

أداة الاستغلال P7 DarkSword لأجهزة iOS تضيف سرقة المحافظ الرقمية وتلقي الأوامر عن بعد



كشفت iVerify عن P7 DarkSword، نسخة جديدة من أداة DarkSword لاستغلال iOS، تترك أثراً أقل على الجهاز وتسرق بيانات سلسلة المفاتيح والمحافظ الرقمية وتتيح اتصالاً ثنائي الاتجاه مع خوادم المهاجم.

- نشرت iVerify تفاصيل P7، وهي نسخة لم تُرصد سابقاً من أداة DarkSword لاستغلال iOS.
- تقلّل P7 أثرها على الجهاز مقارنة بالنسخ التي رُصدت من قبل.
- تضيف سرقة بيانات سلسلة المفاتيح (keychain) وبيانات المحافظ الرقمية من الجهاز.
- تضيف اتصال تحكم وسيطرة (C2) ثنائي الاتجاه مع بنية المهاجم.

كشف باحثو iVerify في تقرير نُشر يوم الخميس عن نسخة جديدة لم تُرصد سابقاً من أداة DarkSword لاستغلال ثغرات iOS، أطلقوا عليها اسم P7 DarkSword.

ما الجديد في P7

وفق iVerify، تختلف P7 عن النسخ التي يرصدها فريقها عادة في ثلاثة أمور. فهي تقلل أثرها على الجهاز، مما قد يصعب اكتشاف آثارها. وتضيف سرقة محتويات سلسلة المفاتيح (keychain) وبيانات المحافظ الرقمية المخزنة على الجهاز. كما تضيف اتصال تحكم وسيطرة (C2) ثنائي الاتجاه، بحيث تتبادل بنية المهاجم الأوامر والبيانات مع الهاتف المصاب.

الأهمية للجهات المنظمة

تحفظ سلسلة المفاتيح في iPhone بيانات الدخول المحفوظة، لذا قد تكشف سرقتها الوصول إلى حسابات مؤسسية وشخصية. كما أن صغر الأثر على الجهاز يعني أن الفحوص الروتينية قد تُظهر أقل. ولا يوضح المقتطف المتاح طريقة الإصابة أو الأهداف أو إصدارات iOS المتأثرة أو التحديثات، ولذلك لا ينبغي افتراض مستوى تعرّض محدد قبل مراجعة تقرير iVerify الكامل.

والاستجابة العملية الهادئة تتمثل في التأكد من شمول إدارة الأجهزة المحمولة لأجهزة iOS، وفرض سياسات التحديث، واعتبار الهاتف المخترق في إجراءات الحوادث حالة تعرّض محتمل لبيانات الاعتماد.

ما يجب فعله الآن

1. مراجعة تقرير iVerify الكامل واستخراج المؤشرات وإصدارات iOS المتأثرة وتقييم انطباقها على بيئتك.
2. التأكد من تسجيل جميع أجهزة iPhone المؤسسية وأجهزة BYOD في نظام إدارة الأجهزة وتشغيلها أحدث إصدار من iOS.
3. التعامل مع الجهاز المشتبه باختراقه كحالة تعرّض لبيانات الاعتماد: إعادة تعيين كلمات المرور وإلغاء الجلسات للحسابات المستخدمة عليه.
4. توجيه الموظفين أصحاب الصلاحيات العالية أو من يتعاملون مع الأصول الرقمية إلى الإبلاغ الفوري عن أي سلوك غير معتاد للجهاز.
5. إضافة سيناريوهات اختراق iOS إلى دليل الاستجابة للحوادث ومراقبة تهديدات الأجهزة المحمولة.