الحكم بالسجن سبع سنوات على مخترق GTA VI والإفراج عنه بترخيص، وجهاز Fire Stick في فندق استُخدم في اختراقات 2022



حكمت محكمة بريطانية على Arion Kurtaj، المتورط في اختراق Rockstar Games وUber وRevolut عام 2022، بالسجن سبع سنوات مع الإفراج بترخيص لمدة الاحتجاز السابقة. وتُظهر القضية أثر الأجهزة الاستهلاكية غير المدارة.

- صدر الحكم بحق Arion Kurtaj (21 عامًا) في محكمة Woolwich Crown Court بلندن، وخُفضت العقوبة الابتدائية البالغة تسع سنوات بمقدار سنتين بسبب فترة الإيداع في مستشفى للأمراض النفسية.
- أُفرج عنه في اليوم نفسه بترخيص، ويمكن إعادته إلى السجن إذا أخلّ بشروط الإفراج.
- في سبتمبر 2022 اخترق، وهو في السابعة عشرة ومفرج عنه بكفالة، أنظمة Uber وRevolut ومطوّر لعبة Grand Theft Auto.

- نفّذ الاختراقات باستخدام جهاز Amazon Fire Stick موصول بتلفاز غرفة في فندق بعد أن صادرت الشرطة حاسوبه.
- أقرّ بالذنب في ست تهم، منها أربع بموجب Computer Misuse Act وتهمة احتيال.

ما الذي حدث

حكمت محكمة بريطانية على Arion Kurtaj (21 عامًا) بالسجن سبع سنوات بعد اختراقه شركة Rockstar Games وتسريبه مقاطع من لعبة Grand Theft Auto VI. وحدّد القاضي عقوبة من تسع سنوات ثم خفّضها سنتين مراعاةً للفترة التي قضاها في مستشفى للأمراض النفسية. ونظرًا لمدة الاحتجاز السابقة أُفرج عنه في اليوم نفسه بترخيص، على أن يقضي ما تبقّى من العقوبة تحت الإشراف في المجتمع، ويجوز إعادته إلى السجن إذا خالف شروط الإفراج.

وكان قد أقرّ بالذنب في ست تهم: أربع منها بموجب Computer Misuse Act، وتهمة احتيال، وتهمة حيازة هاتف محمول داخل السجن. وستبقى سبع تهم أخرى معلّقة في الملف دون أن تُعدّ إدانات. وأفادت الشرطة بأنها ستطلب أمرًا لمنع الجرائم الخطيرة، فيما نقلت BBC News أن أمرًا مدته خمس سنوات صدر بالفعل يمنعه من استخدام Telegram وDiscord.

كيف نُفذت الاختراقات

في سبتمبر 2022، وكان عمره 17 عامًا ومفرجًا عنه بكفالة، اخترق Kurtaj أنظمة Uber وRevolut ومطوّر لعبة Grand Theft Auto. وكان قد أُسكن في فندق لحمايته بعد تهديدات من مخترقين منافسين. ورغم مصادرة الشرطة حاسوبه، نفّذ الهجمات عبر جهاز Amazon Fire Stick موصول بتلفاز غرفته.

الدلالة للجهات المنظَّمة

لا يشرح المصدر الأساليب التقنية التي استُخدمت ضد الضحايا. غير أن الدرس العملي أوسع: فبإمكان مهاجم مصمّم أن يعمل بأجهزة استهلاكية بسيطة، ولذلك لا تزيل مصادرة الحاسوب قدرته على الهجوم. ينبغي للمؤسسات أن تركّز على ضوابط تصمد أيًّا كان جهاز المهاجم، مثل المصادقة القوية ومراقبة الوصول وضبط من يستطيع الوصول إلى الأنظمة الداخلية.

ما يجب فعله الآن

1. مراجعة نطاق المصادقة متعددة العوامل للموظفين والمتعاقدين والأطراف الثالثة الذين يصلون إلى الأنظمة الداخلية.
2. التحقق من أن المراقبة ترصد عمليات الدخول غير المعتادة والوصول من أجهزة غير مُدارة أو غير مألوفة.
3. التأكد من عدم إمكانية اتصال الأجهزة الشخصية والاستهلاكية بشبكة المؤسسة أو الأنظمة الحساسة دون موافقة.
4. إعادة توعية الموظفين بمخاطر الهندسة الاجتماعية وسرقة بيانات الاعتماد، بمن فيهم العاملون عن بُعد والمسافرون.
5. اختبار إجراءات الاستجابة للحوادث والتعامل مع التسريبات، ومنها واجبات إبلاغ الجهات التنظيمية، وفق

سيناريو سرقة بيانات داخلية.