مایکروسافت: چینی‌ها با حمله به سرورهای Exchange سعی در سرقت اطلاعات دارند - دیجیاتو

ایمان صاحبی | چهارشنبه، ۱۳ اسفند ۱۳۹۹

مایکروسافت به مشتریان خود هشدار داده که مراقب حمله عوامل چینی به سرورهای سرویس Exchange باشند. چینی‌ها ظاهرا به چهار آسیب‌پذیری پیش‌تر شناخته‌نشده این سرویس که ارائه‌دهنده خدمات تجاری ایمیل است، حمله کرده‌اند.

این غول بزرگ نرم‌افزاری دیروز در اطلاعیه‌ای گفت معتقد است که گروهی از هکرها موسوم به «هافنیوم» (Hafnium) سعی دارند اطلاعات مجموعه گسترده‌ای از سازمان‌های آمریکایی، از جمله شرکت‌های حقوقی و پیمانکاران وزارت دفاع، را بدزدند. مایکروسافت می‌گوید شرکت‌های تحقیقاتی بیماری‌های عفونی و اندیشکده‌ها هم هدف حمله این هکرها قرار داشته‌اند.

این شرکت مدعی است هافنیوم از چهار آسیب‌پذیری جدید برای نفوذ به سرورهای سرویس ایمیلی Exchange استفاده کرده تا بتواند اطلاعات مدنظر خود را از شرکت‌های هدف به دست آورد و حتی در سرورها بدافزار کار بگذارد. اطلاعات مدنظر هکرها شامل حساب ایمیل و دفاتر آدرس‌های افراد بوده است.

این چهار آسیب‌پذیری در کنار یکدیگر زنجیره‌ای از حملات را به وجود می‌آورد که می‌تواند تمامی سرورهای مجهز به نسخه ۲۰۱۳ سرویس Exchange یا نسخه‌های بالاتر را به خطر بیندازد.

مایکروسافت می‌گوید گروه هافنیوم از داخل چین فعالیت می‌کند، اما برای اجرای حملات خود از سرورهای داخل خاک آمریکا استفاده می‌کند. این شرکت مدعی است که هافنیوم اصلی‌ترین گروه خطری است که از این چهار آسیب‌پذیری جدید برای حمله به شرکت‌ها بهره می‌جوید. البته مایکروسافت ابتدا در وبلاگ خود گفته بود که هافنیوم تنها گروه مهاجم است، اما بعدا این عبارت را تغییر داد.

این شرکت هنوز اعلام نکرده که چه تعداد از این حملات موفقیت‌آمیز بوده، اما تعداد آن‌ها را محدود اعلام کرده است. وصله‌های لازم برای رفع این چهار آسیب‌پذیری حالا زودتر از موعد همیشگی منتشر شده، چون مایکروسافت معمولا وصله‌های خود را در دومین سه‌شنبه هر ماه میلادی منتشر می‌کرد.

«تام برت» معاون بخش امنیت مشتریان مایکروسافت می‌گوید: «با وجود این که ما به سرعت آپدیتی را برای مقابله با حملات گروه هافنیوم منتشر کردیم، ولی می‌دانیم که بازیگران وابسته‌ی دولتی و گروه‌های تبهکار به سرعت در پی نفوذ به سیستم‌های وصله‌نشده خواهند بود.»

مایکروسافت می‌گوید سازمان‌های دولتی آمریکا را در جریان این یافته‌ها قرار داده، اما حملات گروه هافنیوم با حمله بزرگ «سولار ویندز» علیه سازمان‌های آمریکایی ارتباطی ندارد. FBI و سازمان امنیت ملی آمریکا در آخرین روزهای دولت ترامپ اعلام کردند که حمله سولار ویندز احتمالا منشأ روسی داشته است.

ديجياتو