www.javangrp.com

اولین بدافزار سال ۲۰۱۷ سیستم عامل مک شناسایی شد

یک تیم امنیتی، بدافزاری با کد ساده در سیستم عامل مک پیدا کرده‌اند. اپل نام این بدافزار را Fruitifly گذاشته است.

اکثر کاربران و کارشناسان بر این باورند که سیستم عامل مک (که زمانی با نام OS X شناخته می‌شد) به‌طور کامل در مقابل ویروس‌ها و بدافزارها ایمن است. این اطمینان از ایمن بودن سیستم به حدی است که کاربران نیازی به نصب نرم‌افزارهای امنیتی روی این سیستم عامل حس نمی‌کنند. این در حالی است که اکثر کاربران ویندوز باید از یک نرم‌افزار امنیتی برای حفظ اطلاعات خود استفاده کنند.

MacOSهمیشه کمتر از ویندوز هدف حمله قرار گرفته است. دلیل این امر می‌تواند آمار پایین نصب آن باشد که در حدود ۸ درصد رایانه‌های شخصی است. دلیل دیگر می‌تواند امنیت بالای این سیستم عامل باشد. به هر حال مسئله‌ی اصلی این است که کاربران مک نیز نمی‌توانند با خیال راحت در مورد بدافزارها،

به کار با دستگاه‌های خود بپردازند. گروهی از فعالان امنیتی شرکت Malwarebytes اخیرا اولین بدافزار سال ۲۰۱۷ سیستم‌عامل Mac را شناسایی کرده‌اند.

یکی از مدیران شرکت مالوربایتس در زمان استفاده از دستگاه‌های خود متوجه شد که یکی از کامپیوترهای مک، مصرفی غیر عادی از ترافیک شبکه دارد. وقتی کارشناسان این شرکت به بررسی سیستم پرداختند، متوجه بدافزاری شدند که با یک کد قدیمی نوشته شده بود. این نوع کد معمولا در کامپیوترهای مراکز آزمایشگاهی استفاده می‌شده است.

کد این بدافزار ساده ولی هوشمندانه است. این پکیج مخرب از دو فایل تشکیل شده که توانایی ارتباط از راه دور و کنترل سروری دارند. این فایل‌ها می‌توانند تصاویری را از صفحه نمایش کامپیوتر آلوده ثبت و به مقصد مورد نظر ارسال کنند. برخی از توابعی که این بدافزار فراخوانی می‌کند، تا قبل از ساخته شدن OS Xوجود نداشته‌اند و این کدها می‌تواند گواهی بر این قضیه باشد که این سیستم عامل از روزهای ابتدایی در معرض بدافزارها بوده است.

صرف‌نظر از این‌که کد مخرب مربوط به چه زمانی باشد، شناسایی و از بین بردن آن آسان است. نرم‌افزار اختصاصی امنیت شرکت Malwarebytes به‌راحتی این بدافزار را تحت نام OSX.Backdoor.Quimitchin شناسایی می‌کند. این شرکت اعلام کرده است که فایل‌های مخرب، از روشی قدیمی و ساده برای باقی ماندن و مخفی شدن در سیستم استفاده می‌کند. این روش قدیمی توسط اکثر بدافزارهای مک استفاده می‌شود. روش کار بدین صورت است که یک فایل مخفی و یک فایل برای اجرای کدها در این پکیج وجود دارد. به خاطر استفاده از همین روش قدیمی و ساده، این نوع بدافزارها به‌راحتی قابل شناسایی و از بین بردن هستند.

شرکت اپل نیز از وجود این Malware مطلع شده و آن را Fruitfly نامیده است. از زمان شناسایی نیز یک پکیج امنیتی بروزرسانی توسط اپل منتشر شده که از آلودگی‌های آتی جلوگیری می‌کند. نکته‌ی اصلی این جریان برای کاربران مک این است که با وجود کمتر بودن حملات در سیستم عاملMac ، بهتر است همیشه از یک نرم‌افزار امنیتی در کامپیوتر استفاده کرد. بهتر است این نرم‌افزار به‌صورت دوره‌ای بروزرسانی شود و زمان‌های مشخصی برای اسکن کل سیستم توسط آن اختصاص داده شود.