هشدار! هنگام ارتقاء یا بروزرسانی ویندوز ۱۰ کامپیوتر خود را رها نکنید

بیشتر کاربران یک عادت بد دارند که هنگام ارتقاء سیستم عامل ویندوز، آن را رها می‌کنند. البته این مسأله به این مربوط است که فرایند ارتقاء ویندوز ۱۰ طولانی و خسته کننده است. چرا این مسأله نگران کننده است؟

هنگام ارتقاء ویندوز ۱۰، یک شخص نزدیک به قربانی (یا حتی کسی که قربانی او را نمی‌شناسد) می‌تواند بدون نیاز به نرم‌افزار اضافی و با وجود اینکه BitLocker نصب است رابط خط فرمان را با دسترسی کامل هنگام ارتقاء ویندوز ۱۰، کلید های Shift + F10 را فشار دهید تا رابط خط فرمان با دسترسی root برایتان باز شود تا بتوانید BitLocker را دور بزنید!

باز کند و کارهای خرابکارانه انجام دهد. این مسأله به مایکروسافت گزارش شده است و این کمپانی در حال رفع این مشکل است.

اگر برای امنیت سیستم خود به نرم‌افزار کدگذاری Windows Bitlocker اعتماد کرده‌اید، پس آگاه باشید! چون کسی که به سیستم شما دسترسی فیزیکی دارد می‌تواند به اطلاعات شما دسترسی داشته باشد!

کل کاری که لازم اســت هکر انجام دهد، فشــار دادن همزمان کلیدهای Shift+F10 هنگام ارتقاء ویندوز ۱۰ است. محقق امنیتی Sami Laiho این روش دور زدن Bitlocker را کشف کرده است. وقتی شــما در ویندوز ۱۰ در حال نصــب یک ســیســتم عامل جدید هســتید هکر می‌تواند با فشــار دادن Shift+F10 رابط خط فرمان (Command Line Interface) را با دسترسی‌های سیستمی باز کند. ســپس با وجود فعال بودن BitLocker در ســیســتم قربانی، رابط خط فرمان دســترســی کامل هارد دیســک را به هکر می‌دهد. زیرا در زمان ارتقاء ســیســتم عامل، Windows PE (Pre-installation Environment) برای نصب ایمیج جدید ویندوز مجبور است BitLocker را غیرفعال کند.

توجه شــود که یکی از ویژگی های رفع مشــکل ویندوز این اســت که به شــما اجازه می‌دهد کلیدهای Shift+F10 را فشــار دهید تا رابط خط فرمان برایتان باز شــود. متاسـفانه این ویژگی با غیرفعال کردن BitLocker، دسترسی به تمام اطلاعات هارد دیسک را در حین ارتقاء ویندوز ممکن می‌سازد .

بنابراین هکر برای سـوءاسـتفاده نیاز به دسـترسـی فیزیکی کوتاه مدت به کامپیوتر هدف دارد، پس از آن به راحتی می‌تواند BitLocker را دور زده و دســترســی مدیر (Administrator) پیدا کند. مســئله‌ای که می‌تواند روی ابزارهایی که در حوزه اینترنت اشیاء از ویندوز ۱۰ استفاده می‌کنند تأثیر بگذارد.

چگونه ریسک این خطر را کاهش دهیم؟

به عنوان اقدام متقابل، به کاربران توصـیه می‌شـود که در حین ارتقاء ویندوز خود آن را رها نکنند. همچنین می‌تواند به کاربران توصیه کرد از ویندوز ۱۰ نسخه LTSB استفاده کنند چون این نسخه از ویندوز ۱۰۰ به طور خودکار ارتقاء یا بروزرسانی انجام نمی‌دهد.

کـاربران ویـنـدوز ۱۰ می‌تواننـد بـا اســتفـاده از SCCM (System Center Configuration Manager) دســترســی به رابط خط فرمان در حین ارتقاء ویندوز را مســدود نمایند. برای این کار در پوشه‌ی Setup\Scripts سیستم عامل، یک فایل با نام DisableCMDRequest.tag ایجاد کنند.