خونریزی اینترنتی چه‌کسانی را تهدید می‌کند؟

در روزهای اخیر یک حفره امنیتی خطرناک در یکی از استانداردهای رمزگذاری اینترنتی کشف شده که کارشناسان بر پایه ویژگی‌هایی آن را "خونریزی" نامیده‌اند اما این حفره دست هکرها را به چه اطلاعاتی می‌رساند؟ چه کسانی در معرض خطرند؟

"اس‌اس‌ال" برای بیشتر افراد مفهومی ناشناخته است، با وجود این‌که بسیاری هر روز با آن سر و کار دارند. اس‌اس‌ال یک استاندارد رمزگذاری اطلاعات است. در روزهای اخیر یک حفره امنیتی در یکی از نسخه‌های این استاندارد پیدا شده و نگرانی‌های گسترده‌ای را برانگیخته است.

نسخه معیوب استاندارد یاد شده OpenSSL است و این حفره امنیتی به هکرها اجازه می‌دهد داده‌های حساس را از کانال‌های رمزگذاری‌شده بدزدند.

بسیاری از پایگاه‌های اینترنتی، ارائه‌کنندگان خدمات ایمیل و برنامه‌های چت از استاندارد اس‌اس‌ال برای تأمین امنیت ترافیک اطلاعات استفاده می‌کنند. "اُپن‌اس‌اس‌ال" که یکی از نرم‌افزارهای مبتنی بر این استاندارد است، به دلیل رایگان بودن، به صورت گسترده در فضای مجازی منتشر شده است. به همین دلیل است که حفره امنیتی موجود در آن تا این حد خبرساز شده است. بر اساس برخی برآوردها، حدود نیم میلیون پایگاه اینترنتی از "اپن‌اس‌اس‌ال" استفاده می‌کنند.

حفره امنیتی در یکی از بخش‌های "اپن‌اس‌اس‌ال" است که در پس‌زمینه فعال است. در یک ارتباط رمزگذاری‌شده، بخش معیوب با ارسال و دریافت سیگنال‌هایی، آنلاین بودن دو طرف خط را کنترل می‌کند. چون ارسال و دریافت این سیگنال‌ها به صورت مداوم و با ریتم خاصی صورت می‌گیرد، نام این فرایند "ضربان قلب" گذاشته شده است.

چون بخش یادشده معیوب است، هکرها می‌توانند هم اطلاعات مربوط به آنلاین بودن دو طرف را از سرور بگیرند، هم اطلاعاتی دیگر چون گذرواژه‌ها یا محتویات ایمیل‌های رد و بدل شده را. برخی از کاربران برای رمزگذاری‌کردن ارتباطات اینترنتی خود از نرم‌افزارهای رمزگذاری استفاده می‌کنند.

حتی کلیدهایی که توسط این نرم‌افزارهای رمزگذاری تولید شده‌اند هم در دسترس هکرها خواهند بود. به همین دلیل نام این حفره امنیتی "خونریزی" گذاشته شده است.

واقعیت این است که مشکل جدی و سر و صدای روزهای اخیر فراتر از قیل و قال رسانه‌ای است. خطری که کاربران را تهدید می‌کند، نسبت مستقیم با میزان اطلاعاتی دارد که هکرها از آنها جمع‌آوری کرده‌اند. ممکن است یک نفوذگر با استفاده از داده‌هایی که به دستش افتاده موفق شود یک رمزگذاری را به‌طور کامل خنثی کند.

هکری که به کلید خصوصی یک شخص یا پایگاه اینترنتی دسترسی دارد، می‌تواند تمام اطلاعات رمزگذاری‌شده آن شخص یا سایت اینترنتی را بخواند. مجرمان اینترنتی با دسترسی به چنین اطلاعاتی حتی می‌توانند خود را به‌جای سایت‌های دیگر جا بزنند، مثلا سایت یک بانک.

البته تاکنون موردی از سوءاستفاده‌های این چنینی گزارش نشده است؛ هر چند نباید فراموش کرد که حمله با استفاده از حفره ایمنی یاد شده بسیار بی‌سروصدا و به سختی قابل تشخیص است.

نخست نوبت دارندگان یا اجاره‌دهندگان سرورهای اینترنتی است. اگر آنها از استاندارد معیوب استفاده می‌کنند، باید بلافاصله نرم‌افزار خود را به روز کنند. نسخه جدید حفره را می‌بندد. مشکل اما اینجاست که حفره یاد شده پیش از اینکه شناخته شود دو سال وجود داشته است. به بیان دیگر، هکرها ممکن است گذرواژه‌ها و اطلاعات رمزگذاری را به دست آورده باشند.

هیچ کس نمی‌تواند با اطمینان بگوید که ابزار رمزگذاری اطلاعات سایت او به سرقت نرفته است. از همین رو کارشناسان، از جمله اداره فدرال آلمان برای آی‌تی و امنیت اینترنتی، توصیه می‌کنند که دارندگان وبسایت، کلیدهای رمزگذاری و گذرواژه‌ها را عوض کنند.

کاربران فعلا می‌توانند منتظر باشند تا دارندگان سرور و سایت‌های اینترنتی حفره امنیتی اپن‌اس‌اس‌ال را ببندند. فیلیپو واسوردا، برنامه‌نویس کامپیوتر از کشور ایتالیا، سایتی اینترنتی را به آدرس http://filippo.io/Heartbleed درست کرده است که در این سایت می‌توان کنترل کرد که آیا یک سایت اینترنتی حفره امنیتی یاد شده را دارد یا نه. البته نتیجه آزمایش ظاهرا همیشه قابل اعتماد نیست.

کاربران بد نیست دست‌کم گذرواژه‌هایی که با آنها از اطلاعات حساس خود حفاظت می‌کنند را عوض کنند. البته این اقدام در صورتی اثربخش است که دارندگان سایت‌ها و سرورها حفره "اپن‌اس‌اس‌ال" را بسته باشند.