رقابت بر سر تخریب بیشتر

رقیب بدافزار Mirai با قدرت مهیبی به میدان وارد شد

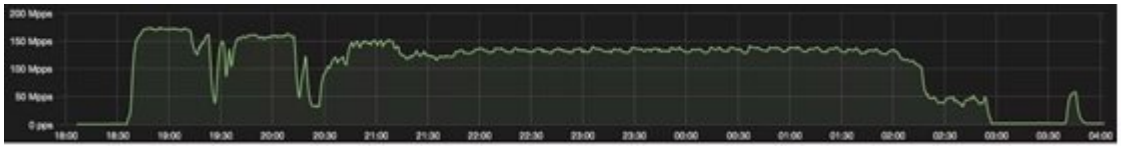
در حال حاضر بسیاری از شرکت‌های بزرگ در سراسر جهان از بات‌نت Mirai واهمه دارند. به واسطه آن‌که خطرناک بوده و به راحتی خسارت‌های میلیون دلاری وارد می‌کند. اما کمی تعمل کنید. اکنون رقیب این بدافزار به میدان وارد شده است. این بدافزار جدید که هنوز نامی برای آن تعیین نشده و به تازگی شناسایی شده است، در اولین برخورد نزدیک خود موفق شده یک حمله 400 گیگابیت بر ثانیه را پیاده‌سازی کند.

کارشناسان امنیتی شرکت CloudFlare به تازگی موفق به شناسایی بات‌نت جدیدی شده‌اند که قادر است قدرتمندتر از اسلاف خود همچون Mirai صدمات سنگینی را وارد کند. اگر از شما درباره مخوف‌ترین تهدیدی که این روزها دنیای فناوری را مورد تهدید قرار می‌دهد سوال کنم، چه جوابی خواهید داد؟ بدون شک جواب شما بات‌نت Mirai است. بدافزاری که به راحتی قادر است سنگین‌ترین حملات منع سرویس انکار شده را پیاده‌سازی کند. حملاتی که به راحتی موفق شدند سرویس DNS متعلق به شرکت داین را از مدار خارج کنند. اکنون کارشناسان حوزه امنیت شبکه تحویل محتوای CloudFlare اعلام کرده‌اند که بات‌نتی به همان اندازه خطرناک را در تاریخ 23 نوامبر شناسایی کرده‌اند.

مطلب پیشنهادی

Mirai خاموش و خطرناک تسخیر می‌کند
نقشه زنده‌ای از آلودگی بدافزار Mirai در سراسر جهان را مشاهده کنید

حمله منع سرویس انکار شده‌ای که این بات‌نت آن‌را پیاده‌سازی کرده بود نزدیک به هشت ساعت و نیم به طول انجامید. هکرها این حمله را در مدت زمان شش روز و در ساعت‌های مشخصی از شبانه‌روز به مرحله اجرا در آوردند. کارشناسان این شرکت اعلام داشته‌اند که شدت این حمله در اوج بار ترافیک آن 400 گیگابیت بر ثانیه و در ساعات پایانی به 320 گیگابیت بر ثانیه رسیده بود. تصویر زیر اوج بار کاری این بات‌نت را نشان می‌دهد.



گزارش ارائه شده از سوی این کارشناسان نشان می‌دهد که این حمله از ساعت شش و سی دقیقه عصر آغاز شده بود و در ساعت 3 بامداد پایان یافته بود. به طوری که نزدیک به هشت ساعت و نیم به طول انجامیده بود. تحلیل اولیه نشان می‌دهد که بات‌نت جدید در مقایسه با Mirai از قدرت کمتری برخوردار است. اما با این وجود کارشناسان بر این باور هستند که این بدافزار در آینده از قدرت بیشتری برخوردار خواهد بود. نکته جالب توجهی که

در این بین وجود دارد این است که بات‌نت جدید از کدهای منبع Mirai استفاده نکرده و با توجه به این‌که از نرم‌افزارهای جدیدی استفاده کرده است و این حملات در لایه‌های سه و چهار پیاده‌سازی شده‌اند در نتیجه این بات‌نت از پایه جدید نوشته شده است. تحلیل‌ها نشان می‌دهند که این حمله نواحی متنهی به سواحل غربی ایالات متحده را نشانه رفته بودند. CloudFlare اعلام کرده است: «هنوز به طور دقیق درباره جزییات این بات‌نت نمی‌توانیم اظهار نظر کنیم. در نتیجه هنوز به درستی مشخص نیست آیا بات‌نت جدید نیز از دستگاه‌های اینترنت اشیا استفاده می‌کند یا از رویکرد متفاوتی در این زمینه بهره می‌برد.»

شرکت CloudFlare اعلام کرده است که این احتمال وجود دارد که این بات‌نت در آینده با پلتفرم‌های دیگر مخرب ترکیب شود و حملات منع سرویس انکار شده بسیار مخربی را به وجود آورد.

تاریخ انتشار:

17 آذر 1395

نشانی منبع: https://www.shabakeh-mag.com/security/5772