چهار شنبه 19 مرداد 1390 - 09:33

نرم افزارهاي آنتي ويروس نفوذپذيرند

یکی از محققان گوگل در کنفرانس کلاه سیاه با گرفتن انگشت اتهام خود به سوی نفوذپذیری آنتی ویروس ها اظهار داشت که هکرها به راحتی می توانند وارد این نرم افزارها شوند.

جام جم آنلاین: یکی از محققان گوگل در کنفرانس کلاه سیاه با گرفتن انگشت اتهام خود به سوی نفوذپذیری آنتی ویروس ها اظهار داشت که هکرها به راحتی می توانند وارد این نرم افزارها شوند.
به گزارش مهر، در طول کنفرانس کلاه سیاه در «لاس وگاس» ، تاویس اورمندی، محقق گوگل اعلام کرد که موفق به کشف یک نفوذپذیری وخیم در نسخه 9.5 آنتی ویروس شرکت امنتیت انفورماتیکی «سوفوس» شده است.

به گفته این محقق، سیستم پنهان سازی در این آنتی ویروس به راحتی نفوذپذیر و مکانیزم امضای این نرم افزار بسیار ضعیف است. این نقاط ضعف به برنامه های مخرب اجازه می دهد که توسط آنتی ویروس شناسایی نشوند.

این محقق در بررسی های خود نشان داد که اغلب تولیدکنندگان آنتی ویروس ها نرم افزارهای خود را به روشی توسعه می دهند که بتوانند تعداد بسیاری از آلودگی های ویروسی را شناسایی کنند اما به کیفیت و امنیت خود نرم افزار توجه چندانی نمی کنند.

درحقیقت مزیت آنتی ویروس خوب تنها شناسایی تعداد بیشتری از ویروس ها نیست بلکه باید بتواند از خود نیز در برابر نفوذ برنامه های مخرب دفاع کند.

این هکر خوب با استفاده از روش مهندسی وارونه در این آنتی ویروس سوفوس کشف کرد که این خانه نرم افزاری از یک سیستم پنهان سازی 64 بیت استفاده می کند که نسبت به سیستم پنهان سازی 256 بیتی که در سایر آنتی ویروس ها وجود دارد ایمنی کمتری دارد.

همچنین کلید پنهان سازی اطلاعات در این نرم افزار در داخل یک فایل ذخیره می شوند و بنابراین هکرها به راحتی می توانند این کلید را پیدا کرده و به آنتی ویروس نفوذ کنند.

پس از این اظهارات، سوفوس به کاربران خود اطمینان داد که آلگوریتم پنهان سازی که در این آنتی ویروس به کار رفته است تنها در تعداد کمی از موارد استفاده شده و در فاز خروج است.

در مورد سایر نفوذپذیری های شناسایی شده نیز، این شرکت به زودی یک نرم افزار روز رسانی شده را ارائه می کند.