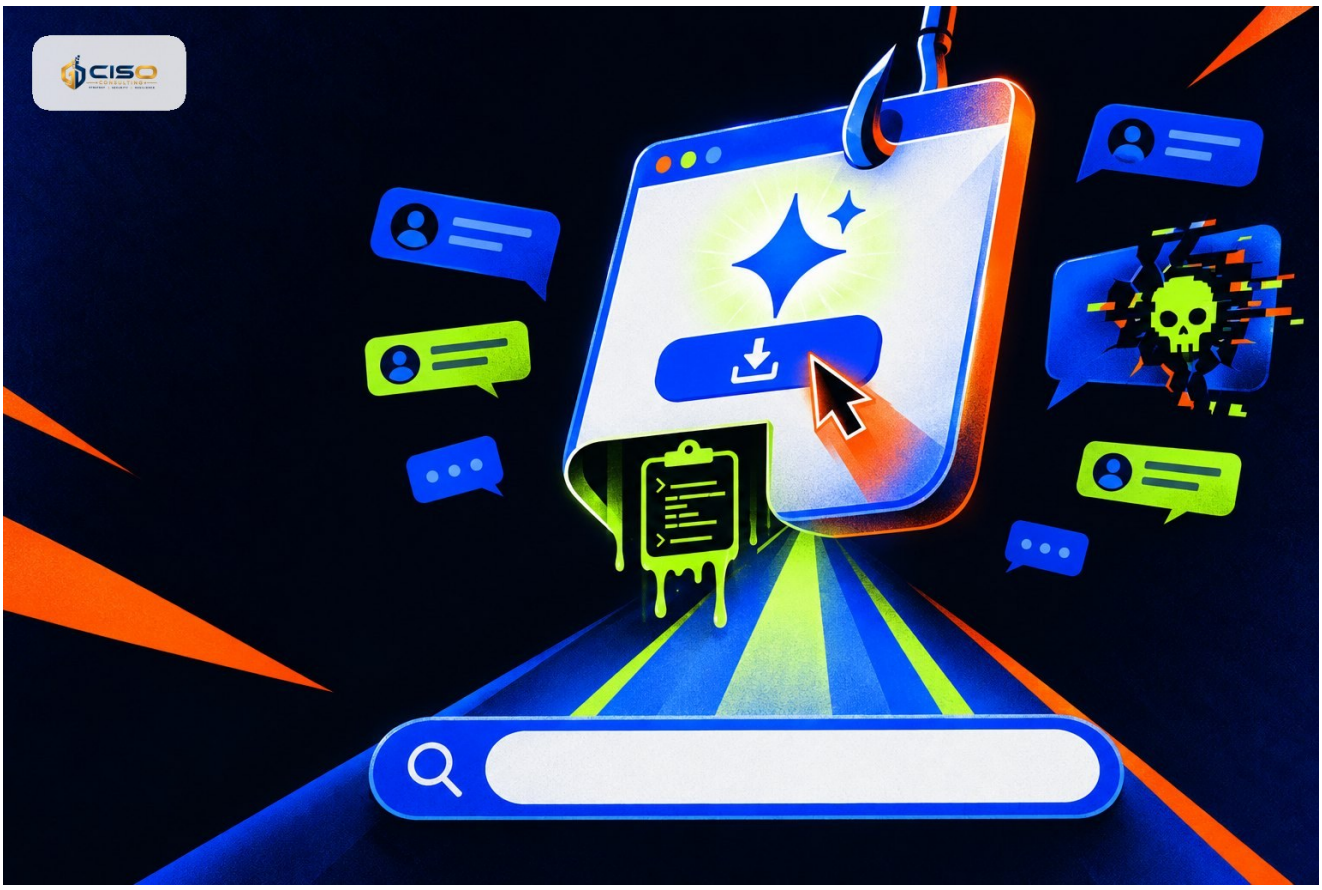
هجمات ClickFix تستخدم صفحات أدوات الذكاء الاصطناعي المزيفة طُعمًا



يفيد تقرير برعاية Push Security بأن ClickFix أصبح أكثر الهجمات عبر المتصفح رصدًا لديها، وأن صفحات تثبيت أدوات الذكاء الاصطناعي المزيفة والمحادثات المشاركة طُعم متزايد الفاعلية. ويصل أغلب الضحايا عبر محركات البحث لا البريد.

- تذكر Push أن ClickFix شكّل في المتوسط 52% من رصدها حتى الربع الثاني 2026 وبلغ 67% في أغسطس، وأن 4 من كل 5 صفحات وُصل إليها عبر محركات البحث.
- يستنسخ InstallFix صفحات تثبيت أدوات الذكاء الاصطناعي ويستبدل الأمر بآخر خبيث، وقد يضع زر النسخ في الحافظة أمرًا مختلفًا عن المعروض.
- يستضيف LLMshare الطُعم في محادثات مشاركة وGPTs مخصصة على ChatGPT وClaude، فتثق به فحوص سمعة الروابط غالبًا.
- ربطت ANY.RUN 1,258 تحليلاً بحملات أدوات ذكاء اصطناعي مزيفة بين 15 أبريل و5 أكتوبر 2026،

وانتحل 81% منها Claude أو ChatGPT وCodex.

- قد تفوّت حماية البريد وسمعة الروابط وأدوات النقطة الطرفية هذه الهجمات، خاصة في الأجهزة الشخصية وأجهزة المقاولين والمطورين. والتقرير برعاية جهة تجارية.

يصف تقرير كتبته Push Security وبرعايتها تقنية ClickFix، التي تخدع المستخدم ليلصق أمرًا بنفسه، بأنها من أكثر أساليب المهاجمين استخدامًا في 2026. والتقرير صادر عن جهة تجارية، لذا تعكس أرقامه بيانات الرصد لدى Push ويحسن قراءتها بهذا الاعتبار.

ما الذي يتغير

تفيد Push بأن ClickFix شكّل في المتوسط 52% من رصدها حتى الربع الثاني 2026، متجاوزًا AiTM وتصيّد رمز الجهاز، وبلغ 67% في أغسطس. وقد وُصل إلى نحو 4 من كل 5 صفحات ClickFix اعترضتها في 2026 عبر محركات البحث، من خلال مواقع مخترقة وإعلانات خبيثة وتسميم نتائج البحث.

تستهدف أحدث الطُعوم من يبحثون عن أدوات الذكاء الاصطناعي. ففي InstallFix ينسخ المهاجمون صفحة تثبيت، مثل صفحة Claude Code، ويستبدلون الأمر بآخر خبيث. وفي إحدى الحالات عرضت الصفحة الأمر الأصلي بينما وضع زر النسخ أمرًا مختلفًا في الحافظة. أما LLMshare فيضع الطُعم داخل محادثات مشاركة وGPTs مخصصة على منصات ذكاء اصطناعي مشروعة، فترى فحوص السمعة نطاقًا موثوقًا.

لماذا تفوت الضوابط هذه الهجمات

بحسب التقرير، لا ترى حماية البريد صفحة جاء إليها المستخدم عبر البحث، وترى فحوص سمعة الروابط نطاقات موثوقة، ويُنفَّذ الأمر الملصوق في صدفة مشروعة وفي الذاكرة. وأكثر الأجهزة عرضة هي التي تخلو من EDR، كالأجهزة الشخصية وأجهزة المقاولين وأجهزة Mac ومحطات المطورين.

يقوم هذا النمط على عادتين لدى الموظفين: تثبيت الأدوات من سطر الأوامر، والبحث عن تطبيقات الذكاء الاصطناعي بدل الوصول إليها مباشرة. ومراجعة هاتين العادتين نقطة بداية مناسبة.

ما يجب فعله الآن

1. توعية الموظفين والمطورين بعدم لصق أي أمر من صفحة ويب أو محادثة ذكاء اصطناعي مشتركة دون التحقق منه، وبالوصول إلى الأدوات المعتمدة عبر المفضلة أو البوابة الداخلية لا الإعلانات.
2. نشر قائمة بأدوات الذكاء الاصطناعي المعتمدة ومصادر تثبيتها الرسمية، وتوفير مسار سريع لطلب أدوات جديدة.
3. تقييد أو مراقبة تنفيذ الأوامر والسكربتات من جلسات المستخدمين، ومراجعة تغطية EDR على الأجهزة الشخصية وأجهزة المقاولين وMac ومحطات المطورين.
4. إضافة رؤية وضوابط على مستوى المتصفح لتغطية الهجمات التي تصل عبر البحث ولا تمر ببوابة البريد.
5. إدراج سيناريوهات ClickFix وصفحات تثبيت أدوات الذكاء الاصطناعي المزيفة في تمارين التوعية وخطط الاستجابة للحوادث، مع حفظ أدلة الصفحات التي قد تختفي.