بسمه تعالی

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر

بررسی بدافزار Lemon Duck

اسفند ۹۸

۱ چکیده

اهداف مالی، همواره یکی از محرک‌های جدی برای مجرمان سایبری بوده است و همچنین همواره مهاجمان برای استخراج رمزارزها، اقدام به سوءاستفاده از قدرت محاسباتی سیستم‌های کاربران و سرورها کرده‌اند. استخراج رمزارزها از جمله روش‌هایی است که منجر به تولید آسان و بدون ریسک پول می‌شود؛ از این رو بدافزارهای استخراج‌کننده روی دستگاه‌ها در حال افزایش و روش‌ها و تکنیک‌های مورد استفاده برای این کار، در حال پیشرفت هستند. در این گزارش به بررسی یک بدافزار جدید برای استخراج رمزارزها به نام Lemon_Duck می‌پردازیم که از اکسپلویت[۱] Eternalblue برای انتشار در شبکه استفاده می‌کند.

۲ محصولات تحت تاثیر

چاپگرها، تلویزیون‌های هوشمند و وسایل نقلیه با هدایت خودکار که به ویندوز ۷ وابسته باشند، از جمله اهداف مناسب برای مجرمان سایبری است که بتوانند بدافزار Lemon Duck را روی آن‌ها به کار گیرند. این بدافزار از انواعی است که می‌تواند خود را انتشار دهد. محققان به تولیدکنندگان دستگاه‌های اینترنت اشیا، هشدار داده‌اند که این نوع بدافزارها در حال گسترش و سوء استفاده از دستگاه‌های آسیب‌پذیر هستند.

۳ تاثیر آسیب‌پذیری

مجرمان پشت موج حملات این بدافزار، از دستگاه‌های اینترنت اشیا برای تشکیل یک مجموعه استخراج‌کننده رمزارز بهره می‌برند و برای این منظور از ابزار استخراج XMRig برای تولید ارزهای مونرو[۲] استفاده می‌کنند. محققان هشدار داده‌اند که تلاش‌ها برای استخراج رمزارز با فشار پردازشی بالا روی تجهیزات و ایجاد اختلال در عملکرد دستگاه‌ها، باعث نقص ایمنی آن‌ها، اختلال در زنجیره‌های تأمین و از بین رفتن داده می‌شوند.

۴ بررسی بدافزار

بررسی‌ها توسط محققان در آزمایشگاه‌های تحقیقاتی TrapX نشان می‌دهد در سال ۲۰۱۹ چندین حمله بزرگ علیه سه تولیدکننده جهانی صورت گرفته است که موضوع مشترک همه آن‌ها، استفاده از بدافزار Lemon

[۱] بهره‌برداری EternalBlue مربوط به یک گروه آسیب‌پذیری بحرانی با شناسه‌های CVE-2017-0143 تا CVE-2017-0148 می‌باشد. این آسیب‌پذیری، نسخه اول پروتکل SMB ماکروسافت را که در ویندوز ۷، ویندوز سرور ۲۰۰۸، ویندوز XP و حتی ویندوز ۱۰ روی درگاه ۴۴۵ مورد استفاده قرار می‌گیرد، تحت تاثیر قرار می‌دهد و بارها توسط بدافزارها و مهاجمان مورد سوءاستفاده قرار گرفته است.

[۲] Monero

Duck و وجود ویندوز ۷ در سیستم‌های تعبیه شده یا تجمیع‌شده است. تخمین زده می‌شود که ویندوز ۷، هنوز توسط ۲۰۰ میلیون دستگاه استفاده می‌شود، در حالی که از ۱۴ ژانویه سال ۲۰۲۰، ویندوز ۷ دیگر توسط مایکروسافت پشتیبانی نشده و بروزرسانی‌های امنیتی را دریافت نمی‌کند.

در هر یک از مطالعات موردی حملات، مشخص شد نقاط ضعف موجود در ویندوز ۷ به عنوان نقطه ورود مهاجم استفاده شده است. بهره‌برداری‌ها مربوط به آسیب‌پذیری‌های وصله نشده در پیاده‌سازی پروتکل بسته پیام سرور (SMB) مایکروسافت در سیستم‌عامل بود که به بهره‌برداری‌های EternalBlue معروف هستند. علاوه بر این، محققان گفتند که مهاجمان حملات تزریق SQL را در برابر آسیب‌پذیری موجود در برنامه پایگاه داده MySQL انجام داده‌اند.

با بررسی بدافزارهای خانواده Lemon Duck مشخص می‌شود که این بدافزارها، با دوبار کلیک کردن و یا از طریق روش‌های پایدار[۳]به اجرا درمی‌آیند. این بدافزار، ابتدا شبکه را برای یافتن اهداف بالقوه از جمله دستگاه-های دارای خدمات SMB (با درگاه ۴۴۵ باز) یا MSSQL (با درگاه ۱۴۳۳ باز) بررسی می‌کند. پس از پیدا کردن یک هدف بالقوه، رشته‌های[۴]متعددی با چندین عملکرد روی دستگاه آسیب‌پذیر به اجرا در می‌آورد.

یکی از این عملکردها شامل حملات جستجوی فراگیر رمز عبور برای شکستن خدمات باز است تا از این طریق، به بارگیری و انتشار بدافزار از طریق پروتکل SMB یا MSSQL بپردازد. مورد دیگر شامل اجرای فراخوانی mimikatz برای بدست آوردن هش‌های NTLM و دستیابی به بارگیری و گسترش بیشتر بدافزار از طریق SMB است.

به گفته محققان، بدافزار Lemon Duck از طریق کارهای زمان‌بندی شده از جمله اسکریپت‌های PowerShell بر روی سیستم‌های آلوده می‌ماند. فراخوانی اسکریپت‌های PowerSell، سبب نصب استخراج‌کننده‌های رمزارزهای مونرو (XMRig) می‌گردد.

بررسی‌ها نشان می‌دهد حملات انجام شده روی دستگاه‌های ویندوز ۱۰ به طور مداوم توسط سیستم‌های دفاعی دستگاه‌ها خنثی شده است. این بدافزار بر روی سیستم‌های دارای ویندوز ۱۰ با قابلیت محافظتی Windows Defender Virus & Threat فعال، قرنطینه می‌شود؛ حتی اگر بدافزار با موفقیت، خود را در سیستم کپی کرده باشد. در مقابل، بدافزار مذکور روی سیستم‌های آلوده ویندوز ۷ حتی با فعال کردن Windows Defender نیز، به فعالیت خود ادامه می‌دهد.

---

[۳] Persistence mechanisms

[۴] Thread

۵ اقدامات جهت کاهش شدت آسیب‌پذیری

اقدامات لازم برای کاهش شدت اثرات این بدافزار، شامل اجرای یک خط مشی قوی برای رمزعبور در همه شبکه‌ها و زیرسیستم‌ها، بروز نگه‌داشتن سیستم‌ها و رعایت احتیاط کامل در هنگام مدیریت شبکه و غیرفعال کردن ورودهای ناشناس به سیستم است. محققان همچنین اکیداً به عدم استفاده از ویندوز ۷ در سیستم‌ها توصیه می‌کنند.

۶ منابع

[1] https://threatpost.com/lemon-duck-malware-targets-iot/152596

[2]https://www.sentinelone.com/blog/eternalblue-and-the-lemon-duck-cryptominer-attack/