Blackmail Scams and Biting Back

Author	josh
Date	2023-10-31

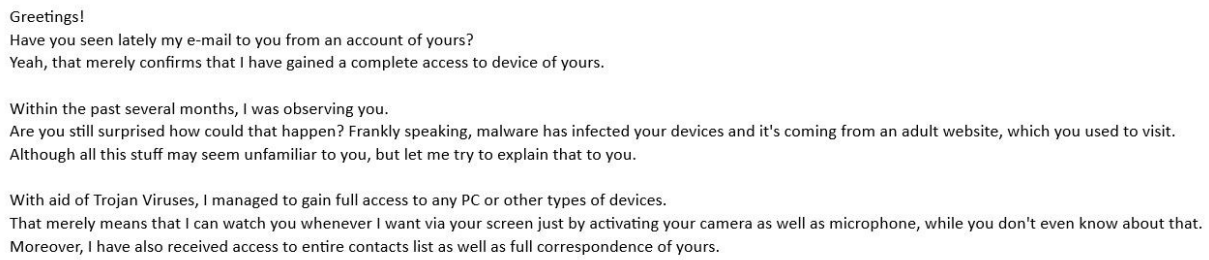
Overview

Social engineering scammers love to operate on fear. Fear makes us act irrationally, and parts us with things that scammers want – such as our money! One type of scam that can be particularly frightening and effective is the *blackmail* scam. What do blackmail scams look like, and how can they be avoided?

Blackmail

How Scammers Instill Fear

A typical blackmail scam starts something like this: you receive an email claiming that you have a “pending payment”. This alone can grab your attention if you’re not expecting it. But the scam quickly gets much worse – the scammer claims that they have gained total access to your device with malware! The scammer claims that they have total control of your device and online accounts – your email, your webcam, your microphone, your files, and your contacts.



Greetings!
Have you seen lately my e-mail to you from an account of yours?
Yeah, that merely confirms that I have gained a complete access to device of yours.

Within the past several months, I was observing you.
Are you still surprised how could that happen? Frankly speaking, malware has infected your devices and it's coming from an adult website, which you used to visit.
Although all this stuff may seem unfamiliar to you, but let me try to explain that to you.

With aid of Trojan Viruses, I managed to gain full access to any PC or other types of devices.
That merely means that I can watch you whenever I want via your screen just by activating your camera as well as microphone, while you don't even know about that.
Moreover, I have also received access to entire contacts list as well as full correspondence of yours.

The scammers often use an interesting trick to make you believe you’ve been compromised – they send the email from “your email”. That is, they put your own email address in the “from” field of the email. If your email is x@y.com, the email states it is from x@y.com. We’ll discuss why this is a trick in the “Prevention” section below.

The scammers then get into the core of the scam – the threat and the demand for payment. Usually, the scammers claim to have used their malware to capture an embarrassing video of you, which they threaten to share with all of your friends, family, coworkers, etc.

The scammers demand payment in cryptocurrency – usually Bitcoin as it is the most popular and well known digital currency. The scammer claims that if you send payment to their Bitcoin address, they will delete the video and leave you alone.

Below are simple steps required for you to undertake in order to avoid that from occurring - transfer $1550 in Bitcoin equivalent to my wallet (if you don't know h

My bitcoin wallet address (BTC Wallet) is: 1N1AvndRxpo3dfKwaMTDmiy1Uaers6hZJk

Once the payment has been confirmed, I shall remove the video without delay, and that is end of story - afterwards you won't hear about me again for sure.
The time for you to perform the transaction is 2 days (48 hours).
After this e-mail is opened by you, I will get an automatic notice, which will start my timer.

Any effort to complain will not change anything at all, because this e-mail is simply untraceable, just like my bitcoin address.
I have been developing these plans for quite an extended period of time; so, don't expect any mistake from my side.

If, get to know that you tried to send this message to anyone else, I will distribute your video as described earlier.

Prevention

So how can one prevent being blackmail scammed? There are several key points to remember if you receive an email like this. It can be scary, but you're not actually in any danger!

The first thing to remember is that the "sent from your own email" part of the scam is *just a trick.* The protocol used for email allows a sender to set any "from" address that they want, it doesn't have to be the actual email account it came from. Even if I send an email from a server with an account called serverx@y.net , I can set the "from" field to something like "noreply@y.net" instead. This is how most "noreply" emails you get from companies work. There's no actual "noreply@y.net" email account to reply to, it's simply a placeholder in the from field. Scammers take advantage of this by setting the "from" field in their blackmail emails to *your email.* If you don't know this fact about how email works, you *think* this is an indication that the scammer has compromised your account, but they really haven't.

The second thing to understand is that scammers use basic human threats to intimidate you, aka *social engineering.* Nobody likes to be embarrassed or afraid, and so scammers rely on fear to get you to act irrationally. If you're afraid, you're less likely to realize you're being tricked, and you're more likely to send the scammers money! The important thing to realize is that all of the threats *are not real.* If a scammer truly had complete access to your device, they likely would not need to blackmail you to get money from you. They could steal your account passwords, your credit card info, your cryptocurrency wallets (if you're not storing seeds properly), or some other easier means of stealing. Blackmailing you is actually more work for the thief if they *truly* had access to your devices.

Seeing Past the Threats

But since scammers don't actually have anything, they simply send you an email with a threat. Remember, *anyone can send an email to anyone*. And, *anyone can set the "from" field of the email to anything they want.* Scammers are relying on fear and time pressure, both of which are classic social engineering tactics. They hope you'll be scared enough to send them cryptocurrency, which is an *irreversible* form of payment. However, you don't have to send them anything! They don't really have access to your email, your device, or any private information about you. It's all a trick using simple, mass email tools and social engineering.

Simply delete the email and move on, or read it, learn, and create educational materials warning others of this common scam – haha!