كيف نجح قراصنة كوريا الشمالية المسؤولون عن فيروس الفدية في تنفيذ عملية سرقة مذهلة للعملة المشفرة؟

مايك أوركت[1]

مايك أوركت هو محرر مشارك في إم آي تي تكنولوجي ريفيو

استخدمت مجموعة لازاروس مخططات خداع رقمي معقدة وأدوات متطورة لتبييض الأموال لسرقة الأموال لصالح نظام كيم جونغ أون.

أصبحت الهجمات السيبرانية ضد شركات تحويل العملات المشفرة أمراً شائعًا، ولكن إحدى هذه العمليات التي تضمنت سرقة ما يربو على ٧ مليون دولار من شركة دراجون إكس في سنغافورة في مارس ٢٠١٩ تتميز عن غيرها لثلاثة أسباب على الأقل:

السبب الأول هو مخطط الخداع الرقمي الذي استخدمه المهاجمون، الذي يتصف بتعقيد شديد، ولم يقتصر على استخدام مواقع ويب مزيفة وحسب، بل أيضًا بوتات مزيفة للتعامل بالعملات المشفرة. أما **السبب الثاني هو الطريقة الخبيثة التي استُخدمت لتبييض الأموال المشفرة المسروقة**. وأخيراً وليس آخراً: **يبدو أن المهاجمين كانوا يعملون لصالح كيم جونغ أون**.

تُبين هذه العملية التي نُشرت تفاصيل جديدة عنها **مؤخراً** من قِبل شركة تحليل البلوكتشين (تشايناليسيس) درجة البراعة التي وصل إليها اللصوص الرقميون. وإذا أصاب هذا التقرير وغيره من **التقارير** في اتهام كوريا الشمالية بالوقوف خلف هذا الهجوم، فيبدو أنه جزء من إستراتيجية شاملة يستخدمها نظام كيم للبقاء والصمود، وذلك بعد أن أدت العقوبات الاقتصادية الدولية إلى عزله عن النظام العالمي المالي في محاولة لدفعه إلى إيقاف برنامجه للأسلحة النووية.

لم تكن (دراجون إكس) أولى شركات التحويل التي تعرضت للهجوم من قِبل هذه المجموعة بالتحديد، التي يسميها بعض محللي الأمن السيبراني بمجموعة (لازاروس)؛ فقد كانت المجموعة تستهدف صناعة العملات المشفرة منذ ٢٠١٧ على الأقل، وذلك في إطار حملة شاملة ضد المؤسسات المالية. وفي أغسطس، **قالت**

[1] نقلا عن: إم أي تكنولوجي ريفيو، ٧-٢-٢٠٢٠، رابط

مجموعة من الخبراء المستقلين في تقرير موجه للأمم المتحدة إن كوريا الشمالية تمكنت من الحصول على مبلغ يقدر بقيمة ٢ مليار دولار لبرنامجها الصاروخي عن طريق استخدام هجمات سيبرانية واسعة النطاق ومتصاعدة التعقيد للسرقة من البنوك وشركات تحويل العملات المشفرة. وإن استخدام النظام للعملات المشفرة من أجل الالتفاف على العقوبات قد أدى إلى إطلاق تحذير جديد من نفس المجموعة من خبراء الأمم المتحدة لتجنب حضور مؤتمر حول البلوك تشين سيُعقد لاحقًا في بيونج يانج.

يُعتَقد أن مجموعة (لازاروس) مسؤولة عن عدد من عمليات الاختراق التي احتلت عناوين وسائل الإعلام، بما فيها اختراق شركة سوني لإنتاج الأفلام في ٢٠١٤، وفيروس الفدية (واناكري) في ٢٠١٧، الذي أثّر على مئات آلاف الحواسيب في ١٥٠ بلداً. ولكن سرقتها لمبلغ ٨١ مليون دولار من البنك المركزي في بنجلاديش في ٢٠١٦ كانت نذيراً لاستهدافها اللاحق لشركات تحويل العملات المشفرة. ووفقًا لمكتب التحقيقات الفدرالي الأميركي، فقد أمضى المهاجمون أكثر من سنة في استطلاع الهدف قبل التمكن من الدخول إلى نظام البنك الحاسوبي عبر حملة احتيال إلكتروني معقدة.

تعاني بيئة العملات المشفرة من تساهل كبير في الحماية، ولهذا كانت هدفًا سهلاً لقراصنة كوريا الشمالية، الذين يتمتعون بخبرة سابقة في اختراق المؤسسات المالية، وذلك كما تقول بريسيلا موريوكي، رئيسة أبحاث الدول في شركة الأمن السيبراني (ريكورديد فيوتشر)، وهي تضيف: إنهم يتمتعون بقدرات أكثر بكثير مما يُعزى إليهم، خصوصاً في مجال الجرائم المالية.

من أجل اختراق (دراجون إكس)، قامت مجموعة (لازاروس) بابتداع شركة مزيفة أعلنت عن (بوت) للمتاجرة الآلية بالعملات المشفرة باسم (وورلد بيت بوت)، وفقًا لشركة تشاينياليسيس. قامت المجموعة بإنشاء موقع ويب للشركة المزيفة، ووصل بها الأمر إلى ابتداع حضور على وسائل التواصل الاجتماعي لموظفيها المزعومين، وعندما قدموا عرضًا لتجربة مجانية لهذا (البوت) المخصص للمتاجرة إلى موظفي (دراجون إكس)، وقع أحدهم في الفخ، وقام بتحميل برنامج خبيث إلى حاسوب كان يحوي المفاتيح الخاصة لمحافظ شركة التحويل.

وصفت مختبرات (كاسبيرسكي) في **بحث** نُشر مؤخرًا واحدًا آخر من مخططات مجموعة (لازاروس) الحديثة، الذي استهدف شركة أخرى للعملات المشفرة على ما يبدو. وفي هذه الحالة، قام المهاجمون ببناء شركات مزيفة واستدرجوا أهدافهم لتحميل برمجيات خبيثة عن طريق برنامج التراسل الشهير تيليجرام.

غير أن الاختراق وسرقة الأموال لا تكفي، فيجب أن يتمكنوا من صرف هذه الأموال في نهاية المطاف. وفي السنة الماضية، أجرت مجموعة (لازاروس) تغييرات شاملة في أسلوب عملها وفقا (لتشاينياليسيس)؛ فقد كانت أساليبها لتبييض الأموال بسيطة إلى حد كبير، خصوصًا في ترك الأموال المسروقة مجمدة لفترة ١٢–١٨ شهرًا قبل صرفها باستخدام شركة تحويل لا تقوم بتتبع هويات العملاء، **وهو بالضبط ما يدعو أغلب السلطات إلى فرض عمليات تدقيق هويات العملاء على شركات تحويل العملات المشفرة**.

ولكن في عملية (دراجون إكس) في مارس المنصرم، استخدمت المجموعة طريقة أكثر تعقيدًا على ما يبدو لنقل الأموال، فقد اعتمدت على عدد أكبر بكثير من الخطوات المرحلية، بما فيها عدد من شركات تحويل العملات المشفرة ومجموعة منوعة من المحافظ الرقمية. وقد انتهى المطاف بالعملات المسروقة في محفظة خاصة تستخدم تكنولوجيا خصوصية متوافقة مع (البيتكوين) تسمى (كوين جوين)، وهي تجمع التعاملات من عدة مستخدمين بطريقة تجعل من الصعب تحديد المرسل والمستفيد في عملية الدفع. وقد حصل القراصنة على المبلغ بسرعة أكبر، فقد تم نقل جميع الأموال تقريبًا إلى خدمات السيولة خلال ٦٠ يومًا، وفقًا (لتشاينياليسيس).

قد لا تعبر الأساليب الجديدة والمحسنة لقراصنة كوريا الشمالية عن قدراتهم الخاصة بقدر ما تعبر عن **تطور أدوات تبييض الأموال المتوافرة حاليًا في عالم العملات المشفرة**. وتقول مديرة الأبحاث في (تشاينياليسيس)، إن فريقها لاحظ في ٢٠١٩ زيادة كبيرة في البنى التحتية المتطورة لتبييض الأموال، والتي يمكن لمنظمات إجرامية أن تستخدمها ببساطة وسهولة، مما يعني أنه أصبح من السهل الوصول إلى أدوات متطورة لتغطية آثار سرقات العملات المشفرة، حتى بالنسبة للمجرمين الذين لا يتمتعون بخبرة كبيرة في البلوكتشين. وعلى أي حال، فإن استمرار وجود الثغرات في الأمن السيبراني لدى شركات تحويل العملات المشفرة يعني أن المجموعات الإجرامية مثل (لازاروس) لن تتوقف عن سرقتها.