اولین بدافزار مک در ۲۰۱۷

بدافزار جدید مک به نام کویمیچین، سازمان‌های تحقیقاتی پزشکی را هدف قرار داده است.

به گزارش واحد متخصصین سایبربان، محققان امنیتی اولین بدافزار مک در سال ۲۰۱۷ را به نام کویمیچین (Quimitchin) شناسایی کردند. کدهای این بدافزار خیلی پیچیده نیستند و حتی دارای کدهای منسوخ‌شده نیز هست.

بنابر گزارش محققان امنیتی، بدافزار کویمیچین در طول چند سال گذشته فعال بوده و سازمان‌های تحقیقاتی پزشکی را هدف قرار داده است.

نحوه شناسایی این بدافزار، تشخیص جریان ترافیکی مشکوک در شبکه توسط مدیر شبکه، از سوی سامانه مک بوده است. این بدافزار دارای دو بخش است:

۱. plist: حفظ فعالیت همیشگی client.
۲. client: ترافیک مخرب نوشته‌شده به زبان پرل و جاوا

ویژگی‌های اصلی نوشته‌شده برای بدافزار، استفاده از دوربین و عکس‌برداری از صفحه‌نمایش است. بخش قدیمی بدافزار نیز مربوط به کتابخانه متن‌باز libjpeg می‌شود که آخرین بار در سال ۱۹۹۸ به‌روزرسانی شده است. بدافزار با سرور مدیریت مرکزی (C&C) با آی.پی ۹۹.۱۵۳.۲۹.۲۴۰ و آدرس eidk.hopto.org ارتباط برقرار می‌کند. همان‌طور که گفته شد این بدافزار مدت‌زمان طولانی است که در حال فعالیت است؛ هم‌چنین کدهای آن نیز از پیچیدگی خاصی برخوردار نیست. دلیل اینکه این بدافزار تاکنون شناسایی نشده بود، حمله به تعداد محدودی قربانی بوده است.

اداره حراست آموزشکده شهید یزدانپناه سنندج