ذخیره‌سازهای متصل به شبکه هدف بدافزار استخراج‌کننده ارز رمزپایه

۷۰ درصد ذخیره‌سازهای NAS سی‌گیت سنترال آلوده به بدافزار هستند!

به تازگی گونه خاصی از بدافزارها به نام PhotoMiner (به نام Mal/Miner-C نیز شناخته می‌شود) در فضای سایبری منتشر شده است. بدافزاری که ذخیره‌سازهای متصل به شبکه NAS (سرنام Network Attached Storage) شرکت سیگیت سنترال را آلوده کرده و از آن‌ها برای آلوده کردن دیگر کامپیوترهای متصل به شبکه استفاده می‌کند. این‌کار با هدف دسترسی به ارز رمزپایه مونرو مورد استفاده قرار می‌گیرد.

مونرو (Monero) یک ارز رمزنگاری شده متن باز است که در سال 2014 ساخت شد. مونرو تمرکزش بر حریم خصوصی، تمرکز زدایی و گسترش‌پذیری است. بر خلاف دیگر ارزهای رمز پایه که از بیت‌کوین مشتق شده‌اند، مونرو بر مبنای پروتکل CryptoNote و الگوریتم‌های مبتنی بر بلاکچین که برای مبهم کردن داده‌ها مورد استفاده قرار می‌گیرند، فعالیت می‌کند.

Miner-C هارددیسک‌های NAS شرکت سیگیت سنترال را هدف قرار داده است

بدافزار Mine-C یا PhotoMiner اولین بار در ماه ژوئن شناسایی شد. زمانی که برای اولین بار یک گزارش نشان داد چگونه بدافزاری موفق شده است سرورهای FTP را هدف قرار داده و بر مبنای ویژگی‌های یک کرم اینترنتی به سرعت ماشین‌های جدید و سرورهای FTP مختلف را با استفاده از یک فهرست از اعتبارنامه‌های پیش فرض آلوده سازد. دستگاه‌های سیگیت سنترال یک پوشه عمومی در اختیار کاربران معتبر و حتا کاربران ناشناس قرار می‌دهند. این هارددیسک‌ها به آسانی آلوده می‌شوند، به سبب آن‌که سیگیت به کاربران اجازه نمی‌دهد، پوشه ویژه‌ای که به اشتراک قرار گرفته است را مادامی که دستگاه به اینترنت متصل است، حذف کرده یا آن‌را غیر فعال سازند.
گزارش‌های منتشر شده نشان می‌دهند که Mincer-C تنها مونرو یکی از سودآورترین ارزهای رمزنگاری شده را هدف قرار داده است. آمارها نشان می‌دهند که چیزی در حدود 5000 دستگاه NAS در سراسر جهان آلوده شده‌اند. تصویر زیر نشان می‌دهد که چگونه این دستگاه‌ها در کشورهای مختلف آلوده شده‌اند.

بدافزار Miner-C کاربران را فریب می‌دهد که یک استخراج کننده ارزرمزپایه را نصب کنند

بدافزار Miner-C روی هر دستگاه NAS سیگیتی که شناسایی کند، فرآیند کپی کردن فایل‌ها درون پوشه عمومی را به مرحله اجرا در می‌آورد. Photo.scr یکی از فایل‌هایی است که درون این پوشه کپی می‌شوند. Photo.scr یک فایل اسکریپتی است که کدنویسان بدافزار آن‌را به گونه‌ای ویرایش کرده‌اند که همانند آیکن استاندارد پوشه ویندوز به نظر برسد. به دلیل این‌که ویندوز در حالت عادی فرمت فایلی فایل‌ها را پنهان می‌سازد، هر زمان مالک دستگاه به NAS مراجعه کند، این فایل را به صورت یک پوشه مشاهده خواهد کرد. زمانی که این فرد سعی کند به پوشه مذکور وارد شود، ناخواسته فایل Photo.scr را اجرا می‌کند. این ترفند باعث نصب یک برنامه کاوشگر ارزرمزپایه روی سیستم قربانی می‌شود. Miner-C یکسری ویژگی‌های خاص دارد که از آن جمله می‌توان به روش منحصر به فرد بارگذاری فایل پیکربندی و قطعات مختلفی که برای انجام کارهای مختلف مورد استفاده قرار می‌گیرند، اشاره کرد.

سردرگمی مالکان سیگیت سنترال باعث شده است که آن‌ها هیچ راهی برای محافظت از دستگاه‌های خود پیدا نکنند. خاموش کردن ویژگی دسترسی از راه دور به NAS مانع از آلوده شدن آن می‌شود، اما اینکار به معنای محروم شدن از یک ویژگی قدرتمند است. ویژگی شاخصی که بسیاری از افراد برای در اختیار داشتن آن حاضر شده‌اند این دستگاه را خریداری می‌کنند.

منبع:
اسلش‌دات
تاریخ انتشار:
23 شهریور 1395

نشانی منبع: https://www.shabakeh-mag.com/security/4598