And if youre about to break into a companys network and you need to come to hackforums to search for info youre even bigger jerk, just saying

Great tut tho.

I agree with you ;)

There are guys on here who don't even know what a VPN is, or what no-IP really does.

This tutorial shouldn't be misused, it's purpose is to bring in some new ideas into the world of spreading.

Yorno00 - October 6, 2013, 7:27 am

Thanks for this idea bro. ?

Anon.Steel - October 6, 2013, 10:24 am

Thanks for the tutorial! :D

35 characters.35 characters.35 characters.

NoCheatBypass - October 8, 2013, 8:09 am

Thanks for this i have some good ideas :D ?

#R00T~ - October 8, 2013, 8:42 am

Great tutorial OP, thanks alot for sharing! ?

DaveKinect - October 8, 2013, 1:14 pm

Thanks for sharing this post i really like it !

grady - October 8, 2013, 3:06 pm

Thank you for this tutorial, it may seem generic to some, but the concepts behind everything is amazingly detailed and helpful for easy spreading. Also, hacking perverts is only fun if you can catch

them watching porn and use ransomware.

partzo - October 14, 2013, 6:30 pm

Thanks for this, I can get some gaming bots now.

?pth?n - November 2, 2013, 8:57 am

Thanks folks,

I hope none of you hacked the library yet ;)

Let's see what other ways of spreading I can think of. The technologies of the future will open new possibilities of spreading.

cherylhandy - February 11, 2014, 1:07 pm

I have my teenage daughters iCloud id for her iPhone 4S and she has given me her password when I ask for it normally within a few hours and always have excuses to put me off. Problem is she keeps changing the password within a day at most after she gives it to me when I ask for it. Now this only bothers me as I feel sure she is hiding things! So I'm wondering if someone can please give me some ideas how to access her password so she is unaware I have it by way of a fake login or whatever. I am not looking to pay anything as I am a single mom of three with now a crappy part time job so money is getting really tight. So any help would be awesome thanks in advance!

Bitcoin Man - February 12, 2014, 2:42 am

hmmmmmm interesting....ill have to try this later lol thanks dude

Strikershocks - February 12, 2014, 7:01 am

Nice Work, thanks for sharing the tutorial :)

Thats are some very good ideas on spreading but i think thats i am not going to test it on my company xD

Viagra - February 12, 2014, 7:08 am

I will try this out soon! Looks good OP!

?pth?n - February 12, 2014, 1:21 pm

Thanks for the nice words guys!

I thought of some other great method which will probably be edited into the main post on the weekend. ?

Have a great time everyone

Nmanpure Pkr - February 16, 2014, 9:44 pm

You could also make a auto-run CD/DVD and "Accidentally forget it" somewhere. Chances are someone will put it in to see what it is. If you have a server binded to a legit application, then they most likely won't think anything of it.

shexx-- - February 16, 2014, 10:46 pm

Waww ! thank's you for this tutorial ;)

jOnathan27 - February 16, 2014, 11:00 pm

(Feb 11, 2014 02:07 PM)cherylhandy Wrote: [\[CITE\]](#) I have my teenage daughters iCloud id for her iPhone 4S and she has given me her password when I ask for it normally within a few hours and always have excuses to put me off. Problem is she keeps changing the password within a day at most after she gives it to me when I ask for it. Now this only bothers me as I feel sure she is hiding things! So I'm wondering if someone can please give me some ideas how to access her password so she is unaware I have it by way of a fake login or whatever. I am not looking to pay anything as I

am a single mom of three with now a crappy part time job so money is getting really tight. So any help would be awesome thanks in advance!

this is the biggest bullshit post i have probably ever read lol????

manhast - February 17, 2014, 12:27 am

mmhhhhh looks interesting I'll try this later :)

?pth?n - February 17, 2014, 8:20 am

(Feb 16, 2014 10:44 PM)Nmanpure Pkr Wrote: [\[CITE\]](#) You could also make a auto-run CD/DVD and "Accidentally forget it" somewhere. Chances are someone will put it in to see what it is. If you have a server binded to a legit application, then they most likely won't think anything of it.

True. But this is a bit too expensive and time consuming for just one random slave.

You're better with leaving it near your target (so for example a company).

By the way, for those guys who still are going to school:

Alot of classes are making CDs with pictures when they go on a trip for example.

I guess everyone get's this hint ?

Tipiqle - February 17, 2014, 3:12 pm

Wow awesome tutorial thanks for ALL the help. Got some great ideas from this.

KOF1998 - February 17, 2014, 4:43 pm

I really like this idea! Great way to mix your real life and your virtual one too :)

Zoef80 - February 26, 2014, 9:52 am

This is a little bit offtopic, but ?pth?n I really hope you read this. I can't PM you to tell you that I have bought your Ebook. Would you like to contact me? Thanks

hackercomienza - February 26, 2014, 7:58 pm

muchas gracias esta muy bueno el tutorial

Appliance Warehouse - March 5, 2014, 1:12 pm

Although USB autorun has been disabled, isn't it possible to format a USB to be just like a CD? Once formatted, couldn't you just upload something?

?pth?n - March 5, 2014, 1:55 pm

Thanks folks ?

(Mar 5, 2014 02:12 PM)????? Wrote: [\[CITE\]](#) Although USB autorun has been disabled, isn't it possible to format a USB to be just like a CD? Once formatted, couldn't you just upload something?

This is possible, you should look up "Rubberducky".

You can do this yourself, but it requires a bit of work ;)

Elana - March 5, 2014, 2:34 pm

Thanks for this detailed tutorial. You helped me alot!

Tromboner - March 5, 2014, 8:47 pm

Some parts of this spreading method are practical for me, but this is more of a philosophy lesson than anything, which I commend you for. I also liked all of the books that you linked, those are nice selections.

I Aspire - March 10, 2014, 3:35 pm

Very well written TUT will be sure to try out

Supreme??????? - March 10, 2014, 3:39 pm

Great tutorial OP. Very informative and helpful!

?pth?n - March 23, 2014, 10:24 am

(Mar 5, 2014 09:47 PM)Tromboner Wrote: [\[CITE\]](#) Some parts of this spreading method are practical for me, but this is more of a philosophy lesson than anything, which I commend you for. I also liked all of the books that you linked, those are nice selections.

Thats what it was meant to be :)

I doubt the regular HF user will try this out.. but knowledge is power ?

Promethazine. - March 23, 2014, 10:27 am

Autorun only works on < XP right? ?

?pth?n - March 23, 2014, 10:39 am

(Mar 23, 2014 10:27 AM)Promethazine. Wrote: [\[CITE\]](#) Autorun only works on < XP right? ?

Autorun from USB works for everything below Windows XP SP 2.

However, autorun from CD still works ?

Other than that, you could purchase rubber ducky. It's an device that still supports autorun. The downside is that it costs a bit more than a normal USB would.

If you want to make your own autorun USB, check this out:

<https://hackforums.net/showthread.php?tid=4096689>

Bollitolli - March 23, 2014, 1:31 pm

Very nice tutorial. I will try. Thank you man!

tigerhand111 - March 25, 2014, 9:33 pm

Nicely written tutorial. Thanks for your time and effort. Will surely come in handy

?pth?n - May 9, 2014, 2:11 pm

Thanks folks ?

If you want me to write another tutorial related to spreading / ratting / whatever, just write me a PM. Going to test out some cheap china USBs soon. They promise to feature auto run.. we'll see ;)