El software malicioso que roba datos está activamente empleando un punto de acceso no especificado de Google OAuth llamado MultiLogin para apoderarse de las sesiones de los usuarios y permitir un acceso ininterrumpido a los servicios de Google incluso tras un cambio de contraseña.

De acuerdo con los informes de CloudSEK, esta vulnerabilidad crítica permite mantener la sesión activa y crear cookies de forma no autorizada, dando a los delincuentes cibernéticos la capacidad de seguir utilizando una sesión válida.

Un individuo identificado como PRISMA fue el primero en divulgar esta técnica el 20 de octubre de 2023, a través de su canal en Telegram. Desde ese momento, se ha integrado en diferentes programas maliciosos como Lumma, Rhadamanthys, Stealc, Meduza, RisePro y WhiteSnake.

La función MultiLogin está principalmente diseñada para coordinar cuentas de Google entre diferentes plataformas cuando los usuarios inician sesión en sus cuentas usando el navegador Chrome, es decir, sus perfiles.

> Un examen detallado del código de Lumma Stealer indica que la táctica se enfoca en la *«tabla token_service de WebData de Chrome para obtener tokens e identificadores de cuentas de los perfiles de Chrome activos. Dicha tabla tiene dos componentes esenciales: el servicio (conocido como ID GAIA) y encrypted_token»,* según Pavan Karthick M, un especialista en seguridad.

Posteriormente, esta combinación de token e ID GAIA se utiliza con el punto de acceso MultiLogin para recrear las cookies de autenticación de Google.

```
foreach (string file in Directory.GetFiles(dirPath, "tokens.txt", SearchOption.AllDirectories))
{
    string[] tokens = File.ReadAllLines(file);
    foreach (string token in tokens)
    {
        bool flag = token == "";
        if (!flag)
        {
            HttpRequest req = new HttpRequest();
            req.IgnoreProtocolErrors = true;
            req.AddHeader("Accept", "*/*");
            req.AddHeader("User-Agent", "com.google.Drive/6.0.230903 iSL/3.4 iPhone/15.7.4 hw/iPhone9_4 (gzip)");
            req.AddHeader("Authorization", "MultiBearer " + token);
            req.AddHeader("Accept-Language", "en-US,en;q=0.9");
            req.AddHeader("Content-Type", "application/x-www-form-urlencoded");
            try
            {
                string resp = req.Post("https://accounts.google.com/oauth/multilogin", new StringContent
                  ("source=com.google.Drive")).ToString();
```

Folder with all Token:GAIA Id Pairs

Endpoint which is exploited

Karthick comentó que se experimentaron tres situaciones distintas con respecto a la generación de tokens y cookies:

1. Si el usuario está activo en el navegador, el token puede ser empleado repetidamente.
2. Si el usuario modifica su contraseña pero mantiene la sesión con Google, el token tiene un uso único, dado que ya se empleó para mantener la sesión activa.
3. Al cerrar la sesión en el navegador, el token se invalida y se elimina del almacenamiento local, aunque se regenerará al iniciar sesión de nuevo.

Al preguntar a Google sobre este tema, la compañía reconoció el método de ataque pero destacó que los usuarios pueden eliminar las sesiones comprometidas al cerrar sesión en el navegador afectado.

> *«Google está al tanto de las noticias recientes sobre un software malicioso que captura tokens de sesión. Los ataques que se basan en el robo de cookies y tokens no son algo novedoso; constantemente reforzamos nuestras medidas de seguridad frente a estas tácticas y protegemos a los usuarios afectados por software malintencionado. En este contexto, Google ha implementado acciones para proteger las cuentas que identificamos como comprometidas»*, informó la empresa.

> *«Es crucial desmentir un error en ciertos informes que sugiere que los tokens y cookies capturados no pueden ser anulados por el usuario. Esta afirmación es errónea, ya que las sesiones afectadas pueden ser canceladas simplemente cerrando la sesión en el navegador perturbado o, de manera remota, a través de la configuración de dispositivos del usuario. Mantendremos un seguimiento continuo y ofreceremos información adicional según sea necesario»*, agregó.

Adicionalmente, la firma instó a los usuarios a activar la opción de Navegación Segura Mejorada en Chrome para prevenir el phishing y descargas de programas maliciosos.

> *«Para evitar que los delincuentes utilicen los mecanismos de recuperación de contraseña para acceder a cuentas, se recomienda cambiar las contraseñas. Es esencial que los usuarios supervisen las actividades sospechosas en sus cuentas, especialmente aquellas provenientes de direcciones IP y lugares desconocidos»*, indicó Karthick.

Alon Gal, cofundador y director tecnológico de Hudson Rock, destacó la claridad de Google sobre este asunto, recordando que había compartido detalles sobre esta vulnerabilidad el año anterior.

> *«A pesar de las medidas adoptadas por Google, este incidente revela la existencia de un método avanzado para comprometer cuentas. Aunque las acciones de Google son efectivas, este caso subraya la demanda de estrategias de seguridad más sofisticadas para enfrentar amenazas digitales en constante evolución, como los programas de robo de información que hoy en día son muy populares entre los ciberdelincuentes».*