دانش و فناوری

سرقت ۱۳۰ میلیون دلار بیت‌کوین با سوءاستفاده از ضعف کیف‌پول‌های آفلاین

رادیو فردا

۱ ساعت پیش

از ابتدای سال جاری تاکنون بیش از ۲۰۰ حملهٔ سایبری به شرکت‌های ارز دیجیتال صورت گرفته که مجموع خسارت آن‌ها بیش از ۹۵۰ میلیون دلار برآورد می‌شود

گزارش‌های امنیتی از یک کارزار گسترده هک خبر می‌دهند که در آن، هکرها با سوءاستفاده از یک آسیب‌پذیری نرم‌افزاری در محفظه‌های آفلاین ارز دیجیتال موسوم به «کولدکارت»، موفق به سرقت بیش از ۱۳۰ میلیون دلار بیت‌کوین شده‌اند.

بر اساس گزارش شرکت‌های امنیت بلاکچین، این حملات توسط دست‌کم ۱۲ هکر مختلف انجام شده است. هویت عاملان این حملات سایبری همچنان ناشناخته است، اما به‌گزارش وب‌سایت «تدکرانچ»، احتمال می‌رود بیش از یک گروه در این حملات نقش داشته باشند.

شرکت «گلکسی ریسرچ» نیز در گزارشی، میزان سرقت تا روز سه‌شنبه ۱۳ مرداد را حدود ۱۳۰ میلیون دلار برآورد کرده است.

این حملات بخشی از موج روبه‌رشد حملات سایبری علیه بخش ارزهای دیجیتال است.

طبق گزارش «تی‌آرام لبز»، که در زمینهٔ تحلیل ارزهای دیجیتال فعالیت می‌کند، از ابتدای سال جاری تاکنون بیش از ۲۰۰ حملهٔ سایبری به شرکت‌های ارز دیجیتال صورت گرفته که مجموع خسارت آن‌ها بیش از ۹۵۰ میلیون دلار برآورد می‌شود.

نکته قابل‌توجه در این حملات آن است که هکرها محفظه‌های آفلاین ارز دیجیتال را هدف قرار داده‌اند؛ ابزارهایی که به‌طور خاص برای ارائه سطح بالاتری از امنیت در مقایسه با «کیف‌پول‌های گرم» (آنلاین) طراحی شده‌اند.

این محفظه‌های آفلاین، عبارتی موسوم به Seed Phrase ذخیره می‌کنند که در واقع کلید مخفی دسترسی به بیت‌کوین است. این کلید به‌صورت داخلی و دور از اینترنت نگهداری می‌شود، در حالی که خود دارایی‌ها روی بلاکچین ثبت شده‌اند.

با این حال، محققان امنیتی دریافته‌اند که برخی از این محفظه‌ها به‌دلیل یک آسیب‌پذیری نرم‌افزاری، کلیدهای رمزنگاری قابل‌پیش‌بینی تولید می‌کنند. هکرها از این نقطه‌ضعف برای دسترسی به دارایی‌ها استفاده کرده‌اند.

به بیان ساده، مهاجمان نیازی به نفوذ مستقیم به دستگاه‌ها نداشتند بلکه توانستند به‌دلیل نقص در نحوه تولید کلیدها، آن‌ها را بازتولید کنند؛ گویی بدون شکستن قفل، نسخه‌ای از کلید را در اختیار گرفته‌اند.

جاناتان گودمن، یکی از قربانیان این حملات، می‌گوید حدود ۱.۶ میلیون دلار بیت‌کوین ذخیره‌شده در کیف‌پول آفلاین خود را از دست داده است.

او در شبکهٔ اجتماعی ایکس نوشت: «احتمالاً سخت‌ترین بخش ماجرا این بود که من تمام اصول امنیتی را رعایت کرده بودم. کلید بازیابی را با کسی به اشتراک نگذاشتم، دستگاه‌هایم هرگز به اینترنت متصل نشدند و آن‌ها را در چندین گاوصندوق و جعبه امن نگهداری می‌کردم».

به گفته او، با وجود این اقدامات احتیاطی، مشکل ناشی از یک خط کد آسیب‌پذیر در نرم‌افزار تولید عبارت بازیابی است که به سال ۲۰۲۱ بازمی‌گردد.

در پی این رخداد، شرکت فناوری کانادایی «کوین‌کایت» از کاربران محفظه‌های آفلاین خواسته است فوراً آخرین به‌روزرسانی‌های امنیتی را نصب کنند، یک عبارت بازیابی جدید بسازند و دارایی‌های خود را به آن منتقل کنند تا از خطر سرقت جلوگیری شود.

این مطلب بخشی از:

دانش و فناوری | بایگانی | امنیت سایبری | گزارش‌های خبری