حملة اختطاف جلسات Google تستخدم دعوات التقويم والوسطاء المباشرين



حملة تصيّد نشطة منذ منتصف أغسطس 2026 تسرق جلسات Google الحيّة من مستخدمي الشركات، وروابطها مصممة لتجتاز فحوص السمعة المعتادة. ويفيد باحثو Material Security بإسقاط مئات النطاقات المهاجمة.

- الحملة قائمة منذ منتصف أغسطس 2026 وتستهدف جلسات Google الحيّة لمستخدمي الشركات.
- تجتاز الروابط بحسب التقرير الفحوص التي يعتمد عليها المدافعون عادةً، وقد صُمّمت لذلك عمدًا.
- يشير عنوان التقرير إلى دعوات التقويم والوسطاء المباشرين كوسيلتي الوصول والاستيلاء على الجلسة.
- اكتشف فريق Threat Research في Material Security الحملة وأسقط مئات النطاقات المهاجمة ضمن عملية CloudFire.

ما الذي ورد في التقرير

منذ منتصف أغسطس 2026 تنفّذ عملية تصيّد استيلاءً على جلسات Google الحيّة العائدة لمستخدمين في شركات. وبحسب The Hacker News، اجتازت الروابط المستخدمة جميع الفحوص التي يعتمد عليها المدافعون عادةً للحكم على الرابط، وقد صمّم المهاجم العملية على هذا النحو عن قصد.

اكتشف فريق Threat Research في Material Security الحملة، وأسقط منذ ذلك الحين مئات النطاقات المهاجمة ضمن جهد يسميه عملية CloudFire. ويشير عنوان التقرير إلى دعوات التقويم والوسطاء المباشرين (live proxies)، ما يوحي بأن الطُّعم يصل على هيئة دعوة تقويم وأن الجلسة تُلتقط عبر وسيط في الوقت الفعلي. أما المقتطف المتاح لنا فلا يتضمن تفاصيل تقنية إضافية.

أهمية الأمر

عند سرقة الجلسة يرث المهاجم حسابًا موثَّقًا بالفعل، وقد لا تكشف ذلك الضوابط التي تركّز على كلمة المرور أو على سمعة الرابط وحدها. وعلى المؤسسات التي تعدّ نتيجة السمعة النظيفة دليل أمان أن تتعامل معها بوصفها مؤشرًا واحدًا بين عدة مؤشرات.

ولأن المقتطف موجز، فلا نعرف من استُهدف من المستخدمين، ولا عدد المتضررين، ولا ما فعله المهاجمون بعد الوصول. ننصح بالاطلاع على التقرير الكامل وعلى ما نشرته Material Security قبل استخلاص أي نتائج.

التعامل المقترح

الاستجابة المطلوبة مراجعة للضوابط القائمة لا حالة طوارئ. ركّزوا على سرعة اكتشاف الجلسات غير المتوقعة وإنهائها، وعلى وعي الموظفين بالتشكك في دعوات التقويم غير المطلوبة.

ما يجب فعله الآن

1. راجعوا سرعة فريقكم في اكتشاف جلسة Google نشطة وإلغائها عند الاشتباه باختراق حساب.
2. نبّهوا الموظفين إلى التعامل مع دعوات التقويم غير المطلوبة التي تحمل روابط على أنها تصيّد محتمل، حتى لو بدا المرسل مألوفًا.
3. لا تعتبروا نتيجة السمعة النظيفة للرابط دليل أمان، وأضيفوا مراقبة السلوك وتسجيلات الدخول لحسابات Google Workspace.
4. تأكدوا من أن دليل الاستجابة للتصيّد يغطي سرقة الجلسات وليس كلمات المرور فقط.
5. اطّلعوا على تقرير Material Security الكامل وطبّقوا أي مؤشرات اختراق منشورة على أنظمة المراقبة لديكم.