چگونه از روتر در مقابل بدافزارها محافظت کنیم

بعضی‌ها نگرانند که دیگران، حتی تبهکاران، بتوانند آدرس IP شان را رصد کنند. «اگر آنها به داخل روترمان راه پیدا کنند چه می‌شود؟». در این مطلب کوتاه یاد می‌گیرید چگونه از روتر بی‌سیم‌تان در مقابل مهاجمان محافظت کنید.

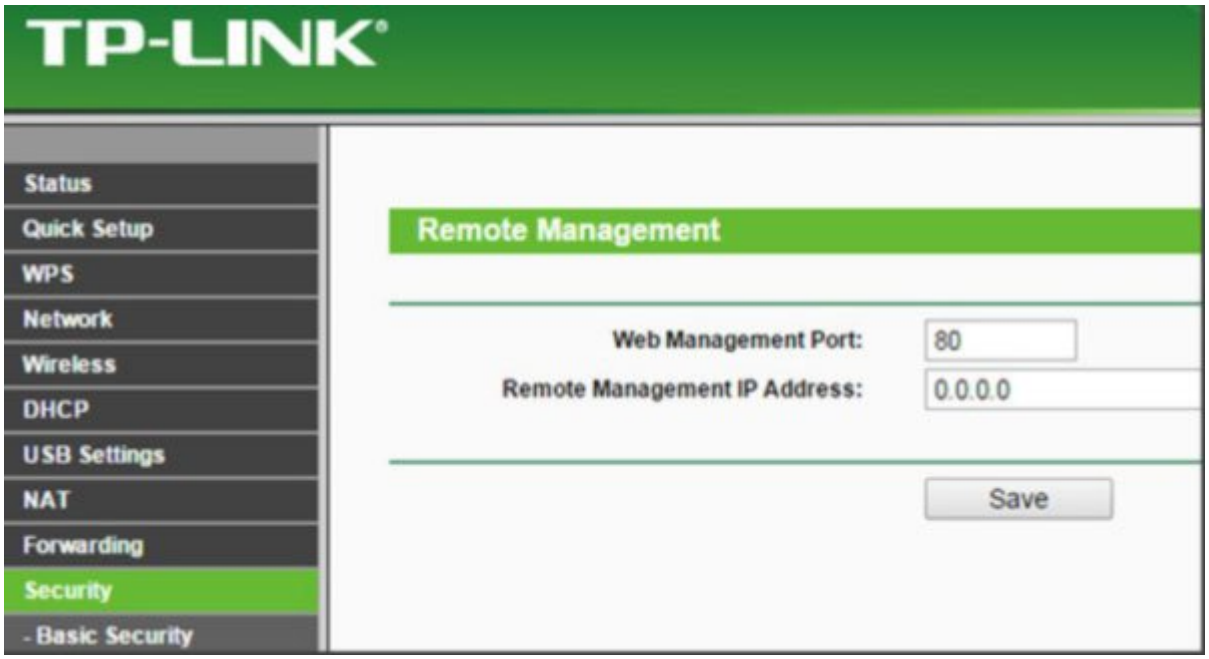
همان‌طور که می‌دانید، آدرس IP اطلاعات چندان سری نیست. به هر وب‌سایتی که سر می‌زنید، با یک نگاه به آدرس IP می‌توان به ISP و موقعیت مکانی آن پی برد. هکرها می‌توانند روترتان را به بدافزار آلوده کنند؟ بعید است اما خطر آنقدر هست که لازم باشد اقدامات احتیاطی صورت بگیرد. سال گذشته، محققان کرمی (Worm) با نام TheMoon کشف کردند که چندین روتر Linksys را آلوده کرده بود. Linksys به سرعت اصلاحیه‌ای برای توقف آن بیرون داد. این اولین حمله از این نوع نبود و قطعا آخری هم نخواهد بود.

در نظر داشته باشید که TheMoon فقط روترهای Linksys را آلوده می‌کند. البته نمی‌شود به Linksys خرده گرفت. شاید حمله بعدی به روترهای D-Link یا Netgear باشد. ماهیت این نوع بدافزارها این است که مختص یک کارخانه‌اند. پس احتمال اینکه کرمی درصدد حمله به روترتان باشد و با آن سازگاری نداشته باشد هست. و یک بار هم که شده این ناسازگاری‌ها سبب خیر شدند.

آنچه در ذیل آمده قدم‌های احتیاطی هستند که همه باید بردارند:

1. فرمویر مرورگرتان را بروز کنید. وب سایت سازنده را برای یافتن نسخه جدید به طور منظم چک کنید.

2. به صفحه تنظیمات روترتان رفته و از خاموش بودن مدیریت از راه دور اطمینان حاصل کنید (اگر آدرس IP موجود 0.0.0.0 است یعنی خاموش است).



3. نام شبکه بی‌سیم‌تان را عوض کنید. نیازی به تبلیغ سازنده روترتان نیست.

4. رمزعبور روترتان را عوض کنید. در مورد رمزعبور وایفای حرف نمیزنم. منظور رمزعبوری است که برای ورود به تنظیمات روتر وارد می‌کنید.

در آخر، اگر خیلی نگرانید می‌توانید آدرس IP خود را با نرم‌افزارهای پراکسی قایم کنید.

منبع:

تک‌هیو

تاریخ انتشار:
28 بهمن 1393

نشانی منبع: https://www.shabakeh-mag.com/networking-technology/300