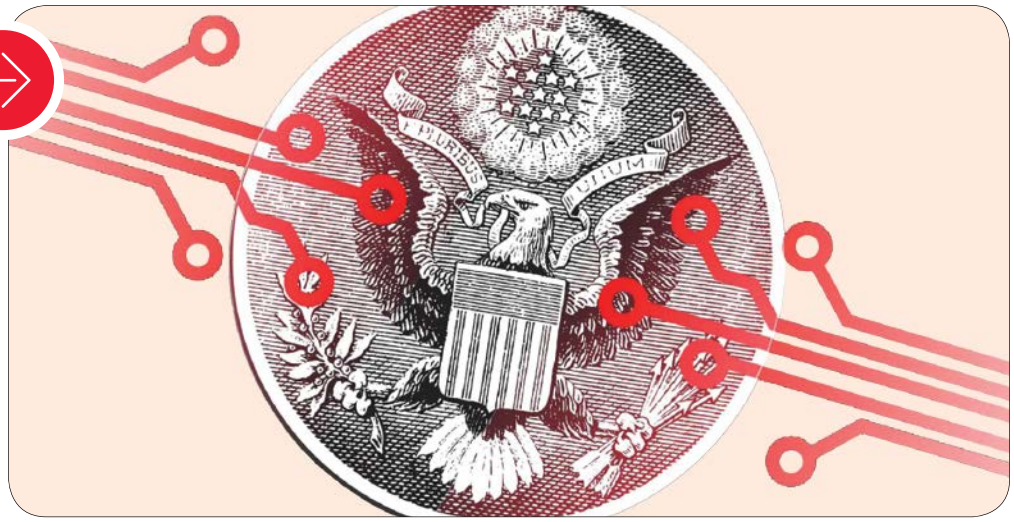
تفاوت اصلی حمله بی‌سابقه سولاروبیندز با دیگر حملات بزرگ سایبری، حمله به زیرساخت‌های اینترنتی به‌جای سرویس‌ها، سازمان‌های دولتی یا سایت‌هاست. این به معنی ایجاد پلتفرمی دائمی برای حملات ویرانگر بعدی است



حمله سولاروبیندز که با نام‌های مختلف دیگری هم مشهور شده، هنوز ادامه دارد و ممکن است مقابله با آن سال‌ها زمان لازم داشته باشد

بزرگ‌ترین حمله سایبری تاریخ چگونه آمریکا را دچار آسیب جدی امنیتی کرد؟

توفان خورشیدی

خشایار مریدپور
روزنامه‌نگار فناوری

داستان از جایی شروع شد که شرکت امنیت سایبری فایر آی که مشتریان بسیاری در حوزه نظامی، امنیتی، مالی و دولتی دارد، متوجه شد مورد حمله قرار گرفته و اطلاعاتش به سرقت رفته است. یک شرکت امنیت سایبری با ابعاد فایر آی قاعدتا نباید مورد دستبرد اطلاعاتی قرار بگیرد، پس باید هرچه زودتر تکلیف این آبروریزی روشن می‌شد. فایرآی به سرعت یافتن ابعاد و عوامل احتمالی حمله را آغاز کرد. ولی بررسی‌ها درباره این حمله آنها را به نتیجه ترسناک‌تری رساند: شرکت سولاروبیندز که از فراگیرترین تامین‌کننده نرم‌افزارهای زیرساخت پایش و امنیت شبکه است، مورد حمله قرار گرفته و از طریق یک فایل آپدیت بیش از ۱۸ هزار مشتری مهم در سراسر جهان را به بدافزار سان‌برست آلوده کرده بود. حالا این رسوایی چند روزی است که ابعاد بزرگ‌تری هم پیدا کرده و به سرعت لقب بزرگ‌ترین حمله سایبری تاریخ را به خود اختصاص داده است. اما چه چیزی این حمله سایبری را اینقدر متفاوت، خطرناک و گسترده کرده و آیا ممکن است شما را هم تحت تاثیر قرار دهد؟ برای دانستن پاسخ همراه ما باشید.

آغاز پایان

در دنیای امروز، جنگ سرد اتمی بین بلوک‌های شرق و غرب جای خود را به نبردهای سایبری داده‌اند که در خفا و دور از چشم مردم عادی در گوشه و کنار شبکه جهانی اینترنت هر روز در جریان هستند. در نتیجه اخباری مثل حمله به زیرساخت‌های دولتی توسط هکرهای دولت‌های متخاصم یا دزدی اطلاعاتی توسط رقبای تجاری درحال تبدیل به خبرهای روزمره هستند، اما چند روز پیش فایر آی که یک شرکت خصوصی متخصص امنیت سایبری با مشتریانی مثل وزارت دفاع ایالات متحده آمریکاست، متوجه نوع جدیدی از حمله شد. نوع جدیدی از حمله که کاملا بی‌سابقه است و می‌تواند عواقب بسیاری برای دنیای فناوری اطلاعات داشته باشد.

بنابر گزارش رویترز، متخصصان این شرکت پس از اطلاع از حمله و پس از بررسی‌های اولیه متوجه حقیقتی هولناک شدند؛ این حمله از طریق فایل به‌روزرسانی امنیتی دریافتی یک شرکت خدمات زیرساخت ارتباطی به نام سولاروبیندز (یا بادهای خورشیدی) وارد سیستم آنها شده و کدها، ابزارها و اطلاعات موردنیاز برای حمله به دیگر مشتریان این شرکت را دزدیده بود. شرکت سولاروبیندز مشتریان نامدار بسیاری در سراسر جهان دارد و خدمات زیرساختی خود را به شرکت‌هایی مثل فایرآی و مایکروسافت ارائه می‌دهد.

این شرکت خود متخصص پایش و امنیت شبکه است و محصولات آن توسط بسیاری از شرکت‌های بزرگ و سازمان‌های دولتی و اقتصادی برای دفاع در برابر حملات سایبری و پایش شبکه برای فعالیت‌های مشکوک به‌کار برده می‌شوند.

در نتیجه سرویس Orion این شرکت که توسط هکرها به‌عنوان ناقل بیماری مورد سوءاستفاده قرار گرفته بود به تمام اطلاعات شبکه کاربران خود دسترسی داشت و حتی در برخی موارد مشتریان از به‌کار بردن نرم‌افزارهای آنتی‌ویروس برای بررسی آن منع شده بودند. همین موضوع یعنی دسترسی تمام و کمال سولاروبیندزو و در ادامه هکرها به اطلاعات کامل مشتریان، باعث شده است تا این حمله سایبری به‌سرعت به‌عنوان یکی از ویرانگرترین و گسترده‌ترین حملات در نوع خود مطرح شود.

یکی از دلایل کشف دیرهنگام این بدافزار، حجم بالای فایل حاوی آن بود. بیشتر آنتی‌ویروس‌ها فایل‌های بزرگ‌تر از ۱۰ مگابایت را پویش نمی‌کنند و به‌همین دلیل هکرها بدافزار خود را سوار بر یک فایل به‌روزرسانی ۲۰۰ مگابایتی کرده بودند

مثل هیچ‌کدام

همان‌طور که گفتیم، حمله سولاروبیندز با تمام حملات سایبری قبلی متفاوت است، چراکه به‌جای هدف قرار دادن یک سیستم به‌خصوص یا بخش مشخصی از یک سازمان دولتی سراغ زنجیره تامین نرم‌افزاری و زیرساخت‌های امنیت شبکه رفته است. هکرها با نفوذ به شبکه سولاروبیندز و دسترسی به اطلاعات شبکه مشتریانی مثل مایکروسافت و فایرآی راه نفوذ به شبکه سایر مشتریان آنها و حتی مشتریان رده سوم را نیز به‌دست آورده‌اند. این یعنی دزدی اطلاعات ناشی از این حمله می‌تواند تا سال‌ها ادامه داشته باشد و محدود به سازمان‌های آسیب‌دیده فعلی نخواهد شد.

هرچند مایکروسافت اعلام کرده موفق به کشف و محدود ساختن بدافزار سان‌برست در شبکه خود شده است و خطری مشتریان این شرکت را تهدید نمی‌کند، اما کماکان همه متخصصان بر این نکته اتفاق نظر دارند که کار بدافزار سان‌برست تمام نشده و هنوز تا روشن شدن ابعاد واقعی ماجرا زمان زیادی لازم است.

درواقع تفاوت اصلی این حمله با دیگر حملات، نبود حد و مرز مشخص برای میزان آلودگی سیستم‌های مختلف به بدافزار و نداشتن ایده‌ای مشخص درباره زمان شروع این حمله و میزان دسترسی به‌دست آمده توسط هکرهاست. درواقع ما تنها به‌تازگی متوجه وقوع این حمله شده‌ایم، اما ممکن است از مدت‌ها پیش بسیاری از سازمان‌های قربانی آلوده شده باشند.

به گفته برد اسمیت، مدیرعامل مایکروسافت، این حمله که کماکان در جریان است «از نظر ابعاد، پیچیدگی و تاثیر» بی‌سابقه است. به نظر مدیرعامل مایکروسافت این حمله «یک تلنگر جدی برای کل سیستم امنیت سایبری است و نشان‌دهنده یک بی‌احتیاطی فاجعه‌بار است که یک آسیب‌پذیری امنیتی جدی برای ایالات متحده و کل جهان ایجاد کرده است».

او همچنین در پست وبلاگی خود در این باره افزود: «این حمله به چند هدف به‌خصوص نیست، بلکه حمله به اعتماد و اطمینان‌پذیری زیرساخت‌های حیاتی ارتباطی جهان برای پیشبرد اهداف سازمان اطلاعاتی یک کشور به‌خصوص است.» منظور اسمیت از یک کشور به‌خصوص روسیه است، کشوری که سابقه حملات متعدد و پیچیده علیه ایالات متحده را در کارنامه دارد و اکنون به‌عنوان مضنون اصلی این حمله شناخته می‌شود.

آتش زیر خاکستر

درست همان‌طور که همه‌گیری کرونا باعث ایجاد زلزله‌ای عظیم در زیرساخت‌های درمانی جهان شد، حمله سولاروبیندز هم تبعات ماندگار و مخربی دارد که تا مدت‌ها گریبانگیر طرفین درگیر خواهد بود. مشخص نیست این حمله توسط روس‌ها انجام شده باشد یا نه، اما ابعاد و پیچیدگی بی‌سابقه این حمله در کنار اهداف بیشتر نظامی سیاسی آن باعث شده است که همه متخصصان متفق‌القول معتقد باشند یک دولت متخاصم و نه مجموعه‌ای از هکرهای مستقل، این حمله را انجام داده‌اند. هرچه باشد، این حمله بدون شک دنیای امنیت سایبری را برای همیشه متحول می‌کند و تا سال‌ها ممکن است باعث دردسرهای پیش‌بینی نشده برای شرکت‌ها و سازمان‌های آسیب‌دیده و تمام مشتریان و کاربران آنها شود. هرچند حداقل در حال حاضر هیچ نشانی از وجود خطر به‌خصوص برای کاربرهای عادی وجود ندارد و نیازی نیست نگران امنیت اطلاعات خود و مقابله با سان‌برست باشید. البته این‌طور که به نظر می‌رسد، ممکن است در آینده‌ای نه‌چندان دور مجبور شویم با این امنیت خداحافظی کرده و برای مقابله با توفان خورشیدی بعدی در دنیای امنیت سایبری آماده شویم.