این بدافزار با استفاده از ابزار NSA پول مجازی استخراج می‌کند - دیجیاتو

محسن خوشنود | جمعه، ۰۶ اردیبهشت ۱۳۹۸

دو سال پس از انتشار اسناد محرمانه سازمان امنیت ملی ایالات متحده «NSA» و افشای رخنه های امنیتی مورد استفاده آن، هکرها هنوز هم از ابزارهای لو رفته برای انجام حملات و توسعه بدافزار ارزکاو بهره می برند.

در یکی از جدیدترین موارد، محققان شرکت امنیت سایبری سیمنتک اظهار کرده اند که فعالیت بدافزار Beapy افزایش قابل توجهی داشته و با انتشار در سطح شبکه شرکت های مختلف، در حال استفاده از توان پردازشی رایانه ها برای استخراج پول مجازی است.

بیش از 80 درصد قربانیان بیپی در چین حضور دارند

بیپی نخستین بار اوایل زمستان سال گذشته رؤیت شد اما در چند روز اخیر فعالیت آن بیشتر شده و طبق اطلاعات سیمنتک، توانسته بیش از 12 هزار آدرس کامپیوتری مختلف از 732 سازمان و شرکت را آلوده کند. طبق اظهارات الن نویل محقق ارشد سیمنتک، بدافزار ارزکاو بیپی خصوصاً شرکت های بزرگ را مورد حمله قرار می دهد که به دلیل تعداد بالای کامپیوترهای موجود روی شبکه آنها، امکان استخراج مقادیر قابل توجهی ارز رمزنگاری شده را فراهم خواهد کرد.

Beapy برای اجرای حمله، ابتدا نیازمند باز کردن ایمیل حاوی بدافزار توسط یکی از کارمندان سهل انگار داخل سازمان بوده که پس از باز شدن ایمیل مورد نظر، بیپی بدافزار «DoublePulsar» که توسط NSA توسعه یافته بود را برای ایجاد درب پشتی روی سیستم نصب می کند.

در مرحله بعد بدافزار «EternalBlue» (باز هم متعلق به NSA) برای انتشار حمله در سطح شبکه مورد استفاده قرار می گیرد که در همکاری با دابل پولسار، برای هکرها در کل شبکه هدف درب پشتی ایجاد خواهد کرد.

در نهایت ابزار سرقت اطلاعات متن باز «Mimikatz» هم روی سیستم ها اجرا می شود تا با سرقت نام کاربری و کلمه عبور افراد مختلف، امکان گسترش سریع تر حمله در سطح سازمان را فراهم کند.

لازم به ذکر است که روش مورد استفاده بدافزار ارزکاو بیپی، مشابه حملات باج افزار واناکرای در سال 2017 است که کامپیوترهای زیادی را در سطح جهان (و ایران) درچار مشکل کرد.

گفتنی است حملات سایبری برای استخراج پول مجازی در حالت عادی، برای حریم خصوصی و اطلاعات کاربران خطری ندارند اما با درگیر کردن منابع سیستم، منجر به کندی رایانه و فرسودگی زودهنگام آن خواهند شد.

دیجیاتو