HOWTO STEAL BITCOIN 4.0

Table of Contents

1 Foreword

My motivation is purely technical. I am using this method over a year with huge success. About half a year ago I wrote the first version of this guide and started to sell it in Evolution. The reason was because I got stucked and lazy and was not developing the method further, but when I put it on the market, I suddenly recieved a bunch of feedback. My guide quickly became one of the most popular item on Evo, as a result I gained back my motivation and amazing things were happening with not just this software but with my wallet, too. But after that Evolution exit scam happened and I decided to buy some flight ticket and go on a crazy holiday until a nice new market emerges. ***The time has come and I am back.***

```
So do not get fooled and think, because of the cheap price, this guide does not worth shit, in fact, I am not aware of any guide in the market that would be more valuable than this one. As I said, my motivation is to develop further this method and I don't give a fuck about thaose few bitcoins I can get out of this market.
```

2 Justification

When a system get attacked it becomes more resilient.

I honestly hope this method will not work in 2-3 years from now, but if we don't attack it now, then someone will do it, after my grandpa and your grandma start to use bitcoin and that would be a huge disaster.

You have to attack bitcoin in order to make it better.

3 Introduction

It is an easy-to-follow, comprehensive, step-by-step guide. If you follow this you will never have to worry about finances again.

This is an advanced, tested, professional hacking method. This is the first (and right now the only) guide that makes it possible the first time for an average person to use this classic and effective method.

This software is unique, developed by me. The reason why this method is not being used by the average Joe is because you actually have to hardcode your btc address into the program and then build the project by yourself.

The good news are, if you have the source code and clear instructions, it is not difficult at all.

The package contains the source code (C#) of a malware (BITCOIN STEALER) that **watches Windows clipboard for Bitcoin addresses and replaces them with your own. So the target will send the coins to you by mistake.**

Also there is a trick that makes your bitcoin address looks similar to the copied address...

For example, if the target's address is like this:

1JRCnFwbr4wwtzGJ1gkqpVgwCZg9MSwdJE

Yours will be like this:

1JRCfyjr1yvZzH9JuoEYZyYY5tWconhyhpgIE

An other advantage of having the source code is that it keeps you safe (from me), because you can revise it by yourself, also you can trust it has been revised by others many times before.

This guide also will show you how to use this software effectively. The package will show you the social engineering and phishing methods in order to reach your goal.

Your only goal is to make the targets to run your exe and from there you can lay back in the rest of your life, go to Malibu and watch the money flowing in.

This guide is NOT for you if

- *you want to invest your money into illegal activity*
- *you want to take risk*

This guide is for you if

- *you are average person, who wants to make easy money*
- *you are an average techie, who wants to know how to use an advanced*

hacking technique

- you are a programmer, who needs the source code of a masterpiece

4 The development process of the guide

It is important to know, the developement of this software is continious. As it becomes more and more powerful tool, the price will raise simultaneously. Well, I have good news for you. If you buy this product and then contribute to its forum topic you'll get the next version for free, you don't even have to buy the price difference. All you have to do is to send me a pm with a link to your forum post when you notice a new version is out.

5 Awesome tutorial video

Wakawakala9 made a nice tutorial video. It won't be compatible with newer versions, but it will definitely help you get some idea.
https://www.youtube.com/watch?v=kTVJna6VhuA

6 Keep in mind before you start

I know there are so many bullshit and poorly written article on the internet and people tend to rush through them. This is not one of them. You have to read and follow it carefully and you will make money. Do not rush, it won't be a waste of time!

7 Get a safe bitcoin wallet and learn how to launder your coins

Assuming you have bought this guide on the black market, there is a big chance you already have a reliable wallet, that nobody knows is yours, but let me say the truth, most of you guys are so careless.

The coin laundering extremely critical here here, because you are about to steal other people's money and I bet they will try to follow you on the blockchain.

Store your coins

I recommend using blockchain.info wallet over TOR, because it has onion address. (http://blog.blockchain.com/2014/12/03/improved-security-for-tor-users/)

You can also store your coins on a desktop wallet, too, it is your decision, but right now I cannot recommend any other web wallet that would have an onion address. This is critical, because it will keep your money safe from malicious TOR exit nodes.

Steps:

1. *Use TOR browser*
2. *Go to the onion address of the blockchain.info wallet: https://blockchainbdgpzk.onion/*
3. *Create a wallet for the coins you steal.*

Laundering

However the common belief is that bitcoin mixing techniques are just fine and they works and maybe they are right about that, my belief is different.

The most common way to launder coins is Blockchain.info Shared Coins

```
example:
btc address -> blockhain.info shared send -> an other btc address
```

**note: DarkWallet will be nice and might be the ultimate solution, but it's too baby to use it yet. If not neccessary, don't use anything that's not stable.*

The most secure way to launder your coins is through anonimous altcoins

There are some stealthy anonymous coins like Darkcoin (DRK) and Monero (XMR). They are working. I cannot tell too much about other anoncoins, since I did not looked into them.

```
NOTE: DRK has been renamed to DASH, because its developers are a bunch of pussy. Fuck them I'm not going to use that name.
```

So there is this amazing service, called Shapeshift from Erik Voorhees.

No account needed, only an altcoin address and an amount and you can send there bitcoin.

```
example:
btc address -> blockhain.info shared send -> shapeshift.io -> drk address -> DarkSend-> shapeshift.io -> btc address
```

8 Generate a bunch of addresses

«Are you insane? Why would I do that?» you ask... Listen, here is the trick. You want your bitcoin address to look similar to the target's copied adress. Then let's create a bunch of addresses first and let our malware to choose the most similar one.

You'll need my Mass Address Generator, that I've written for this. You can find it in the package, accompanied by it's source code.

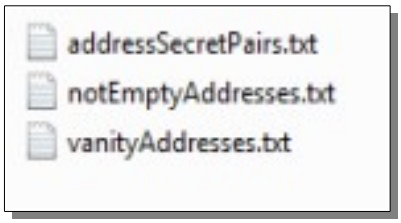
```
/*
Programmer's note: If you want to build the source yourself,
you can do it in exactly the same way that you'll do it with
the Bitcoin Stealer application in the following sections of
this guide.
The only differences are, the project has to be in at least
.NET4.5 and you'll need two NuGet package: NBitcoin and the
Blockchain.info's API
*/
```

To run this app, you'll need to install the .NET 4.5 framework. https://www.microsoft.com/en-us/download/details.aspx?id=30653

Set how many addresses you want to generate and press start, you're cool. You've just generated a bunch of bitcoin addresses and their secret key pairs. I'd recommend you at first start with 100 addresses for testing purposes.

After you've generated your addresses, at the « Wallet » tab, with the « Refresh » button you can check if there are some not empty among them. (There won't be, until sb send money to it.)

- *If you've generated 100 000 addresses, refreshing will take for a day.*
- *If you've generated 10 000 addresses, refreshing will take for about 40min.*
- *Refreshing 100 addresses takes less than a minute.*



Generated files :

***addressSecretPairs.txt** – stores all the generated addresses and their corresponding secret keys.*
***vanityAddresses.txt** – stores all the generated addresses only. This is what our malware will need.*
***notEmptyAddresses** – stores not empty addresses and their corresponding secret keys. When you click « Refresh » it will generate this file.*

Notes:

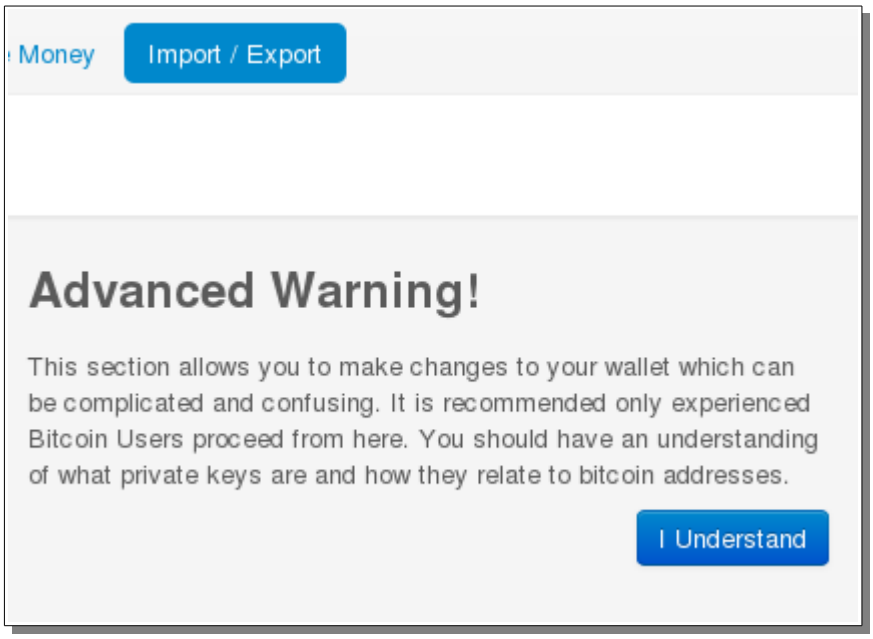
- *When you generate new files, they'll overwrite the old ones.*
- *You probably wants to store them safely and make a backup.*

Testing the Mass Address Generator

1. *Open the program, click start. This will generate 100 addresses and their*

corresponding secrets.

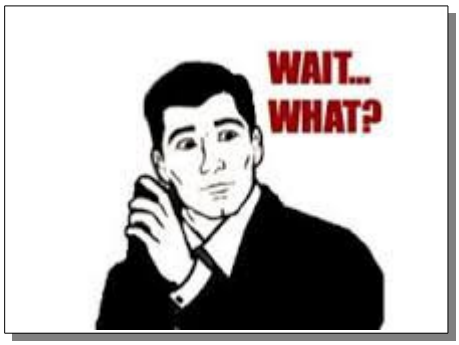
2. *Check out generated addresses. Send a small amount, like (0.0001btc) to one of them.*
3. *When the coins has arrived, change to the « Wallet » tab and click « Refresh ».*
4. *Check out not empty addresses ! (Format: address:secretKey)*
5. *Go to your Bitcoin wallet and import the secret key. (Preferably Blockchain.info (https://blockchainbdgpzk.onion/)*
   It's extremely easy, 3 click :



   You click « I Understand », because you're an advance user. (If they'd have any idea how advanced you are:)
6. Congratulations ! You're done, you can spend the money.

7. Create your own BITCOIN STEALER malware

This is the core of the guide. It's time to do the geeky stuff. We're gonna change a few lines in the code and build our C# project. After this you can write it into your CV. Wait... what?



First of all, you have to know C# is a Microsoft slave language. This means, from now on we're working on Windows. More accurately, we're going to code in .NET Framework 4.0, that means you have to use Windows XP SP3 or higher version (like Windows 7,8).
If you don't have Windows I recommend you to use VirtualBox (https://www.virtualbox.org/). You install it, then you set up a Windows virtual machine in it.

> ***Note:*** *it is important to use the latest version of VirtualBox*

Next we need to get the Visual Studio.
I recommend you to use the Visual Studio Community version.
http://www.visualstudio.com/

> ***Note:*** *the Visual Studio is the longest taking installing software in the whole world: (Ok, it's not, but you get the point.)*

Now, that we have set up the requirements it's finally time to code.

From here you should follow these instructions very strictly, because if you are not familiar with coding, you can't make any mistake here. If you have done a mistake, delete everything and start this chapter from here again.

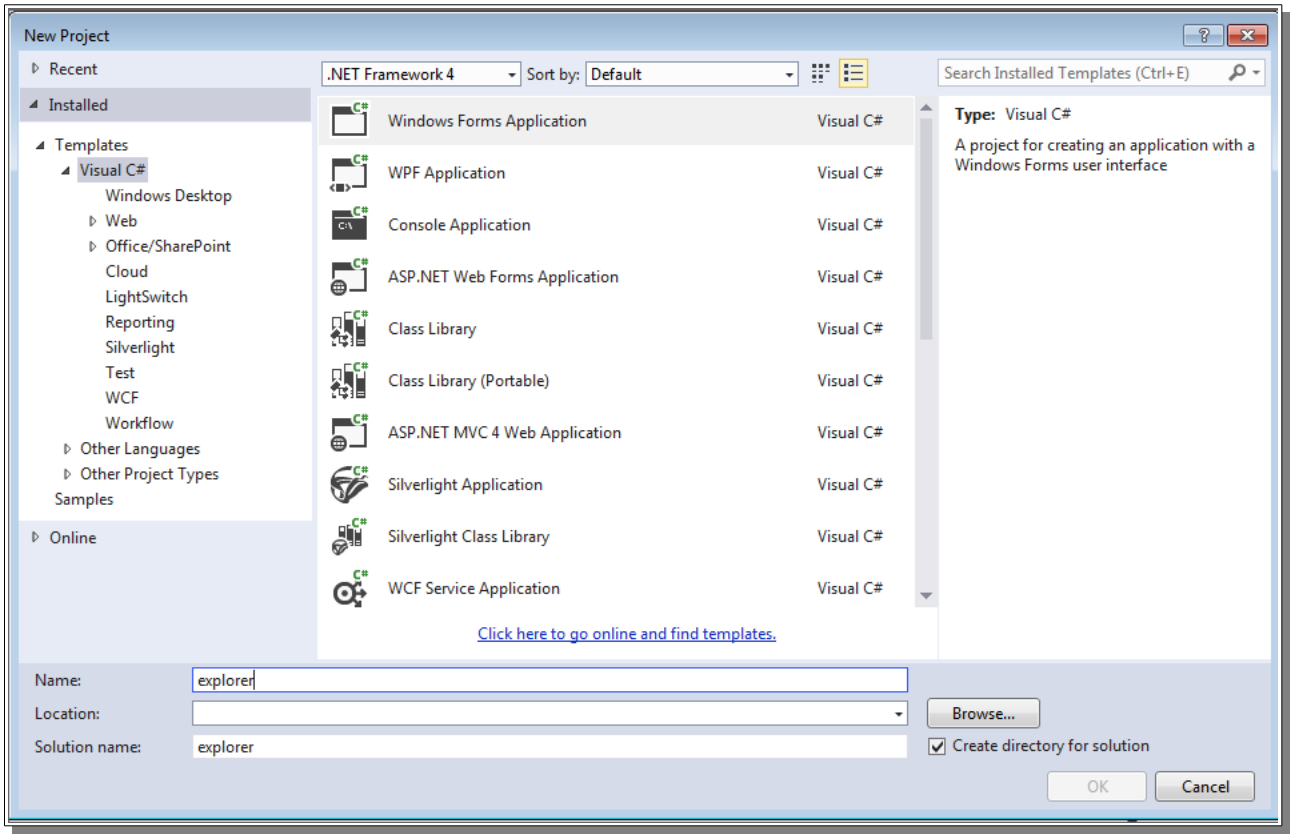
1. *Run Visual Studio*
2. *File/New/Project/*
   *Select Templates/Visual C#/**Windows Forms Application***
   *Select **.NET Framework 4***
   ***Name: Adobe Reader** - you want to choose a name that is not suspicios for the a user when it is looking at the processes. I mean "BITCOIN STEALER" would be a very bad idea. However in this tutorial I will not show you how to go*

with an other name (eg. « chrome » or sth), if you don't want any conflict, just let it be "Adobe Reader". As you can see on the pictures, I was using « explorer », but it turns out to be not a good idea, because with this name it won't work on winxp.

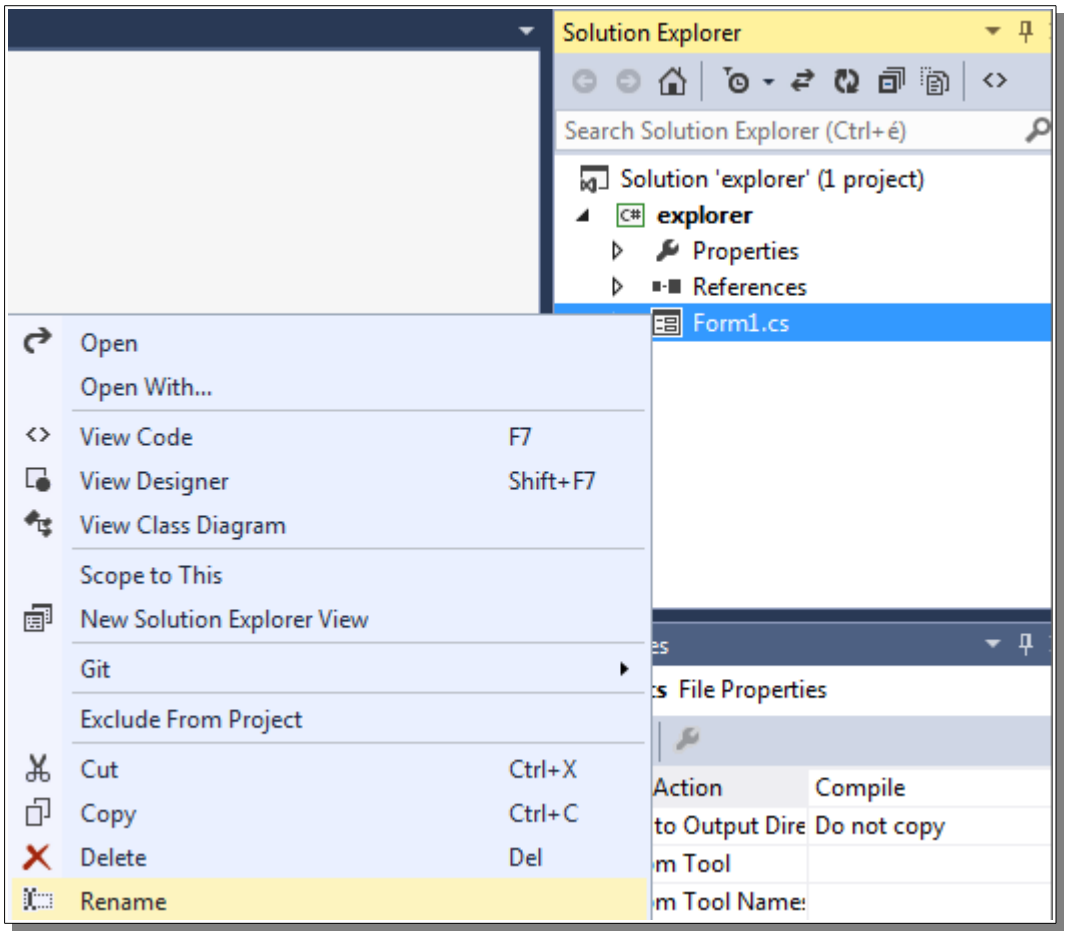
***Programmers note:** If you want to go with an other name find and change the «adobe» string everywhere in the solution. (ctrl+F, search in whole solution)*

Solution name: Adobe Reader

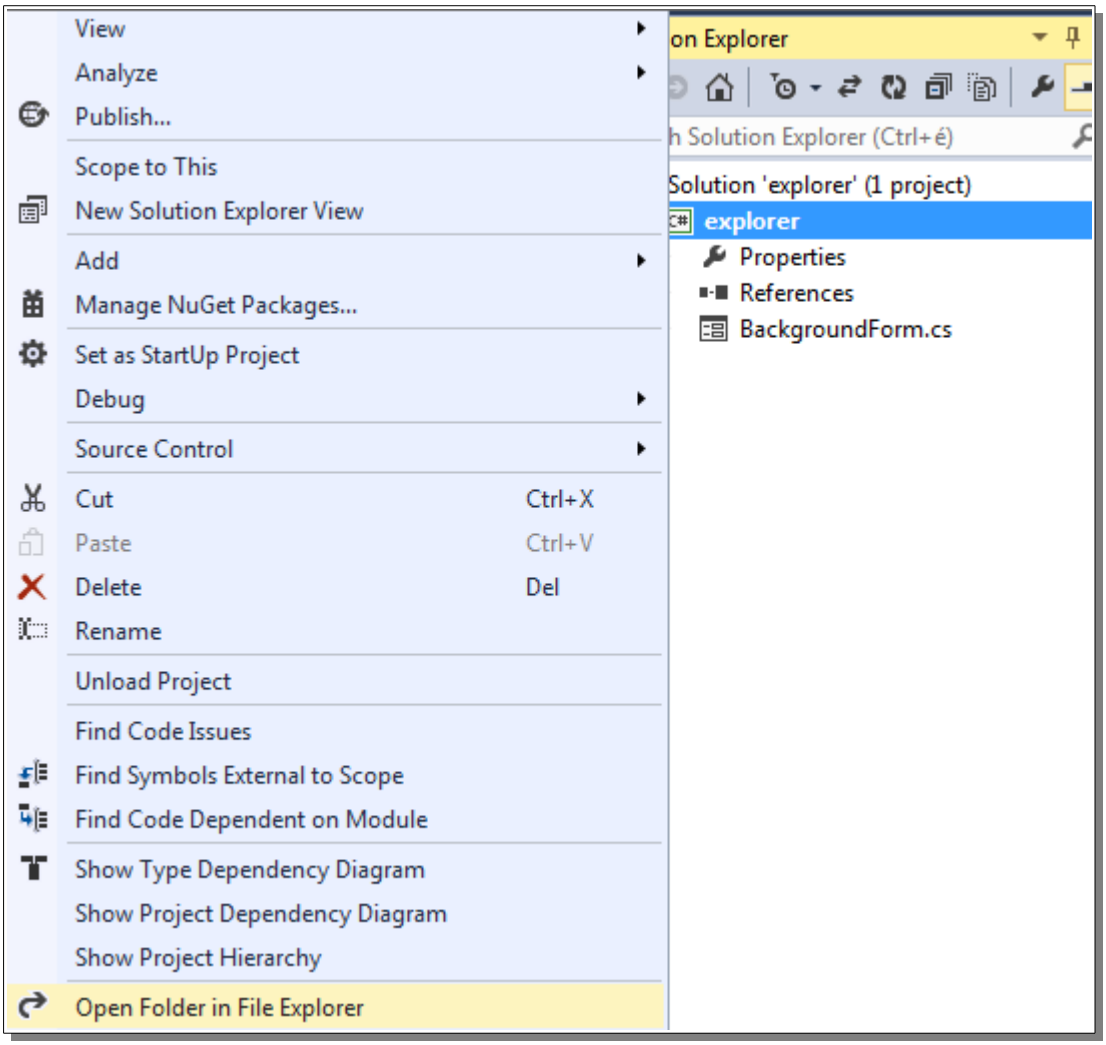
***Location:** here you want to select some folder that you'll never let anybody to see.*



3. *In the Solution Explorer rename the "Form1.cs" to "BackgroundForm.cs".*

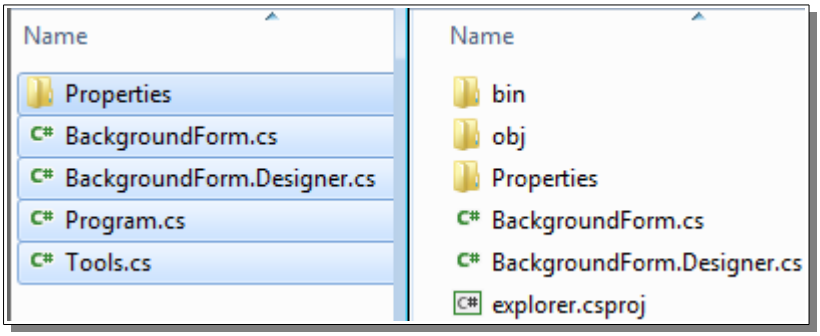


4. *Open the project folder (Adobe Reader).*

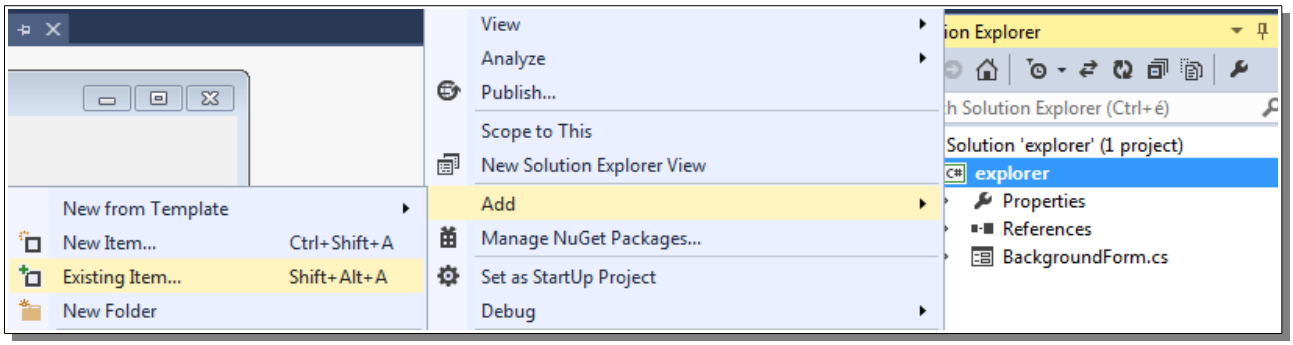


5. Open the Bitcoin Stealer/sources (it's next to this pdf what you're reading right now).

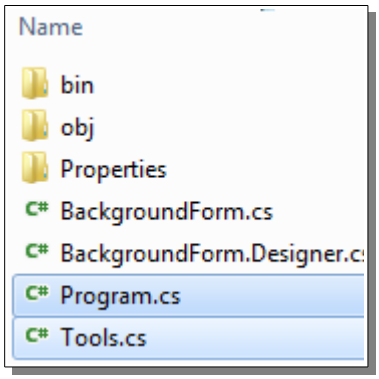
6. Copy and replace everything from Bitcoin Stealer/sources folder to the project folder (Adobe Reader).



7. Right click on Adobe Reader / Add existing Item...

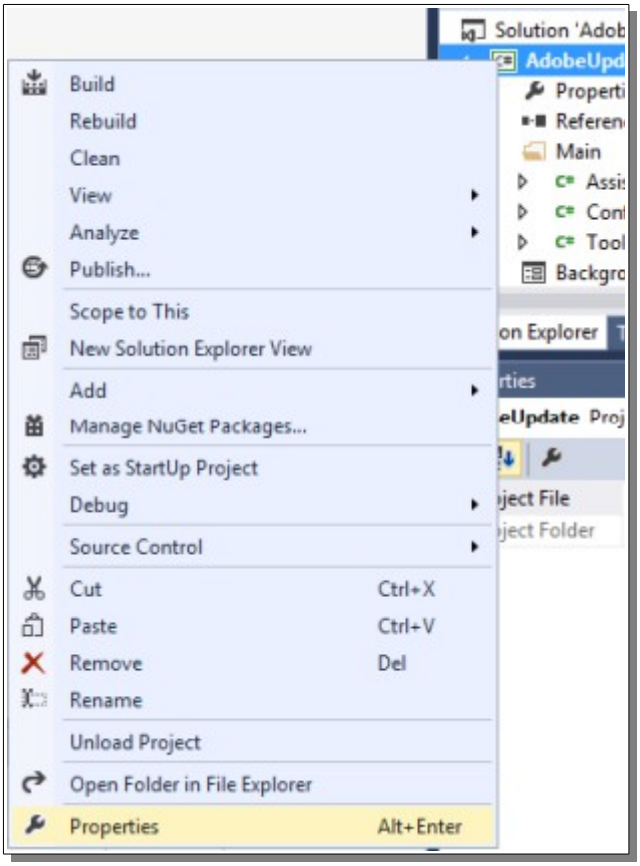


8. Select Program.cs and Tools.cs from the project folder (Adobe Reader).

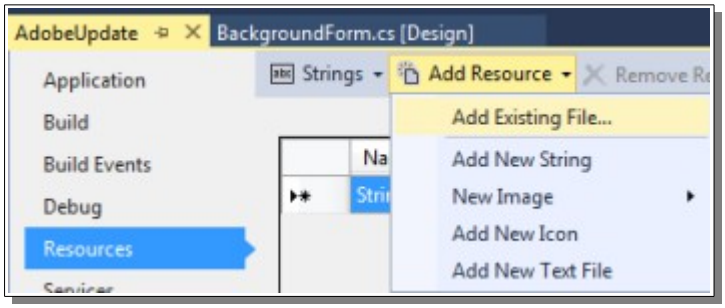


9. Right click on project (Adobe Reader) / select Properties.

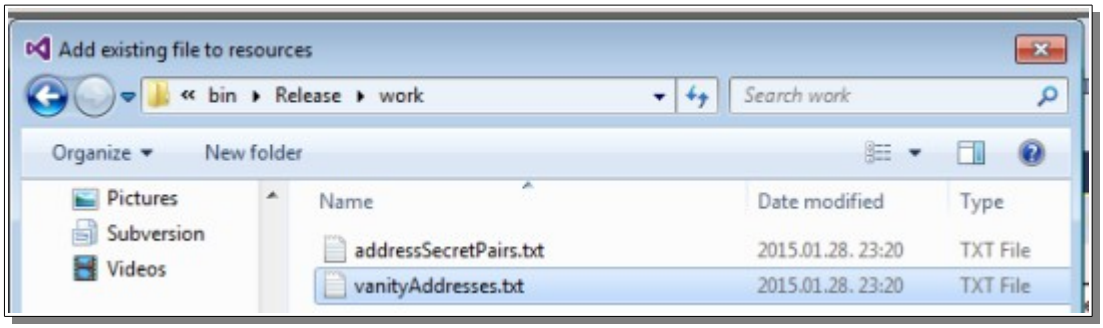
***Note:** On some picture the name of the project is «AdobeUpdate» instead of «explorer». Do not get confused by that.*



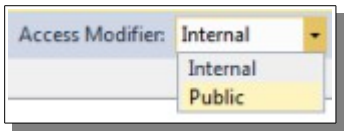
10. Select Resources / click Add Resource from Existing file.



11. Choose your vanityAddresses.txt you've just generated with the MassAddressGenerator.

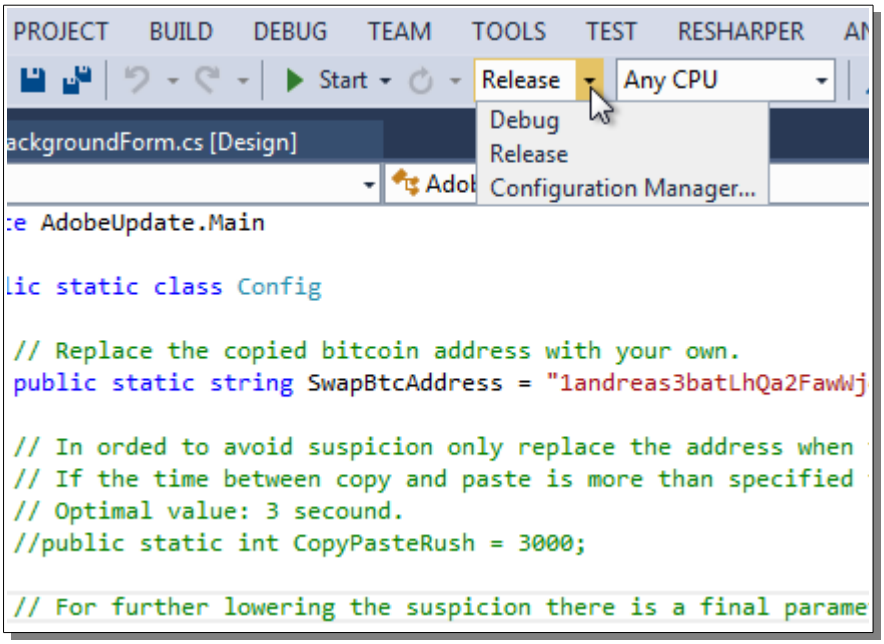


12. Set Access Modifier to «Public»

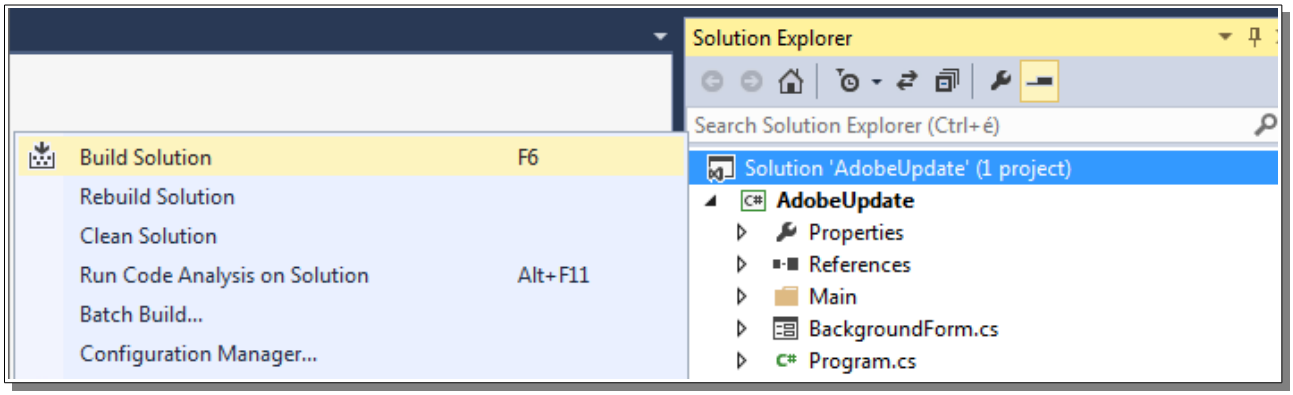


13. There is one more last setting we want to set. We want to build our project in Release mode.

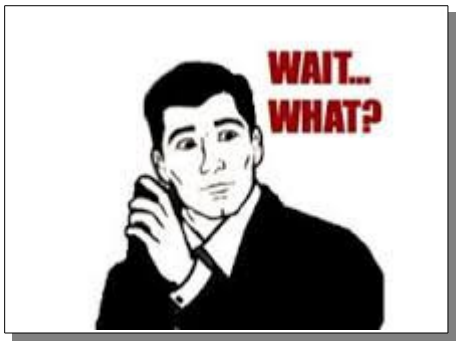
> *Programmer's note: you can use choose Debug mode if you want to mess around with the code.*
> *If you use debug, then you don't need to remove the malware from your computer, since it doesn't copy itself into it and will not start with the Windows.*



14. Now it's time to build our solution. If we have done everything right we won't get any error here.



Congratulations, you've created your first malware, now you're officially a hacker. You can tell everybody about it. Wait... what?


WAIT...
WHAT?

9 Testing your malware

Now it's time to do the testing.

First locate the exe file: Adobe Reader/bin/Release/Adobe Reader.exe (you can rename it as you wish). From here you won't need any other file to work with, only the executable.

1. *Copy the exe to your Desktop*
2. *Run the executable! (Attention: you're not going to see any welcome windows or anything, like that. Just imagine, how would you react if a window would pop up every time you start your computer with a message like this: "Hey man, what's up?! I'm a virus, I've infected your computer... sucker.")*
3. *Check if our program is running: Windows Task Manager/Processes. (Press ctrl+shift+esc) Here you should see "Chrome32.exe" program is running.*
4. *Now copy a bitcoin address and paste it somewhere. Does it work? No? Do it again WITH AN OTHER ADDRESS! Still don't work? Do it again with an other address! Repeat!*
   The reason why it doesn't work all the time, because it would be too suspicios. Furthermore if you copy the same address twice, it won't work, too in order to avoid suspicion.

```
There is a variable at the beginning of BackgroundForm.cs, called
OppToMissDef. If you change it's value to 0, it will work every
time (exept when you try to paste the same address twice)
```

5. *Finally restart your computer and check if it starts running with the Windows. But now the name of the program will be "AcroRd32.exe" and not "Chrome32.exe". Why is that?*

```
When you run your exe it will copy itself somewhere on your
computer and change it's name to Chrome32.exe and copy itself to
somewhere else with a name as AcroRd32.exe. Then execute this
Chrome32.exe, then delete itself.
So now Chrome32.exe is running, but if the user is so smart, it
will realize, "OMG, I've just launched a malware", so it goes to
processes, find this Chrome32.exe, delete it and stop it.
Well not quite yet. When the user next starts the windows, the
AcroRd32 will run, even if it deleted the Chrome32.

If you didn't understand what I was just saying, don't worry,
it's my fault. It's enough to know, when the target launches the
exe, it will delete itself.
```

10 Remove the malware

Finally remove it from your computer:

1. *Start Windows Task Manager and terminate the Chrome32.exe or AcroRd32.exe process!*
2. *Go to %appdata% in your file browser.*
3. *Delete AppData/Roaming/Adobe (x86) folder.*
4. *Delete AppData/Local/Google (x86) folder.*

```
If you don't terminate the malware manually, as it is described
in the first point you can't delete one of the folder.
If you've deleted the Adobe folder it won't start again on your
computer, so you're good, but to completly remove it you have to
do one more thing:
```

- *Start the Registry Editor (regedit) and delete our software from "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"*

```
If you don't find it, check HKEY_LOCAL_MACHINE instead of
HKEY_CURRENT_USER
```

11 Summing up: how the malware works

You only have a standalone exe file. You can rename it to anything. Let's say InnocentSoftware.exe.
Someone click on InnocentSoftware.exe, then it will disappear. What happens is, InnocentSoftare.exe copies our malware to AppData/Roaming/Adobe (x86)/AcroRd32.exe and AppData/Local/Google (x86)/Chrome32.exe and make sure AcroRd32.exe starts with Windows every time.
Then it starts Chrome32.exe.
Then InnocentSoftware.exe stop running.
Then Chrome32.exe deletes InnocentSoftware.exe.
When the user copies a btc address then it pastes yours instead of the user's. Furthermore, it will look similar to the the copied address.
However there are some mechanisms in place in order to avoid suspicion, for example when the user copies the same address twice in a row the copypaste will work normally and it will only work for every 3rd opportunities. (Or whatever what you set the OppToMissDef in the BackgoundForm.cs file)

```
For better understanding you might also want to take a look at
the BackgroundForm.cs file's comments (and maybe the code).
```

12 Experiences / FAQs / ideas

blowmoney1996
This guide is great. Stole about 2.3 btc already. This is the fuckin shit. He delivered it within 5 min and is a great vendor.

real_barreface
Got the guide within an hour of ordering and scammed 5 BTC in 2 days. Learn to spread this and your good

Scheynkine
fun fact #1
got robbed today from my own malware.
...
not robbed exactly, i just wanted to transfer from wallet to evo. instead it ended up in the scam-wallet.. i thought i deleted it, but i didnt clear the appdata. but it's great, that it really works!

What about Anti virus softwares, do they detect it?
It is a pretty "harmless" software, you won't have any problem with it. It does not communicate with the internet, or does anything fairly suspicious.

gavioesdafiel
Hi All,
I just have started my learning process to spread/spam this malware. As i dont have too many skills on that Im getting some basics tips that I wanted to share with you. I appreciate any kind of information/tips that you can share with me. |o|
"
11 Hacks to Increase Your Email Open Rates
The grim reality of email marketing is that very few people actually pay attention to the messages they receive. Email is the primary mode of communication for so many businesses that an opt-in just doesn’t have the value it once did. 100 people might claim they want your newsletter, but when it comes time for the mental investment of opening it and reading what’s inside, maybe 5-10 of them actually do.
1. Make sure your newsletter looks good.
The idea behind this hack is that, when a user signs up for your mailing list, they’re going to open the first message you send.

If they open that message and they discover a newsletter that looks broken or skewed, they'll figure your message is broken in some way. Maybe they'll let you know, maybe they'll just delete the message. Either way, that bad experience lingers, and the next time a newsletter comes by it languishes in their inbox. You can test your newsletters using Litmus, to see how it will look on various platforms, including mobile. Litmus will also tell you if something in your message or subject line will trip spam filters.

2. Keep your subject lines short.

According to a survey presented by Salesforce, your email open rates will almost definitely be much higher when your subject line is short. A subject line under 10 characters is enticing enough to give you a nearly 60% open rate on average. Chances are this is well above what you typically experience.

What can you do in ten characters? You only have two or three short words to play with. Fortunately, short language is enticing on its own. In a world of subject lines that run long enough to be truncated, a short subject line stands out. It almost doesn't matter what you write.

3. Use title case capitalization in your subject line.

Use-title-case-capitalization-in-your-subject-line

It's much more attention-grabbing to use title case – that is, Capitalization of the First Letter of Each Major Word – in your subject line than it is to use a standard sentence. Treat your email subject line in the same way you might treat the title of a blog post for your rich snippet. While a subject line should be short, it doesn't have to be, and a compelling question can break the length rule and maintain a high open rate.

4. Send and send and send again.

Whenever you send out a message, track who opens it and who doesn't. Anyone who doesn't open it should be added to a new list of people you can target again. If they don't open your message, it's as though they never saw it in the first place. It might be buried in their inbox, they might have deleted it without thinking or it might have ended up in an archive. In any case, you can safely send the email a second time, potentially drawing quite a bit of additional attention. You may not want to send a third time, however; the rule of threes lends extra potency to a third dismissal.

You might like:

How to Turn Your Mailchimp Subscribers Into CustomersHow to Turn Your Mailchimp Subscribers Into Customers Your mailing list, as powered by Mailchimp, is one of…

5. Proof your message, and have someone else do it.

When you spend a lengthy amount of time working on a single project, you grow a sort of mental blindness to its flaws. Your mind fills with the concepts and thoughts behind each word you write, rather than what you write itself. In the end, you might

end up with a message you think is perfect, with a prominent typo you keep missing. Enlist the aid of someone, it doesn't matter who; just someone who will put a second pair of eyes on the piece and proofread it for you.

6. Satisfy the subject line.

The point of a subject line, at least a good one, is to stir thoughts in the reader. Your goal is to make them ask what could possibly come as a follow-up from that subject line, with the promise that the answer is inside the email.

That means you need to live up to your promise and follow up on your subject line in the message itself. You can't draw in attention with one concept, only to disregard it in the body; it's a bait and switch that leaves users disappointed.

7. Invite replies.

Invite-replies

Here's one thing you don't see every day; "If you have any questions, feel free to respond to this message." Most emails from large companies are sent from automated accounts that no one checks. Users are used to needing to find your contact information on your site if they have a question, and that's too much work. It means a lot of questions go unanswered. Instead, open up your newletter as a two-way communication. Even if you then forward the replies you get to your customer service email address, you're still giving users a direct route back to you.

8. Use bright, colorful buttons for your CTA.

Your call to action should be preceded by a question, and it should take the form of a bright colored button. Users tend to gloss over plain text links in their emails, just as they do on your landing page. And, just like your landing page, you need to optimize your CTA in the newsletter. After all, it's the newsletter that helps funnel traffic to your landing page.

9. Segment your newsletter mailing list and test variations.

Split testing isn't just for ads or landing pages; you can split test your newsletters as well. Segment your audience into groups and send variations on your message to each. Try to keep representative groups if you're testing general changes, like tweaks to your subject line or the color of your CTA button. You might skew your results if you segment by demographics to run your tests.

10. Don't forget the other messages you send.

When a user decides to download your white paper or ebook, do you send them a confirmation email and thank-you letter? If so, you might be missing out on a great opportunity. Consider that content delivery message as a chance to include more hooks for future actions, both in the immediate short term and the long term. There's always something you can encourage the user to do to support your brand.

11. Maintain a consistent voice.

Users feel like they're interacting with an impersonal, robotic

corporate face if they receive drastically different messages from different marketing channels. If their experience with customer service is much more casual, how are they to trust that it's not some outsourced company doing the work? A consistent voice allows them to trust your business that much more.

He man, i messed around with your V1 of the bitcoin stealer and got deeper in the spreading method.
I found some method to spread it that works for me so i want to share it to you.
I hide the .exe in a .rar with images and changed the .exe to .jpg and changed the icon from .exe to the one of .jpg , so you don't see the .exe file until you click the image but then its already to late wink
I have a little not proud method to spread this .rar file with images , i do it on teen chat sites and login as female and ask if they want to see pictures.
So far your method give me like $200,- , i want to thank you for that !

I've gave some thought to this. Maybe you can scam some pedos with it. Upload the pics and write a post to a pedo forum. Pedos probably use bitcoin, cos they're on tor.

1.0 review
TheSaint
So, I finally found time for this.
Nothing much to say. The guide might be confusing to a complete newb, I wouldn't call it total noob friendly, however it is easy to follow and the whole thing can be done in about 3 minutes, from the moment You get all the tools on point.
This stealer MIGHT steal something, but it needs spreading. And spreading is pain. If You are willing to bare the pain, I rather recommend setting up a rat or a botnet as it's way more profitable and fun. But then You need to crypt it (preferably FUD) and that would cost something.
To sum things up - This is bitcoin stealing for noobs.
The Guide - 4/5 (could be more noob friendly)
The program - 3/5 (I saw that You are twisting it, so it might get better)

PS. I check the addresses like 5 times, so I would never fall for this.
Think about that.
Cheers.

2.0 review

TheSaint
I finally decided to look at the updated version. You've done a wonderful job here. With the 100000 addresses it will be even better. The guide is alright, it looks a bit messy though, but that's not a problem. The stealer is amazing, works flawlessly. Now, I don't know if this is possible, but I'd love to see this stealer infecting usb sticks. That would spread it like a plague. What this really needs is a FUD Crypter, binder and extension spoofer.
The very best thing about this tool, is that it can't be traced back to You, rather than a botnet for instance.
I thank You for your work.
Waiting for more updates.
Cheers!

Virtualbox vs Visual Studio
swimmar
Currently attempting to see it work in real-time, but I am using a virtual machine and it seems to not like that.. will keep trying and use a real machine as well.
funWithCodes
There are some memory corruption problems I know about with virtualbox and visual studio together, the solution is to update the virtualbox for the newest version. I'm not sure there should be a problem with specifically with these softwares.
swimmar
Got it working. Updated virtualbox (as recommended... foolish mistake), but also set the auto-start in the configuration settings in Visual Studio.

besmart
if anyone can get a cracked version of this http://www.exejoiner.com/ would be great. Seems to be the perfect tool to make this stealer ready for spreading.

Kefkalink777
So, after about 1 week of using torrent services to spread files infected with this program, I have finally seen some success. Only got a little over $25 in bitcoin, which may not seem like much, but is much more than I have invested in this, and also PROVES that this malware works. For those who are interested, I used a free crypter/binder program called aegis crypter to bind the malware to other files, mostly cracked video game files, and also a few bitcoin mining programs. I then used Utorrent to turn those into torrent files, and uploaded the torrents to every sharing website I could find. The downside is, I am now banned

from pretty much every single major torrent sharing site out there. If anyone has any experience with crypters, I am looking for an up-to-date FUD stub for the Aegis Crypter program.
tl;dr This program works, confirmed. It's just really hard to effectively spread.

Once i find a spammer to send out the malware. What will i give the spammer to send. Im guessing i piece together the malware via the coding instructions given, then submit the finished product to the spammer to send out?
Exactly, as you've said. Only the exe what the spammer need.

Do you have Jabber or ICQ?
Sorry, I consider to be too risky the use of instant messaging apps.

I saw on the forum that you give the update free to the buyers who bought it before?
Yes, I do.

btw, do not recommend bitfogger. they are a mess. read this: https://bitcointalk.org/index.php?topic=50037.340

Does it work on Mac?
No.

Advices on how to get your malware running on other computers
Now that we have everything what we need, it is time for action. The only goal of this chapter is to make people to run your exe. It is the interesting part, because you have to be creative from here, think about what you have, what you can use. In this chapter I'm going to give you ideas that you might haven't thought of.
You can target specific people.
A good tactic could be is to get a pendrive and put on the virus to every computer you meet. You'd be surprised how many there are. If somebody don't use Bitcoin don't hesitate he will eventually! That's even better, you know... mistakes of the beginners.
Go to libraries, schools, net cafes, basically any place that has computers in it in your city.
What about your company?
Ask for help on deepweb forums. Team up with other people. Buy a hacking service or something...
Read the guides I've included to the pack and get some ideas from there.

Gotta tell you something funny that happen to me, I stole from myself, well, not exactly lol..This is how it happened, I executed the malware on my laptop just for a test, but forgot to totally delete it. So i'm doing this deal out of evo with somebody who wanted a ID scan, so he was like give me your wallet addy, I copied, and pasted it into ICQ messenger, and I didn't even think twice to check the address, just sorta just sent it. I wouldn't have noticed I gave him 1 of my vanity addresses until he said "You know you have fbi in your address?" ya know just for a little laugh, so I laughed an was like really? jokingly, so something told me to glance at the addy I copied, and seen it wasn't my copied address, but it was too late, he had already sent payment to it lol..

Moral is, if I can just send that addy without even checking it, this malware is golden if spreaded right, bcuz if I was a victim, it would already be too late, an my coins would be gone.

Now it's just the spreading I'm having issues with without it being detected. The binding is alright if your mark isn't too smart about downloads, and file types. My method was binding the malware with a actual real PDF carding guide,with a adobe icon. when you execute the file, the guide comes up, and the exe executes in the background, which is perfect BUT what gives it away is the file type being "Application" whenever they unpack the rar file, and then they are like, hey nice try asshole lol..I

been doing some studying on how to crypt it, but haven't been lucky, bcuz I'm not good at coding in that department. what I've read so far, that's what's gotta be done for this to be effective. Hope you can come up with a solution. On the forum, that seems to be mostly everybodies only problem.

noname
Hey there,
i wanted to check my adresses, if somebody transfered something to my faked adresses. but i accidentally pressed the wrong button and it generated new adresses. is there any way i can check the old ones?
Regards
funWithCodes
I'm sorry, you've just lost your secret keys.