Password-Phishing Bitcoin Scam - 10/2/2018

Over the last month, there have been several Bitcoin scam emails reported to Abuse. Each of them claims they have hacked your account and provide you with a password that they have stolen. They also explain they have caught you visiting less than reputable websites and will expose your secrets to your colleagues unless you pay some sum in Bitcoin to their wallet address. The examples below have been obfuscated, but can be used to reference this scam. Do not respond (even as a joke) to these messages, as this proves that there is a real person on the other side of the mailbox, and will likely only increase the amount of spam & phishing attempts you will receive.

Example 1:

From: Gianna Friendly <hrmariettavyp@outlook.com>
Sent: Tuesday, October 2, 2018 6:04 PM
To: User, Joe
Subject: juser – dog123

I am aware dog123 is your pass. Lets get directly to purpose. None has compensated me to investigate you. You do not know me and you're most likely thinking why you're getting this e mail?

Let me tell you, i placed a malware on the xxx video clips (porn) web site and you know what, you visited this site to experience fun (you know what i mean). While you were watching videos, your web browser started operating as a Remote Desktop with a key logger which provided m e accessibility to your screen and also webcam. Just after that, my software program obtained every one of your contacts from your M essenger, Facebook, and emailaccount. and then i made a double video. First part shows the video you were viewing (you have a good taste ;)), and 2nd part displays the view of your cam, & it is u.

You will have two different options. We are going to go through these types of solutions in aspects:

Very first choice is to dismiss this message. in this case, i will send out your video to all of your contacts and you can easily imagine about the disgrace you feel. in addition should you be in a relationship, just how it would affect?

in the second place alternative should be to give me $3000. We are going to name it as a donation. as a result, i will immediately erase your vi deotape. You will go on your daily routine like this never happened and you are never going to hear back again from me.

You'll make the payment via Bitcoin (if you do not know this, search for 'how to buy bitcoin' in Google search engine).

BTC address: 7NMlsZGzP4GBAduGbVJxFOIUdPl8Bk5y2S
[CaSe SeNSiTiVe, copy & paste it]

if you have been planning on going to the authorities, okay, this e-mail can not be traced back to me. i have dealt with my steps. i am not tryi ng to ask you for money a whole lot, i just want to be paid. You now have one day in order to make the payment. i've a unique pixel in this m essage, and at this moment i know that you have read through this e mail. if i don't get the BitCoins, i will definitely send out your video to all o f your contacts including family members, co-workers, and so forth. Having said that, if i do get paid, i'll destroy the recording immediately. it's a nonnegotiable offer and thus please don't waste my personal time and yours by responding to this message. if you want proof, reply Yes! & i definitely will send your video to your 15 contacts.

Example 2:

From: anotheruser@tntech.edu
Date: 10/17/18 9:14 PM (GMT-06:00)
To: "User, Joe" <juser@tntech.edu>
Subject: anotheruser@tntech.edu is hacked

Hello!

My nickname in darknet is pavel22.
I hacked this mailbox more than six months ago,
through it I infected your operating system with a virus (trojan) created by me and have been monitoring you for a long time.

So, your password from anotheruser@tntech.edu is password1

Even if you changed the password after that - it does not matter, my virus intercepted all the caching data on your computer
and automatically saved access for me.

I have access to all your accounts, social networks, email, browsing history.
Accordingly, I have the data of all your contacts, files from your computer, photos and videos.

I was most struck by the intimate content sites that you occasionally visit.
You have a very wild imagination, I tell you!

During your pastime and entertainment there, I took screenshot through the camera of your device, synchronizing with what you are watching.
Oh my god! You are so funny and excited!

I think that you do not want all your contacts to get these files, right?
If you are of the same opinion, then I think that $875 is quite a fair price to destroy the dirt I created.

Send the above amount on my BTC wallet (bitcoin): MNgkOxG3slr2pvboX9XEzohgb5CzTf2La2
As soon as the above amount is received, I guarantee that the data will be deleted, I do not need it.

Otherwise, these files and history of visiting sites will get all your contacts from your device.
Also, I'll send to everyone your contact access to your email and access logs, I have carefully saved it!

Since reading this letter you have 48 hours!
After your reading this message, I'll receive an automatic notification that you have seen the letter.

I hope I taught you a good lesson.
Do not be so nonchalant, please visit only to proven resources, and don't enter your passwords anywhere!
Good luck!

Example 3:

From: <joeuser@tntech.edu>
Date: October 23, 2018 at 11:47:43 AM CDT
To: 123456 <joeuser@tntech.edu>
Subject: password (123456) for joeuser@tntech.edu is compromised

Hello!

I'm a hacker who cracked your email and device a few months ago.
You entered a password on one of the sites you visited, and I intercepted it.
This is your password from joeuser@tntech.edu on moment of hack: 123456

Of course you can will change it, or already changed it.
But it doesn't matter, my malware updated it every time.

Do not try to contact me or find me, it is impossible, since I sent you an email from your account.

Through your email, I uploaded malicious code to your Operation System.
I saved all of your contacts with friends, colleagues, relatives and a complete history of visits to the Internet resources.
Also I installed a Trojan on your device and long tome spying for you.

You are not my only victim, I usually lock computers and ask for a ransom.
But I was struck by the sites of intimate content that you often visit.

I am in shock of your fantasies! I've never seen anything like this!

So, when you had fun on piquant sites (you know what I mean!)
I made screenshot with using my program from your camera of yours device.
After that, I combined them to the content of the currently viewed site.

There will be laughter when I send these photos to your contacts!
BUT I'm sure you don't want it.

Therefore, I expect payment from you for my silence.
I think $831 is an acceptable price for it!

Pay with Bitcoin.
My BTC wallet: wi8z6zdaiAhodTKrPEnyCSpZvAmrmabHck

If you do not know how to do this - enter into Google "how to transfer money to a bitcoin wallet". It is not difficult.
After receiving the specified amount, all your data will be immediately destroyed automatically. My virus will also remove itself from your operating system.

My Trojan have auto alert, after this email is read, I will be know it!

I give you 2 days (48 hours) to make a payment.
If this does not happen - all your contacts will get crazy shots from your dark secret life!
And so that you do not obstruct, your device will be blocked (also after 48 hours)

Do not be silly!
Police or friends won't help you for sure ...

p.s. I can give you advice for the future. Do not enter your passwords on unsafe sites.

I hope for your prudence.
Farewell.

Example 4:

From: joeuser@tntech.edu [mailto: joeuser@tntech.edu]
Sent: Monday, October 29, 2018 7:21 AM
To: User, Joe <joeuser@tntech.edu>
Subject: joeuser@tntech.edu has password 321passworD. Password must be changed

Hello!

I'm a programmer who cracked your email account and device about half year ago.
You entered a password on one of the insecure site you visited, and I catched it.
Your password from joeuser@tntech.edu on moment of crack: 321passworD

Of course you can will change your password, or already made it.
But it doesn't matter, my rat software update it every time.

Please don't try to contact me or find me, it is impossible, since I sent you an email from your email account.

Through your e-mail, I uploaded malicious code to your Operation System.
I saved all of your contacts with friends, colleagues, relatives and a complete history of visits to the Internet resources.
Also I installed a rat software on your device and long tome spying for you.

You are not my only victim, I usually lock devices and ask for a ransom.
But I was struck by the sites of intimate content that you very often visit.

I am in shock of your reach fantasies! Wow! I've never seen anything like this!
I did not even know that SUCH content could be so exciting!

So, when you had fun on intime sites (you know what I mean!) I made screenshot with using my program from your camera of yours device.
After that, I jointed them to the content of the currently viewed site.

Will be funny when I send these photos to your contacts! And if your relatives see it?
BUT I'm sure you don't want it. I definitely would not want to ...

I will not do this if you pay me a little amount.
I think $854 is a nice price for it!

I accept only Bitcoins.
My BTC wallet: cy2SPy7gflAI10h5mME0WfS9L0BkoUEpBJ

If you have difficulty with this - Ask Google "how to make a payment on a bitcoin wallet". It's easy.
After receiving the above amount, all your data will be immediately removed automatically.
My virus will also will be destroy itself from your operating system.

My Trojan have auto alert, after this email is looked, I will be know it!

You have 2 days (48 hours) for make a payment.
If this does not happen - all your contacts will get crazy shots with your dirty life!
And so that you do not obstruct me, your device will be locked (also after 48 hours)

Do not take this frivolously! This is the last warning!
Various security services or antiviruses won't help you for sure (I have already collected all your data).

Here are the recommendations of a professional:
Antiviruses do not help against modern malicious code. Just do not enter your passwords on unsafe sites!

I hope you will be prudent.
Bye.

Example 5:

From: joeuser@tntech.edu [mailto:joeuser@tntech.edu]
Sent: Monday, October 29, 2018 4:28 PM
To: User, Joe <joeuser@tntech.edu>
Subject: joeuser@tntech.edu has password abc1234. Password must be changed

Hello!

I'm a programmer who cracked your email account and device about half year ago.
You entered a password on one of the insecure site you visited, and I catched it.
Your password from joeuser@tntech.edu on moment of crack: abc1234

Of course you can will change your password, or already made it.
But it doesn't matter, my rat software update it every time.

Please don't try to contact me or find me, it is impossible, since I sent you an email from your email account.

Through your e-mail, I uploaded malicious code to your Operation System.
I saved all of your contacts with friends, colleagues, relatives and a complete history of visits to the Internet resources.
Also I installed a rat software on your device and long tome spying for you.

You are not my only victim, I usually lock devices and ask for a ransom.
But I was struck by the sites of intimate content that you very often visit.

I am in shock of your reach fantasies! Wow! I've never seen anything like this!
I did not even know that SUCH content could be so exciting!

So, when you had fun on intime sites (you know what I mean!) I made screenshot with using my program from your camera of yours device.
After that, I jointed them to the content of the currently viewed site.

Will be funny when I send these photos to your contacts! And if your relatives see it?
BUT I'm sure you don't want it. I definitely would not want to ...

I will not do this if you pay me a little amount.
I think $880 is a nice price for it!

I accept only Bitcoins.
My BTC wallet: jnf88zbvjcSMy58TT7DUnAkxBgkY5wW7Hg

If you have difficulty with this - Ask Google "how to make a payment on a bitcoin wallet". It's easy.
After receiving the above amount, all your data will be immediately removed automatically.
My virus will also will be destroy itself from your operating system.

My Trojan have auto alert, after this email is looked, I will be know it!

You have 2 days (48 hours) for make a payment.
If this does not happen - all your contacts will get crazy shots with your dirty life!
And so that you do not obstruct me, your device will be locked (also after 48 hours)

Do not take this frivolously! This is the last warning!
Various security services or antiviruses won't help you for sure (I have already collected all your data).

Here are the recommendations of a professional:
Antiviruses do not help against modern malicious code. Just do not enter your passwords on unsafe sites!

I hope you will be prudent.
Bye.

If you have responded to any of these or similar phishing campaigns, contact the Information Security Office

immediately at x6859.

Please report any suspicious emails to abuse@tntech.edu