عکس: todaysecurity.net

محافظت از اطلاعات شخصی

چند توصیه ساده

آتوساشیرازی

بسیاری از کاربران، از این‌که به شبکه‌ای، چه شبکه‌های محلی و چه اینترنت، متصل شوند هراس دارند که مبادا نفوذگران غیرمجاز یا دیگر کاربران شبکه، بدون آگاهی و اجازه ایشان، به اطلاعات شخصی‌شان دست یابند.

با توجه به‌آن‌که چنین ترسی بی‌اساس نیست و در شبکه‌ها امکان سرقت اطلاعات وجود دارد، چند راه‌کار ساده را برای کاهش احتمال دستیابی‌های غیرمجاز توصیه می‌شود:

۱- مطمئن شوید که فایل یا پوشه مورد نظر شما به‌اشتراک گذاشته نشده است. در این حالت یک نماد دست زیر پوشه شما قرار می‌گیرد و شما می‌توانید با کلیک راست بر آن و انتخاب گزینه ... Sharing and security و سپس روتن به لبه Sharing فایل یا پوشه دلخواه خود را به‌اشتراک بگذارید یا از آن حالت درآورید.

۲- از ابزارها و نرم‌افزارهای محافظتی (ضدویروس، فایروال، اسپای‌ور و...)، به‌ویژه در هنگام اتصال به اینترنت، استفاده کنید. این نرم‌افزارها را به‌روز نگه‌دارید و گزینه‌های مناسب را به‌کمک یک فرد آگاه انتخاب کنید.

۳- بر روی فایل‌های حیاتی خود رمز بگذارید. این کار به‌کمک ابزارهای درون خود نرم‌افزارها (مانند محیط مایکروسافت ورد) و نرم‌افزارهای جانبی (مانند وین‌زیپ) و برخی روش‌های دیگر امکان‌پذیر است. هر چند که برداشتن این مانع چندان دشوار نیست، اما به هر حال از امکان دستیابی غیرمجاز می‌کاهد. برای آگاهی بیشتر در این زمینه به بخش پرسش و پاسخ کلیک در شماره‌های گذشته رجوع کنید.

۴- نام فایل‌های خصوصی را به‌گونه‌ای نگذارید که جلب توجه کند. خوب معلوم است که نام «اطلاعات بانکی من» یا چیزی شبیه به‌آن، توجه هر نفوذگری را به‌خود جلب می‌کند؟!

۵- فایل‌های‌تان را بر کامپیوتر نگذارید. اگر اطلاعات‌تان این‌قدر مهم و شبکه‌تان این‌قدر ناامن است، خوب اطلاعات‌تان را بر یک دیسک جانبی ذخیره کنید!

پروتکل RFB و VNC چیست؟

پارساستوده‌نیا

پروتکل RFB[1] یک پروتکل ساده است که برای دسترسی از راه دور به واسط‌های گرافیکی کاربر استفاده می‌شود و همان‌طور که از نامش پیدا است، در سطح فریم‌بافر کار می‌کند. این پروتکل قابل اعمال بر همه برنامه‌های کاربردی و سیستم‌هایی است که به‌نوعی با پنجره‌ها سر و کار دارد. از میان این سیستم‌ها می‌توان به X11، ویندوز و مکینتاش اشاره کرد. RFB پروتکلی است که در محاسبات شبکه‌های مجازی (VNC)[2] نامیده می‌شود و کاربرد دارد.

هرچند RFB در ابتدا به‌عنوان یک پروتکل نسبتا ساده به‌وجود آمد، به مرور زمان گسترش یافت و امکانات مختلفی به آن افزوده شد. گسترش RFB امکانات انتقال فایل و فشرده‌سازی به‌روش‌های پیچیده را امکان‌پذیر ساخت و امنیت سیستم را افزایش داد. برای حفظ سازگاری این سیستم با پیاده‌سازی مختلفی کلاینت و سرور VNC، کلاینت‌ها و سرورها باید بتوانند با استفاده از RFB با یکدیگر ارتباط برقرار کنند و اطلاعات را رد و بدل کنند. پروتکل RFB تضمین می‌کند که مناسب‌ترین انتخاب‌های فشرده‌سازی و تامین امنیت را که هر دو سیستم کلاینت و سرور قادر به پشتیبانی از آن باشند را به‌کار گیرد.

پیدایش RFB به سال ۱۹۹۸ باز می‌گردد. RFBدر ابتدا به‌عنوان یک فناوری ساده برای نمایش از راه دور سیستم‌ها به‌وجود آمد. در حقیقت کاربرد اولیه آن ساده کردن فناوری‌های موجود در آن زمان بود. به‌زودی با توسعه VNC، پروتکل RFB یک کاربرد ثانویه و مهم‌تر پیدا کرد. VNC به‌عنوان یک نرم افزار کد باز منتشر شد و RFB را به‌عنوان پروتکل استاندارد به‌کار گرفت.

یکی از امتیازات جالب توجه RFB این است که توسعه‌دهندگان کد می‌توانند انواع مختلفی از روش‌های رمزگذاری و سیستم‌های امنیتی را به دلخواه خود به سیستم RFB موجود اضافه کنند. تنها تغییر لازم در این حالت، رزرو کردن شماره شناسایی منحصربه‌فرد است تا به این ترتیب، شماره‌های شناسایی تداخل پیدا نکنند. تداخل شماره‌ها می‌تواند در طول فرایند معارفه[3] ایجاد اشکال کند و منجر به قطع ارتباط شود. نسخه کنونی RFB به نام RFB 3.8 شناخته شده و در ماه ژوئن سال ۲۰۰۷ منتشر شده است.

اغلب سیستم‌های دسترسی از راه دور که با آنها آشنایی داریم قادر به کار با برنامه‌های گرافیکی یا برنامه‌های دارای پنجره نیستند و تنها با فایل‌های متنی و خط دستور سر و کار دارند. RFB به‌سبب امکان ایجاد ارتباط با این گونه نرم‌افزارها از جایگاه ویژه‌ای برخوردار است. با این حال RFB نیز خالی از اشکال نیست و نیازمند اعمال یک سری تغییرات است. مهم‌ترین محدودیت کنونی RFB انتقال داده‌ها به حافظه موقت[4] است.

البته در حال حاضر هیچ راهی برای انتقال داده‌های متنی که به‌فرمتی به غیر از Latin-1 character set نوشته شده باشند، وجود ندارد.

پی‌نوشت‌ها

1. Remote Framebuffer
2. Virtual Network Calculation
3. Handshaking
4. Clipboard

پرسش و پاسخ

clickhelp@jamejamonline.ir
مهدی رشنو

مهرداد آزادگان، تهران - چند سوال دارم:

۱- فایل‌هایی با پسوند ra، ram، awb و pmr چه فایل‌هایی هستند؟

۲- آیا هک‌کردن سایت جرم است و اگر هست، حکمش چیست؟

فایل‌های اطلاعاتی با پسوند pmr. گزارشی است که توسط Microsoft Performance Monitor تولید می‌شود و اطلاعات پردازش‌های مختلف سیستم را بر روی حافظه و پردازشگر خود ذخیره می‌کند. این فایل در سیستم‌های ویندوز NT و ویندوز Server تولید می‌شود.

فایل‌هایی با پسوند awb. نیز گونه‌ای از قالب‌های صوتی هستند که در برخی از موبایل‌ها از آن استفاده می‌شود.

فایل‌هایی با پسوند ra. و ram. فایل‌های صوتی هستند که توسط نرم‌افزار Real Player ساخته و اجرا می‌شوند. این نوع قالب‌ها (به ویژه ra.) بیشتر برای پخش کلیپ‌های صوتی در اینترنت به‌کار می‌رود. به این معنا که چنین فایل‌هایی باعث باز شدن فایلی‌های صوتی از اینترنت می‌شود و به‌طور معمول بر روی سیستم شما ذخیره نمی‌شود. به چنین فایل‌هایی، فایل صوتی Stream می‌گویند.

در مورد سوال دوم شما باید گفت که خیر، در ایران هنوز هک کردن سایت جرم محسوب نمی‌شود. اما در کشورهای دیگر از چند ماه تا چند سال زندانی و جبران خسارت مالی، برای مجازات آن مقرر شده است. البته در کشور قوانینی عمومی وجود دارند که زیان رسانیدن به منافع یا اموال دیگران را به‌هر حال جرم می‌داند و قضات محترم نیز می‌توانند در مورد هک نیز به‌آنها استناد کنند.

محمد حسینی، تهران - حجم فایل‌های درایو C کامپیوترم ۳ مگابایت است. در حالی که وقتی روی درایو راست کلیک می‌کنم، حجم فایل ها را ۷ گیگابایت نشان می‌دهد، علت این اختلاف چیست که باعث شده سرعت کامپیوترم کم شود؟ در ضمن من از آنتی‌ویروس مک‌آفی استفاده می‌کنم. به‌نظر می‌رسد که حجم فایل هایی که شما می‌بینید ۳ گیگابایت باشد! در درایوی که ویندوز نصب می‌شود، به‌طور معمول، فایل‌های دیگری نیز وجود دارد که خود سیستم عامل از آنها استفاده می‌کند. همین‌طور چنانچه نرم‌افزارهایی بر روی این درایو نصب کرده‌اید که فایل‌های Temp زیادی می‌سازند و به‌علل مختلف این فایل‌ها بر روی هارد باقی می‌مانند نیز می‌تواند باعث چنین اختلافی شده باشد. برای