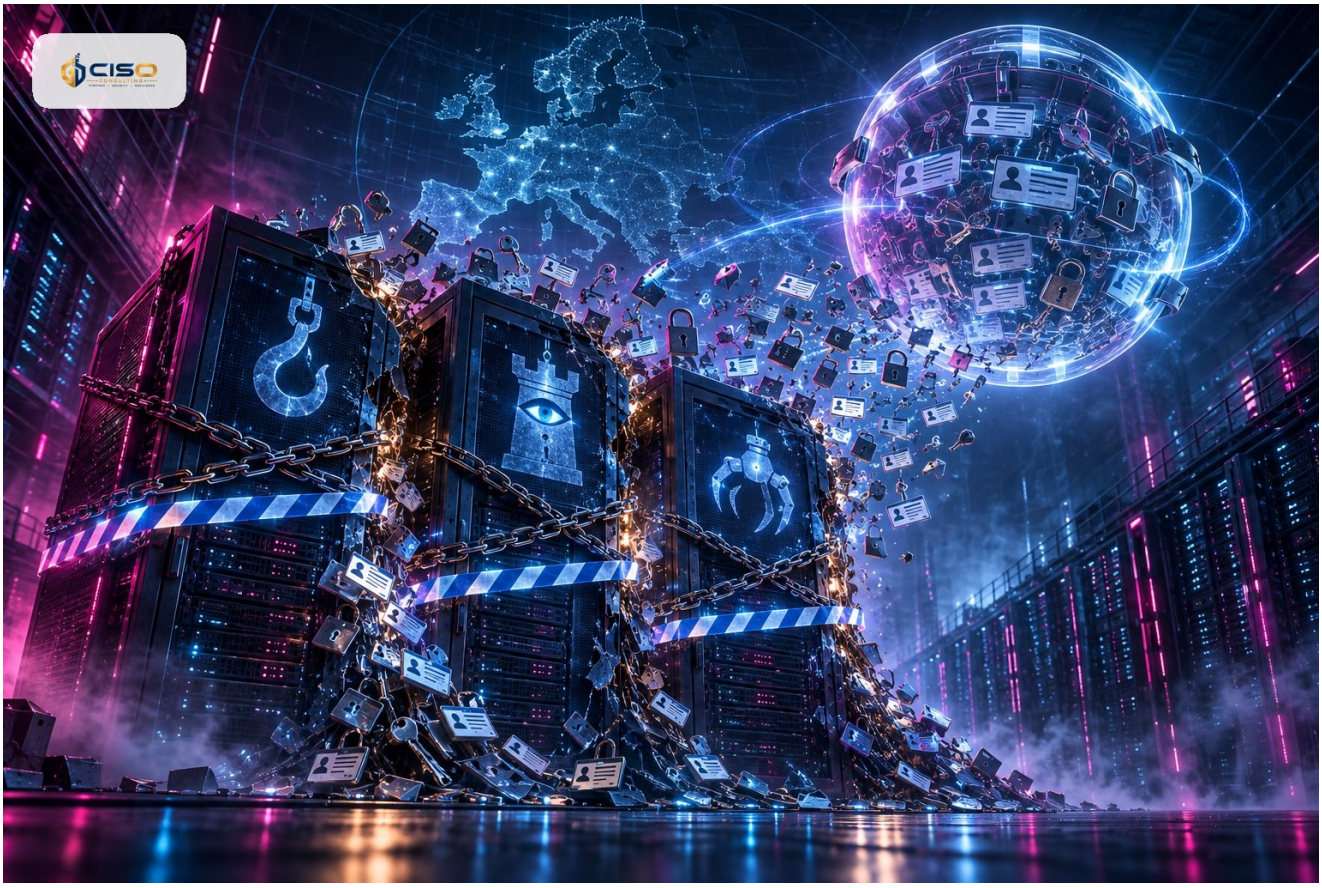
عملية Endgame تعطّل خوادم Gootloader وCastleRAT وStealC



عملية شرطية دولية عطّلت خوادم ثلاث أدوات خبيثة تُستخدم للوصول إلى الأجهزة وسرقة كلمات المرور وتنفيذ هجمات الفدية. وأفاد مكتب الشرطة الجنائية الألماني (BKA) بضبط نحو 6.4 مليون بيانات دخول مسروقة تخص أكثر من 40 ألف ضحية.

- عُطّلت خوادم Gootloader وCastleRAT وStealC ضمن عملية شرطية دولية.
- استُخدمت هذه الأدوات للوصول إلى الأجهزة وسرقة كلمات المرور وإطلاق هجمات الفدية.
- ضُبط نحو 6.4 مليون بيانات دخول مسروقة تخص أكثر من 40 ألف ضحية بحسب BKA.
- قد تبقى بيانات الدخول المسروقة صالحة للحسابات المتأثرة إلى حين إعادة تعيينها.

عطّلت عملية شرطية دولية، أُعلن عنها هذا الأسبوع باسم Endgame، خوادم ثلاث أدوات خبيثة هي Gootloader وCastleRAT وStealC. وبحسب التقرير، استخدم المجرمون هذه الأدوات للوصول إلى الأجهزة وسرقة كلمات

المرور وإطلاق هجمات الفدية.

ما الذي ضُبط

أفاد مكتب الشرطة الجنائية الألماني (BKA) بأن الشرطة ضبطت نحو 6.4 مليون بيانات دخول مسروقة تخص أكثر من 40 ألف ضحية. ويصف المقتطف المتاح Gootloader بأنه أداة تحميل (loader) دون تفاصيل تقنية إضافية عن كل أداة، ولا يسمّي الجهات أو الدول المتضررة.

الأثر على المؤسسات

يعطّل إسقاط الخوادم البنية التحتية التي تقف خلف هذه الأدوات، لكنه لا يزيل بذاته الإصابات القائمة على الأجهزة، ولا يجعل بيانات الدخول المسروقة سابقًا آمنة. فإذا سُرقت بيانات دخول موظفين أو عملاء، تبقى الحسابات معرّضة للخطر إلى حين تغيير كلمات المرور وإنهاء الجلسات.

تنصح الجهات المنظّمة باعتبار ذلك فرصة لمراجعة مؤشرات نشاط سارقي البيانات وأدوات التحميل، وفحص ممارسات إدارة بيانات الدخول، والتأكد من أن خطط الاستجابة للحوادث تغطي سرقة بيانات الدخول التي تسبق عادةً هجمات الفدية.

ما يجب فعله الآن

1. البحث في الأجهزة وسجلات EDR والوكيل (proxy) عن مؤشرات نشاط Gootloader وCastleRAT وStealC.
2. فرض إعادة تعيين كلمات المرور وإنهاء الجلسات والرموز النشطة للحسابات المشتبه في تعرضها.
3. تطبيق المصادقة متعددة العوامل على الوصول عن بُعد والبريد والحسابات ذات الامتيازات.
4. التحقق مما إذا كانت بيانات دخول المؤسسة ظاهرة في مصادر استخبارات التسريبات وسجلات سارقي البيانات المتاحة.
5. التأكد من أن خطة الاستجابة للحوادث تغطي سرقة بيانات الدخول المؤدية إلى الفدية، بما في ذلك التصعيد إلى الهيئة الوطنية للأمن السيبراني عند الاقتضاء.