درآمد میلیون دلاری هکر طراح باج افزار SamSam - دیجیاتو

یونس مرادی | چهارشنبه، ۱۰ مرداد ۱۳۹۷

بر اساس گزارش موسسه امنیتی Sophos باج افزار SamSam که احتمالا یک نفر طراح آن است، تا کنون ۵.۹ میلیون دلار باج از قربانیان خود اخذ کرده و این در حالی است که تخمین های کارشناسان به مراتب کمتر از این مقدار بوده است.

هکرها در حملات خود تقریبا هر روزه از SamSam بهره برده اند اما با توجه به خاص بودن اهداف آنها اغلب کاربران از این حملات در امان مانده اند. مهاجمان ابتدا در برابر برگرداندن فایل های قربانی خواهان یک بیت کوین می شدند اما این مقدار رفته رفته به ۱.۵ و پس ۱.۷ بیت کوین رسید.

Sophos در گزارش خود از احتمال دست داشتن تنها یک هکر در توسعه این باج افزار خبر داده است:

یک دست بودن زبان طراحی باج افزار، سایت های پرداخت، نمونه فایل ها و دانش پشت آنها حاکی از توسعه SamSam توسط یک نفر است. موارد دیگری نظیر عدم افشای اطلاعات توسط هکرهای دیگر و مخفی ماندن هویت طراح نیز این ظن را تقویت می کند.

باج افزارهای دیگر معمولا از طریق لینک های آلوده در ایمیل روی سیستم نصب شده و به سرعت شروع به کدگذاری فایل های سیستم می کند. با این حال داستان در مورد SamSam متفاوت است. در این کمپین هکر از طریق آسیب پذیری های معمول یا روش جستجوی احتمالی و شکستن کلمات عبور ضعیف در سرویس ریموت دسکتاپ وارد سیستم شده، آن را اسکن کرده و باج افزار را اجرا می کند.

پیش از این تصور می شد که این باج افزار سرور اصلی سازمان‌های خاص مانند بیمارستان‌ها، مراکز بهداشتی و مدارس را مورد هدف قرار می‌دهد، اما بررسی های عمیق تر حاکی از این است که بخش عمده ای قربانیان آن را شرکت های خصوصی تشکیل می دهد که علاقه ای به افشای جزئیات باج های پرداختی خود ندارند.

بر این اساس کسب و کارهای بخش خصوصی ۵۰ درصد، مراکز بهداشتی ۲۶ درصد، سازمان های دولتی ۱۳ درصد و بخش آموزشی ۱۱ درصد از قربانیان SamSam را تشکیل می دهند که اغلب در کشورهای آمریکا، انگلیس، بلژیک، کانادا، استرالیا و دانمارک واقع شده اند.

چند ماه قبل مرکز ماهر به مدیران و راهبران شبکه‌ها هشدار داد برای در امان ماندن از این باج افزار پس از بروزرسانی سیستم‌عامل و نصب آخرین وصله‌های امنیتی، نسبت به امن سازی سرویس‌های موجود در شبکه خصوصاً RDP اقدام کنند و حتماً از پشتیبان‌گیری منظم داده‌ها مطمئن شوند.

دیجیاتو