Cibercriminales están robando datos de Gmail por medio de Chrome y Microsoft Edge

29/03/2023

Un grupo de **ciberdelincuentes** está utilizando una extensión compatible con los navegadores de **Google Chrome**, **Microsoft Edge** y **Brave** para robar información de correos electrónicos, según los reportes de instituciones de los gobiernos de Alemania y Corea del Sur.

Según la Oficina Federal Alemana para la Protección de la Constitución (BfV) y el Servicio Nacional de Inteligencia de la República de Corea del Sur (NIS), identificó el programa al que se refieren con el nombre "**AF**", estaría centrada en una operación de **espionaje** a la que podrían ser vulnerables algunos oficiales de alto rango en diferentes gobiernos del mundo.

Según el documento, este tipo de personas serían los objetivos principales de estos ataques.

Cómo funciona la extensión "AF"

El **ciberataque** empieza como un correo electrónico de **phishing** que llega a la bandeja de entrada con vínculos maliciosos que redirigen a los usuarios a sitios web donde son impulsados a descargar e instalar extensiones para sus

navegadores.

Luego de finalizar ese proceso, la víctima podría iniciar su sesión en el servicio de **Gmail**, lo que detonaría la activación de la extensión maliciosa, cuya misión es robar todo el contenido disponible en los **correos electrónicos** y enviarlos a un lugar seguro al que solo tiene acceso el cibercriminal y sus cómplices.

Los cibercriminales podrían tomar el control de la tienda de Android para instalar aplicaciones maliciosas en los celulares de sus víctimas.

Esta metodología para ejecutar **ciberataques** puede dirigirse a los celulares pues se pueden instalar **aplicaciones** de forma remota en estos dispositivos.

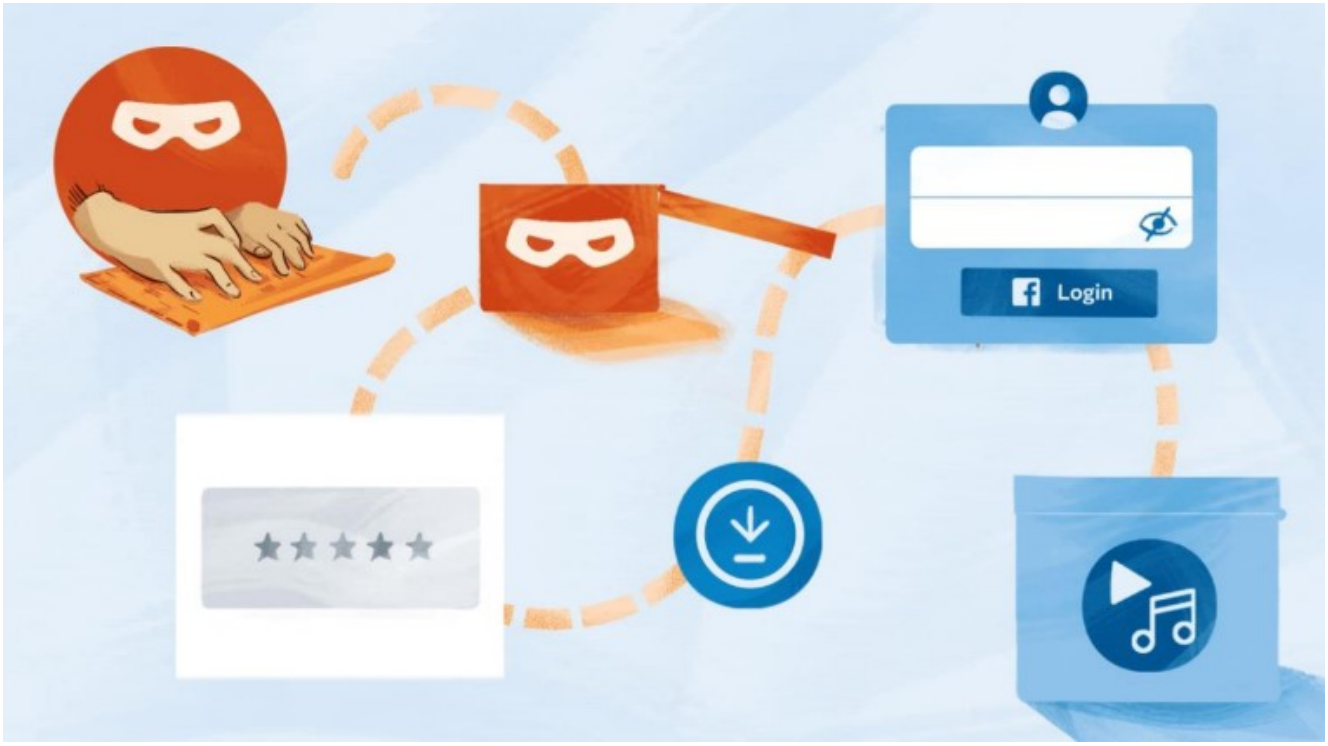
Los criminales inician su intervención por medio de un correo

electrónico de **phishing** que tiene acceso a las funciones de **Google Play Store** como la sincronización de dispositivos.

Al ejecutarse esta función, el ciberdelincuente indicará al sistema de la tienda de aplicaciones que se instalará un programa adicional, pero que en realidad se trata de un **software malicioso** que tiene un objetivo similar al ejemplo mencionado previamente: robar los datos del dispositivo y del correo electrónico.

Los usuarios podrían no darse cuenta de la **instalación** de estos nuevos programas en sus dispositivos debido a que estas tareas son ejecutadas en segundo plano y no están disponibles a no ser que se busque en el sistema del celular.

Es por ello que las instituciones encargadas de la realización del reporte indican que es adecuado ejecutar una revisión a fondo de las **aplicaciones** presentes en el celular para corroborar que se conoce a todas las que forman parte de la lista.



Las aplicaciones maliciosas suelen estar dirigidas al robo sistemático de la información contenida en un dispositivo. Su instalación puede ser accidental por parte del usuario o

provocada por un cibercriminal. (Meta)

Si bien esta modalidad de ciberataque estaría dedicada a extraer **información** sensible de algunas autoridades, no es poco probable que pueda utilizarse como parte de una campaña de ciberataques con el potencial de afectar a más personas.

Medidas de prevención

Es por ello que para prevenir estas vulneraciones a la **seguridad** y **privacidad** de las cuentas, se recomienda seguir algunas o todas las opciones:

– Verificar minuciosamente que la **página web** a la que se ha ingresado por medio de un link enviado por correo. Las que son promovidas por cibercriminales pueden presentar algunas diferencias como mala ortografía o el reemplazo de unas letras por otras para confundir a los usuarios (goog1e en vez de google).

– También se recomienda la activación de un método de **verificación** de la identidad. Esta puede ser por medio de **SMS** (aunque no es del todo seguro porque las aplicaciones maliciosas también podrían acceder a los textos enviados), además de usar una aplicación de autenticación como Google Authenticator, que emite claves dinámicas para validar que el acceso al dispositivo o una plataforma en específico.

– En el caso de la instalación de **aplicaciones**, es recomendable no hacerlo desde plataformas no seguras o de dudosa credibilidad. Estas podrían ser en realidad **softwares** maliciosos.

Fuente: Infobae