# خمس إشارات مبكرة على اختراق برنامج فدية قبل بدء التشفير



تعرض Acronis خمس إشارات تحذيرية تكشف اختراق برنامج الفدية قبل التشفير أو سرقة البيانات، إذ يسبق ذلك عادةً سرقة بيانات الاعتماد والتنقل الجانبي ومحاولة تعطيل الضوابط الأمنية.

- تنطوي هجمات الفدية عادةً على نشاط خبيث طويل قبل بدء التشفير.
- من المراحل المبكرة المعتادة سرقة بيانات الاعتماد والتنقل الجانبي ومحاولة تعطيل الضوابط الأمنية.
- تصف Acronis خمس إشارات تحذيرية تساعد المدافعين على اكتشاف الاختراق مبكراً.
- الاكتشاف المبكر يدعم الاحتواء وحماية الأنظمة الحيوية والنسخ الاحتياطية.

نشرت Acronis إرشادات حول رصد اختراقات برامج الفدية في مراحلها المبكرة، وفق ما أوردته BleepingComputer. والفكرة الأساسية أن التشفير نادراً ما يكون الخطوة الأولى؛ فالمهاجمون يقضون غالباً وقتاً في سرقة بيانات

الاعتماد والتنقل بين الأنظمة ومحاولة تعطيل الضوابط الأمنية قبل قفل أي ملفات أو سحب بيانات.

## ما الذي تتناوله الإرشادات

تستعرض Acronis خمس إشارات تحذيرية يمكن للمدافعين مراقبتها. والمقتطف المتاح لنا لا يسرد هذه الإشارات الخمس، لذلك لا يتناولها هذا الخبر فرداً فرداً. والهدف المعلن هو مساعدة الفرق على اكتشاف الاختراق مبكراً واحتواء النشاط الخبيث وحماية الأنظمة الحيوية والنسخ الاحتياطية.

## أهمية ذلك للجهات المنظمة

الفترة بين الوصول الأولي والتشفير هي الأنسب للاستجابة الفعالة. وقد يدل على هجوم قيد التنفيذ استخدام غير معتاد للحسابات، أو تنقل بين الأنظمة الداخلية، أو العبث بأدوات الحماية. والجهات التي ترصد هذه السلوكيات بدل انتظار ظهور الضرر تملك فرصة أكبر للحد من الأثر.

يحسن بقادة الأمن الاطلاع على إرشادات Acronis كاملة ومقارنة إشاراتها الخمس بتغطية الرصد لديهم. وتستحق النسخ الاحتياطية عناية خاصة، إذ تشدد الإرشادات على حمايتها إلى جانب الأنظمة الحيوية.

## الخطوات التالية

اعتبروا مراحل ما قبل التشفير أولوية في الرصد، وتأكدوا من وصول التنبيهات إلى من يستطيع التصرف، وتدرّبوا على الاحتواء ليكون اتخاذ القرار سريعاً عند ظهور أولى الإشارات.

## ما يجب فعله الآن

1. الاطلاع على إرشادات Acronis كاملة وربط إشاراتها الخمس بقواعد الرصد الحالية.
2. مراقبة إساءة استخدام بيانات الاعتماد والتنقل الجانبي غير المعتاد بين الأنظمة الداخلية.
3. إطلاق تنبيه عند أي محاولة لتعطيل أدوات الحماية أو العبث بها، مثل حماية نقاط النهاية.
4. التحقق من حماية النسخ الاحتياطية من التلاعب ومن اختبار استعادتها.
5. التدرب على خطة احتواء لاختراق يُكتشف قبل بدء التشفير.