سه شنبه 09 فروردین 1390 - 07:24

30 میلیارد هرزنامه در جهان، هر روز فقط توسط 2 نفر ارسال می‌شد!

کارشناسان معتقدند باتنت راستاک (Rustock) که هر روز بیش از 30 میلیارد هرزنامه به سراسر جهان ارسال می‌کرده، احتمال توسط یک تیم 2 یا 3 نفره اداره می‌شد.

کارشناسان معتقدند باتنت راستاک (Rustock) که هر روز بیش از 30 میلیارد هرزنامه به سراسر جهان ارسال می‌کرده، احتمال توسط یک تیم 2 یا 3 نفره اداره می‌شد.

تحلیل‌های اولیه بعد از حمله و از کار انداختن بزرگ‌ترین شبکه ارسال هرزنامه در جهان نشان می‌دهد، یک تیم بسیار کوچک مسوول اداره آن بوده‌اند.

به گزارش بی‌بی‌سی، راستاک با سوء استفاده از امکانات بیش از یک میلیون کامپیوتر شخصی یا به اصطلاح با hijack کردن آن‌ها، هر روز میلیاردها هرزنامه به سراسر جهان ارسال می‌کرد. تیم مدیریت این شبکه از روش‌های متعددی استفاده می‌کردند تا خود را از دسترس برنامه‌های امنیتی و کارشناسان دور نگاه دارند.

بعد از حمله سخت‌افزاری به این شبکه و از کار انداختن آن، حجم هرزنامه‌های ارسال شده در سراسر جهان به عدد نسبتا پائینی کاهش پیدا کرده و در همان وضعیت هم باقی مانده است.

الکس لانستین مهندس سابق شرکت امنیتی FireEye که در عملیات تحقیق و بررسی در مورد راستاک همکاری داشته است در این باره گفت: «به نظر نمی‌رسد بیش از 2 یا 3 نفر مسوولیت اداره این باتنت را به عهده داشته باشند.»

آقای لانستین در طول چند سال گذشته مشغول فعالیت برای از کار انداختن این باتنت بوده و به همین دلیل آشنایی زیادی با آن دارد.
او در این باره می‌گوید: "خصوصیات کدی که در بدافزار راستاک به کار رفته و روشی که این شبکه عظیم اداره می‌شده است، نشان می‌دهد باستاک حداکثر توسط یک تیم کوچک چند نفره اداره می‌شده است.»

در تاریخ 16 مارس /25 اسفند 1389، تیمی متشکل از FireEye، مایکروسافت، Pfizer و چند شرکت دیگر به صورت همزمان به مراکز اطلاعاتی این باتنت در 8 شهر آمریکا حمله کرده و 96 سرور را که وظیفه فرمان‌دهی و کنترل این باتنت را داشتند، از کار انداختند.
آقای لانستین اعلام کرد، هارد دیسک‌های این سرورها به یک شرکت قانونی فرستاده شده است تا بتوان سرنخ‌هایی در مورد هویت افرادی که وظیفه کنترل این شبکه را داشتند به دست آورد.

این موضوع که یک تیم کوچک مسوول کنترل راستاک بوده، یکی از دلایل متفاوت بودن این باتنت با دیگر شبکه‌های پراکندن هرزنامه مانند زئوس (zeus) است. به گفته لاستین، آن شبکه توسط تعداد زیادی از گروه‌های مختلف و مجرمان فضای سایبر اداره می‌شد.
اما در عوض باستاک توسط تعداد معدودی اداره می‌شد و البته این افراد نیز مشکلات زیادی برای مدیریت منابع خود و فرستادن بسته‌های آپدیت به یک میلیون کامپیوتر داشتند. با این وجود به دلیل شیوه هوشمندانه اداره باستاک، این شبکه سال‌ها از دسترس شرکت‌ها و کارشناسان امنیتی به دور مانده بود.

قربانیان این شبکه بعد از ملاقات سایت‌هایی با لینک‌ها و تبلیغات گمراه‌کننده به دام می‌افتادند. زمانی که یک کامپیوتر آلوده می‌شود، آپدیت‌ها با استفاده از رمزگذاری‌های متفاوت به آن‌ها ارسال می‌شد. این دانلودها شامل یک ماشین ارسال هرزنامه بود که میلیاردها تبلیغ مختلف برای داروهای تقلبی ارسال می‌کرد.

حتی گاهی اوقات آپدیت‌های راستاک مشابه با کامنت‌هایی در بردهای مباحثه‌ای بودند و همین امر تشخیص را برای نرم‌افزارهای امنیتی که به دنبال نشانه‌های معمول برای شناسایی بدافزارها هستند، دشوار می‌کرد.

آقا لاستین در این باره گفت: «با شناسایی تمام سرورهای کنترل و فرمان‌دهی در آمریکای میانه، ما توانستیم این باتنت را از کار بیندازیم. هزینه نگهداری این سرورها هر ماه به 10 هزار دلار می‌رسید. اما تخمین درآمد حاصل از باستاک برای اداره‌کنندگان آن

چندان ساده نیست.»

به نظر نمی‌رسد بعد از حمله به راستاک، کنترل‌کنندگان آن، تلاش جدیدی را برای دوباره به راه انداختن آن انجام داده باشند. مراحل تکنیکی که توسط مایکروسافت برای از کار انداختن این بات‌نت انجام شده است، تلاش‌های بعدی برای دوباره به راه انداختن این شبکه را بسیار محدود می‌کند.