(Approx. 1006 words)

The Anatomy of a Scam: Ransom for My Files

By Kurt Jefferson, Editor, Central Kentucky Computer Society

https://www.ckcs.org

lextown2 (at) gmail.com

In mid–February, I checked my Gmail account as I do several times a day. Lurking in my Junk folder was a mysterious email message that appeared to come from Germany.

The email address used to send the message might be stolen or forged. But the subject is clear:

Payment for your account.

This is a new form of what’s called “ransomware.” It used to be that criminals would install software on a user’s computer and encrypt all the files – basically locking them so the user can’t read them. The victim would get his or her data back after meeting ransom demands.

Hospitals and other health care facilities have been targeted in recent years, and these attacks have escalated.

Now scammers are sending emails containing ransom demands – even without installing any software.

That is the gist of the email I received in my Gmail account. So, it appeared on both my Macs and iPad.

I’m sharing the message with readers of this newsletter to alert you – should you receive a similar threat.

Payment for your account

Feb. 17, 2021 at 4:33 P.M.

From: webmaster@dreirad\*\*\*\*\*\*\*.de

To: Kurt

Greetings!

I have to share bad news with you. Approximately few months ago I have gained

access to your devices, which you use for internet browsing.

After that, I have started tracking your internet activities.

Here is the sequence of events:

Some time ago I have purchased access to email accounts from hackers (nowadays, it is quite simple to purchase such thing online).

Obviously, I have easily managed to log in to your email account [email account name deleted].

Obviously, I have easily managed to log in to your email account [email account name deleted].

One week later, I have already installed a Trojan virus to Operating Systems of all the devices that you use to access your email.

In fact, it was not really hard at all (since you were following the links from your inbox emails). All ingenious is simple. =)

This software provides me with access to all the controllers of your devices (e.g., your microphone, video camera and keyboard).

I have downloaded all your information, data, photos, web browsing history to my servers.

I have access to all your messengers, social networks, emails, chat history and contacts list.

My virus continuously refreshes the signatures (it is driver-based), and hence remains invisible for antivirus software.

Likewise, I guess by now you understand why I have stayed undetected until this letter…

While gathering information about you, I have discovered that you are a big fan of adult websites.

You really love visiting porn websites and watching exciting videos, while enduring an enormous amount of pleasure.

Well, I have managed to record a number of your dirty scenes and montaged a few videos…

If you have doubts, I can make a few clicks of my mouse and all your videos will be shared to your friends, colleagues and relatives.

I have also no issue at all to make them available for public access.

I guess, you really don't want that to happen, considering the specificity of the videos you like to watch, (you perfectly know what I mean) it will cause a true catastrophe for you.

Let's settle it this way:

You transfer $950 USD to me (in bitcoin equivalent according to the exchange rate at the moment of funds transfer), and once the transfer is received, I will delete all this dirty stuff right away.

After that we will forget about each other. I also promise to deactivate and delete all the harmful software from your devices. Trust me, I keep my word.

This is a fair deal and the price is quite low, considering that I have been checking out your profile and traffic for some time by now.

In case, if you don't know how to purchase and transfer the bitcoins - you can use any modern search engine.

Here is my bitcoin wallet: (Bitcoin wallet deleted)

You have less than 48 hours from the moment you

opened this email (precisely 2 days).

Things you need to avoid from doing:

\*Do not reply me (I have created this email inside your inbox and generated the return address).

\*Do not try to contact police and other security services. In addition, forget about telling this to you friends. If I discover that (as you can see, it is really not so hard, considering that I control all your systems) - your video will be shared to public right away.

\*Don’t try to find me – it is absolutely pointless. All the cryptocurrency transactions are anonymous.

\*Don't try to reinstall the OS on your devices or throw them away. It is pointless as well, since all the videos have already been saved at remote servers.

Things you don't need to worry about:

• That I won't be able to receive your funds transfer.

• Don't worry, I will see it right away, once you complete the transfer, since I continuously track all your activities (my trojan virus has got a remote-control feature, something like TeamViewer).

• That I will share your videos anyway after you complete the funds transfer.

• Trust me, I have no point to continue creating troubles in your life. If I really wanted that, I would do it long time ago!

Everything will be done in a fair manner!

One more thing... Don't get caught in similar kind of situations anymore in future!

My advice - keep changing all your passwords on a frequent basis

\_\_\_\_\_\_\_\_

So there you have it. Obviously, I’m not about to pay a ransom. And my files have not been locked.

Hucksters are sending out these emails worldwide, hoping someone will be terrified and meet their demands. It makes the Nigerian email scams and pleas for help via email (please send money now – John or Mary has been hurt while visiting London or Paris or Sydney or Madrid or…) seem rather tame, doesn’t it?

