زنگ خطر برای ویندوز؛ ویکی لیکس بدافزار «آتنا» متعلق به سازمان سیا را منتشر کرد - دیجیاتو

حمید مقدسی | دوشنبه، ۰۱ خرداد ۱۳۹۶

همان طور که مایکروسافت چند روز قبل اعلام کرد، جمع آوری حفره های امنیتی از سوی نهادهای اطلاعاتی به عنوان یکی از بزرگ ترین نگرانی های کنونی متخصصین امنیت سایبری مطرح است، چون اطلاعات شخصی و حریم فردی میلیون ها کاربر را در معرض خطر قرار می دهد. در ادامه افشاگری های چند وقت اخیر، ویکی لیکس به تازگی یک نمونه اکسپلویت دیگر را منتشر شده که سازمان های اطلاعاتی آمریکا از آن برای هدف قرار دادن سیستم های کامپیوتری مبتنی بر ویندوز استفاده می کردند.

بدافزار آتنا روی تمامی نسخه های ویندوز با تمام قوا عمل می کند

این اکسپلویت با نام رمز «آتنا» (Athena) نوعی بدافزار است که توسط سازمان جاسوسی سیا با همکاری شرکت تخصصی «Siege Technologies» توسعه یافته. آتنا به مهاجم اجازه می دهد کنترل کامل کامپیوتر را در دست بگیرد، اطلاعات را از راه دور بارگذاری یا بارگیری نماید، داده ها را حذف کند، و کدهای مخرب دیگری را نیز روی سیستم به اجرا درآورد. این بدافزار روی تمامی نسخه های ویندوز، از اکس پی گرفته تا ویندوز 10، به طور یکسان و با تمام قوا عمل می کند.

عملکرد آتنا به صورت زیر توصیف شده:

پس از نصب، بدافزار قابلیت سیگنال دهی پیوسته (بیکنینگ) از پیکربندی و تسک های سیستم را فراهم ساخته، قطعات مخرب داده را روی حافظه مربوط به تسک های خاص بارگذاری کرده، و انتقال یا بازیابی فایل ها از یک پوشه خاص را میسر می سازد. بدافزار توانایی تغییر پیکربندی و تنظیمات سیستم را در حین اجرا دارد تا به قابلیت های بیشتری دست یابد.

احتمالاً به زودی شاهد موج تازه ای از حملات باج افزاری روی کامپیوترهای ویندوزی باشیم

آتنا جدیدترین بدافزار ویندوزی است که توسط نهادهای امنیتی/جاسوسی آمریکا ساخته شده و از طریق ویکی لیکس منتشر می گردد. حمله گسترده و بی سابقه هفته گذشته باج افزار «واناکرای» حاصل یکی از همین نوع افشاگری ها بود و احتمال می رود طی هفته های آتی با حملات شدیدتری روبرو شویم. تمام این موارد نشان می دهند به سازوکار و قوانین سختگیرانه تری نیاز داریم تا نهادهای اطلاعاتی نتوانند اینگونه به جمع آوری و نگهداری اکسپلویت ها و حفره های امنیتی مبادرت ورزیده و امنیت کاربران را به مخاطره بیندازند.

دیجیاتو