ShinyHunters تعلن عودتها بعد الاعتقالات، ومفاتيح PGP القديمة لا تحسم هوية القائمين عليها



موقع تسريب جديد على شبكة Tor يزعم عودة ShinyHunters بعد سلسلة اعتقالات. الرسائل الموقّعة بمفاتيح PGP قديمة تثبت امتلاك المفاتيح لا عودة المشغّلين الأصليين.

- موقع تسريب جديد على Tor أُطلق في 23 نوفمبر يعلن عودة المجموعة بالروسية والإنجليزية.
- وُقّعت رسالتان بمفاتيح PGP تعود إلى 2020، وأكدت BleepingComputer صحة التوقيعين.
- أُلغيت هذه المفاتيح في مارس 2026 وتداولها أشخاص كثيرون، فلا تثبت الهوية.
- لم تُوقَّع أي من رسائل نوفمبر بمفتاح الاستبدال الصادر في مارس 2026.
- يقول المشغّلون إنهم سيطلقون شبكة CDN جديدة لاستضافة البيانات المسروقة وسيتخلون عن خوادم النسخ الاحتياطي الحالية.

ما الذي أُعلن

تقول مجموعة الابتزاز ShinyHunters إنها عادت، وذلك في منشورات على موقع تسريب جديد على شبكة Tor أُطلق في 23 نوفمبر. تعلن الرسائل، بالروسية والإنجليزية، العودة، وتنأى بالمجموعة عمّن تصفهم بالمنتحلين، وتهاجم عضوًا سابقًا أُفيد باعتقاله وتعاونه مع جهات إنفاذ القانون.

ويقول المشغّلون إنهم سيتواصلون فقط عبر حساب في منتدى Exploit يزعمون أنهم يتحكمون به منذ 2020 وعبر الموقع الجديد. كما يخططون لشبكة CDN جديدة لاستضافة البيانات المسروقة، ويقولون إنهم لن يستخدموا خوادم النسخ الاحتياطي الحالية.

لماذا لا تكفي مفاتيح PGP دليلاً

لدعم ادعائهم، نشر المشغّلون رسالتين موقّعتين بمفاتيح PGP تاريخية للمجموعة أُنشئت في 2020. وأكدت BleepingComputer صحة التوقيعين، أي أن الموقّعين يملكون المفاتيح الخاصة. وكان أحد هذه المفاتيح قد استُخدم لتوثيق مراسلات مع الموقع في أغسطس 2025.

غير أن المفاتيح، بحسب ما يُتداول، انتقلت بين أشخاص كثيرين، وقد أُلغي كلاهما في مارس 2026 عندما أعلنت المجموعة مفتاحًا بديلاً. ويستخدم إعلان نوفمبر المفتاحين الملغيين لتزكية مفتاح جديد آخر، ولم تُوقَّع أي من الرسائل المفحوصة بمفتاح مارس البديل. لذلك يبقى غير واضح هل يقف خلف الموقع الأعضاء الأصليون أم مشغّلون جدد أم منتحلون.

السياق

يأتي الإعلان بعد اعتقالات طالت أعضاء مزعومين خلال الشهرين الماضيين، في هولندا والأردن والولايات المتحدة، وذلك بعد أن زعمت المجموعة في سبتمبر اختراق أنظمة FBI عبر ثغرة في Oracle PeopleSoft. وبعدها صمت المتحدث الرئيسي باسمها وتوقف موقع التسريب السابق.

والخلاصة العملية للمؤسسات الخاضعة للتنظيم أن عودة هذا الاسم غير مؤكدة، وأن ادعاءات الابتزاز باسمه ينبغي تقييمها بالأدلة لا بالتوقيع وحده.

ما يجب فعله الآن

1. تعامل مع أي رسالة ابتزاز تنسب نفسها إلى ShinyHunters على أنها غير مؤكدة إلى أن تُطابَق البيانات المزعومة مع سجلاتكم.
2. راجع دليل الاستجابة للحوادث الخاص بالابتزاز وادعاءات التسريب، وحدّد من يتحقق من الادعاءات ومن يقرر الإفصاح والتواصل.
3. تأكد من تحديث أنظمة Oracle PeopleSoft وغيرها من الأنظمة المؤسسية المكشوفة خارجيًا ومن مراقبتها.
4. أطلع الإدارة التنفيذية والشؤون القانونية والالتزام على آلية التعامل مع ظهور اسم المنظمة في موقع تسريب، بما يشمل تقييم الإشعار وفق PDPL.
5. أبلغ الهيئة الوطنية للأمن السيبراني والجهة التنظيمية القطاعية عن أي تواصل أو إدراج يخص منظمتكم وفق المتطلبات.