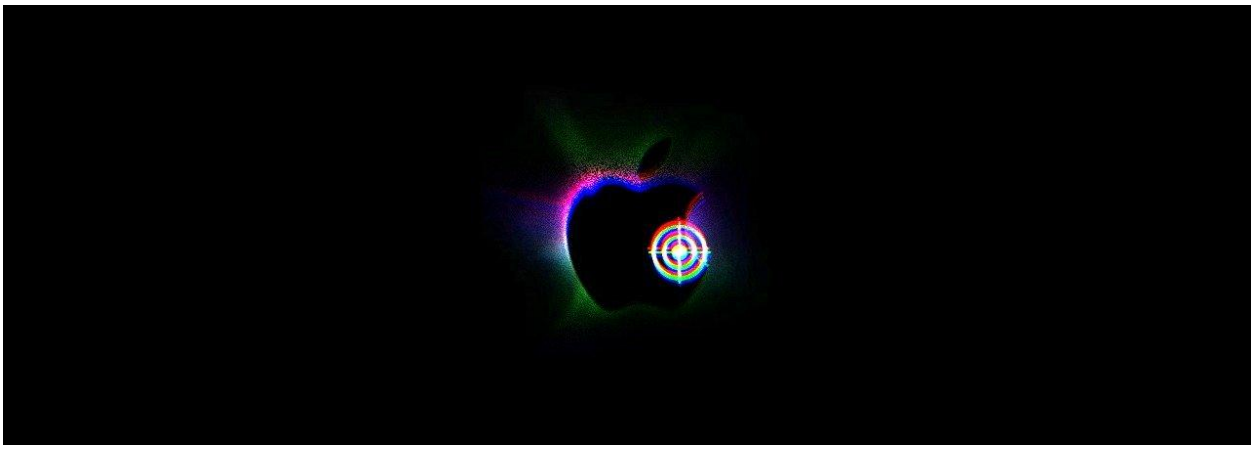
آسیب‌پذیری‌های روزصفرم iOS به طور فعال علیه قربانیان هدف‌گذاری شده، استفاده می‌شوند.



خلاصه‌ی خبر:

بهره‌برداری موفق از نقص‌های امنیتی OOB Write و سرریز ساختار هیپ ازراه دور، مهاجمین را قادر به بهره‌برداری از آیفون و آیپد کاربران که از نسخه‌ی ۶ و یا بالاتر iOS، از طریق برنامه‌ی پیش‌فرض Mails کرده‌است. با توجه به وصله‌نشدن این آسیب‌پذیری و عدم ظهور علائم خاصی به‌خصوص در iOS۱۳، لازم است کاربران مذکور به‌جای برنامه‌ی Mails از برنامه‌هایی مانند Outlook یا Gmail استفاده کنند. همچنین با توجه به بالارفتن تعداد بهره‌برداری‌های پیداشده در iOS، قیمت اکسپلویت‌های روزصفرم آن در Zerodium نیز کاهش یافته‌است.

پس از کشف یک سری حملات مداوم از راه دور که حداقل از ماه ژانویه سال ۲۰۱۸ کاربران iOS را هدف قرار داده است، دو آسیب‌پذیری روز صفرم که بر روی دستگاه‌های آیفون و آیپد تأثیر می‌گذارد، توسط استارت‌آپ امنیت سایبری ZecOps پیدا شد.

محققان ZecOps گفتند: "محتوای این حمله شامل ارسال ایمیلی دستکاری‌شده‌ی خاص به صندوق‌پستی یک قربانی است که آن را قادر می‌سازد آسیب‌پذیری را در متن برنامه iOS MobileMail در iOS ۱۲ راه‌اندازی کند یا در iOS ۱۳ ارسال کند".

بهره‌برداری موفقیت‌آمیز از نقص‌های امنیتی- نوشتن خارج از محدوده (OOB Write)و یک سرریز در ساختار هیپ ازراه دور- مهاجمان را قادر می‌سازد تا کد از راه دور را بر روی دستگاه‌های تحت کنترل iPhoneو iPad اجرا کنند و به آن‌ها امکان دسترسی، نشت، ویرایش و حذف ایمیل‌ها را می‌دهند.

ZecOps در ادامه توضیح داد: "آسیب‌پذیری اضافی هسته، دسترسی کامل به دستگاه را فراهم می‌کند- ما گمان می‌کنیم که این مهاجمین آسیب‌پذیری دیگری نیز داشته‌اند."

هکرهای دولتی، پشت حملات مداوم

محققان، حملات از راه دور را با دنبال کردن یک روش روتین جرم‌شناسی دیجیتال در iOS و پاسخگویی حوادث (DFIR) پیدا می‌کردند، در حالی که کاربران iOS ۱۱,۲,۲ از طریق برنامه‌ی پیش‌فرضMail ، هدف قرار گرفته‌اند.

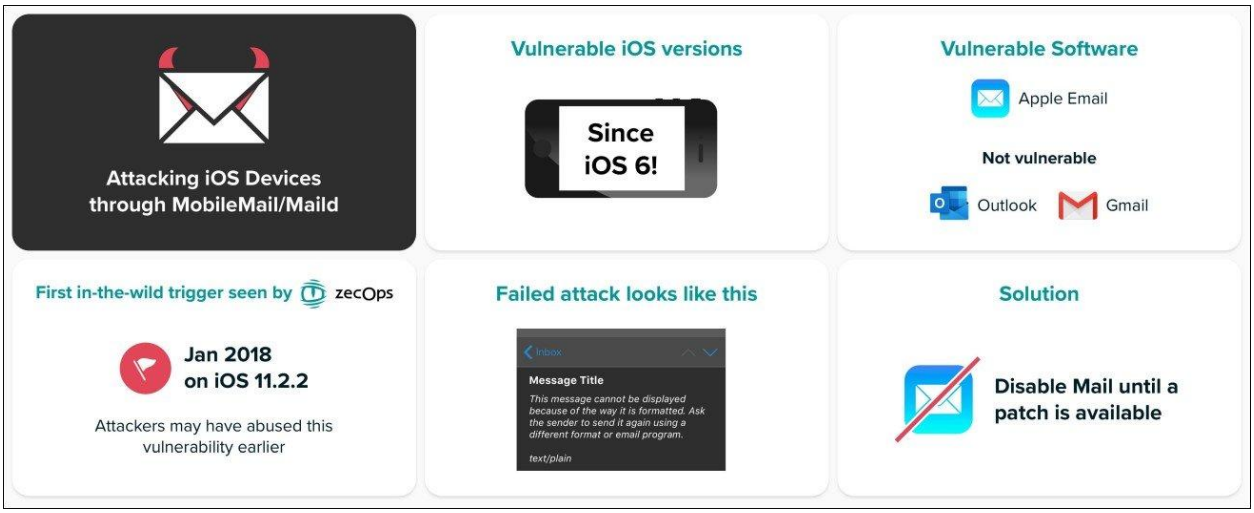
در حالی که علائم اولیه نشان می‌داد حملات از نظر زمانی از ژانویه ۲۰۱۸ تا اکنون انجام شده‌اند، اما این امکان وجود دارد که این روزصفرم حتی در حملات مرتبط قبلی نیز استفاده شده باشد.

ZecOps می‌گفت: "ما معتقدیم که این حملات به حداقل یک اپراتور تهدید دولتی وابسته است یا این اکسپلویت یا POC، از یک محقق شخص ثالث خریداری شده و با "as-is "یا ایجاد تغییرات و اصلاحات جزئی، از آن استفاده شده‌است."

ZecOps چندین مورد بسیار قابل‌توجه که مورد هدف بهره‌برداری از روزصفرم‌های iOS قرار گرفته‌اند را شناسایی کرد، از جمله:

- افراد یکی از سازمان‌های ۵۰۰ Fortune در آمریکای شمالی
- مدیر اجرایی یک شرکت هواپیمایی در ژاپن
- یک VIP از آلمان
- MSSP های عربستان سعودی
- یک روزنامه نگار در اروپا
- مورد مشکوک: یک مدیر اجرایی از یک شرکت سوئیسی

اگرچه ZecOps نمی‌خواست این حملات را به یک عامل تهدید خاص نسبت دهد، اما محققان گفتند که آن‌ها از وجود حداقل یک سازمان که " اکسپلویت‌هایی که با استفاده از آدرس‌ایمیل‌ها به عنوان شناسه‌ی اصلی نفوذ می‌کنند، را می‌فروشند " آگاه هستند.



۱- تصویر : ZecOps

تمام دستگاه‌های دارای iOS ۶ و بالاتر آسیب‌پذیر هستند.

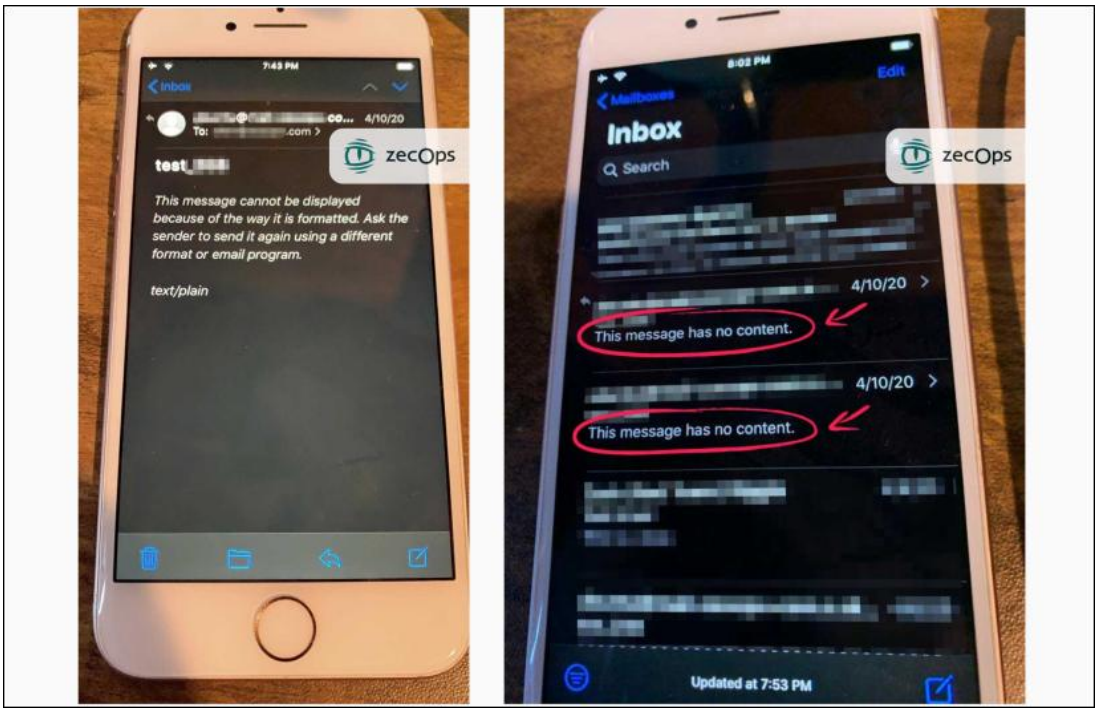
تمام آیفون‌ها و آیپدهایی که از iOS ۶ یا بالاتر - از جمله آخرین نسخه (iOS ۱۳,۴.۱) استفاده می‌کنند، در برابر حملات آسیب‌پذیر هستند، هرچند با توجه به اینکه ZecOps تست را پس از

iOS ۶ متوقف کرد، دستگاه‌های iOS که حتی نسخه‌های قدیمی تر را اجرا می‌کنند نیز می‌توانند، در معرض خطر قرار داشته‌باشند.

در iOS ۱۳ ، بهره‌برداری از آسیب‌پذیری‌ها نیازی به تعامل کاربر ندارد، در حالی که در iOS ۱۲ برای هک‌شدن آیفون یا آیپد، لازم است کاربران بر روی ایمیل کلیک کنند.

مهاجمان همچنین می‌توانند چندین بار از مسائل امنیتی بهره‌برداری کنند بدون اینکه هیچ علامتی جدا از کند شدن موقتی در iOS ۱۳، ظاهر شود در حالی که در iOS ۱۲ برنامه Mail ناگهان از کار می‌افتد.

در صورت عدم موفقیت حملات، قربانی هیچ علامتی در iOS ۱۳ مشاهده نمی‌کند، در حالی که در iOS ۱۲ ایمیل‌هایی با پیام "This message has no content" در صندوق‌ورودی ظاهر می‌شوند.



۲- حملات ناموفق

ZecOps توصیه می‌کند: "اگر نمی‌توانید این نسخه را وصله کنید، مطمئن شوید از برنامه‌ی Mail استفاده نمی‌کنید، در عوض از Outlook یا Gmail استفاده کنید که در حال حاضر، آسیب‌پذیر نیستند".

"با داده‌های بسیار محدود توانستیم ببینیم حداقل شش سازمان تحت تأثیر این آسیب‌پذیری قرار دارند و دامنه‌ی کامل سوء استفاده از این آسیب‌پذیری بسیار بزرگ است. قطعاً باید برای اینچنین مسائلی با محرک‌های عمومی هرچه سریعتر وصله‌هایی فراهم شود."

اپل پیش از این برای روزصفرم‌های نسخه‌ی iOS ۱۳,۴,۵ beta ۲ که در ۱۵ آوریل منتشر شد، وصله‌هایی را با یک راه‌حل امنیتی در اختیار کاربران قرار داده است که در نسخه‌های ثابت و اصلی iOS در دسترس است.

روزصفرم‌های iOS

با تجربه‌ی دو مورد بهره‌برداری فعال در iOS ۱۲,۱,۴ که وصله شدند و چند مورد دیگر که بعد از بهره برداری واقعی از کاربران به عنوان بخشی از زنجیره‌ی ۵ مورد افزایش مجوزهای دسترسی، اصلاح شدند، می‌بینیم که این روزصفرم‌های iOS که توسط ZecOps کشف شدند اولین مواردی نیستند که اپل تاکنون مجبور به وصله‌ی آن‌ها شده است.

Zerodium پلتفرم دستیابی به اکسپلویت‌های روزصفرم، در سپتامبر ۲۰۱۹ پرداخت روزصفرم‌های iOS را کاهش داد، با تداوم زنجیره‌ی کامل اکسپلویت اپل (۱-click) از $ ۱،۵۰۰،۰۰۰ به ۱،۰۰۰،۰۰۰ دلار کاهش یافت، در حالی که اکسپلویت‌های (۱-Click) iMessage RCE + LPE بدون دوام و ماندگاری، کاهشی ۵۰۰،۰۰۰ دلاری نسبت به قیمت قبلی $ ۱،۰۰۰،۰۰۰را تجربه کرد.

مدیر عامل شرکت Zerodium ، Chaouki Bekrar به BleepingComputer گفت: "طی چند ماه گذشته، ما شاهد افزایش تعداد اکسپلویت‌های iOS ، به‌خصوص در زنجیرهای Safari و iMessage بوده‌ایم که توسط محققان سراسر دنیا توسعه و فروخته می‌شوند. بازار روزصفرم‌ها طوری از اکسپلویت‌های iOS پر شده است که اخیراً شروع به رد کردن برخی از [آن‌ها] کرده‌ایم."

منبع:

https://www.bleepingcomputer.com/news/security/new-ios-zero-days-actively-used-against-high-profile-targets/