با BlackNurse آشنا شوید؛ حمله محروم سازی از سرویس فقط با یک لپ تاپ - دیجیاتو

حمید مقدسی | دوشنبه، ۲۴ آبان ۱۳۹۵

اخیراً شدت حملات محروم سازی از سرویس یا همان DoS بسیار بالا گرفته و همان طور که مطلع شدید، هکرها با بهره گیری از بات نت های بزرگ موفق شدند سرورهای عظیم و حتی بخشی از شبکه اینترنت جهانی را از کار بیندازند.

حال محققین مرکز عملیات امنیتی TDC می گویند برای اجرای این نوع عملیات، نیاز به شبکه گسترده ای از دیوایس های آلوده ندارید، بلکه حتی با یک کامپیوتر شخصی و ارتباط اینترنتی معمولی نیز می توانید چنین کاری را انجام دهید.

این پژوهشگران تکنیکی با نام BlackNurse را معرفی کردند که تنها با استفاده از یک لپ تاپ و پهنای باند 15 مگابیت بر ثانیه، قادر است سرورهای بزرگ را به زانو درآورد.

در این روش به جای بمباران ترافیک داده، بسته های ICMP خاصی به سمت هدف ارسال می شود که پردازنده های تعبیه شده روی فایروال سرورهای سیسکو، پالو آلتو و غیره را به شدت درگیر می سازد. در نهایت فایروال آنقدر داده دراپ می کند که سرور مربوطه از کار می افتد، حتی اگر ظرفیت شبکه کاملاً آزاد باشد.

اما خبر خوب اینکه همواره روش هایی برای مقابله با BlackNurse وجود دارد. TDC پیشنهاد می کند از فیلترهای نرم افزاری برای پیشگیری از این نوع حمله فلودینگ استفاده شود. همچنین سازندگان فایروال نیز باید به وضعیت بسته های ICMP توجه ویژه ای نشان دهند.

به عنوان مثال پالو آلتو می گوید فایروال های این کمپانی به صورت پیش فرض چنین درخواست هایی را دراپ می کنند، مگر اینکه تنظیمات را به صورت دستی تغییر دهید و از راهنماهای محافظت در برابر فلودینگ پیروی نکنید. سیسکو نیز اعلام کرده در برابر حملات مذکور آسیب پذیر نیست.

با این حال تمامی فایروال ها از قوانین یکسانی تبعیت نمی کنند، ضمن اینکه برخی از کسب و کارها بنا به دلایل خاصی باید تنظیمات را تغییر داده و ورود داده های ICMP را میسر سازند. بنابراین اجرایی بودن این نوع حمله می تواند به متخصصین حوزه امنیت گوشزد کند که حملات DoS به شکل های مختلف قابل اجرا هستند.

بنابراین تحت شرایط مناسب، شاید یک فرد در منزل و با امکانات ساده بتواند به اندازه یک گروه سایبری حرفه ای، خطرناک ظاهر گردد.

دیجیاتو