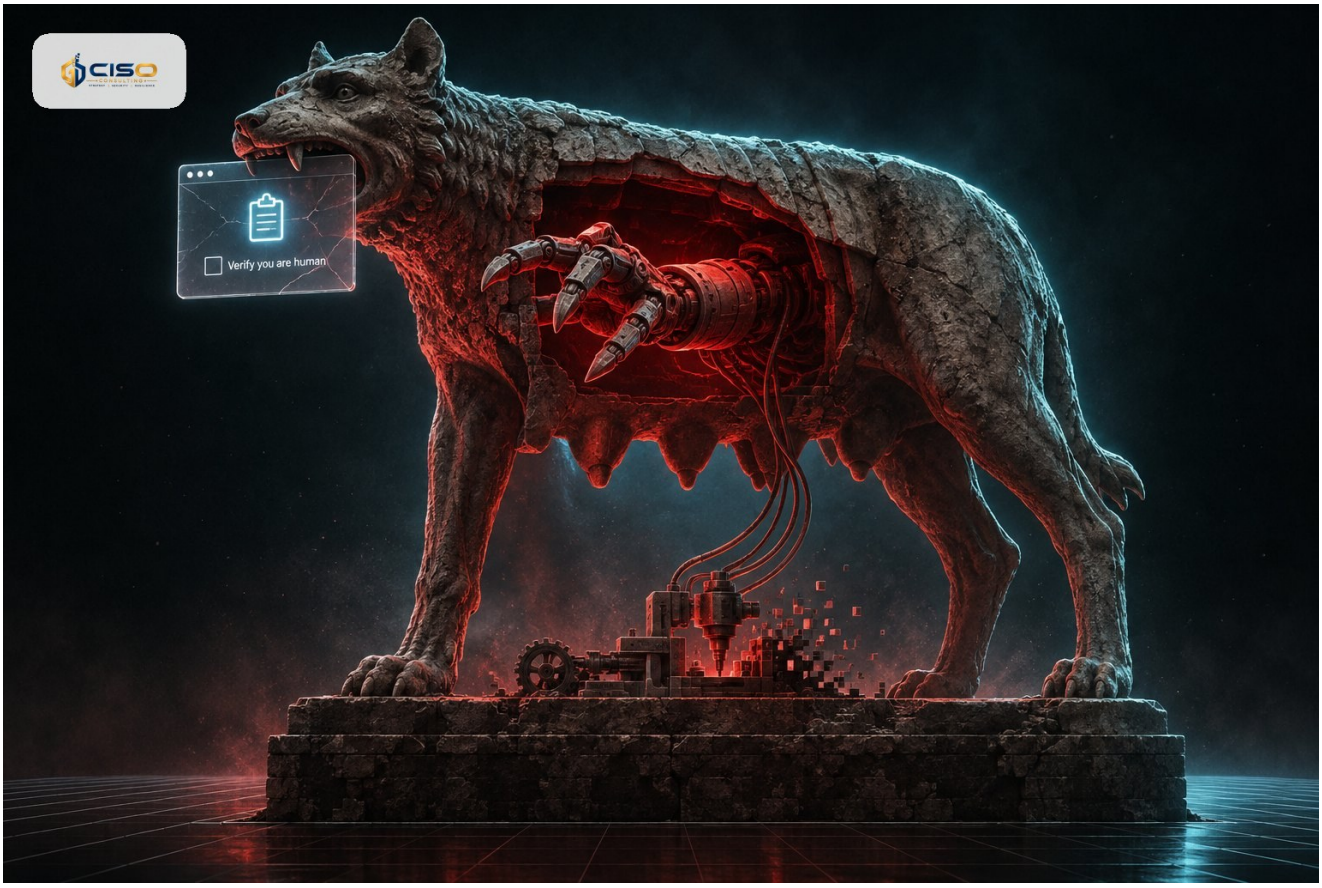
حملة ClickFix عبر منصة ROMULUS تنشر حصان طروادة جديدًا للتحكم عن بُعد



يستخدم مهاجمون منصة ROMULUS لتوزيع حصان طروادة جديد غير موثّق يشبه CNCMachineRMS. وترجّح Blackpoint أن المنصة تعمل كخدمة توزيع.

- ROMULUS منصة لتوزيع البرمجيات الخبيثة تعتمد أسلوب ClickFix، وارتبطت الآن بحصان طروادة جديد غير موثّق.
- يتشابه هذا الحصان مع CNCMachineRMS.
- ترجّح Blackpoint أن ROMULUS تعمل كخدمة توزيع.
- توزّع المنصة CNCMachineRMS وLegion Loader عبر سلاسل هجوم منفصلة.
- تحتفظ السلاسل بأسلوبَي ClickFix والتحميل الجانبي لملفات تنفيذية موقّعة.

ما الذي رُصد

رُصد مهاجمون يستخدمون منصة ROMULUS لتوزيع البرمجيات الخبيثة بأسلوب ClickFix في نشر حصان طروادة للتحكم عن بُعد (RAT) لم يُوثَّق سابقًا. ووفق التقرير يتشابه هذا البرنامج مع CNCMachineRMS، ويصفه عنوان الخبر بأنه قادر على التجسس على المستخدمين والتحكم بالأجهزة.

كيف تعمل المنصة

تقدّر Blackpoint أن ROMULUS تعمل على الأرجح كخدمة توزيع لا كأداة بغرض واحد. فهي توزّع CNCMachineRMS وLegion Loader عبر سلاسل منفصلة، مع إبقاء أسلوبين مشتركين: ClickFix الذي يعتمد على إقناع المستخدم بتنفيذ إجراء بنفسه، والتحميل الجانبي لملفات تنفيذية موقّعة تستغل موثوقية التوقيع.

أهمية الأمر

لأن المنصة تخدم أكثر من حمولة خبيثة، فلا يكفي التركيز على عائلة برمجيات واحدة. ينبغي أن تعالج الضوابط أساليب التوصيل نفسها: التنفيذ بمبادرة المستخدم، وإساءة استخدام البرمجيات الموقّعة الموثوقة. ولا يتضمن المقتطف تفاصيل عن الأهداف أو أعداد الضحايا أو المناطق أو مؤشرات الاختراق، لذا لا يصح افتراض التعرض أو السلامة دون فحص بيانات الرصد الداخلية.

والاستجابة العملية هي مراجعة محتوى التوعية وضوابط نقاط النهاية وتغطية الكشف لهذين الأسلوبين، ومتابعة بحث الجهة الأصلية للحصول على مؤشرات تقنية عند نشرها.

ما يجب فعله الآن

1. أضيفوا إلى برامج التوعية أمثلة على خدع ClickFix التي تطلب من المستخدم لصق أوامر أو تشغيلها.
2. قيّدوا أو راقبوا تشغيل المستخدمين لمفسّرات الأوامر انطلاقًا من المتصفح أو نوافذ الطلب.
3. راجعوا قواعد الكشف عن التحميل الجانبي لملفات موقّعة من مسارات غير معتادة.
4. ابحثوا عن مؤشرات CNCMachineRMS وLegion Loader فور نشرها من الجهات المختصة.
5. تأكدوا من أن خطط الاستجابة للحوادث تغطي احتواء أحصنة طروادة للتحكم عن بُعد وإعادة تعيين بيانات الاعتماد.