

CHOSEN BRICK: تحذير بريطاني وأمريكي وهولندي من برمجية إيرانية تستهدف المعارضين والصحفيين



تصف جهات بريطانية وأمريكية وهولندية برمجية CHOSEN BRICK التي تستهدف نظام Windows عبر الهندسة الاجتماعية في تطبيقات المراسلة، وقد تصيب الأجهزة الشخصية والمؤسسية.

- استُخدمت CHOSEN BRICK منذ عام 2025 على الأقل ضد أفراد في بريطانيا والولايات المتحدة وهولندا.
- يني المهاجمون ألفة مع الضحية عبر WhatsApp أو Telegram منتحلين صفة معارف أو دعم فني، ثم يدفعونه لفتح تطبيق أو ملف مزيف.
- تعمل البرمجية على Windows وتتثبت بقاءها عبر مفتاح Run في السجل وتضيف استثناءات في Microsoft Defender وتستخدم Telegram للتحكم والسيطرة.
- تستطيع التقاط الشاشة والصوت ونسخ بيانات Telegram وWhatsApp من المتصفحات وسرقة البريد، ولم يُرصد انتقال جانبي آلي.

- ينتقل المهاجمون من الجهاز المؤسسي إلى الشخصي عند فشل التسليم، لذا ينبغي للمؤسسات مساعدة الموظفين على فحص الجهازين.

نشر المركز الوطني للأمن السيبراني في المملكة المتحدة ومكتب التحقيقات الفيدرالي الأمريكي وجهاز الاستخبارات والأمن العام الهولندي (AIVD) إرشادًا مشتركًا حول CHOSEN BRICK، وهي عائلة برمجيات خبيثة تستخدمها جهات إيرانية رسمية. وتفيد الجهات بأنها استهدفت أفرادًا في عدة دول منذ عام 2025 على الأقل، وفي مقدمتهم المعارضون والناشطون والصحفيون. وقد ظهرت بيانات شخصية لبعض الضحايا السابقين على مواقع تسريب موالية لإيران.

كيف يجري الهجوم

يدرس المهاجمون هدفهم أولاً، ثم يتواصلون معه عبر منصات المراسلة مثل WhatsApp وTelegram منتحلين صفة شخص يعرفه أو دعماً فنياً للمنصة، ويقنعونه بفتح ملف يبدو أصيلاً، كتطبيق معروف أو نتائج أشعة رنين مغناطيسي. وتُعرض شاشة مقنعة بينما تُنبت البرمجية في الخلفية. وغالباً يبدأ التواصل على جهاز العمل، فإذا فشل طلب المهاجم من الضحية فتح الملف على جهازه الشخصي لتجاوز ضوابط المؤسسة.

بعد التثبيت على Windows تبقى البرمجية بعد إعادة التشغيل عبر مفتاح Run في السجل، وتضيف استثناءات في Microsoft Defender، وتستخدم بوت Telegram منفصلاً لكل ضحية. وتستطيع النقاط الشاشة والميكروفون، ونسخ بيانات WhatsApp وTelegram من المتصفحات، وسرقة البريد، وتنزيل برمجيات إضافية. وتخرج البيانات عبر Telegram وخدمات تخزين سحابية. ولم يُرصد انتقال جانبي آلي.

الكشف والتخفيف

يوصي الإرشاد المؤسسات التي تشبه في التنفيذ بأن تبحث فرق تقنية المعلومات في السجلات عن مؤشرات الاختراق المنشورة وتشغل توقيعات الكشف. وتستحق المراجعة أي اتصالات غير متوقعة في DNS أو الوكيل نحو lightningproxies.netg iproyal.comg storjshare.io وvultrobjects.comg backblazeb2.comg api.telegram.org. كما ينبغي إبلاغ الموظفين المعرّضين للاستهداف ومساعدتهم على فحص أجهزتهم الشخصية. والضوابط الموصى بها: مصادقة متعددة العوامل مقاومة للتصيد، وقوائم السماح بالتطبيقات، ومكافحة الفيروسات، وفحص البريد، ومراقبة النقاط الطرفية والشبكة، والتوعية.

ما يجب فعله الآن

1. ابحثوا في سجلات DNS والوكيل عن النطاقات المذكورة وراجعوا الاتصالات غير المتوقعة، خاصة نحو api.telegram.org.
2. افحصوا الأجهزة بحثاً عن مدخلات Run في HKCU والمسار غير القياسي «Windows» (بمسافة بعد الاسم) ضمن SysWOW64 كما ورد في الإرشاد، وشغلوا توقيعات الكشف المنشورة.
3. نبّهوا الموظفين الأكثر عرضة للاستهداف، كالتنفيذيين وفرق الإعلام والعلاقات العامة، وساعدوهم على فحص أجهزتهم الشخصية.
4. طبّقوا المصادقة متعددة العوامل المقاومة للتصيد وقوائم السماح بالتطبيقات ومكافحة فيروسات مُدارة، وراقبوا أي تعديل على استثناءات Microsoft Defender.

5. أدرجوا في التوعية حيل انتحال دعم تطبيقات المراسلة أو إرسال برامج تثبيت عبر WhatsApp وTelegram.
6. أبلغوا عن الحوادث المؤكدة وفق إجراءاتكم الداخلية وإلى الهيئة الوطنية للأمن السيبراني بحسب المتطلبات.