خبرنامه مرکز تخصصی آپای دانشگاه ایلام

شماره پنجم - بهمن ماه ۱۳۹۶

جدیدترین اخبار مربوط به حوزه امنیت

معرفی جدیدترین بد افزارها

هشدارها و راهنمایی های امنیتی

اخبار مرکز تخصصی آپای دانشگاه

بررسی جاسوس افزار Skygofree

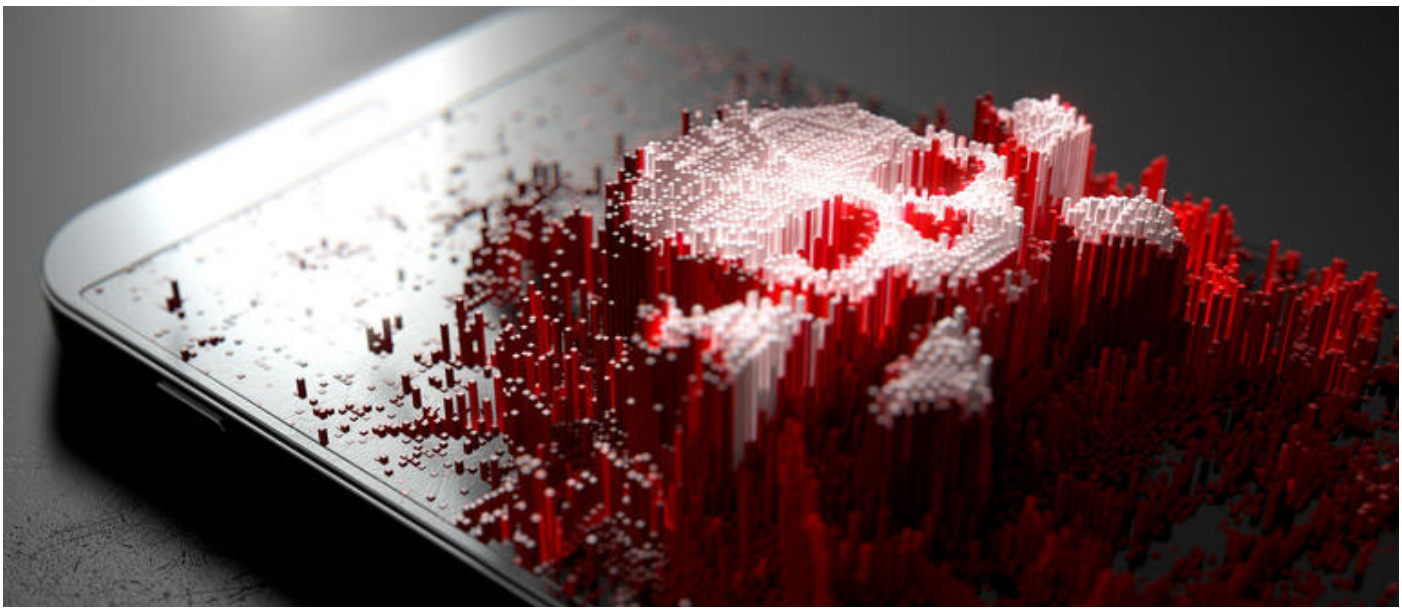
فهرست

بررسی جاسوس افزار Skygofree

محققان امنیتی یک جاسوس‌افزار اندرویدی بسیار پیشرفته و قدرتمند را کشف کرده‌اند که به هکرها امکان کنترل کامل دستگاه آلوده را از راه دور می‌دهد. این ابزار که Skygofree نام دارد، یک جاسوس‌افزار اندرویدی است که برای نظارت هدفمند طراحی شده است. برخی ویژگی‌های قابل توجه آن شامل ضبط صوت مبتنی بر مکان با استفاده از میکروفون دستگاه، استفاده از سرویس‌های دسترسی‌پذیری اندروید(Android Accessibility Services) برای دزدیدن پیام‌های WhatsApp و قابلیت متصل کردن دستگاه‌های آلوده شده به شبکه‌های وای‌فای مخرب کنترل شده توسط مهاجمان می‌باشد. Skygofree از طریق صفحات وب تقلبی توزیع می‌شود. پس از نصب، Skygofree آیکون خود را پنهان می کند و سرویس‌های پس‌زمینه را برای پنهان کردن فعالیت‌هایش از کاربر، راه‌اندازی می کند. این جاسوس‌افزار همچنین شامل یک ویژگی محافظتی است که از کشتن (killing) سرویس‌ها جلوگیری می کند.

Skygofree یک ابزار جاسوسی پیشرفته‌ی چندسکویی است که به مهاجمان امکان کنترل از راه دور کامل دستگاه‌های آلوده با استفاده از payload reverse shell و یک معماری سرور کنترل و فرمان (C&C) را می دهد. با توجه به جزئیات فنی منتشر شده توسط محققان، Skygofree شامل چندین اکسپلویت برای افزایش امتیاز برای دسترسی root است، و این مورد قابلیت اجرای payloadهای پیشرفته‌تر بر روی دستگاه‌های اندرویدی آلوده را فراهم می کند. یکی از این payloadها، امکان اجرای shellcode و دزدیدن داده‌های متعلق به برنامه‌های دیگر مانند فیسبوک، لاین و وایبر را ارائه می‌کند.

سرور کنترل و فرمان (C&C) Skygofree همچنین مهاجمان را قادر به گرفتن عکس و فیلم از راه دور، ضبط تماس‌ها و SMS و همچنین نظارت بر موقعیت جغرافیایی کاربر، رخدادهای تقویم و هر اطلاعات ذخیره شده در حافظه‌ی دستگاه را می‌دهد. بهترین راه برای جلوگیری از اینکه قربانی این جاسوس‌افزار شوید این است که از دانلود برنامه‌ها از طریق وب‌سایت‌ها ولینک‌هایی که از طریق پیام یا ایمیل برایتان ارسال می‌شود، حذر کنید.



بررسی بات نت Mirai Okiru

چشم‌انداز اینترنت اشیا لینوکس به‌سرعت درحال تغییر است، و مهاجمان شروع به هدف قرار دادن دستگاه‌های IoT برپایه‌ی ARC CPU کرده‌اند. این اولین باری است که یک بدافزار، به‌طور خاص سیستم‌های مبتنی بر ARC را هدف قرار می‌دهد. بدافزار Mirai Okiru در زمان کشف برای بیشتر آنتی‌ویروس‌ها غیرقابل تشخیص بوده است.

به‌گفته‌ی محققان تاثیر این بات‌نت می‌تواند خرابکارانه باشد. با توجه به تخمین‌ها، تعداد پردازنده‌های جاسازی‌شده‌ی ARC به‌ازای هر سال به بیش از ۱/۵ میلیار دستگاه می‌رسد. این به این معنی است که تعداد دستگاه‌هایی که به‌صورت بالقوه در معرض خطر هستند بسیار زیاد است و بنابراین یک بات‌نت قدرتمند می‌تواند برای بسیاری از اهداف خرابکارانه استفاده شود.

پردازنده‌های ARC خانواده‌ای از CPUهای ۳۲ بیتی هستند که توسط ARC International طراحی شده‌اند. آن‌ها به‌طور گسترده در دستگاه‌های SoC برای home، Storage، موبایل و برنامه‌های اینترنت اشیاء استفاده شده‌اند. Mirai Okiru بسیار خطرناک است، و توسعه‌دهنده‌ی آن اصلاحات نوآورانه‌ای را در رمزگذاری آن به‌وجود آورده است و این اولین بدافزاری است که هسته‌ی ARC را هدف قرار می‌دهد.

محققان معتقدند با وجود شباهت‌های بات نت جدید Okiru با بات نت Satori که آن‌هم از نوع Mirai بوده و دستگاه‌های IOT بسیاری را آلوده کرده است، این بات نت جدید کاملاً عملکردی متفاوت از خود ارائه کرده است.

پیکربندی Okiru در دو قسمت رمزگذاری کدهای عبور تل‌نت مورداستفاده قرار می‌گیرد این در حالی است که تروجان Satori در دو مرحله فعالیت خود را پیش نمی‌برد و رمزهای عبور پیش‌فرض را مورداستفاده قرار نمی‌دهد.

بررسی‌ها نشان می‌دهد که Satori به‌عنوان یک ابزار تکراری توزیع‌شده مورداستفاده قرار می‌گیرد که از طریق UDP های تصادفی از TSource Engine Query استفاده می‌کند. این در حالی است که تروجان Okiru از این قاعده پیروی نمی‌کند. پایگاه داده پردازنده مرکزی ARC توسط بدافزار Okiru کامپایل می‌شود؛ این در صورتی است که خطر ساخت بات نت‌ها برای میلیون‌ها دستگاه روزبه‌روز در حال افزایش است.

آلوده سازی سیستم مدیریت محتوا WordPress توسط Keylogger

محققان امنیت سایبری بیش از ۲۰۰۰ سایت که از سیستم مدیریت محتوا Wordpress استفاده می کنند را شناسایی کرده اند که توسط یک اسکریپت برای دزدیدن username و password در صفحه ی ورود به بخش مدیریت سایت، آلوده شده بودند و همچنین در صفحات و بخش های اصلی سایت از یک اسکریپت مخصوص عملیات cryptojacking بر روی مرورگر استفاده می کرده اند. این خبر در حالی منتشر شده است که در ماه دسامبر ۲۰۱۷ میلادی، عملیاتی شبیه به همین نفوذ بر علیه سایت های بسیاری که از Wordpress استفاده می کنند رخ داده بود.

روش انجام این گونه حملات ساده و مشخص می باشد. نفوذگران به دنبال سایت های Wordpress هستند که نسخه ی هسته مرکزی آنها قدیمی بوده و دارای آسیب پذیری می باشند؛ ویا اینکه سایت های Wordpress که دارای Plugin ها و Theme های آسیب پذیر می باشند را پیدا کرده و برای انجام حمله خود از آنها استفاده می کنند و با استفاده از Exploit های موجود، کدهای آلوده خود را به source این گونه سایت ها تزریق می کنند.

کدهای آلوده تزریق شده دارای دو بخش کلی مباشد. بخش اول کدهایی که در قسمت login سامانه قرار داده می شوند و هدف آن دزدیدن اطلاعات ورود به بخش مدیریت سایت می باشد. بخش دوم، کدهای Coinhive Miner می باشد که برای استفاده از منابع CPU بازکنندگان سایت به صورت غیرمجاز و ساخت ارز Monero مورد استفاده قرار می گیرد.

در شش ماه دوم سال ۲۰۱۷ میلادی گروه های کلاه برداری اینترنتی از دامنه هایی همچون cloudflare.solutions برای دریافت داده های دزدیده شده از کاربران و انتقال آنها توسط Keylogger ها استفاده می کردند. در آن حملات بیش از ۵۵۰۰ سایت Wordpress مورد حمله قرار گرفت که با غیرفعال کردن دامنه ی فوق در ۸ دسامبر ۲۰۱۷ این حملات به کار خود پایان دادند. بر اساس گزارش کمپانی تحقیقات امنیت سایبری Sucuri، این کمپانی که از همان سال ۲۰۱۷ این گروه ها را مورد شناسایی و رصد قرار داده بود، اعلام کرد که هم اکنون این گروه های کلاهبرداری از دامنه های زیر برای دریافت و ذخیره اطلاعات ارسالی از جانب Keylogger ها استفاده می کنند:

- cdjs.online
- cdns.ws
- msdns.online

همچنین با تحقیقات بیشتر مشخص شده است که بیش از ۲۰۰۰ سایت Wordpress که اسکریپت های آلوده بر روی آنها قرار داده شده است، این اسکریپت ها توسط دامنه های فوق بر روی سیستم مدیریت محتوا آنها بارگزاری شده است. مرکز Sucuri اعلام کرد که به احتمال بالا، تعداد سایت های آلوده شده بیشتر از میزان تخمین زده شده می باشد. مدیران سایت توسط بررسی فایلهای به روز رسانی شده و تغییر داده شده می توانند وجود این گونه اسکریپت ها در سایت خود را مورد بررسی قرار دهند. فراموش نکنیم که همواره CMS Wordpress خود را برای جلوگیری از حملات نفوذگران به روز کنیم.

سوءاستفاده از ویژگی subDoc در Microsoft Word به‌منظور سرقت اعتبارنامه‌ها

طبق یافته‌های محققین گروه امنیتی Rhino Labs (شرکت امنیتی سایبری ایالات‌متحده امریکا) عاملین مخرب می‌توانند با سوءاستفاده از یکی از ویژگی‌های Microsoft Word به نام subDoc، رایانه‌های ویندوزی را فریب دهند و هش NTLM را مورد سرقت قرار دهند. هش NTLM قالب استانداردی است که اعتبارنامه‌های حساب کاربری در آن ذخیره شده‌اند.

قلب این تکنیک، حمله‌ی (pass-the-hash attack (NTLM است که از سال‌های پیش وجود داشته است. به گفته‌ی Rhino Labs، تفاوت حمله‌ی کلاسیک با حمله‌ی جدید، در روش انجام آن است. حمله‌ی جدید از طریق یکی از ویژگی‌های Word به نام subDoc انجام می‌شود. ویژگی subDoc به فایل‌های Word اجازه می‌دهد تا زیرسندها را از سند اصلی بارگیری کنند.

به گفته‌ی متخصصین Rhino Labs، روش حمله به این صورت است که مهاجمان یک فایل Word را که زیرسندی را از یک کارگزار مخرب بارگذاری می‌کند، ایجاد می‌کنند. از طرف دیگر یک کارگزار SMB را میزبان قرار می‌دهند و به‌جای ارائه‌ی زیرسند درخواستی، رایانه‌ی شخصی قربانی را فریب می‌دهند تا هش NTLM را که برای احرازهویت در دامنه‌ی جعلی موردنیاز است، ارایه دهد.

ابزارهای برخط متعددی برای کرک هش‌های NTLM و به‌دست آوردن اعتبارنامه‌های ویندوز موجود در آن در دسترس است. مهاجمان می‌توانند از این اعتبارنامه‌های ورودبه‌سیستم برای دسترسی به رایانه یا شبکه‌ی قربانی استفاده کنند و خود را به‌عنوان کاربر اصلی جا بزنند. این نوع از هک معمولاً در شرکت‌ها و سازمان‌ها دولتی استفاده می‌شود.

به گفته‌ی محقق امنیتی کلمبیایی به نام Juan Diago، این حمله مشابه تکنیک‌های دیگری همچون استفاده از فایل‌های SCF و درخواست‌های SMB به‌منظور فریب ویندوز جهت ارایه‌ی هش‌های NTLM است.

این حمله اولین روش حمله‌ای نیست که از یک ویژگی کمتر شناخته‌شده‌ی Microsoft Word سوءاستفاده می‌کند. تکنیک‌های دیگری مانند استفاده از ویژگی DDE یا ویژگی قدیمی ویرایشگر معادله‌ی Office نیز در حملات استفاده شده‌اند. با این وجود، در حال حاضر تشخیص حملات subDoc مشکل است.

مایکروسافت به‌تازگی پشتیبانی از DDE را در Word غیرفعال کرده است، زیرا این ویژگی بارها توسط توزیع‌کنندگان بدافزار مورد سوءاستفاده قرار گرفته است. سرنوشت subDoc هنوز مشخص نیست زیرا این ویژگی برای کمپین‌های توزیع بدافزار یک آسیب¬پذیری کلیدی نیست و ممکن است به‌اندازه‌ی حملات DDE موردتوجه مایکروسافت قرار نگیرد. ازآنجایی‌که این ویژگی عموماً به‌عنوان یک حمله برای اعمال مخرب شناخته نشده است، توسط نرم‌افزار آنتی‌ویروس شناسایی نمی‌شود.

مرکز تخصصی آپای دانشگاه ایلام

پست الکترونیکی cert@ilam.ac.ir

وب سایت cert.ilam.ac.ir