باسمه تعالی

حملات DDoS با سوءاستفاده از پیکربندی نامناسب mDNS

mDNS[1] به منظور تبدیل نام به آدرس IP در شبکه‌های کوچک که فاقد یک سرور نام محلی می‌باشند، استفاده می‌شود (در برخی از چاپگرها، تلفن‌های IP، ذخیره‌گاه‌های NAS و ... پیاده‌سازی شده و دایمون‌های آن برای سیستم عامل ویندوز و لینوکس نیز وجود دارد). ساختار بسته‌های mDNS همانند بسته‌های DNS می‌باشد. mDNS از پروتکل UDP و شماره پورت ۵۳۵۳ و آدرس IP های چندپخشی[2] زیر استفاده می‌کند:

IPv4: 224.0.0.251
IPv6: FF02::FB

زمانی که یک کلاینت mDNS نیاز به ترجمه یک نام دارد، یک پیام درخواست به صورت چندپخشی در طول شبکه ارسال می‌کند و از سیستمی که دارای این نام می‌باشد درخواست می‌کند تا خودش را معرفی کند. پس از آن سیستم مورد نظر در پاسخ یک پیام که شامل آدرس IP خودش می‌باشد، در طول شبکه به صورت چندپخشی ارسال می‌کند. تمام سیستم‌های موجود در این زیرشبکه می‌توانند از این اطلاعات برای به‌روز رسانی mDNS cache مربوط به خودشان استفاده کنند.

با توجه به تحقیقات انجام شده بعضی از پیاده‌سازی‌های mDNS به درخواست‌هایی که از خارج شبکه محلی نیز می‌آیند، پاسخ می‌دهند. این امر می‌تواند توسط حمله‌کنندگان مورد سوء استفاده قرار بگیرد و موجب نشت اطلاعات حساس و همچنین سوء استفاده به منظور انجام حملات DDoS شود.

بیشترین سوء استفاده‌ای که از mDNS می‌شود، به کارگیری آن به منظور اجرای حملات DDoS می‌باشد. برای اجرای حمله، فرد حمله‌کننده کوئری درخواست تحلیل نام را ارسال نموده ولی به‌جای 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 می‌گرداند نسبت به تعداد بایت موجود در پرسش ارسال شده از سوی کلاینت قابل توجه است، حمله‌کننده می‌تواند به ضریب تقویت[3] بالایی دست پیدا کند. بدین صورت با به‌کارگیری یک شبکه باتنت می‌توان حجم بسیار زیادی ترافیک به سوی فرد

[1] multicast Domain Name System
[2] multicast
[3] Amplification factor

قربانی هدایت نمود. درنتیجه یک سرویس‌دهنده mDNS که پیکربندی صحیحی ندارد می‌تواند به‌طور ناخواسته در حمله DDoS مورد سوءاستفاده قرار گیرد.

تخمین دقیق ضریب تقویت ترافیک به راحتی قابل پیش‌بینی نیست و به تنظیمات مختلف سرور و اندازه بسته درخواست ارسال شده به سمت سرور بستگی دارد، ولی در بعضی آزمایش‌های صورت گرفته ترافیک خروجی تا میزان ۹۷۵ درصد ترافیک ورودی نیز رشد داشته است! البته با توجه به نتایج آزمایش‌های مختلف، میزان ضریب تقویت برای این حمله به طور متوسط ۱۳۰ درصد پیش‌بینی شده است.

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

- بایستی در صورت عدم نیاز به mDNS، این سرویس غیرفعال گردد.
- بایستی در صورت نیاز به mDNS، ترافیک وارد شده از بیرون شبکه به mDNS و همچنین ترافیک خروجی از mDNS از داخل شبکه به بیرون مسدود شوند. این کار با کنترل کردن ترافیک UDP/5353 توسط دیواره آتش قابل انجام است.