راهزنان بر سر راه قطارهای شهری

سیستم حمل‌ونقل شهر سانفرانسیسکو هک شد!

زیرساخت‌های شهری سان‌فرانسیسکو جمعه خوبی را سپری نکردند. به دلیل این‌که سیستم حمل و نقل Muni واقع در سان‌فرانسیسکو قربانی یک حمله باج‌افزاری شد. بعد از این حمله اپراتورها روی سامانه‌های خود پیغام شما "مورد نفوذ قرار گرفته‌اید. تمامی داده‌های شما رمزنگاری شده‌اند" را مشاهده کردند.

در این پیام از اپراتورهای سامانه‌های قربانی درخواست شده بود در سایت yandex.com با کاربری به نام cryptom27 تماس برقرار کنند تا کلید مربوط به رمزگشایی فایل‌ها را در اختیار آن‌ها قرار دهد. زمانی که مسافران به سیستم پرداخت کرایه در ایستگاه‌ها مراجعه می‌کردند پیغام سرویس‌دهی امکان‌پذیر نیست را مشاهده می‌کردند. به همین دلیل راه‌آهن شهری سان‌فرانسیسکو که Muni نام دارد به مشتریان خود اجازه داد از خطوط ریلی به طور رایگان استفاده کنند، به سبب آن‌که امکان دریافت کرایه از مسافران مقدور نبود.

مقامات مربوطه به سایت CBS گفته‌اند: «این هک برای چند روز پیرامون این سامانه حمل و نقل قرار داشت و بر روند کاری کارکنان این شرکت تاثیرگذار بوده است. ما بر این باور هستیم که هکرها به سرورهای بانک‌اطلاعاتی، ایمیل، حمل و نقل و حتا سامانه‌های پرداختی حمله کرده‌اند. به طوری که نزدیک به یک چهارم کامپیوترها (2112 کامپیوتر از تعداد 8656 کامپیوتر) قربانی این حمله شده‌اند. همین تعداد سامانه هک شده برای اعلام یک وضعیت اضطراری کافی بود. با این وجود ما متوجه شده‌ایم که سرورهای پشتیبان در امنیت و سلامت کامل قرار دارند.» بزرگ‌ترین نگرانی Muni این بود که شاید در این مدت اطلاعات کاملا از درست رفته باشند و هیچ‌گونه نسخه پشتیبانی از اطلاعات در دسترس نباشد.

مطلب پیشنهادی

باج‌افزار محتاج کمک

هکرها در اقدامی کم سابقه درخواست کمک کردند

پژوهشگران امنیتی بر این باور هستند که این باج‌افزار به احتمال زیاد نسخه‌ای از باج‌افزار HDDCryptor است. باج‌افزاری که برای رمزنگاری فایل‌های اشتراکی روی شبکه از ابزارهای تجاری استفاده می‌کرد. شرکت امنیتی ترندمیکرو در سپتامبر (شهریور) گزارش کرد که این باج‌افزار تهدید بزرگی برای کامپیوترهای شخصی و شرکت‌ها است. به سبب آن‌که تنها منابع اشتراکی شبکه همچون درایوها، چاپگرها، فایل‌ها، پوشه‌ها و درگاه‌های سریالی را

هدف خود قرار نداده و قادر است یک درایو را به طور کامل رمزنگاری کند. روز گذشته مدیران حمل و نقل سان‌فرانسیسکو گزارش کردند که موفق شدند سامانه‌های کامپیوتری این شرکت را که روز جمعه قربانی این حمله شدند را ترمیم کنند. این شرکت اعلام کرد، هکرها برای دسترسی مجدد به فایل‌های قفل شده چیزی در حدود 73 هزار دلار باج را درخواست کرده بودند.

مطلب پیشنهادی

باج‌افزاری که نیامده هک شد
اولین باج‌افزار مبتنی بر زبان Go کار خود را با شکست آغاز کرد!

این احتمال وجود دارد که هکرها از تکنیک فیشینگ استفاده کرده باشند. جایی که یکی از کارمندان این شرکت فریب خورده و از طریق یک ایمیل فریبنده یا یک سایت فریبنده یک محتوای مخرب را نصب کرده باشد. هر چند هنوز هیچ چیز در تحقیقات اولیه مشخص نیست. با این وجود هنوز به درستی مشخص نیست که آیا Muni در نهایت این باج را پرداخت کرده است یا برای رمزگشایی فایل‌های قفل شده از راهکارهای دیگری استفاده کرده است. لازم به توضیح است که کیف بیت‌کوینی که هکرها برای دریافت باج مربوطه، شناسه موردنظر خود را از طریق ایمیل برای Muni ارسال کرده بودند تا حوالی بعد از ظهر یکشنبه خالی بود. با این توصیف می‌توانیم این‌گونه نتیجه‌گیری کنیم که احتمالا باج مربوطه به شیوه دیگری برای هکرها ارسال شده است.

تاریخ انتشار:

09 آذر 1395

نشانی منبع: https://www.shabakeh-mag.com/security/5696