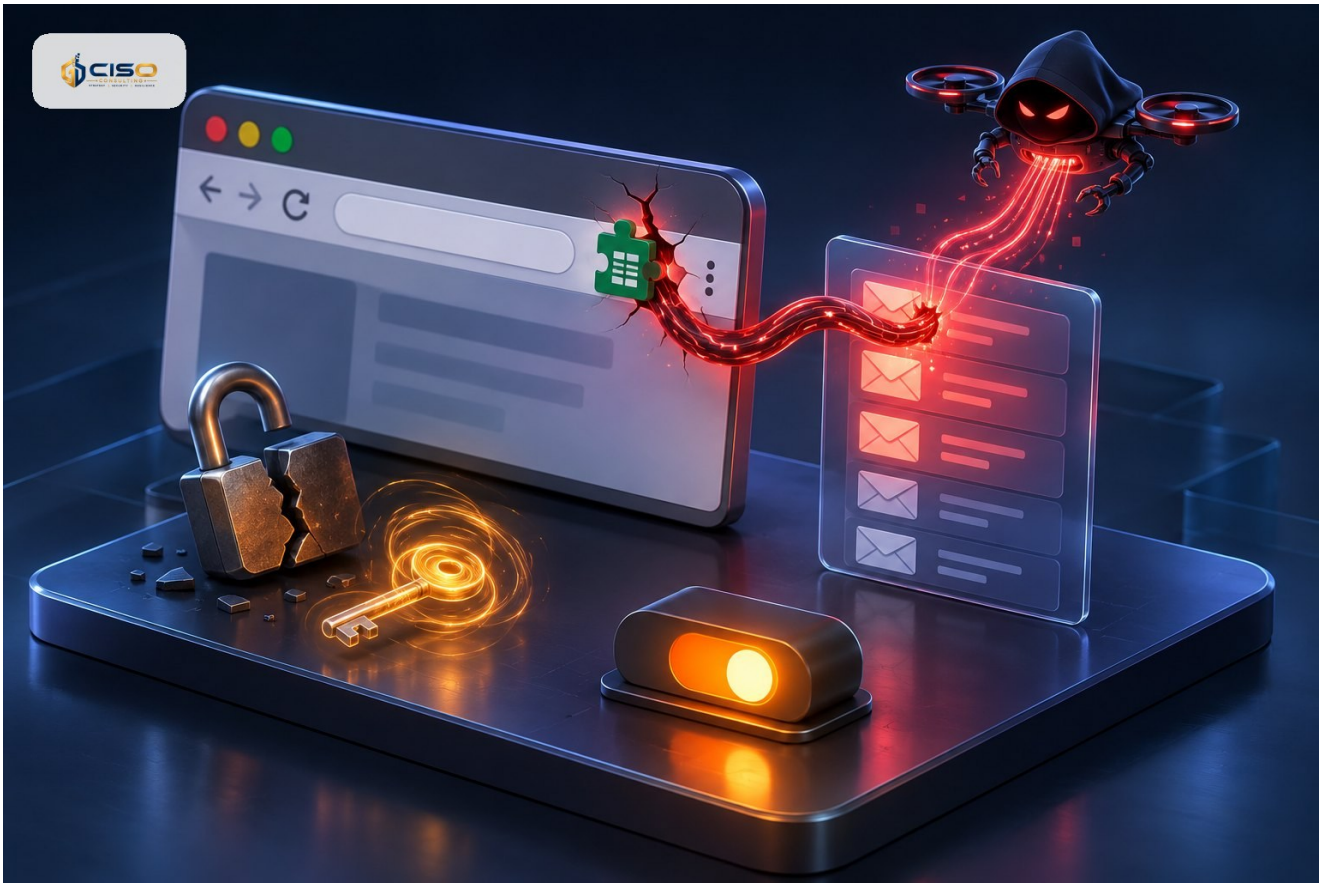
برمجية Remus تسرق رسائل Gmail عبر إضافة Chrome مزيفة باسم Google Sheets



تبيّن أن ما روّجت له Remus كثغرة «يوم الصفر» في Gmail هو إضافة Chrome خبيثة تواصل قراءة الرسائل غير المقروءة بعد تغيير كلمة المرور. يُنصح بمراجعة الإضافات ووضع المطوّر.

- روّج مشغّلو Remus منذ 8 نوفمبر لثغرة يوم صفر في Gmail، وتبيّن أنها إضافة Chrome خبيثة لا ثغرة لدى Google.
- تبقى الإضافة بعد تغيير كلمة المرور وإلغاء الجلسات لأنها مثبتة في المتصفح، ولا تصل إلى البريد إلا أثناء تسجيل دخول المستخدم.
- تتخفى باسم «Google Sheets» وتنسخ وصف Google Docs Offline وتطلب الوصول إلى جميع المواقع.
- تفحص الرسائل غير المقروءة كل دقيقة عبر ما يصل إلى 10 حسابات، وترسل العنوان والنص والمرسل وعنوان الضحية إلى خادم التحكم.

- تعدّل Remus ملف تعريف Chrome وتفعّل وضع المطوّر لتجاوز إزالة خيار سطر الأوامر في الإصدار 137 وما بعده.

نشر باحثون من GenDigital وInvoke RE تحليلًا يشرح كيف تقرأ برمجية Remus الخبيثة لسرقة المعلومات رسائل Gmail. فقد بدأ مطوّرها في 8 نوفمبر الترويج لثغرة يوم صفر في Gmail، مدّعياً إمكان جمع الرسائل حتى بعد تغيير كلمات المرور وإلغاء الجلسات. وبحثت Hudson Rock الادعاء دون أن تتوصل إلى نتيجة حاسمة، ولم تجد دليلًا تقنياً على وجود ثغرة.

كيف تعمل الآلية

يفيد التحليل المستقل بأنه لا توجد ثغرة أصلًا. تُنزِّل البرمجية مكتبة DLL أصلية وظيفتها الوحيدة تثبيت إضافة خبيثة في Google Chrome، وهو المتصفح الوحيد المستهدف. وتأتي الإضافة مضمّنة داخل المكتبة في أرشيف ZIP غير مشفّر.

أزال Chrome في الإصدار 137 وما بعده خياراً في سطر الأوامر كانت البرمجيات الخبيثة تستخدمه لتحميل الإضافات. وتتجاوز Remus ذلك بتعديل ملف تعريف Chrome لدى الضحية لتسجيل الإضافة، ثم تفعيل «وضع المطوّر» الذي تتطلبه الإضافات غير المحزّمة.

تظهر الإضافة باسم «Google Sheets» وتنسخ وصف Google Docs Offline وتطلب الوصول إلى جميع المواقع. وبعد تشغيلها تفحص الرسائل غير المقروءة كل دقيقة عبر ما يصل إلى 10 حسابات وتجلبها كاملة، ثم ترسل العنوان والنص والمرسل وعنوان الضحية إلى خادم التحكم مع معرّف للحملة. وتُعاد محاولة الرفع الفاشل، ويمنع سجل محلي تكرار الإرسال.

ما يعنيه ذلك للمدافعين

لأن الإضافة تبقى في المتصفح، فإن تغيير كلمة المرور أو إلغاء الجلسات لا يزيلها. يتوقف وصولها عند انتهاء الجلسة ويعود عند تسجيل المستخدم دخوله مجدداً. لذا يجب أن تشمل الاستجابة لأي إصابة مشتبه بها تنظيف الجهاز لا إعادة تعيين بيانات الدخول فقط. وينصح المصدر بتنزيل البرامج من مصادر موثوقة فقط وفحص chrome://extensions بحثاً عن إضافات مشبوهة أو تفعيل غير متوقع لوضع المطوّر.

ما يجب فعله الآن

1. مراجعة إضافات Chrome على الأجهزة المُدارة وإزالة غير المعتمد منها، خاصة أي إضافة باسم «Google Sheets» لا تأتي من المتجر الرسمي.
2. رصد تفعيل «وضع المطوّر» في Chrome والتنبيه عليه، وتقييده عبر سياسات المتصفح حيثما أمكن.
3. عند الاشتباه باختراق حساب Gmail، تنظيف الجهاز أو إعادة بنائه إلى جانب تغيير كلمات المرور وإلغاء الجلسات.
4. حصر تثبيت البرامج في مصادر موثوقة ومعتمدة وتذكير الموظفين بعدم تنزيل أدوات من مواقع غير موثقة.
5. فحص حركة الاتصالات الصادرة من الأجهزة بحثاً عن اتصالات غير متوقعة قد تدل على تسريب عبر الإضافات.