| | |
|---|---|
| Alerta de seguridad informática | 8FPH20-00113-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing - Sextorsion |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 14 de Febrero de 2020 |
| Última revisión | 14 de Febrero de 2020 |

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los IoC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los IoC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Estos casos de phishing no involucran directamente a las entidades ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma el mencionado phishing, para construir el engaño. Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño.

## Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing a través de un correo electrónico que intenta extorsionar a un usuario.

El mensaje informa a la víctima que un atacante ha logrado acceder a su sistema y a las cuentas del usuario. La intromisión, perpetrada hace meses atrás, se habría producido cuando la víctima supuestamente visitó un sitio para adultos, oportunidad en la cual el equipo fue infectado con un malware. Este malware habría permitido al atacante acceder a la pantalla, cámara, micrófono, correspondencia y a los contactos del usuario afectado. El atacante amenaza al usuario indicándole que compartirá un video comprometedor de la víctima a sus contactos. Para evitar esta situación, la víctima debe transferir $594 dólares a la dirección de bitcoin del hacker.

## Observación

Este tipo de amenazas son comunes en internet. Los temas de extorsión van desde: cuentas hackeadas; peticiones de dinero por motivos altruistas como construcción de hospitales, enfermedades terminales; negocios supuestamente muy beneficiosos para el usuario, entre otros; Todos tienen el factor común que solicitan depositar sumas de dinero significativas. Además el mensaje suele estar en distintos idiomas.

Este tipo de campaña llega continuamente y de forma masiva a casillas de correo a nivel global. El objetivo principal es amedrantar al usuario con información falsa. En campañas masivas es improbable que el atacante hay tenido acceso a los dispositivos electrónicos. Por este motivo, se advierte a los usuarios que reciban este tipo de correos, no dejarse persuadir por el atacante para depositar dinero en las cuentas indicadas.

Como recomendación siempre se debe validar la identidad del usuario que envía el correo, si realmente es quien dice ser y si el proyecto o idea que intenta traspasar es real. Finalmente como consejo "dudar de todo lo que parece ser muy bueno".

## Indicadores de compromisos

### Sender

Anacker[@]vicentecostanera[.]cl
anacker[@]t-com[.]sk
hackeron[@]sitel[.]com[.]ua
anacker[@]stonline[.]sk

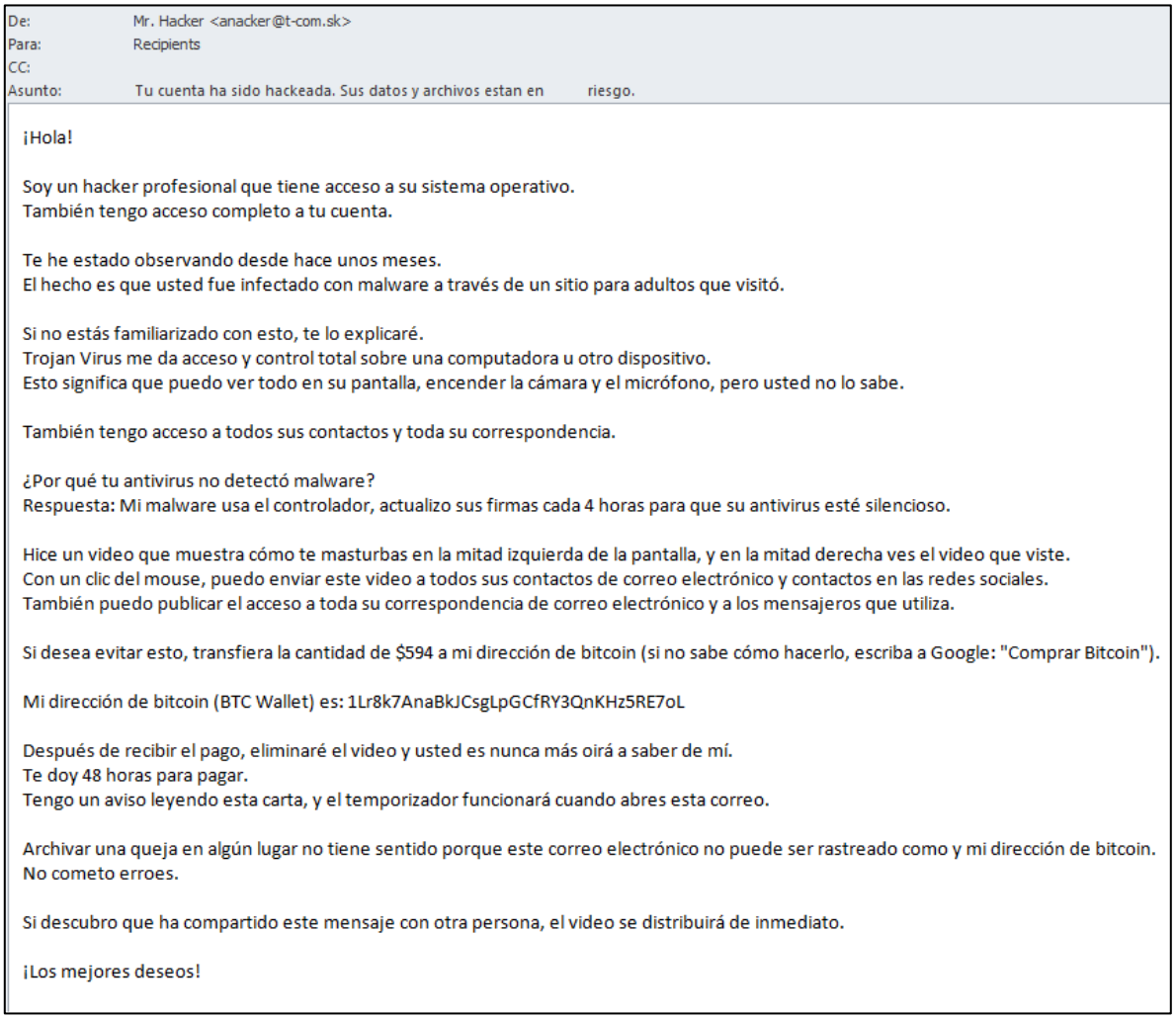
### Smtp Host

[194.126.106.86]
[194.126.106.78]
[194.126.106.70]
[194.150.66.176]
[194.150.66.175]

### Subject

Tu cuenta ha sido hackeada. Sus datos y archivos están en riesgo.

Imagen del correo



De: Mr. Hacker <anacker@t-com.sk>
Para: Recipients
CC:
Asunto: Tu cuenta ha sido hackeada. Sus datos y archivos estan en riesgo.

¡Hola!

Soy un hacker profesional que tiene acceso a su sistema operativo.
También tengo acceso completo a tu cuenta.

Te he estado observando desde hace unos meses.
El hecho es que usted fue infectado con malware a través de un sitio para adultos que visitó.

Si no estás familiarizado con esto, te lo explicaré.
Trojan Virus me da acceso y control total sobre una computadora u otro dispositivo.
Esto significa que puedo ver todo en su pantalla, encender la cámara y el micrófono, pero usted no lo sabe.

También tengo acceso a todos sus contactos y toda su correspondencia.

¿Por qué tu antivirus no detectó malware?
Respuesta: Mi malware usa el controlador, actualizo sus firmas cada 4 horas para que su antivirus esté silencioso.

Hice un video que muestra cómo te masturbas en la mitad izquierda de la pantalla, y en la mitad derecha ves el video que viste.
Con un clic del mouse, puedo enviar este video a todos sus contactos de correo electrónico y contactos en las redes sociales.
También puedo publicar el acceso a toda su correspondencia de correo electrónico y a los mensajeros que utiliza.

Si desea evitar esto, transfiera la cantidad de $594 a mi dirección de bitcoin (si no sabe cómo hacerlo, escriba a Google: "Comprar Bitcoin").

Mi dirección de bitcoin (BTC Wallet) es: 1Lr8k7AnaBkJCsgLpGCfRY3QnKHz5RE7oL

Después de recibir el pago, eliminaré el video y usted es nunca más oirá a saber de mí.
Te doy 48 horas para pagar.
Tengo un aviso leyendo esta carta, y el temporizador funcionará cuando abres esta correo.

Archivar una queja en algún lugar no tiene sentido porque este correo electrónico no puede ser rastreado como y mi dirección de bitcoin.
No cometo erroes.

Si descubro que ha compartido este mensaje con otra persona, el video se distribuirá de inmediato.

¡Los mejores deseos!

## Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras)
- Evaluar el bloqueo preventivo de los indicadores de compromisos
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas
- Revisar los controles de seguridad de los AntiSpam y SandBoxing
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas
- Visualizar los sitios web que se ingresen que sean los oficiales
- No confiar en remitentes desconocidos

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.02.14 13:06:30 -03'00'