禪

.[illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible]

[illegible] [illegible] [illegible] [illegible]

Exploiting Mac OSX to Install
Permanent Backdoor Malware
Hack

[illegible] [illegible] [illegible] .[illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [

برای این کار وارد شدن کامپیوتر در یک نشست به حالت تعلیق است . تا زمان نگارش این مقاله، سیمانتک چهار مدل مختلف از کامپیوترهای مک را مورد بررسی قرار داده است . این شرکت امنیتی متوجه شده است مدل‌های Mac Mini 5.1 و MacBook Pro 9.2 به این آسیب‌پذیری آلوده هستند، اما مدل‌های MacBook Pro 11.3 و MacBook Air 6.2 به این آسیب‌پذیری آلوده نیستند . آزمایش‌های ویکالا تأیید کرده است که مدل‌های MacBook Air 5.1، MacBook Pro 8.2، MacBook Pro Retina 10.1 و Mac Pro 9.1 به این آسیب‌پذیری آلوده هستند . همه کامپیوترهای که مورد آزمایش قرار گرفته‌اند، به جدیدترین نسخه از میان‌افزار اپل تجهیز بود .

ویکالا در یادداشت‌های خود نوشته است : «من اطمینان دارم اپل از وجود این باگ روی محصولات خود باخبر بوده یا حداقل این امر می‌تواند یک سهل‌انگاری غیرمسئولانه از طرف آنها تلقی شود که سیستم بایوس پیاده‌سازی شده خود را درباره این آسیب‌پذیری که به حمله Dark Jedi منجر می‌شود، موردِ آزمایش قرار نداده‌اند . من مشکلی با آزمایش‌های PoC نداشتم، اما لازم است مردم این آزمایش را شخصاً انجام دهند تا حداقل متوجه شوند چه مدل‌های دیگری از مک به این آسیب‌پذیری آلوده هستند .» تا زمانی که اپل وصله لازم را برای برطرف کردن این رخنه امنیتی در فریمویر خود ارائه نکرده است، بهتر است کاربران سیستم خود را بجای آنکه در وضعیت sleep قرار دهند، بهطور کامل خاموش کنند .

نویسنده :
حمیدرضا_تائبی
دسته بندی:
امنیت
تاریخ انتشار :
17:44 - 12/04/1394
برچسب:
مک - روتکیت - سیمانتک

منبع: https://www.shabakeh-mag.com/security/954