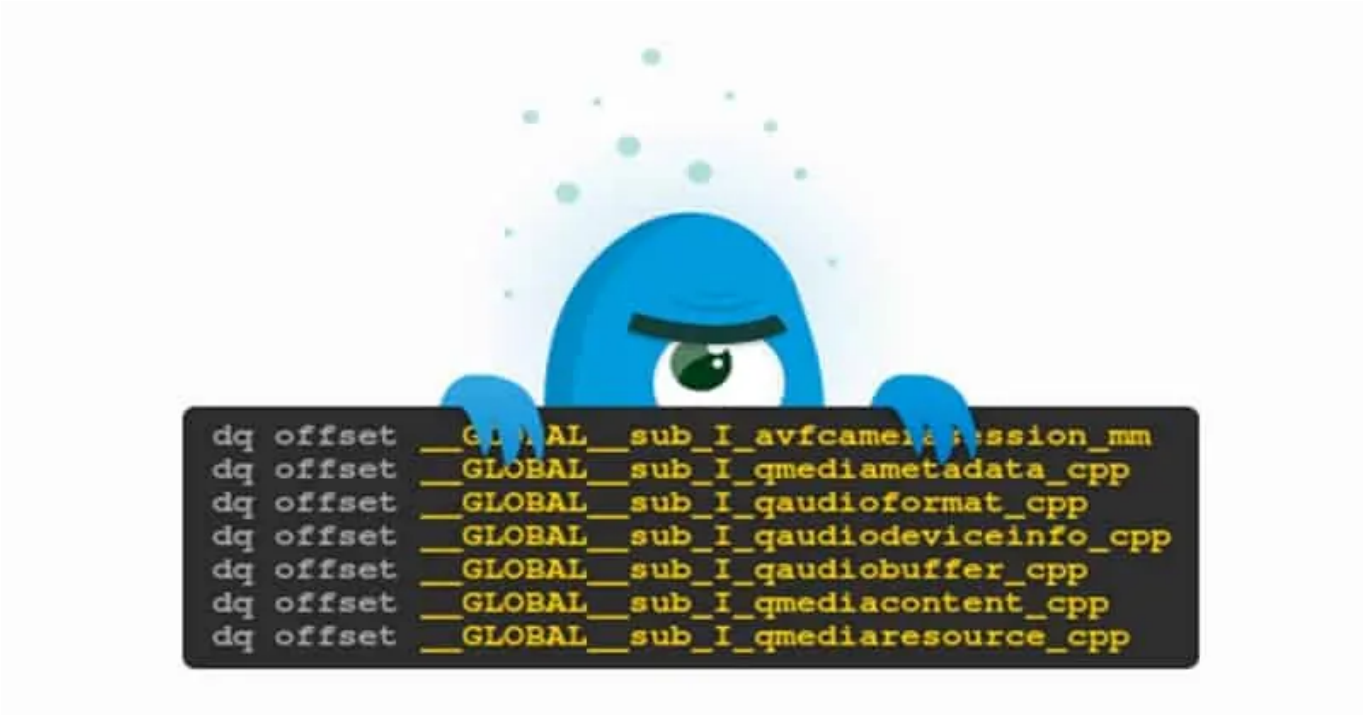
خرابکاری جدید گروه لازاروس؛ حمله به مکینتاش با بدافزار بدون فایل - دیجیاتو

کورش چایچی | سه شنبه، ۱۹ آذر ۱۳۹۸

شواهد حاکی از آن است که گروه هکری لازاروس این بار سیستم‌عامل macOS را هدف قرار داده است. بر اساس بررسی‌های انجام شده، بدافزاری که این گروه توسعه داده‌اند، یک بدافزار بدون فایل بوده که توسط بیشتر آنتی ویروس‌ها شناسایی نمی‌شوند. این روش بسیار پیشرفته بوده و اکثرا توسط گروه‌های هکری وابسته به دولت‌ها استفاده می‌شود.

این بدافزار چگونه کار می کند؟



آنتی ویروس‌ها همیشه نوشتن ها و خواندن‌های روی هارد دیسک را بررسی می‌کنند تا ویروس‌ها و بدافزارها را شناسایی کنند. اما این بدافزار بدون نوشتن داده‌ای روی دیسک، مستقیم از طریق حافظه دستگاه، اجرا می‌شود و هیچ ردی هم از خود روی دیسک باقی نمی‌گذارد. در نتیجه این گونه بدافزارها، به بهترین در نوع خود تبدیل می شوند زیرا اکثر آنتی ویروس‌ها نمی‌توانند آن‌ها را تشخیص دهند.

چرا لازاروس متهم اصلی است؟

این سیستم بدافزارها که معمولا تحت نام بدون فایل (Fileless) شناخته می‌شوند، بدون استفاده از هارد دیسک و فقط از طریق مموری یا همان حافظه، نوشتن و خواندن‌ها را انجام می‌دهند. اما این نحوه از توسعه بدافزارها، آن قدر پیچیده و سخت است که تنها هکرهای وابسته به دولت می‌توانند آن‌ها را توسعه دهند. از آن جایی که لازاروس (Lazarus) قبلا هم با نوشتن این گونه بدافزارهای بدون فایل شناخته شده است، یکی از متهمان اصلی توسعه این بدافزار به شمار می‌رود.

البته این اتهام با دانش قبلی زده شده است. لازاروس مسئول توسعه بدافزاری به نام اپل جوس (AppleJeus) بوده که کارکردی مشابه این بدافزار بدون فایل داشته است. یکی از تحقیق کنندگان حوزه امنیت macOS به نام پاتریک واردل (Patrick Wardle) صحت این قضیه را تا حدودی تایید می‌کند. او با بررسی خط به خط کد این بدافزار و مقایسه آن با بدافزارهای قبلی توانسته شباهت این دو را تشخیص دهد.

فرایند آلوده شدن چگونه است؟

- move a hidden plist (`.vip.unioncrypto.plist`) from the application's `Resources` directory into `/Library/LaunchDaemons`
- set it to be owned by root
- create a `/Library/UnionCrypto` directory
- move a hidden binary (`.unioncryptoupdater`) from the application's `Resources` directory into `/Library/UnionCrypto/`
- set it to be executable
- execute this binary (`/Library/UnionCrypto/unioncryptoupdater`)

او همچنین فرایند آلوده شدن مکینتاش را گام به گام توضیح داده که در ادامه با هم مرور می‌کنیم:

- انتقال یک لیست مخفی (.vip.unioncrypto.plist) از فهرست منابع اپلیکیشن‌ها به مسیر رو به رو: / Library / LaunchDaemons
- تنظیم آن برای شناخته شدن توسط دسترسی روت
- درست کردن کتابخانه / Library / UnionCrypto
- انتقال یک باینری مخفی (.unioncryptoupdater) از فهرست منابع اپلیکیشن به مسیر رو به رو: / Library / UnionCrypto /
- اجرایی کردن باینری
- اجرای باینری رو به رو: / Library / UnionCrypto / unioncryptoupdater

تمامی مراحل بالا باعث می‌شود بدافزار فوق، خود را به عنوان یک برنامه تراکنش‌های ارز دیجیال به نام unioncryptoupdated معرفی کند، اما سپس خود را به برنامه‌ای «پایدار» تبدیل می‌کند که حتی با خاموش و روشن شدن لپ تاپ نیز از حافظه پاک نمی‌شود.

بدافزار بدون فایل چه کاربردی دارد؟

بسیاری از این بدافزارها باعث می‌شوند تا اطلاعات پایه سیستم ماند، شماره سریال، نسخه سیستم‌عامل و دیگر داده‌ها برای توسعه‌دهندگان آن‌ها نمایان شود. پس از آن سیستم آلوده شده سعی می‌کند با سرور / Vip (.) unioncrypto // :hxxps ارتباط برقرار کند. در صورت موفق بودن ارتباط، فایل Object File Image را دریافت می‌کند که بدون هیچ ردی روی هارد دیسک، توسط حافظه اجرا می‌شود.

کاربران چگونه می‌تواند سیستم خود را امن کنند؟

خبر خوب برای کاربران مکینتاش این است که این بدافزار بدون فایل UnionCryptoTrader.pkg، فایلی امضا نشده است. یعنی خود macOS قبل از نصب آن به شما هشدار می‌دهد که این قایل امن نیست. پس هرگاه چنین هشدارهایی را برای هر نرم‌افزاری دریافت کردید، از نصب آن خودداری کنید. زیرا این گونه بدافزارها آن قدر قوی هستند که تنها یک سوم از آنتی ویروس‌ها آن‌ها را تشخیص می‌دهند.

اما اگر آنتی ویروس ندارید یا این که آنتی ویروس شما این بدافزار را پیدا نکرده است، می‌توانید به صورت دستی دایرکتوری‌های زیر را چک کنید:

- Launch Daemon property list: /Library/LaunchDaemons/vip.unioncrypto.plist
- Running process/binary: /Library/UnionCrypto/unioncryptoupdater

البته این تیم، آنتی ویروسی به نام KnockKnock نیز برای پیدا کردن این برافزار توسعه داده است که می‌توانید آن را دانلود کرده و سیستم خود را اسکم کنید.

دیجیاتو