تعداد قربانیان هک سرویس Exchange مایکروسافت به ۳۰ هزار شرکت رسید - دیجیاتو

ایمان صاحبی | شنبه، ۱۶ اسفند ۱۳۹۹

مایکروسافت هفته گذشته وصله امنیتی مهمی را برای سرورهای سرویس Exchange منتشر کرد تا چهار آسیب‌پذیری روز صفر آن‌ها را اصلاح کند، اما این اتفاق ظاهرا از تداوم حملات هکرها جلوگیری نکرده است. مطابق گزارش وب‌سایت Krebs on Security و خبرگزاری Wired، گروه هکری «هافنیوم» (Hafnium) که به دولت چین وابسته است، پس از انتشار این وصله امنیتی با توان بیشتری به حملات خود ادامه داده است.

این گروه در آمریکا به حداقل ۳۰ هزار سازمان نظیر اداره‌های پلیس، بیمارستان‌ها، فرمانداری‌های محلی، بانک‌ها، شرکت‌های اعتباری، ارائه‌دهندگان خدمات ارتباطی و شرکت‌های غیرانتفاعی نفوذ کرده است. شمار قربانیان جهانی حمله به سرویس ایمیلی Exchange به چند صد هزار می‌رسد.

یک منبع آگاه به وب‌سایت Krebs گفت: «تقریبا همه کسانی که از سرویس Outlook Web Access میزبانی شخصی داشتند و وصله‌ی امنیتی مایکروسافت را نصب نکرده بودند، تحت حمله‌ی روز صفر قرار گرفتند.» یکی از کارمندان سابق امنیت ملی آمریکا در گفتگو با وایرد اعلام کرد که در هر ساعت به هزاران سرور در سراسر جهان حمله می‌شود.

زمانی که مایکروسافت از انتشار وصله امنیتی خود خبر داد، از شرکت Volexity بابت اطلاع‌رسانی پیرامون فعالیت‌های گروه هافنیوم تشکر کرد. حالا «استیون ادِیر» مدیر Volexity می‌گوید حتی شرکت‌هایی که وصله امنیتی را از همان روز اول نصب کرده بودند هم ممکن است هنوز در معرض خطر باشند.

وصله یادشده فقط آسیب‌پذیری‌های سرور Exchange را برطرف می‌کند، در حالی که قربانیان همچنان باید درهای پشتی کارگذاشته‌شده روی سیستم‌های خود را از بین ببرند. هافنیوم با استفاده از آسیب‌پذیری این سرویس «وب شل‌هایی» (Web Shell) را روی سرورهای قربانیان کار گذاشته که با ارائه دسترسی مدیریتی امکان سرقت اطلاعات را برای هکرها فراهم می‌کند. به گفته وب‌سایت Krebs، آقای ادیر و سایر متخصصان امنیت نگرانند که همزمان با تلاش قربانیان برای

حذف درهای پشتی موجود، هکرها درهای پشتی بیشتری را روی این سیستم‌ها کار بگذارند.

مایکروسافت از همان ابتدا گفته بود که این حملات ارتباطی با حمله بزرگ SolarWinds ندارد. ولی تعداد قربانیان گروه هافنیوم می‌تواند خیلی بیشتر از حمله «سولار ویندز» باشد. مقامات آمریکا معتقدند که در حمله سولار ویندز حدود ۱۸ هزار قربانی تحت تاثیر گرفتند. ولی برخلاف هکرهای حمله سولار ویندز که شرکت‌های بزرگ فناوری و سازمان‌های بزرگ دولتی را هدف قرار داده بودند، هافنیوم تمرکز خود را روی شرکت‌ها و سازمان‌های کوچک و متوسط قرار داده، بنابراین پای اشخاص بسیار بیشتری در میان است.

مایکروسافت در گفتگو با وب‌سایت Krebs اعلام کرد که مشغول همکاری نزدیک با سازمان امنیت سایبری و زیرساخت امنیتی آمریکا و چند سازمان دولتی و شرکت امنیتی دیگر است تا تحقیقات خود را کامل و راهنماهای لازم را منتشر کند. این شرکت تاکید کرده که بهترین کار نصب فوری آپدیت‌های جدید روی سیستم‌های قربانی است. این حمله ظاهرا فقط روی سرورهای Exchange نسخه ۲۰۱۳، ۲۰۱۶ و ۲۰۱۹ صورت گرفته است.

دیجیاتو