یکشنبه 24 اردیبهشت 1396 - 08:21

آنچه تاکنون درباره بزرگ‌ترین باج‌گیری سایبری جهان می‌دانیم

حمله سایبری گسترده‌ای که از روز جمعه ۱۲ مه (۲۲ اردیبهشت) شروع شد و به حدود ۱۰۰ کشور جهان گسترش یافت، به اختلال کامپیوترها و از دسترس خارج شدن فایل‌ها انجامید که از موارد شاخص آن اختلال در سرویس ملی بهداشت بریتانیا (NHS) بود.

همشهری آنلاین:حمله سایبری گسترده‌ای که از روز جمعه ۱۲ مه (۲۲ اردیبهشت)‌ شروع شد و به حدود ۱۰۰ کشور جهان گسترش یافت، به اختلال کامپیوترها و از دسترس خارج شدن فایل‌ها انجامید که از موارد شاخص آن اختلال در سرویس ملی بهداشت بریتانیا (NHS) بود.

کارشناسان امنیت کامپیوتری هم‌اکنون در این کشورها در تلاش برای مهار کردن این حمله هستند که به‌وسیله بدافزاری که باج‌افزار نامیده می‌شود، هستند. این باج افزارها داده‌های موجود در کامپیوترها را با رمزگذاری از دست کاربران خارج می‌کند و برای بازگرداندن آن‌ها پول طلب می‌کند.

گسترش این حمله سایبری در ایالات‌متحده کمتر از اروپا و آسیا بوده است و ظاهراً بلاگر جوان بریتانیایی با نام توئیتری MalwareTechBlog@، به‌طور اتفاقی در این زمینه نقش داشته است. هک کننده‌ها که هنوز هویتشان مشخص نیست، شیوه‌ای را برای از کار انداختن این بدافزار در مواردی که خودشان بخواهند حمله را متوقف کنند، تعبیه کرده بودند. این شیوه شامل کدی در باج‌افزار می‌شد که درصورتی‌که این ویروس درخواست آنلاینی برای ورود به وب‌سایت ایجادشده به‌وسیله خود هک کننده‌ها بفرستد، مانع از انتشار آن می‌شد.

این جوان بریتانیایی نام دامنه این به‌اصطلاح سوئیچ مرگ را یافت. هنگامی این سایت فعال شد، در کمال تعجب او گسترش حمله متوقف شد. البته به گفته او این توقف موقتی است زیرا مهاجمان می‌توانند بدافزاری با یک نام دامنه متفاوت بسازند.

هک کننده‌ها ظاهر از یک نقطه‌ضعف در سیستم‌عامل ویندوز مایکروسافت استفاده کردند که سازمان امنیت ملی آمریکا آن را یافته بود. این خطا و ابزاری که می‌تواند از این خطا با یک بدافزار به نام WanaCryptor 2.0 بهره ببرد در ماه آوریل به‌وسیله گروهی هکر به نام Shadow Borders روی اینترنت علنی شد.

در اینجا مروری می‌کنیم بر چیزهای که تابه‌حال درباره این حمله می‌دانیم:

- کامپیوترهای آلوده پیامی را نشان می‌دهند که خواستار باجی ۳۰۰ دلاری به ازای هر کامپیوتر است که باید به‌صورت پول مجازی به یک آدرس «کیف پول بیت‌کوین» فرستاده شود.

شما فقط سه روز وقت دارید تا باج را بپردازید. پس‌ازاین مدت میزان باج دو برابر می‌شود و اگر پس از هفت روز باج را نپردازید، دیگر هرگز نمی‌توانید فایل‌های‌تان را بازیابی کنید. کارشناسان می‌گویند مهاجمان ممکن است بتوانند پیش از پایان یافتن مهلت داده‌شده بیش از یک میلیارد دلار از افراد در سراسر جهان به جیب بزنند.

- در میان شرکت‌ها و سازمان‌های دولتی دچار این حمله شده می‌تواند به شرکت آمریکایی انتقال محموله فدکس، سرویس ملی بهداشت بریتانیا و وزارت کشور روسیه اشاره کرد.

- در آسیا، گزارش‌های فراوانی از حمله‌ها به دانشگاه‌ها داده شده است، به‌طوری‌که دانشجویان با رمزگذاری شدن پایان‌نامه‌ها و مقالات نهایی‌شان در آستانه فارغ‌التحصیلی و ناتوانی در دسترسی به آن‌ها روبرو شده‌اند.

- درمجموع بیش از ۴۵۰۰۰ حمله در حدود ۱۰۰ کشور ثبت شده است. به گفته شرکت روسی امنیت سایبری کسپرسکی، روسیه بیشترین حملات را متحمل شده است و در رده‌های بعدی اوکراین، هند و تایوان قرار دارند.

- شرکت مایکروسافت پس از حمله یک پچ یا وصله امنیتی جدید برای نرم‌افزار ویندوز منتشر کرده است.

- دست‌کم ۴۵ بیمارستان و تأسیسات درمانی دیگر در بریتانیا تحت تأثیر حملات قرار گرفته‌اند، به‌طوری‌که پزشکان نمی‌توانند به پرونده‌های بیماران دست یابند و بخش‌های اورژانس بیماران را به مراکز درمانی دیگر ارجاع داده‌اند. البته ترزا می، نخست‌وزیر بریتانیا می‌گوید شاهدی در دست نیست که داده‌های بیماران دزدیده شده باشد.

- روز شنبه مقامات بریتانیایی اعلام کردند که ۴۸ بنیاد از ۲۴۸ بنیاد بهداشت عمومی در این کشور یعنی حدود ۲۰ درصد نظام بهداشتی این کشور تحت تأثیر این حمله سایبری قرار گرفته‌اند.

- شرکت‌های اروپایی مانند دویچ باهن، غول حمل‌ونقل در آلمان، تلفونیکا، یک شرکت مخابراتی در اسپانیا و شرکت خودروسازی رنو در فرانسه اعلام کرده‌اند که برخی از سیستم‌هایشان تحت تأثیر قرار گرفته است، هرچند اشکال عمده‌ای در شبکه‌های حمل‌ونقل و مخابراتی در این منطقه اروپا گزارش نشده است.

- وزارت کشور روسیه در بیانیه‌ای تأیید کرد که هزار کامپیوترش مورد تهاجم قرار گفته‌اند.

- شرکت امنیت اینترنتی چینی کیهو ۳۶۰ درباره این ویروس هشدار داد و گفت بسیاری از شبکه‌ها موردحمله قرارگرفته‌اند و برخی از کامپیوترها در چین برای «نقب زدن بیت‌کوین» در چین استفاده می‌شوند، در میان ماشین‌های آلوده شده هستند.

- سخنگوی شرکت فدکس گفت که این شرکت مانند بسیاری از شرکت‌های دیگر به علت این بدافزار دچار اختلال در برخی از سیستم‌های بر اساس ویندوزش شده است و با حداکثر سرعت ممکن در حال انجام اقداماتی برای حل این مشکل است.

- گزارش‌هایی که سال گذشته منتشر شد نشان داد که برخی از بیمارستان‌های دولتی بریتانیا تقریباً هیچ پولی صرف دفاع سایبری نکرده‌اند و از نرم‌افزارهای منسوخ‌شده مثلاً ویندوز XP که دیگر به‌وسیله مایکروسافت پشتیبانی امنیتی نمی‌شوند، روی سیستم‌هایشان استفاده می‌کنند.

درست یک روز پیش از این حمله، دکتر کریشنا چینتاپالی، متخصص نورولوژی در بیمارستان ملی نورولوژی و جراحی اعصاب در لندن مقاله‌ای در ژورنال پزشکی بریتانیا منتشر کرد که در آن هشدار داده بود بیمارستان‌های نظام بهداشتی بریتانیا باید آماده مواجهه با حوادثی دقیقاً از همین نوع باشند. او نوشت: «بیمارستان‌ها به‌احتمال قریب‌به‌یقین امسال درنتیجه حمله باج‌افزارها از کار خواهند افتاد.»

منبع: نیویورک‌تایمز