CherryBlossom ابزاری برای نفوذ به روترها

سازمان سیا سال‌ها است که روترهای مردم را هک می‌کند

اسنادی که ویکی‌لیکس به تازگی و به صورت عمومی آن‌ها را منتشر کرده نشان می‌دهند که سازمان جاسوسی سیا از ابزاری ویژه به منظور نفوذ به روترها و نقاط پایانی استفاده می‌کرده است. ابزاری که در طول این سال‌ها روترهای بی‌سیم را مورد نفوذ قرار می‌داده است.

این ابزار که CherryBlossom نام دارد، به منظور نظارت و کنترل روی فعالیت‌های سایبری ماشین‌های هدف و همچنین بهره‌برداری از رخنه‌هایی که روی دستگاه‌های بی‌سیم وجود دارد، توسعه داده شده است. در این اسناد آماده است که ابزار فوق ماحصل همکاری مشترک سازمان سیا و یک مرکز تحقیقات بین‌المللی موسوم به SRI است. این اسناد نشان می‌دهند که ابزار فوق حداقل از یازده سال پیش (2006 میلادی) در حال توسعه بوده و قادر است 200 مدل مختلف روترهای تولید شده از سوی 20 شرکت تولیدکننده مختلف را رصد کرده و شنود کند.

مطلب پیشنهادی

اشتباهات رایج کاربران

۷ اشتباه امنیتی مرگ‌بار که احتمالا شما هم مرتکب می‌شوید

در حالی که نام بسیاری از تولیدکنندگان مطرح روتر در این لیست دیده می‌شود، نامی از اپل در آن به چشم نمی‌خورد. Flytrap یکی از مولفه‌های مهم این ابزار این پتانسیل را دارد تا به اشکال مختلفی روی ماشین‌های هدف نصب شود. مرسوم‌ترین روشی که این ابزار به منظور نفوذ به سامانه‌های قربانی از آن استفاده می‌کند، Clymore نام دارد. این مولفه به ابزار فوق اجازه می‌دهد از طریق به‌روزرسانی میان‌افزار روتر روی ماشین هدف نصب شود. در این میان دستگاه‌هایی وجود دارند که اجازه نمی‌دهند میان‌افزار آن‌ها به‌روزرسانی شود، در این حالت مولفه فوق قادر است از طریق بسته‌های به‌روزرسانی بی‌سیم، ماشین قربانی را آلوده سازد. جالب آن‌که سازندگان، ابزار فوق را به گونه‌ای طراحی کرده‌اند که امکان نصب این مولفه به شیوه فیزیکی روی روتر از طریق زنجیره تامین (عرضه و تقاضا) نیز امکان‌پذیر باشد.

مطلب پیشنهادی

باج‌افزارها این‌بار در مسیر اپل
اولین زیرساخت باج‌افزار به عنوان سرویس ویژه سامانه‌های مک شناسایی شد

هنگامی که این مولفه به شکل کاملی روی دستگاه قربانی نصب شد، با سرور کنترل و فرمان‌دهی خود به نام CherryTree ارتباط برقرار می‌کند. نویسندگان این ابزار قادر هستند مولفه Flytrap را از طریق یک رابط کاربری مبتنی بر وب موسوم به CherryWeb کنترل کنند. این مولفه به توسعه‌دهندگان این ابزار اجازه می‌دهد اطلاعاتی همچون آدرس‌های ایمیل، شماره‌های VoIP، نام کاربری مورد استفاده در گفت‌وگو، تغییر مسیر مرورگر، فیلتر کردن ارتباطات شبکه قربانی و اجرای برنامه‌های کاربردی را به شکل دقیقی مدیریت کنند.

ویکی‌لیکس از 23 مارس به‌طور نسبتا منظم اسنادی را در ارتباط با فعالیت‌های استراق سمع و شنود مکالمات از سوی آژانس‌های جاسوسی در قالب فایل‌هایی موسوم به Valut7 منتشر می‌کند. اسنادی که تا به امروز این سازمان منتشر کرده است نشان می‌دهند که سازمان‌های جاسوسی از چنین ابزارهایی به منظور جایگزینی فایل‌های موجود روی سیستم‌عامل قربانی، نفوذ به تلویزیون هوشمند سامسونگ، پیاده‌سازی حمله مرد میانی، گذر از مکانیزم‌های تشخیص و شناسایی بدافزارها و همچنین آماده‌سازی زیرساختی به منظور ایجاد بدافزارهای سفارشی استفاده کرده‌اند. در این اسناد به وضوح به این نکته اشاره شده است که امنیت ضعیف روترهای بی‌سیم باعث شده است تا سازمان‌های جاسوسی به راحتی به این ابزارها نفوذ کنند. جالب آن‌که حتا شرکت‌های امنیتی نیز موفق شده‌اند ارتباطی میان ابزارهای نفوذ و گروه‌های هکری همچونی Longhorn و The Lamberts پیدا کنند.

تاریخ انتشار:

28 خرداد 1396

نشانی منبع:
https://www.shabakeh-mag.com/security/8268/%D8%B3%D8%A7%D8%B2%D9%85%D8%A7%D9%86-%D8%B3%DB%8C%D8%A7-%D8%B3%D8%A7%D9%84%E2%80%8C%D9%87%D8%A7-%D8%A7%D8%B3%D8%AA-%DA%A9%D9%87-%D8%B1%D9%88%D8%AA%D8%B1%D9%87%D8%A7%DB%8C-%D9%85%D8%B1%D8%AF%D9%85-%D8%B1%D8%A7-%D9%87%DA%A9-%D9%85%DB%8C%E2%80%8C%DA%A9%D9%86%D8%AF