بدافزار تازه روسی ارزهای مجازی را براساس پیکره بندی سیستم ها استخراج می کند - دیجیاتو

Maryam Mousavi | چهارشنبه، ۲۳ آبان ۱۳۹۷

اگر کامپیوتر خانگی تان کند شده و بیش از اندازه داغ می کند شاید قربانی یک بدافزار تازه روسی شده باشید که برای سرقت توان محاسباتی سیستم شما و در نهایت استخراج ارزهای مجازی طراحی شده است.

محققان شرکت مک آفی نوع جدیدی از بدافزار سرقت ارز مجازی را کشف کرده اند که با استفاده از توان پردازشی سیستم های کامپیوتری اقدام به استخراج ارز مجازی مونرو یا Zcash می کند.

اما نکته جالب در این باره آن است که این بدافزار تازه روسی با نام WebCobra بسته به پیکره بندی سیستم شما ارز مجازی متفاوتی را استخراج خواهد کرد. کارشناسان مک آفی با بررسی و تحلیل دقیق این بدافزار دریافتند که هکرها از طریق یک پکیج مخرب اینستالر مایکروسافت اقدام به توزیع آن می کنند. جالب آنکه این پکیج برای نصب ماینرها یا استخرج کننده های Cryptonight روی سیستم های x86 و همچنین ماینر Zcash روی سیستم های x64 طراحی شده است.

لازم به یادآوری است که استخراج کننده Cryptonight صرفا محدود به مونرو نیست. در واقع این ابزار با طیف وسیعی از دیگر سکه های مجازی که از الگوریتم Cryptonight استفاده می کنند سازگاری دارد.

با وجود آنکه محققان منشاء این بدافزار را روسیه اعلام کرده اند گزارش جدید منتشر شده در این باره حکایت از آن دارد که هم اکنون آلودگی به کشورهای برزیل، آمریکای جنوبی و آمریکا رسیده است. با این حال اما یک نکته روشن است: بدافزارهای سرقت ارز مجازی روز به روز پیشرفته تر می شوند.

هفته گذشته دانشمندان به تاکتیک تازه ای برای تمیز دادن بدافزارهای استخراج ارز از فایل های قانونی نصب ویندوز دست یافتند. محققان امنیتی سوئیس نیز در همین راستا هشدار داده اند که کلاهبرداران ارزهای مجازی مرتبا تکنیک های تازه ای نظیر حملات تروجان را برای سوء استفاده از قربانیان خود به کار می برند. حالا لابراتوارهای مک آفی اعلام کرده اند که این روند احتمالا تا

آینده نزدیک ادامه پیدا می کند.

افزایش ارزهای مجازی همچنین مجرمان سایبری را بر آن داشته تا از بدافزارهایی برای دستیابی به اهداف خود استفاده کنند که منابع سیستم های کامپیوتری را برای استخراج سکه های ارز مجازی بدون رضایت قربانیان به سرقت می برند. این گزارش برای آنکه حزئیات بیشتری را در این باره ارائه دهد اشاره می کند که CoinHive (یکی دیگر از ابزارهای استخراج ارز مجازی مونرو که غالبا توسط هکرها مورد استفاده قرار می گیرد) ماهانه سودی بالغ بر ۲۵۰ هزار دلار را به ارمغان می آورد.

همزمان با تلاش مجرمان سایبری برای بهره برداری از این روش آسان درآمدزایی، بدافزارهای استخراج ارز مجازی نیز مرتبا پیچیده تر می شوند. بنابراین محققان بر این باورند که ارزکاوی روی سیستم متعلق به دیگران نیازمند سرمایه کمتری است و ریسک پایین تری را نسبت به ارسال باج افزار به دنبال دارد.

دیجیاتو