باگ Mac OS به هکرها اجازه دسترسی به کامپیوتر از راه دور و بدون پسورد را می دهد - دیجیاتو

علی باقرزاده | شنبه، ۲۶ اسفند ۱۳۹۶

آسیب پذیری جدید مک بوک امکان دسترسی به سیستم عامل از طریق افزونه ریموت دسکتاپ مرورگر کروم را از راه دور و بدون نیاز به وارد کردن پسورد فراهم می کند.

بر اساس گزارش ها این آسیب پذیری که با افزونه ریموت دسکتاپ مرورگر کروم گوگل در ارتباط است، برای سایرین امکان ورود به اکانت میهمان (Guest) را بدون ورود به پسورد فراهم می کند. البته تا به اینجای کار مشکلی نیست و خطری کاربر را تهدید نمی کند.

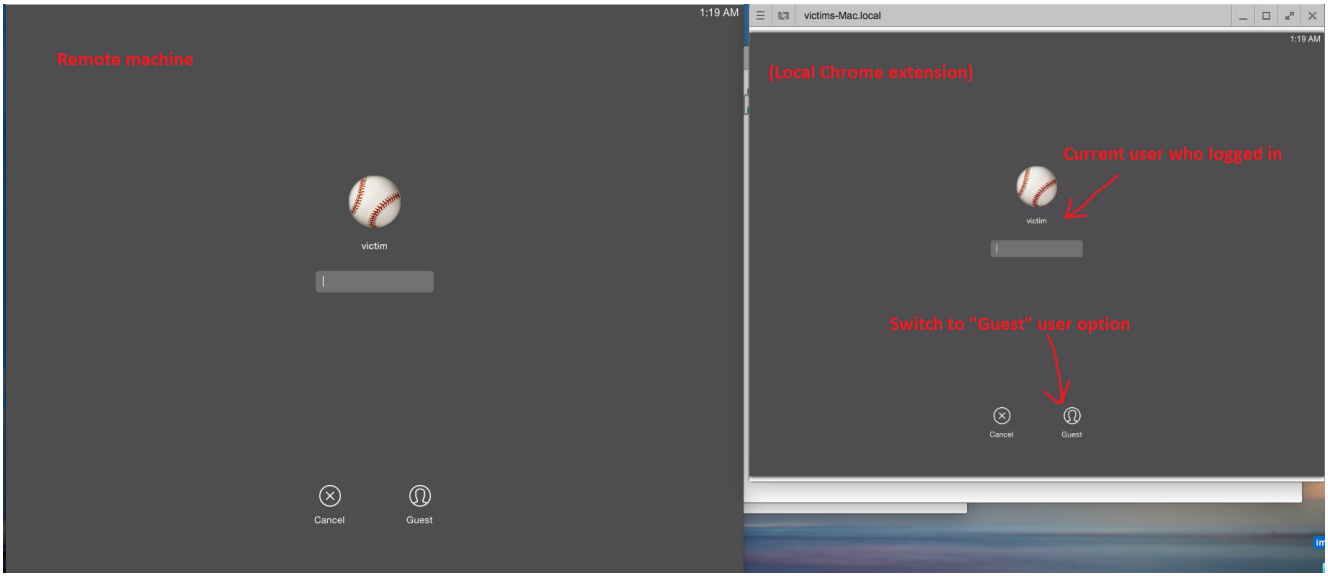
اکانت میهمان در واقع یک اکانت موقت است که فایل هایی که توسط کاربر این اکانت تولید می شود، به صورت موقت ذخیره شده و پس از خروج از اکانت نیز این اطلاعات حذف می شوند.

مشکل از جایی شروع می شود که فرد سوء استفاده کننده پس از ورود به این اکانت، می تواند به محیط دسکتاپ سایر اکانت هایی که پیش از این به سیستم عامل وارد شده و هنوز از آن خارج نشده اند، دسترسی داشته باشد.

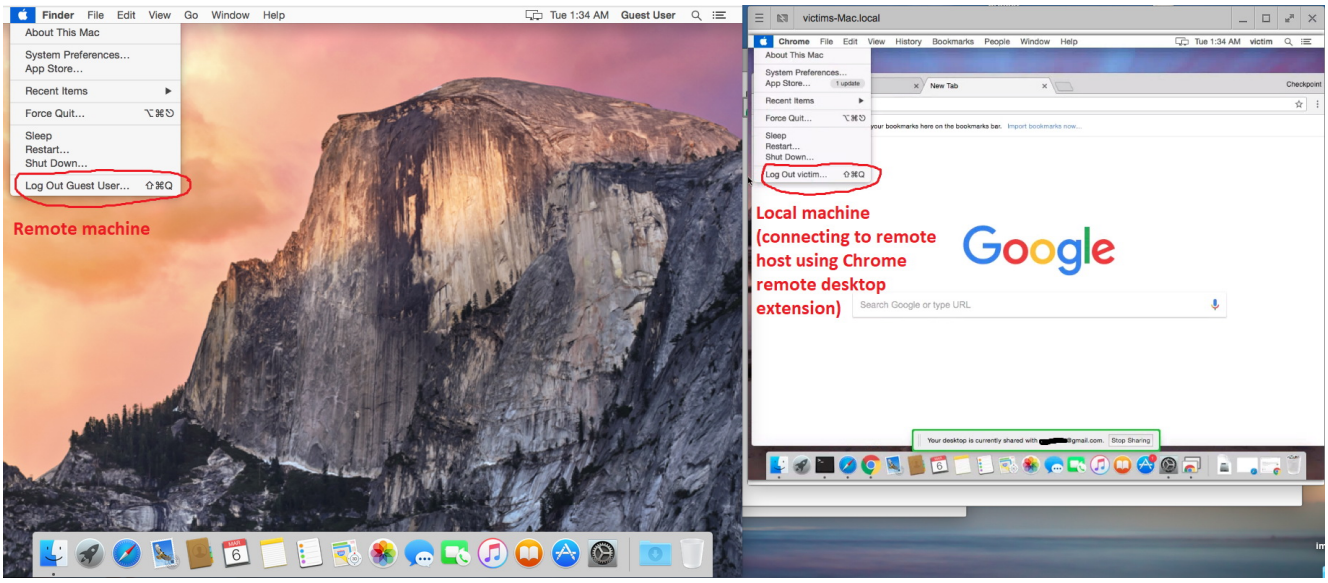
افزونه کروم مورد بحث امکان دسترسی از طریق کامپیوتر دیگر یا موبایل را با استفاده از مرورگر کروم و یا لپتاپ های کروم بوک فراهم می کند. البته این افزونه به منظور هک کردن طراحی نشده است.

البته برای سوء استفاده هکرها باید از پیش دسترسی اکانت میهمان (Guest) در سیستم عامل مک او اس فعال شده باشد که خوشبختانه به صورت پیش فرض فعال نیست، مگر آنکه کاربر اقدام به فعال کردن آن کرده باشد.

به گفته کارشناسان امنیتی برای اینکه این باگ برای سوء استفاده کنندگان قابل بهره برداری باشد، باید از قبل حداقل یک نفر با اکانت دیگری وارد سیستم عامل شده باشد و از آنجایی که در صفحه لاگین، کاربر مهمان نیازی به ورود پسورد ندارد، فرد سوء استفاده کننده به راحتی می تواند وارد سیستم عامل شود و به دسکتاپ کاربر اصلی دسترسی داشته باشد.



برای سوء استفاده، باید یک کاربر به صورت محلی به سیستم عامل وارد شده باشد (در اینجا کاربر با نام victim در کامپیوتر سمت چپ). پس از آن هکر می تواند با استفاده از نام کاربری Guest از راه دور (کامپیوتر سمت راست) به سیستم وارد شده و به دسکتاپ کاربر victim دسترسی داشته باشد.



در نهایت دسکتاپ کاربر victim به کاربری که از راه دور متصل شده (در کامپیوتر سمت راست) نشان داده می شود.

اپل پیش از این سابقه خوبی در برطرف کردن سریع مشکلات سیستم عامل مک او اس داشته، ولی این بار شاید مشکل از سمت اپل نباشد و این گوگل است که باید مشکل را حل کند.

به این منظور مشکل مورد بحث در 26 بهمن ماه به گوگل اعلام شده، ولی این کمپانی اعلام کرده از آنجایی که این صفحه لاگین یک مرز امنیتی به حساب نمی آید، تصمیمی برای رفع این مسئله وجود ندارد.

ديجياتو