مسائل و راه‌حلهای امنیتی برای اینترنت

فکر می‌کنید کوچه‌های تاریک خطرناکند؟ کوچه‌های تاریک وب چطور؟ تعداد تهدیدهای دیجیتال همیشه در حال رشد است، و کاربران باید همیشه یک گام جلوتر از **کراکرها** و **هکرها** باشند تا بتوانند امنیت کامپیوترهای خود را حفظ کنند. اما اگر مشکل به وجود آمد چه باید کرد؟ خوشبختانه، کاربران می‌توانند اکثر مسائل امنیتی را با زحمتی نسبتاً کم حل کنند.

مسئله: کامپیوترم با آگهیهای پاپ-آپ (pop-up) اشباع شده است، حتی زمانی که به اینترنت وصل نیستم.

راه‌حل: آگهی پاپ-آپ، یک آگهی بازرگانی ناخواسته است که در پنجرهٔ خودش بر روی صفحه نمایش به نمایش درمی‌آید. بعضی از این آگهیها به وسیلهٔ پایگاههای وب معتبر به عنوان روشی برای کسب درآمد تولید می‌شوند، آگهی‌دهندگان، حامیان چنین پایگاههای وبی هستند. چنین آگهیهایی معمولاً تنها و در پیوند با یک عمل اینترنتی، مانند باز کردن یک صفحهٔ وب ظاهر می‌شوند. بقیهٔ پاپ-آپها به وسیلهٔ **برنامه‌های جاسوسی** (spyware) و **تبلیغاتی** (adware) به منظور جمع‌آوری اطلاعات شخصی درباره رفتارهای اینترنتی شما تولید می‌شوند؛ محصولات نامطلوب را تبلیغ می‌کنند، شامل پورنوگرافی و طرحهای «سریعاً ثروتمند شوید»؛ یا به کراکرها امکان می‌دهند که به آسانی سیستم شما را دستیابی کنند. این آگهیها به صورت گله‌ای می‌آیند، و **میزکار** (Desktop) را با یک رشته آگهی بمباران می‌کنند که ممکن است ربطی به آنچه از اینترنت خواسته‌اید نداشته باشند.

می‌توانید آگهیهایی را که در گروه شرارت قرار می‌گیرند با اجرای برنامه‌های ضدجاسوسی، مانند برنامهٔ Spy Sweeper، eTrust PestPatrol Anti-Spyware، حذف کنید. نشانی پایگاه وب این دو برنامه به ترتیب به قرار زیر است:

www.webroot.com

www.ca.com

چنین برنامه‌هایی، برنامه‌های جاسوسی یا تبلیغاتی تولیدکنندهٔ آگهیهای پاپ-آپ را شناسایی و نابود می‌کنند. سپس، باید نرم‌افزار مسدودسازی آگهی را برای پاکسازی سایر آگهیهای پاپ-آپ که باز هم سعی می‌کنند جلو بیایند نصب کنید. نرم‌افزار مسدودسازی معمولاً خودش را بر روی نوارابزار برنامهٔ مرورگر نصب می‌کند و از آنجا ترافیک ورودی را زیرنظر می‌گیرد و ورود پاپ-آپهای ناخواسته را مسدود می‌کند.

یک برنامهٔ مسدودسازی آگهی را با دریافت یک نوارابزار رایگان مانند Yahoo! Toolbar از اینترنت می‌توانید به دست بیاورید:

toolbar.yahoo.com

برنامهٔ Pop-Up Blocker در آخرین نگارش Internet Explorer و ویندوز اکس‌پی SP2 را هم می‌توانید اجرا کنید. اما برنامه‌هایی چون PopUpCop و PopUpSentry قدرتمندتر هستند:

www.popupcop.com

www.popupsentry.com

مسئله: سراصفحهٔ (home page) برنامهٔ مرورگر من بدون هیچ دلیلی تغییر کرده است.

راه‌حل: برنامهٔ مرورگر شما به گروگان گرفته شده است. به گروگان گرفته شدن مرورگر وقتی رخ می‌دهد که یک برنامهٔ جاسوسی یا تبلیغاتی، یک قطعه برنامه را برای تغییردادن **سراصفحهٔ** مرورگر به کار بگیرد. در بسیاری از موارد، سراصفحهٔ جدید یا یک موتور جستجو یا یک پایگاه پورنو است. گروگان گرفته‌شدن مرورگر همچنین می‌تواند شامل اضافه‌کردن نوارابزارهای ناخواسته در پنجرهٔ مرورگر یا لینکهایی در پوشهٔ Favorites باشد. همچنین می‌تواند موتور جستجوگر ترجیحی شما را نیز تغییر بدهد.

اگر از IE استفاده می‌کنید، می‌توانید سراصفحه را با باز کردن منوی Tools، انتخاب Internet Options، انتخاب صفحهٔ General، تایپ نشانی وب سراصفحهٔ موردنظر خود در کادر Address، و کلیک‌کردن روی OK به سلیقهٔ خود تغییر بدهید. برای حذف یک لینک Favorites نامطلوب، منوی Favorites را باز کنید، Organize Favorites را انتخاب کنید، محتویات پوشهٔ Favorites را بررسی کنید، لینک نامطلوب را انتخاب (هایلایت) کنید، و روی Delete کلیک کنید. و در اکثر موارد، می‌توانید از گزینهٔ Add Or Remove Programs در Control Panel برای حذف نوارابزارهای خارجی بهره بگیرید. همچنین، برای بازگرداندن موتور جستجوی مطلوب خود، روی Customize در بخش Search مرورگر کلیک کنید، گزینهٔ Use One Search Service را انتخاب کنید، و موتور جستجوی موردنظر خود را در منوی پایین-آمدنی Choose The Search Service انتخاب کنید.

با این همه، اجرای همهٔ این کارهای بازگردانی کافی نیست. چنین روشهایی ممکن است مسئله را به طور موقتی حل کنند، اما آنها برنامهٔ جاسوسی یا تبلیغاتی گروگان‌گیرندهٔ مرورگر را که همهٔ این مسائل را به وجود آورده‌اند حذف نمی‌کنند. از این روی، برنامهٔ مرورگر را ببندید، و بلافاصله **برنامهٔ ضدجاسوسی** خود را به اجرا درآورید. پس از این کار، **برنامهٔ ضدویروس** خود را نیز اجرا کنید، که **اسب تروایی** را شناسایی و حذف خواهد کرد که برنامهٔ جاسوسی را وارد کامپیوتر شما کرده است.

یادآوری: اسب تروا برنامه‌ای زیان‌آور است که چهرهٔ یک برنامهٔ مفید را به خود می‌گیرد، اما در نهان عملیات زیان‌آور خود را اجرا می‌کند.

مسئله: کامپیوترم به تازگی عجیب شده است. ارتباط اینترنت آن آهسته شده است، و پیامهای «عدم دریافت نامه» از سوی کسانی را می‌گیرم که نمی‌شناسم. به نظر می‌رسد که دیسک سخت پیوسته در حال کار است، و گاهی صفحه‌کلید به کلیدهایی که می‌زنم پاسخی نمی‌دهد. چه خبر شده است؟

راه‌حل: به عنوان یک قاعدهٔ عمومی، باید هر نوع رفتار غیرعادی سیستم را به عنوان نشانهٔ یک آلودگی ویروسی تلقی کنید. بدین معنی که پاسخ نخست شما باید یک بررسی ویروسی با برنامهٔ ضدویروس باشد. اگر برنامهٔ ضدویروس ندارید، بی‌درنگ یک برنامهٔ ضدویروس بخرید و نصب کنید. و اگر برنامهٔ ضدویروس شما بیش از یک سال است که روزآمد نشده است، یا یک برنامهٔ جدید بخرید و نصب کنید یا آن را از طریق اینترنت روزآمد کنید.

اما این راه‌حل که گفتیم برای مبتدیان است. نشانه‌های خاصی که شما ذکر کردید برای **زامبی‌ها** (zombie) متداول است. **زامبی** کامپیوتری است که به عنوان یک وسیلهٔ تهاجمی برای **کراکری** (cracker) عمل می‌کند که می‌خواهد اقدامات مجرمانه‌ای را بی‌آن که هویتش فاش گردد انجام دهد. کراکر معمولاً کنترل یک سیستم یا چند سیستم را با ارسال یک **اسب تروا** (Trojan horse) به دست خود می‌گیرد. وقتی کاربر بی‌خبر از همه‌جا، این اسب تروا را باز می‌کند، این برنامه خودش را نصب می‌کند، معمولاً با به‌کارگیری یک حفرهٔ امنیتی در سیستم‌عامل یا مرورگر وب کاربر، انتقال داده‌ها را به کراکر آغاز می‌کند.

پس از آن که کراکر کنترل کامپیوتر را به دست بگیرد، او به سیستم آلوده زامبی _ و منابع موجود آن _ فرمان می‌دهد، معمولاً به منظور ارسال **هرزنامه** (spam) یا به وجود آوردن حملات DoS (حملات خارج از سرویس‌سازی). یک حملهٔ DoS سیستم قربانی را بلااستفاده می‌کند و بار سنگینی را روی کامپیوتر زامبی که در وسط عملیات قرار می‌گیرد، می‌گذارد.

یادآوری: DoS سرواژهٔ عبارت زیر است:

Denial of Service

در حملهٔ DoS، تهاجم‌کننده سیلی از داده‌ها را به سوی یک کامپیوتر یا **خدمات‌دهنده** (server) ارسال می‌کند تا ترافیک سنگینی برای شبکه به وجود بیاورد.

یک بررسی ویروسی باید اسب تروایی را که زامبی را به وجود آورده است حذف کند. با نصب یک **دیوارهٔ آتش** (firewall) می‌توانید سیستم خود را در آینده محافظت کنید. دیوارهٔ آتش نه تنها ترافیک ورودی را از لحاظ دستیابی‌های کاربران غیرمجاز زیرنظر می‌گیرد، بلکه به ترافیک خروجی از برنامه‌هایی نگاه می‌کند که به طور عادی داده‌ها را از طریق شبکه انتقال نمی‌دهند. به این ترتیب، یک دیوارهٔ آتش می‌تواند یک حملهٔ DoS را که از پی‌سی شما اجرا می‌گردد شناسایی کند، به شما هشدار بدهد، و از ادامهٔ حملهٔ برنامهٔ مهاجم جلوگیری کند.

سرانجام، کاربران باید نرم‌افزار خود را روزآمد کنند. سازندگان نرم‌افزار معمولاً وصله‌هایی نرم‌افزاری برای تعمیر اشکالات نرم‌افزار خود درست می‌کنند که حفره‌های امنیتی را پرمی‌کنند.

مسئله: وقتی سعی می‌کنم که وارد بعضی از حسابهای اینترنتی خود شوم (مانند آنهایی که به داده‌های مالی ربط دارند)، پیامهای «access denied» دریافت می‌کنم که مشخص‌کنندهٔ نادرستی کلمه‌های عبور یا نام کاربری هستند.

راه‌حل: پیش از آن که علت را نتیجهٔ مسائل امنیتی بدانید، اطمینان یابید که کلمهٔ عبور و نام کاربری خود را درست تایپ می‌کنید. سپس، فرض کنید که این اطلاعات را فراموش کرده‌اید و از طرفهای خود بخواهید که نام کاربری و کلمهٔ عبور درست را برای شما ارسال کنند. امیدوار باشید که این اطلاعات را دریافت خواهید کرد و آنها برایتان درست عمل خواهند کرد. در غیر این صورت، مسئله‌ای به وجود آمده است.

اگر به نظر برسد که کسی بدون اجازهٔ شما نام کاربری و/یا کلمهٔ عبور را تغییر داده است _ به احتمال زیاد به عنوان بخشی از سرقت هویت _ خیلی فوری با شرکتی که حساب مسئله‌دار را فراهم کرده است تماس بگیرید و مسئله را باآنها درمیان بگذارید. این شرکت احتمالاً حساب شما را خواهد بست (و شاید از شما بخواهد که مسئله را به پلیس گزارش بدهید). همچنین باید همهٔ حسابهای اینترنتی خود را –دست‌کم به طور موقت– ببندید. بعد از این کارها ریشهٔ مسئله را پیدا کنید. سرقت هویت معمولاً به دلیل جاسازی یک **برنامهٔ ثبت کلیدزنی** (یا سخت‌افزار ثبت کلیدزنی)

در کامپیوتر انجام می‌گیرد. این برنامه‌ها که به **key logger** مشهورند نوعی برنامهٔ جاسوسی هستند که عملیات صفحه‌کلید شما را ثبت می‌کنند و این اطلاعات را از طریق اینترنت و شبکه به کراکرها ارسال می‌کنند. در پی آن، کراکرها با بررسی کلیدهای زده شده، سعی می‌کنند کلمه‌های عبور و نامهای کاربری، شماره‌های کارت اعتباری، و اطلاعات شخصی دیگر شما را کشف و از آنها سوءاستفاده کنند.

ویروسها، کرمها، و اسبهای تروا می‌توانند با خود برنامهٔ ثبت‌کنندهٔ کلیدزنی را حمل و در کامپیوترهای بدون محافظ نصب کنند. برای حذف این نوع تهدید، یک برنامهٔ خدماتی ضدویروس را نصب و کامپیوتر خود را از لحاظ کدهای زیان‌آور بررسی کنید. همچنین باید یک یا چند برنامهٔ ضدجاسوسی را نصب کنید و به طور منظم آنها را به اجرا درآورید. پس از حذف برنامهٔ ثبت‌کنندهٔ کلیدزنی، یک برنامهٔ دیوارهٔ آتش قدرتمند در کامپیوتر خود نصب کنید که تلاش برنامه‌های ناشناس برای انتقال داده‌ها، مانند انتقال فایل کلیدهای زده‌شده، را به اطلاع شما خواهد رساند.□

چهار گام برای امنیت بهتر

۱.یک برنامهٔ خدماتی **ضدویروس** نصب کنید. برنامهٔ **ضدجاسوسی** نصب کنید. یک برنامهٔ **دیوارهٔ** آتش (firewall) نصب کنید. همهٔ آنها را به طور منظم به اجرا درآورید و به طور منظم همهٔ آنها را روزآمد کنید.

۲.برنامهٔ مرورگر، ویندوز، و همهٔ نرم‌افزارهای امنیتی خود را با آخرین وصله‌ها، و service packها روزآمد کنید. از مزیت automatic updates آنها بهره بگیرید.

۳.از کلمه‌های عبوری بهره بگیرید که در داخل خود، هم از حروف و هم از اعداد بهره گرفته‌اند و دست‌کم شش کاراکتر طول دارند. هرچند گاه، آنها را تغییر بدهید.

۴.تا جای ممکن به پایگاههای وب ناشناخته سرنزنید. ایمیل فرستندگان ناشناس را نادیده بگیرید. فایلهایی را که بدون اجازهٔ شما وارد کامپیوتر شده‌اند حذف کنید.□