

منصة ROMULUS لهجمات ClickFix تُستخدم لتوزيع LegionLoader وبرمجيات خبيثة أخرى



تصف أبحاث (Vedere Labs) Forescout منصة ROMULUS لتوزيع البرمجيات الخبيثة عبر أسلوب ClickFix، وتُستخدم لنشر Legion Loader من خلال صفحات هبوط مزيفة.

- كشفت Forescout Research - Vedere Labs تفاصيل منصة ROMULUS لتوزيع البرمجيات الخبيثة بأسلوب ClickFix.
- تعمل المنصة كخدمة لتوزيع البرمجيات الخبيثة وليست حملة منفردة.
- تعتمد صفحات هبوط مزيفة بطُعم على طريقة ClickFix لإقناع المستخدمين بتنفيذ أوامر خبيثة.
- يصيب الضحايا أجهزتهم بأنفسهم، مما يتجاوز بعض الضوابط التقنية.
- يُذكر Legion Loader ضمن البرمجيات الخبيثة التي توزعها المنصة.

نشر باحثو Forescout Research - Vedere Labs تفاصيل منصة ROMULUS، وهي منصة مصممة لتوزيع البرمجيات الخبيثة باستخدام أساليب ClickFix. ويشبهها التقرير بخدمة لتوزيع البرمجيات الخبيثة، أي أن بنيتها يمكن أن تتقل أكثر من نوع من الحمولات، ويُذكر Legion Loader مثالاً على ذلك.

آلية الأسلوب

تعتمد ROMULUS على صفحات هبوط مزيفة تحمل طُعوماً على طريقة ClickFix. فبدلاً من استغلال ثغرة برمجية، تُقنع الصفحة الزائر بتنفيذ أوامر خبيثة بنفسه، فينفذ المستخدم العدوى فعلياً. وهذا يجعل نجاح الهجوم مرتبطاً بسلوك المستخدم بقدر ارتباطه بالضعف التقني.

أهمية الأمر

لأن المستخدم هو من يبدأ الإجراء، قد لا تمنع مرشحات التنزيل والمرفقات المعتادة الهجوم. لذلك يصبح وعي الموظفين والتحكم فيما يستطيعون تنفيذه من أوامر عنصرين أساسيين في الدفاع. ولا يتضمن المقتطف المتاح تفاصيل عن الأهداف أو المناطق أو أعداد الضحايا أو مؤشرات الاختراق، ويُنصح بالرجوع إلى بحث Forescout الكامل للتفاصيل التقنية.

على الجهات المنظمة اعتبار ذلك تذكيراً بإدراج طُعوم نسخ الأوامر ولصقها في برامج التوعية، ومراجعة ضوابط الأجهزة الطرفية بناءً على ذلك.

ما يجب فعله الآن

1. إضافة طُعوم ClickFix، التي تطلب من المستخدم لصق أوامر وتشغيلها، إلى برامج التوعية الأمنية.
2. توجيه الموظفين بعدم تنفيذ أوامر منسوخة من صفحة ويب أو من رسالة تحقق.
3. مراجعة سياسات الأجهزة الطرفية التي تقيد تشغيل السكريبتات وسطر الأوامر للمستخدمين العاديين.
4. التأكد من أن حلول كشف الأجهزة الطرفية ترصد نشاط سطر الأوامر المشبوه الصادر من جلسات المستخدمين.
5. الاطلاع على بحث Forescout Vedere Labs كاملاً وإدخال مؤشرات الاختراق المنشورة في منظومة الكشف.