روش احتمالی نفوذ هکرها به وزارتخانه‌های آمریکا شناسایی شد؛ ۱۸ هزار سازمان در معرض خطر - دیجیاتو

محمد قریشی | سه شنبه، ۲۵ آذر ۱۳۹۹

نزدیک به ۱۸ هزار سازمان در سراسر جهان ابزارهای مدیریت شبکه‌ای را دانلود کرده‌اند که حاوی یک در پشتی (Backdoor) است. شرکت «SolarWinds» که این ابزارها را ارائه می‌کند، اعلام کرده یک کشور از این در پشتی برای نصب بدافزار در سازمان‌ها و حمله سایبری بهره می‌برد.

کمپانی SolarWinds که مقر آن در «آستین» ایالت تگزاس قرار دارد، چنین موضوعی را یک روز پس از اینکه سازمان‌های دولتی آمریکا مانند وزارت خزانه‌داری، وزارت بازرگانی و وزارت امنیت ملی مورد حمله سایبری هکرهای روسی قرار گرفتند، اعلام کرده. طی این حمله به سازمان‌های فدرال، هکرها به ایمیل‌ها و سایر منابع حساس دسترسی پیدا کردند.

کمپانی امنیتی «FireEye» چند روز پیش از شناسایی یک رخنه امنیتی جدی به شبکه خود خبر داد. طبق اعلام این شرکت، هکرها که از سوی یک کشور حمایت می‌شوند، از مکانیزم آپدیت نرم افزار SolarWinds سوءاستفاده کرده‌اند و سپس از آن برای آلوده کردن برخی مشتریان که نسخه دستکاری شده ابزار مدیریت شبکه «Orion» را نصب کرده‌اند، بهره برده‌اند.

SolarWinds اعلام کرده سیستم مشتریانی که یک آپدیت را در فاصله ماه مارس تا ژوئن سال جاری میلادی نصب کرده‌اند، به این در پشتی آلوده شده. طبق گفته این کمپانی، بیلد سیستمی نرم افزار Orion دارای مشکل بوده و در کد منبع مخزن محصولات Orion چنین مشکلی وجود ندارد. SolarWinds از ۳۰۰ هزار مشتری Orion خبر داده که تعداد کل مشتریان آلوده به این در پشتی را به ۱۸ هزار می‌رساند.

این حملات سایبری و قرارگیری در پشتی در نرم افزار SolarWinds از سوی یک گروه از هکرهای تحت حمایت دولت روسیه به نام «Cozy Bear» صورت گرفته. طبق اعلام مقامات دولتی، مقامات FireEye و مایکروسافت این حملات بخشی از یک جاسوسی گسترده هستند که مهاجمان از طریق حمله زنجیره تامین انجام می‌دهد.

FireEye اعلام کرده در تحلیل‌های خود، سازمان‌های مختلفی را شناسایی کرده که مورد حمله سایبری قرار گرفته‌اند. بر اساس اعلام این کمپانی، هر کدام از حملات نیاز به برنامه‌ریزی دقیق و همچنین تعامل دستی داشته‌اند. FireEye همچنان به تحقیقات خود ادامه می‌دهد و اطلاعات بیشتری را در روزهای آینده منتشر خواهد کرد.

در پشتی Orion که FireEye آن را «Sunburst» و مایکروسافت «Solorigate» نامگذاری کرده، به هکرها دسترسی محدود اما مهمی به دستگاه‌های شبکه داخلی می‌دهد. پس از ورود به دستگاه‌ها، هکرها از تکنیک‌های دیگری برای دسترسی به اطلاعات بیشتر استفاده می‌کنند. طبق اعلام مایکروسافت، هکرها در ادامه امضای گواهینامه‌ها را سرقت می‌کنند که به آن‌ها اجازه می‌دهد هویت هریک از کاربران موردنظر خود را جعل کنند.

مقابله با حملات زنجیره تامین بسیار دشوار است چرا که از یک نرم افزار قابل اعتماد و محبوب استفاده می‌کنند. حالا Cozy Bear می‌تواند به شبکه‌های ۱۸ هزار مشتری SolarWinds نفوذ کند و حمله سایبری انجام دهد. در حال حاضر نمی‌دانیم چه تعدادی از این سازمان‌ها واقعا هک شده‌اند.

دیجیاتو