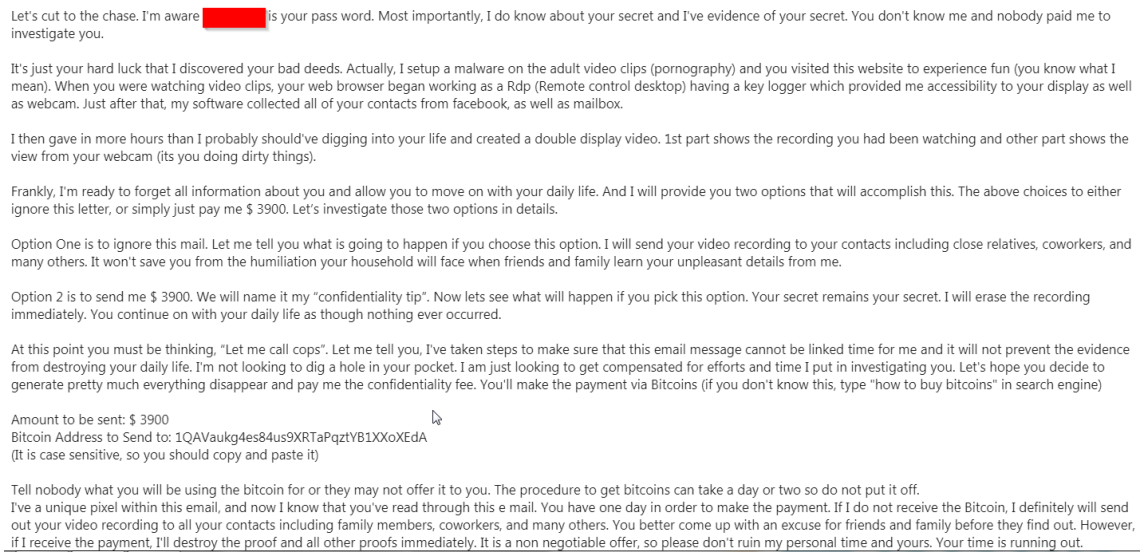
Nuevo Phishing con chantaje

Ya hemos hablado de otras campañas de Phishing muy presentes en la actualidad como la estafa del CEO (https://www.audea.com/es/fraude-del-ceo/) en el que interviene la confianza de los empleados o el fraude bancario en el que participan los llamados muleros (https://www.audea.com/es/los-muleros-bancarios/) en el que interviene además un fraude bancario.

Como se puede observar en este tipo de phishing intervienen otros factores que ayudan a que el ataque sea mucho mas completo, dirigido y exitoso, como el fraude bancario u otras técnicas.

Hoy vamos a hablar de un phishing que se apoya en otros factores como **una filtración de contraseñas y el chantaje a las personas**, podemos ver una imagen del mismo a continuación:



Let's cut to the chase. I'm aware [redacted] is your pass word. Most importantly, I do know about your secret and I've evidence of your secret. You don't know me and nobody paid me to investigate you.

It's just your hard luck that I discovered your bad deeds. Actually, I setup a malware on the adult video clips (pornography) and you visited this website to experience fun (you know what I mean). When you were watching video clips, your web browser began working as a Rdp (Remote control desktop) having a key logger which provided me accessibility to your display as well as webcam. Just after that, my software collected all of your contacts from facebook, as well as mailbox.

I then gave in more hours than I probably should've digging into your life and created a double display video. 1st part shows the recording you had been watching and other part shows the view from your webcam (its you doing dirty things).

Frankly, I'm ready to forget all information about you and allow you to move on with your daily life. And I will provide you two options that will accomplish this. The above choices to either ignore this letter, or simply just pay me $ 3900. Let's investigate those two options in details.

Option One is to ignore this mail. Let me tell you what is going to happen if you choose this option. I will send your video recording to your contacts including close relatives, coworkers, and many others. It won't save you from the humiliation your household will face when friends and family learn your unpleasant details from me.

Option 2 is to send me $ 3900. We will name it my "confidentiality tip". Now lets see what will happen if you pick this option. Your secret remains your secret. I will erase the recording immediately. You continue on with your daily life as though nothing ever occurred.

At this point you must be thinking, "Let me call cops". Let me tell you, I've taken steps to make sure that this email message cannot be linked time for me and it will not prevent the evidence from destroying your daily life. I'm not looking to dig a hole in your pocket. I am just looking to get compensated for efforts and time I put in investigating you. Let's hope you decide to generate pretty much everything disappear and pay me the confidentiality fee. You'll make the payment via Bitcoins (if you don't know this, type "how to buy bitcoins" in search engine)

Amount to be sent: $ 3900
Bitcoin Address to Send to: 1QAVaukg4es84us9XRTaPqztYB1XXoXEdA
(It is case sensitive, so you should copy and paste it)

Tell nobody what you will be using the bitcoin for or they may not offer it to you. The procedure to get bitcoins can take a day or two so do not put it off.
I've a unique pixel within this email, and now I know that you've read through this e mail. You have one day in order to make the payment. If I do not receive the Bitcoin, I definitely will send out your video recording to all your contacts including family members, coworkers, and many others. You better come up with an excuse for friends and family before they find out. However, if I receive the payment, I'll destroy the proof and all other proofs immediately. It is a non negotiable offer, so please don't ruin my personal time and yours. Your time is running out.

En el mismo lo primero que nos llama la atención es que es verdad que tiene una de las contraseñas que solemos utilizar, lo que aparece sombreado en realidad es una contraseña real del destinatario que previsiblemente pueda reconocer a que lugar accedemos con la misma.

El hecho de que tengan nuestra contraseña esta directamente relacionado con alguna de las filtraciones de contraseñas que últimamente han existido, sin hacer ninguna mención especial, alguna con un gran número de cuentas de usuarios comprometidos y alguna de las páginas de gran prestigio (todos estos datos la verdad que llegan a asustar).

Haciendo un inciso en este momento del artículo existen páginas que informan al usuario de si su dirección de correo está comprometida, algunas con otro tipo de fines por lo que debemos de tener cuidado con la información que introducimos en las mismas.

Por ejemplo, en la página https://haveibeenpwned.com/ se nos informa de ello y nos indica en qué filtración debemos de prestar especial atención para tomar medidas inmediatas.

De todos modos, aunque se haya puesto el ejemplo anterior de la página, nunca aconsejamos introducir ningún tipo de dato personal en ninguna página que no sea de total confianza ya que podemos duplicar el riesgo inicial que habíamos comentado.

Volviendo al correo visto en la imagen, se hace referencia al **chantaje alegando que tiene contenido comprometido nuestro que van a difundir** entre todos nuestros contactos.

Con este hecho nos dan dos opciones, primero nos chantajean para proceder a su borrado por una cantidad de dinero o en caso contrario lo difundirán de manera inmediata (nos dan el plazo de un día).

Además, este dinero solicitado es **en bitcoins** (en esta artículo hablamos un poco más técnicamente de esta criptomoneda: https://www.audea.com/es/criptomonedas-bitcoin-funcionamiento/) y, de esta forma, la transferencia de la "recompensa" no dejara ningún rastro.

Una de las características que tienen las cuentas en bitcoin, es que cualquier usuario que pertenezca a la red puede ver la cantidad de dinero que tiene una cartera y se ha podido discernir que la que aparece en el mail solicitando el dinero sube exponencialmente.

Por todo lo comentado, tenemos que seguir concienciados ante este tipo de ataques y si hemos recibido este correo o cualquiera de una índole similar deberemos eliminarlo de inmediato y proceder a cambiar las contraseñas de manera inmediata de todos los portales o redes sociales que tengamos e independientemente realizar esta acción periódicamente.

Fernando Saavedra

Cybersecurity Manager

Áudea Seguridad de la Información