باسمه تعالی

حملات DDoS با سوءاستفاده از پیکربندی نامناسب TFTP

TFTP (Trivial File Transfer Protocol) یک پروتکل ساده برای انتقال فایل در درون شبکه می‌باشد که این امکان را در اختیار کلاینت قرار می‌دهد تا فایل مورد نظرش را به یک سیستم راه دور ارسال و یا از آن دریافت کند. این پروتکل قدیمی بوده و در سال ۱۹۸۱ میلادی در قالب یک استاندارد ارائه شده است. در سال‌های بعد نسخه‌های تکمیلی به استاندارد افزوده شده است. از عمده‌ترین کاربردهای این پروتکل می‌توان به انتقال خودکار فایل‌های مربوط به تنظیمات یک دستگاه و یا فایل‌های مورد نیاز یک دستگاه برای بوت شدن در یک شبکه محلی اشاره کرد.

TFTP از پروتکل UDP و شماره پورت ۶۹ برای انتقال فایل استفاده می‌کند. این پروتکل از TCP و شماره پورت ۸۰۹۹ نیز گاهی به منظور انتقال اطلاعات مربوط به رابط کاربری استفاده می‌کند. هدف طراحی پروتکل TFTP کوچک بودن و سادگی پیاده‌سازی آن بوده و بنابراین فاقد بسیاری از ویژگی‌هایی است که توسط دیگر پروتکل‌های انتقال فایل قدرتمند ارائه می‌گردد. تنها کاری که TFTP انجام می‌دهد، خواندن و یا نوشتن فایل‌ها از و یا روی سیستم راه دور می‌باشد و نمی‌تواند فایل‌ها و یا دایرکتوری‌ها را حذف، تغییر نام و یا لیست کند. همچنین فاقد قابلیت احراز اصالت کاربران می‌باشد که بزرگترین نقطه ضعف امنیتی آن محسوب می‌شود. TFTP بهترین مصداق "امنیت از طریق گمنامی[۱]" می‌باشد و اگر شخصی قصد سوء استفاده از این سرویس را داشته باشد، باید نام فایل مورد نظرش را حتماً بداند. اگرچه این مورد ساده به نظر می‌رسد ولی با توجه به عدم امکان ارسال درخواست مبنی بر لیست کردن فایل‌ها و یا دایرکتوری‌ها در پروتکل TFTP، این گمنامی می‌تواند زمان نتیجه گرفتن حمله را به تأخیر بیاندازد. با توجه به امنیت بسیار پایین این پروتکل، توصیه شده است که این پروتکل حداکثر در شبکه‌های محلی به‌کار گرفته شود.

یکی دیگر از تهدیدهای پر اهمیت پروتکل TFTP، امکان سوء استفاده از آن برای انجام حملات DDOS می‌باشد. عدم تعیین سایز پیش فرض برای برخی از فیلدهای پرسش و پاسخ پروتکل، Stateless بودن پروتکل و عدم استفاده از روش‌های احراز اصالت از مهمترین دلایل پیدایش این حمله است. برای اجرای حمله، فرد حمله‌کننده ابتدا اقدام به یافتن سرورهای TFTP ای می‌نماید که از طریق شبکه اینترنت قابل دسترسی هستند. پس از آن یک درخواست PRQ TFTP با حداقل سایز ممکن را ارسال نموده که پاسخ آن حداکثر بوده و به‌جای

[۱] obscurity

قرار دادن آدرس IP خود در فیلد آدرس IP فرستنده، آدرس IP فرد قربانی را قرار می‌دهد. درنتیجه پاسخ تولیدی برای فرد قربانی ارسال خواهد شد. به دلیل اینکه تعداد بایت موجود در پیامی که سرور در پاسخ باز می-گرداند نسبت به تعداد بایت موجود در پرسش ارسال شده از سوی کلاینت قابل توجه است، حمله‌کننده می‌تواند به ضریب تقویت[2] بالایی دست پیدا کند. بدین صورت با به‌کارگیری یک شبکه بات‌نت می‌توان حجم بسیار زیادی ترافیک به سوی فرد قربانی هدایت نمود. درنتیجه یک سرویس‌دهنده TFTP که پیکربندی صحیحی ندارد می‌تواند به‌طور ناخواسته در حمله DDoS مورد سوءاستفاده قرار گیرد.

اگر تمام شرایط مورد نظر به درستی وجود داشته باشد، با استفاده از این حمله، ترافیک خروجی می‌تواند به میزان ۶۰ برابر ترافیک اولیه نیز برسد. بررسی‌ها نشان می‌دهد بسیاری از نرم‌افزارهای TFTP به طور خودکار ترافیک خروجی در حدود ۶ برابر ترافیک ورودی تولید می‌کنند.

برای امن‌سازی تجهیزات در برابر سوء استفاده از این آسیب‌پذیری، موارد زیر باید اعمال شوند:

- بایستی در صورت عدم نیاز به TFTP، این سرویس غیرفعال گردد.
- بایستی در صورت نیاز به TFTP، تنها در شبکه محلی قابل دسترسی باشد. در صورت نیاز به دسترسی به این سرویس از طریق شبکه اینترنت، بایستی ترافیک وارد شده از بیرون شبکه به این سرویس و همچنین ترافیک خروجی از آن از داخل شبکه به بیرون کنترل شوند. این کار با کنترل کردن ترافیک UDP/69 توسط دیواره آتش قابل انجام است.

[2] Amplification factor