Uber hacked, internal systems breached and vulnerability reports stolen

سال ۲۰۲۲ توسط هکر ۱۸ ساله انگلیسی هک شد و اطلاعات زیادی از جمله ایمیل ها، پسورد ها و اطلاعات حساس دیگر متعلق به این شرکت در اینترنت افشا شد. با توجه به اسناد موجود توسط BleepingComputer بنظر می‌رسد هکر ها دسترسی کامل به اکثر سرویس های اوبر داشته اند که از طریق یکی از کارمندان این شرکت موفق به نفوذ شدند و خسارات زیادی به بار آوردند.

در ادامه نحوه حمله، تکنیک های استفاده شده و خسارات وارده را مورد بررسی قرار می‌دهیم.

نحوه حمله و تکنیک استفاده شده

هکر ها با استفاده از تکنیک مهندسی اجتماعی (social engineering) بر روی یکی از کارمندان این شرکت توانسته بودند به سیستم این کارمند دسترسی پیدا کنند. اما به دلیل وجود MFA [1] یا سیستم چند مرحله ای ورود، نیاز به کد دو عاملی داشتند که با جای زدن خود به جای آن کارمند بخش امنیت و ارسال مکرر اعلان امنیتی که نتیجه آن، خسته شدن آن کارمند و فاش کردن کد دو عاملی خود شد، موفق شدند تایید بخش امنیت شرکت را گرفته و وارد حساب شوند. بعد از دسترسی به حساب کاربری، بر روی vpn [2] ها و شبکه های داخلی شنود گذاشته و نام کاربری و پسورد یکی از کارمندان سطح بالا را یافته بودند که با استفاده از آن به بخش های مختلف شرکت دسترسی پیدا کردند.

پس تکنیک مورد استفاده این هکر ها، مهندسی اجتماعی بود که اخیرا گسترش زیادی در بین هکر ها شده است.

نتایج و خسارات

طی این حمله، خسارات زیادی به شرکت اوبر وارد شد از جمله برداشته شدن کد های مرکزی این سیستم عظیم و هم همینطور اطلاعات متعدد و متنوعی از دیتابیس ها که توسط تایید را رد نشده اند یا هکر ها مدعی بوده اند که این اطلاعات لو رفته است.

از مهم ترین خساراتی که به این شرکت وارد شده فاش شدن برنامه گزارش حفره های امنیتی موجود بود. طی این برنامه حفره های امنیتی موجود شناسایی شده و گزارش داده می‌شوند تا طی نسخه های بعدی مورد بررسی قرار گرفته و در نهایت حل شوند، اما با فاش شدن این حفره ها توسط تیم هکر ها، این شرکت در معرض حملات متعددی قرار گرفته است.

این اطلاعات توسط هکر ها دانلود شده اما اخباری برای افشار یا استفاده آنها منتشر نشده، اما این شرکت باید آمادگی مواجهه با این حملات را داشته باشد.

[1] Multi-Factor Authentication
[2] Virtual Private Network