مجموعة SilentAir تستغل شبكات اتصالات آسيوية لاعتراض رموز التحقق عبر الرسائل النصية



أفادت شركة Enea برصد مجموعة تجسس على مستوى دولة تُدعى SilentAir، استخدمت معدات مخترقة داخل مشغلي اتصالات آسيويين لاعتراض مكالمات ورسائل أشخاص مختارين، معظمهم في تايوان.

- أطلقت Enea، وهي شركة برمجيات اتصالات وأمن سيبراني مقرها ستوكهولم، اسم SilentAir على المجموعة.
- استخدمت المجموعة معدات مخترقة داخل مشغلي اتصالات آسيويين لاعتراض المكالمات والرسائل.
- استهدفت أشخاصاً مختارين، معظمهم في تايوان.
- تم تتبع مصادر الهجوم إلى ست دول آسيوية على الأقل.
- قيّمت Enea بثقة عالية أن SilentAir جهة فاعلة على مستوى دولة.

ما الذي ورد في التقرير

حددت شركة Enea، وهي شركة برمجيات اتصالات وأمن سيبراني مقرها ستوكهولم، مجموعة تجسس جديدة أطلقت عليها اسم SilentAir. ووفق التقرير، استخدمت المجموعة معدات مخترقة داخل شبكات مشغلي الهاتف المحمول في آسيا لاعتراض مكالمات ورسائل نصية لأشخاص مختارين، معظمهم في تايوان.

ورصدت Enea مصادر الهجوم في ست دول آسيوية على الأقل، وقيّمت بثقة عالية أن SilentAir جهة فاعلة على مستوى دولة.

الأثر على التحقق الثنائي

يشير عنوان التقرير إلى اعتراض رموز التحقق الثنائي المرسلة عبر الرسائل النصية. فعندما تُقرأ الرسائل داخل شبكة المشغل، يصل الرمز إلى المهاجم كما يصل إلى المستخدم، بصرف النظر عن مستوى حماية الجهاز نفسه. ولا يتضمن المقتطف المتاح تفاصيل تقنية إضافية، لذا تبقى الأساليب الدقيقة وقائمة المشغلين المتأثرين غير واضحة.

قراءة عملية للجهات في المملكة

كان الاستهداف انتقائياً ومركزاً على تايوان، ولا يشير المصدر إلى المملكة العربية السعودية. ومع ذلك، تذكّر الحالة بأن الرسائل النصية عامل تحقق ثانٍ أضعف للحسابات عالية القيمة، خصوصاً للتنفيذيين ومديري الأنظمة والموظفين المسافرين أو المتنقلين على شبكات أجنبية. وينبغي للجهات مراجعة المواضع التي لا تزال تعتمد على رموز SMS في حماية الوصول الحساس والتخطيط للانتقال إلى وسائل أقوى.

ما يجب فعله الآن

1. حصر الأنظمة والحسابات التي ما زالت تعتمد على رموز SMS كعامل ثانٍ، بدءاً بالحسابات ذات الصلاحيات العالية وحسابات التنفيذيين.
2. نقل المستخدمين الأعلى خطراً إلى تطبيقات المصادقة أو مفاتيح الأمان المادية أو وسائل أخرى مقاومة للتصيّد.
3. مراجعة الوصول عن بعد وأثناء التجوال للموظفين المسافرين، وتشديد الضوابط على الدخول من شبكات أجنبية.
4. الاستفسار من مشغلي الاتصالات عن حماية معدات الإشارات والشبكة الأساسية وآلية إبلاغ العملاء عند الاشتباه بالاعتراض.
5. إدراج اعتراض الرسائل النصية في نموذج التهديدات وتحديث معايير المصادقة ضمن برامج الضوابط الأساسية للأمن السيبراني (NCA ECC) وإطار الأمن السيبراني لقطاع البنوك (SAMA CSF).