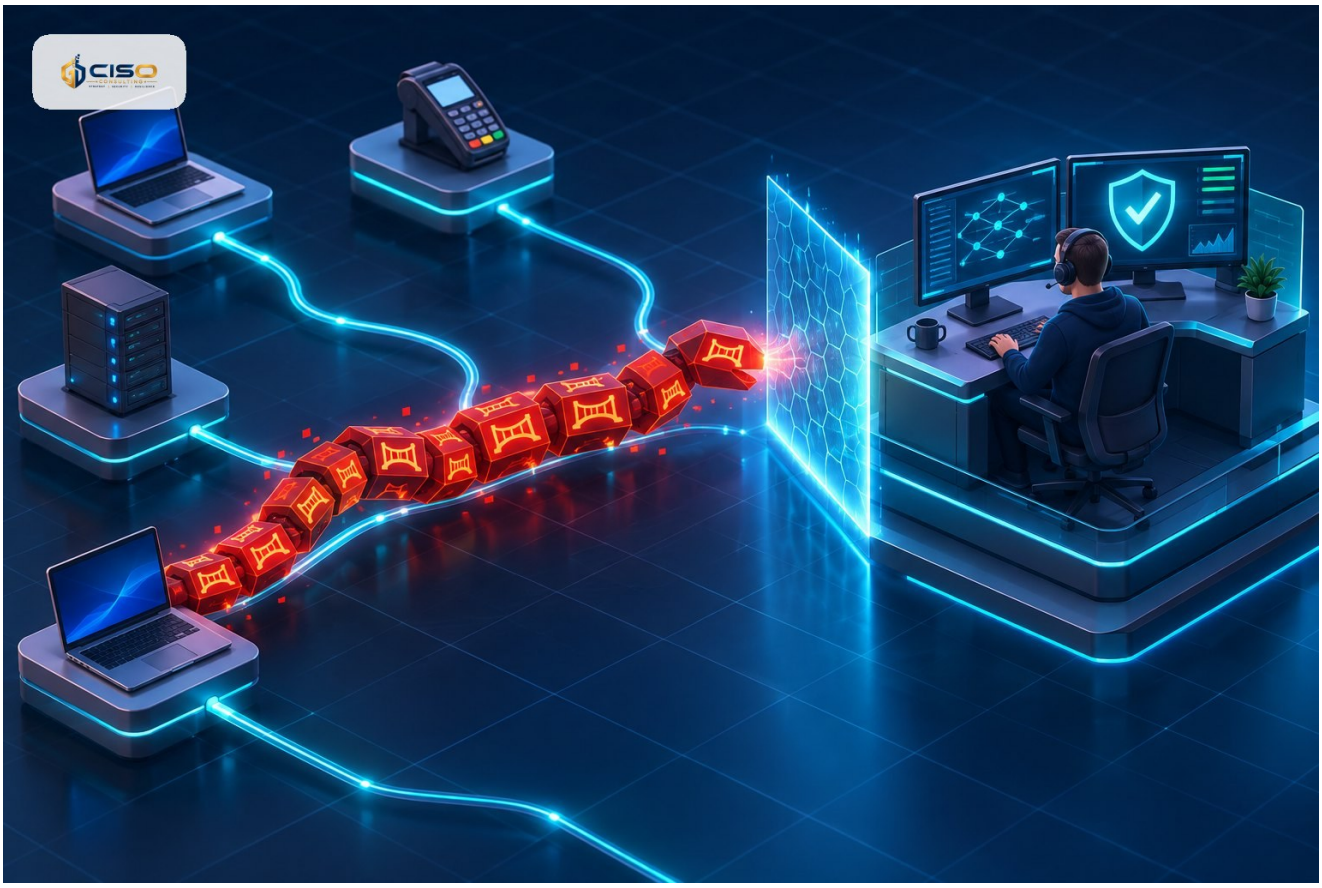
برمجية SCKit في هجمات ScreenConnect تحاول الانتقال من أجهزة العملاء إلى حواسيب فنيي مزودي الخدمات المُدارة



استُخدمت أداة SCKit الشبيهة بالديدان في هجمات ScreenConnect الأخيرة على مزودي الخدمات المُدارة. لم يرصد الباحثون نجاح انتشارها، لكن يُنصح بتحديث العملاء ومراجعة النشاط.

- SCKit مجموعة من 16 سكربتًا ومكوّنًا صُممت لإبقاء الوصول عن بُعد وللانتشار بين الأنظمة المُدارة عبر ScreenConnect.
- تحاول الأداة استغلال الثغرة CVE-2026-84869 في نقل الملفات من جهة العميل، وقد صدر إصلاحها في الإصدار 26.6.5، لتنفيذ شيفرة على حاسوب الفني.
- لم ترصد Blackpoint Cyber وHuntress استغلالاً ناجحًا، وفشل اختبار Blackpoint ضد عميل محدَّث.
- طالت الهجمات الأوسع ما لا يقل عن 288 جهازًا في 48 جهة خلال 90 دقيقة، ويُرجَّح أن بدايتها

عبر الإصدارين 1.0.31 و1.0.32 من RMM+.

- عطّلت ConnectWise خمس إضافات تابعة لجهات خارجية في نحو 400 بيئة شريكة، مؤكدة أن وجودها لا يعني حدوث اختراق.

حلّل باحثو Blackpoint Cyber وHuntress أداة SCKit الشبيهة بالديدان، والتي استُخدمت في هجمات ScreenConnect الأخيرة على مزودي الخدمات المُدارة. صُممت الأداة للانتقال من جهاز عميل مصاب إلى حاسوب فني لدى المزوّد، ومن ثم إلى شبكات أخرى يديرها.

آلية عمل الأداة

يثبّت المهاجمون أولاً عملاء ScreenConnect Access إضافيين يتصلون بخوادمهم، للحفاظ على الوصول حتى لو انتهت جلسة المزوّد الأصلية. ثم يحلّ مكوّن يسمى RelayTrap محل عملية ScreenConnect Guest الشرعية وينتظر اتصال الفني، ويحاول إرسال ملف خبيث إلى الفني بالاتجاه المعاكس مستغلاً الثغرة CVE-2026-84869 في نقل الملفات من جهة العميل، وقد أصلحتها ConnectWise في الإصدار 26.6.5.

وتحاول مكوّنات أخرى سرقة ملفات تعريف الارتباط الخاصة بمصادقة ScreenConnect من المتصفحات، ما قد يتيح الاستيلاء على جلسة الفني دون بيانات دخول أو طلب MFA جديد. بعدها تستخدم صلاحياته لحصر الأجهزة وتوزيع الأوامر، ومنها عبر Shared Toolbox.

ما الذي رُصد فعليًا

يؤكد الفريقان أن هذا السلوك الشبيه بالديدان لم ينجح في الحملة الحالية. فقد أعادت Blackpoint تنفيذ محاولة الاستغلال ضد عميل حديث ووجدت أن الإصلاح منع التنفيذ، ولاحظت Huntress فشل محاولة السيطرة على وحدة التحكم في كل سجل جهاز استعادته.

وطالت الهجمات الأوسع ما لا يقل عن 288 جهازًا في 48 جهة خلال 90 دقيقة. وتعتقد Huntress أن الوصول الأولي تم عبر الإصدارين 1.0.31 و1.0.32 من RMM+، حيث سمح مفتاح وصول فارغ بتنفيذ أوامر دون مصادقة أو MFA. وعطّلت ConnectWise خمس إضافات ذات صلة في نحو 400 بيئة شريكة.

الدرس العملي أن حاسوب الفني جزء من سطح الهجوم، وأن تحديث العملاء ضروري حتى لو لم يُرصد استغلال ناجح بعد.

ما يجب فعله الآن

1. حدّثوا جميع عملاء ScreenConnect إلى الإصدار 26.6.5 أو أحدث وتأكدوا من التحديث على حواسيب الفنيين.
2. عطّلوا الإضافات الخارجية المتأثرة ومنها الإصداران 1.0.31 و1.0.32 من RMM+، وعيّنوا مفتاح وصول غير فارغ إن استُبقيت الإضافة.
3. ابحثوا عن عمليات تثبيت غير مصرح بها لعملاء ScreenConnect Access على الأجهزة المُدارة.
4. راجعوا نشاط Run Command وShared Toolbox بحثًا عن أوامر لا يقابلها تسجيل دخول مستخدم.
5. تجنبوا الجلسات التفاعلية عبر ScreenConnect مع الأجهزة المشتبه بإصابتها، وافحصوها بأدوات أمنية

منفصلة.

6. إذا كنتم تسندون خدمات تقنية إلى مزود مُدار، فاطلبوا منه تأكيدًا كتابيًا بتعرّضه لـ ScreenConnect وإجراءات المعالجة.