اچ پی بسته امنیتی برای حذف بدافزار کی لاگر از لپ تاپ هایش را منتشر کرد - دیجیاتو

حمید مقدسی | دوشنبه، ۲۵ اردیبهشت ۱۳۹۶

دیروز مطلع شدید درایور صوتی نصب شده روی چندین مدل از لپ تاپ های شرکت اچ پی حاوی یک بدافزار «کی لاگر» (keylogger) است که تمامی دکمه های کیبورد فشرده شده را در قالب یک فایل لاگ ذخیره می نماید. مؤسسه امنیتی «مادزیرو» (ModZero) می گوید هر فردی که به فایل های محلی کاربر در این کامپیوترها دسترسی داشته باشد، به راحتی می تواند رمزهای عبور، سابقه بازدید آدرس های وب، پیام های خصوصی و دیگر اطلاعات حساس او را در اختیار بگیرد.

لپ تاپ های اچ پی با درایور صوتی Conexant به بدافزار کی لاگر آلوده هستند

اچ پی با تأیید این موضوع و ملامت کمپانی توسعه دهنده این درایور، بسته امنیتی را برای حذف این کی لاگر ارائه کرده است که فایل های لاگ را نیز از کامپیوتر کاربر حذف می نماید. سخنگوی این کمپانی می گوید «اچ پی به امنیت کاربران اهمیت می دهد و حریم شخصی مشتریانش را محترم می شمارد. ما از مشکل امنیتی کی لاگر باخبر هستیم و تصریح می کنیم که هیچگونه دسترسی به داده های جمع آوری شده از طریق آن نداشته ایم».

این طور به نظر می رسد که درایورهای شرکت معروف Conexant به این بدافزار آلوده بوده اند. کی لاگر مورد بحث با ورود کاربر به محیط ویندوز آغاز به کار کرده و در هر بار، فایل لاگ را بازنویسی می کند. اگر فایل لاگ موجود نباشد، کی لاگر به صورت مخفیانه اطلاعات حساس را ذخیره می سازد. محتوای این فایل در قالب هگزادسیمال به شکل زیر است:

گفتنیست بسته امنیتی برای حذف این بدافزار برای لپ تاپ های مدل 2016 و پس از آن از روز پنجشنبه در وب سایت اچ پی در بخش Windows Update قرار گرفته، و مدل های 2015 و ماقبل آن نیز از روز جمعه این بسته آپدیت را دریافت کرده اند.

دیجیاتو