BOLETÍN DE NOTICIAS Y NOVEDADES DE

SEGURIDAD INFORMÁTICA

!ENTERATE! Nuevo Malware roba 26 millones de credenciales de ordenadores Windows

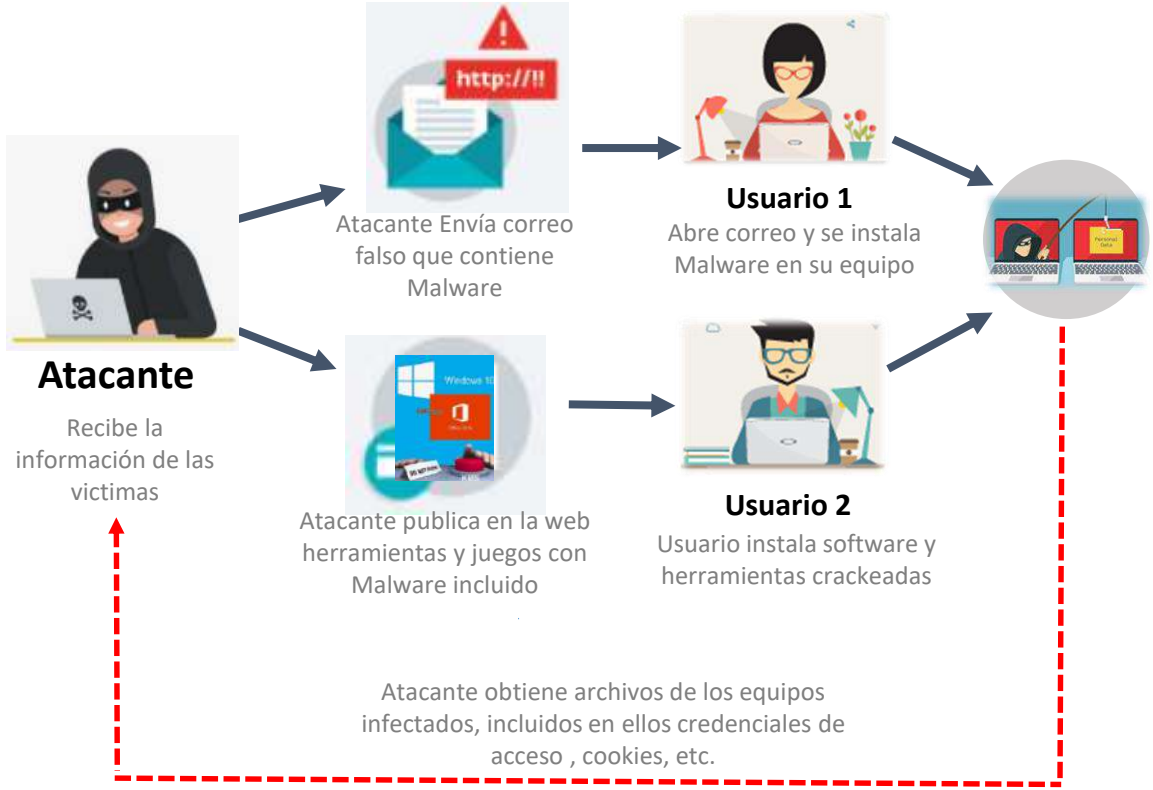


Imagen 1. Descripción del ataque

Investigadores descubrieron recientemente un malware sin nombre que ha sido utilizado para robar 1.2 TB de información de ordenadores de Windows a nivel mundial entre 2018 y 2020 los cuales incluyen 1 millón de direcciones de correo, más de 2 billones de cookies y 6.6 millones de archivos.

A pesar de ello, los atacantes dieron a conocer por error el lugar donde almacenaban la base de datos, lo que hizo que fuese posible avisar al proveedor de hosting y que la información se eliminara.

Sin embargo, es casi imposible recuperar el control de la información luego de ser filtrada. Se recomienda utilicen métodos seguros de almacenamiento de claves y otro tipo de información sensible y, por último, que en la medida de lo posible utilicen software que ayuden en la detección de este troyano.

Tomado y adaptado de https://unaaldia.hispasec.com/2021/06/nuevo-malware-roba-26-millones-de-credenciales-de-millones-de-ordenadores.html

BOLETÍN DE NOTICIAS Y NOVEDADES DE

SEGURIDAD INFORMÁTICA

¡ALERTA! PHISHING circulando en la Red

Se encuentra circulando falso correo a través de la red, en el cual se informa sobre una suspensión de cuenta de Outlook, por favor hacer caso omiso a este comunicado ya que corresponde a un caso de Phishing en el que se busca robar los datos personales de los usuarios. Se recomienda bloquear el remitente y eliminar el mensaje.

De: Daniela Aponte Villamil <dra_danielaav@hotmail.com>
Fecha: 19 de junio de 2021 a las 13:40:03 COT
Para: communications_msn_cs_esxlu@outlook.es
Asunto: Alerta - Caso B-883454278912

Outlook.com

Estimado usuario debido a cambios reciente en nuestra plataforma es necesario que confirme su cuenta de lo contrario será suspendida en las próximas **72Horas, Términos y Condiciones** de uso. Este cambio fue realizado pensando en la seguridad y bienestar de nuestros usuarios. Agregamos nuevos parámetros de seguridad al ingreso a nuestros servidores, **Hotmail, Outlook, Live y MSN**.

Esta condición no suprime la cuenta de nuestros servidores inmediatamente, todos los usuarios tendrán un plazo de **3** días para confirmar su cuenta en nuestra plataforma. Durante estos dos días usted podrá enviar y recibir mensajes normalmente, ya pasado este lapso su cuenta quedará permanentemente borrada de nuestros servidores.

Cuenta Microsoft

CONFIRMAR SU CUENTA

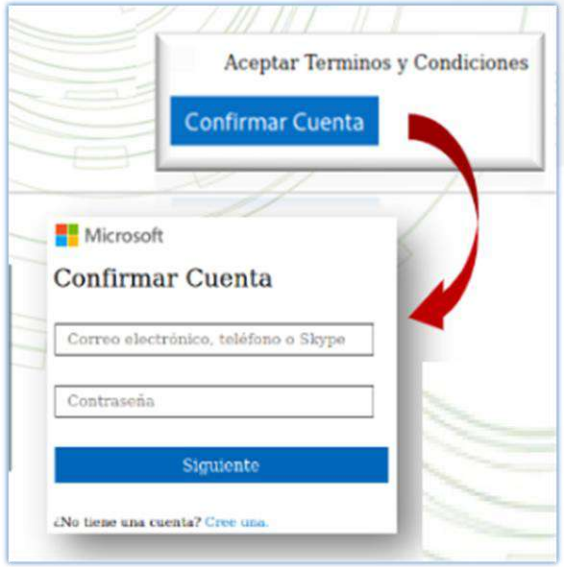
Dirige al siguiente link https[:]//i.gal/cqhOy, posteriormente al link http[:]//procolosdesistemas-com.preview-domain.com/Cargando....html

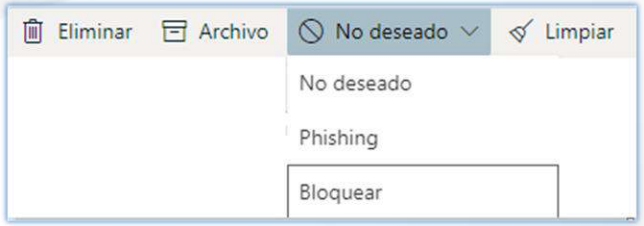
El sistema le pedirá crear una clave adicional a la contraseña de su cuenta la cual deberá ser una clave de 4 dígitos solo numérica, fácil de recordar ya que se le pedirá cada vez que inicie en un nuevo dispositivo.

Este mensaje es un mensaje emitido por nuestro sistema.

Atentamente.
Windows Live Outlook®
Microsoft

Imagen 2. Correo de suplantación Outlook





Nota: En la opción (No deseado) en office 365 puede clasificar un correo como No deseado, Phishing o Bloquear remitente.

Tomado y adaptado de: https://cc-csirt.policia.gov.co/

BOLETÍN DE NOTICIAS Y NOVEDADES DE

SEGURIDAD INFORMÁTICA

¡ALERTA! PHISHING circulando en la Red

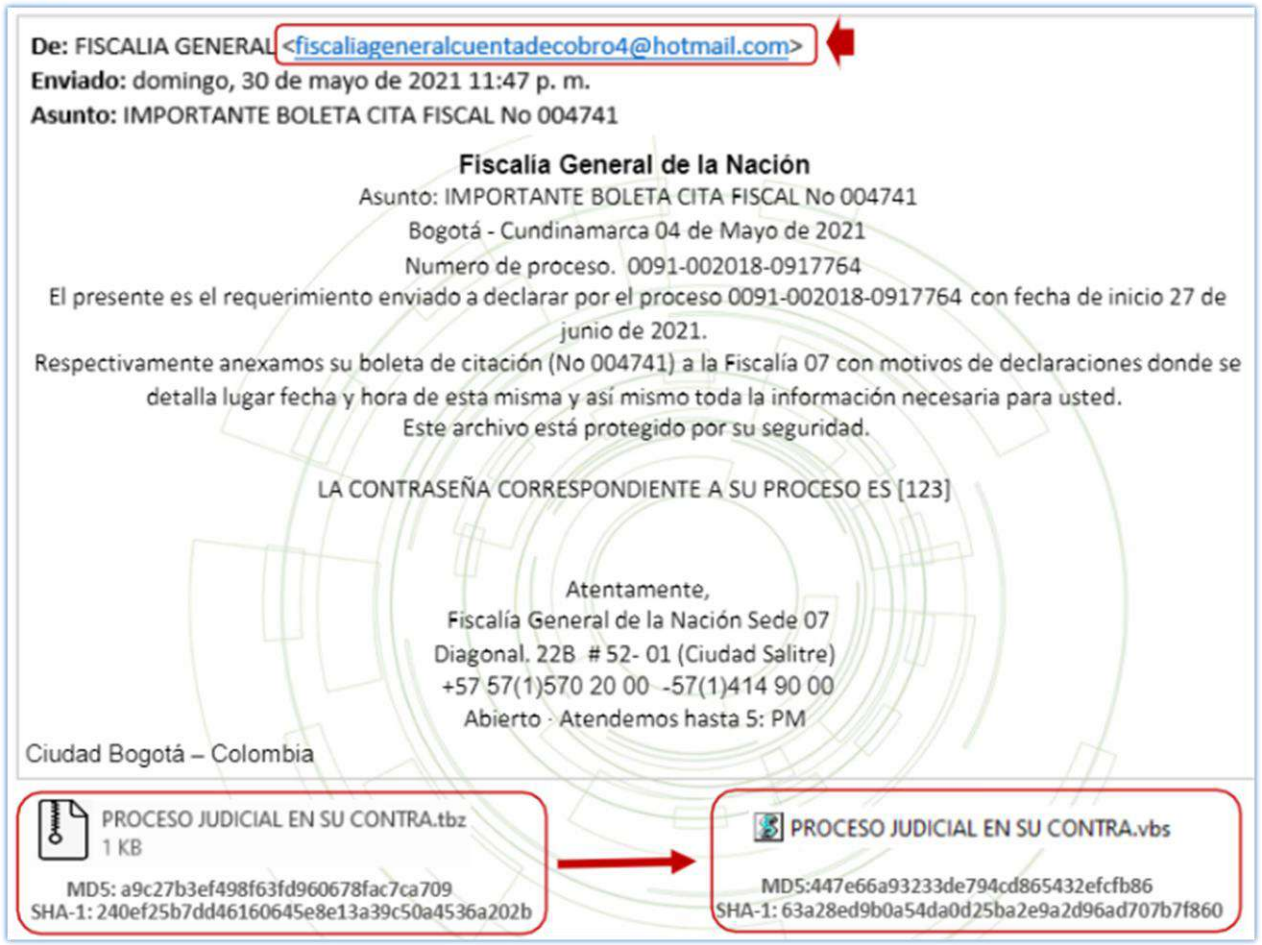


Imagen 3. Correo de suplantación Fiscalía General de la Nación

Falso correo electrónico circula en la red informando sobre una supuesta notificación realizada por parte de la Fiscalía General de la Nación en el cual utilizan un remitente con cuenta de correo de Hotmail (fiscaliageneralcuentadecobro4@Hotmail.com)

Dicho correo contiene documentos adjuntos comprometidos con Malware, si recibe este tipo de mensaje, Se recomienda revisar el remitente el cual debe corresponder a una cuenta oficial de la Entidad, de lo contrario no descargue archivos adjuntos y repórtelo al área de Seguridad Informática para bloquear el remitente y por ultimo elimínelo de su bandeja de entrada y papelera.

Tomado y adaptado de: https://cc-csirt.policia.gov.co/

BOLETÍN DE NOTICIAS Y NOVEDADES DE

SEGURIDAD INFORMÁTICA

¡ENTERATE! ¿Sabes cuanto pueden valer tus datos personales en la Dark Web?

Imagen 4. Dark Web

Tomar una la selfie del dedo pulgar o la “V” de la victoria no es suficiente, ya que a menudo las personas publican en redes sociales la foto del pasaporte, la identificación oficial o, incluso, el carné del empleado, en el afán por compartir la alegría de un viaje, la emoción de haber votado en un proceso electoral o de presumir la primera licencia de conducir, o de estar estrenando empleo.

La publicación de ciertas imágenes conlleva a riesgos. Una investigación de Kaspersky comprobó cuánto se paga por una selfie de documentos que sirve para falsificar identidades y reveló que documentos de identidad, como licencias de conducir y pasaportes, pueden llegar a comercializasen en la dark web por entre US$0.50 centavos de dólar hasta los US$25 dólares. Una selfie con documentos puede encontrarse desde los US$40 hasta los US$60 dólares.

Tomado y adaptado de: https://www.valoraanalitik.com/2021/06/21/cuanto-valen-sus-datos-personales-en-el-mercado-dark-web/

BOLETÍN DE NOTICIAS Y NOVEDADES DE

SEGURIDAD INFORMÁTICA

¡ALERTA! Para evitar que se comprometa su privacidad en las selfies y post que publica, se recomienda:

- Minimice la exposición de sus datos biométricos en Internet. Por ejemplo, si va a subir tu selfie con el “pulgar hacia arriba” o la “V” de la victoria, cuide que sea a una distancia considerable.
- Abstenerse de publicar imágenes de documentos oficiales. Estos a menudo incluyen un número de registro, su firma y datos personales que pueden facilitar la suplantación de identidad.
- Sea consciente de la información personal que comparte en línea. Recuerde que todo lo que sube al Internet corre el riesgo de caer en manos equivocadas y/o puede utilizarse para cometer delitos.
- Compruebe siempre la configuración de los permisos de las aplicaciones que utiliza. Esto minimizará la probabilidad de que sus datos sean compartidos o almacenados por terceros y otros sin tu conocimiento.
- Verifique qué servicios están conectados a sus cuentas en línea y quién tiene acceso a ellos. Puede averiguar cómo cambiar la configuración de privacidad en los servicios en línea, incluyendo redes sociales, y tomar el control de tus datos personales.

Tomado y adaptado de: https://www.valoraanalitik.com/2021/06/21/cuanto-valen-sus-datos-personales-en-el-mercado-dark-web//