آنچه برنامهٔ Firewall از شما می‌پرسد

کدام برنامه‌ها را قبول کنیم، کدام برنامه‌ها را رد کنیم؟

iTunes.

The application indicated

above is trying to access the network.

What would you want to do?

Allow, Deny, More Options.

پیام پیچیدهٔ فوق از طرف برنامهٔ Nvidia Firewall صادر شده است (این برنامه یکی از برنامه‌های نرم‌افزاری ارائه شده به همراه مادربوردهای مبتنی بر nForce4 است). این پیام در بخش پایین–راست صفحه‌نمایش، پس از آن که برنامهٔ iTunes را نصب کردیم و برای اولین بار به اجرا درآوردیم ظاهر شد. برنامهٔ Nvidia Firewall همچون یک سگ نگهبان عمل می‌کند، به طرف کسانی که نمی‌شناسد آن‌قدر پارس می‌کند تا صاحب سگ مشخص کند که آن غریبه، دوست است یا دشمن.

برنامه‌های **دیوارهٔ آتش** (firewall)، انواعی از برنامه‌های امنیتی هستند که کار آنها زیرنظر گرفتن داده‌هایی است که سعی می‌کنند از کامپیوتر خارج شوند یا وارد کامپیوتر شوند، مانند وقتی که برنامهٔ مرورگر خود را برای دریافت آخرین خبرها از CNN.com به اجرا درمی‌آورید. بسیاری از دیواره‌های آتش دارای فهرستی از برنامه‌ها، فایلها، و **پراسسهای**[1] «مطمئن» و «نامطمئن» هستند. موافقت یا عدم موافقت با هر کدام از آنها را بدون اطلاع دادن به شما (یعنی بدون اذیت کردن شما) و به گونه‌ای کاملاً ساکت انجام می‌دهند. اگر یک برنامهٔ دیوارهٔ آتش، یک برنامهٔ کاربردی یا یک پراسس را که سعی می‌کند داده‌هایی را ارسال یا دریافت کند نشناسد، ممکن است از خود شما بپرسد که تکلیف چیست. هر چند، می‌توانید تنظیمی را در برنامهٔ دیوارهٔ آتش بیابید و فعال کنید که بر اساس آن خود برنامه همهٔ تصمیمها را به جای شما می‌گیرد، که در عمل ما توصیه نمی‌کنیم. دیواره‌های آتش سخت‌افزاری، مانند آنهایی که در دستگاههای gateway router (**مسیریاب دروازه**) دیده می‌شود، معمولاً از شما چنین سؤالاتی را نمی‌پرسند.

تصمیم در مورد کلیک کردن روی Allow، برای این که دیوارهٔ آتش ما به iTunes اجازه بدهد که کارش را انجام دهد، آسان بود. اما پیامهای دیگری وجود دارد که در مورد آنها با قاطعیت نمی‌توانیم تصمیم بگیریم. به عنوان مثال، وقتی دیوارهٔ آتش از ما پرسید که آیا باید به Cli.exe یا Alg.exe اجازهٔ دستیابی اینترنت را بدهد یا نه، پیش از آن که بتوانیم تصمیم بگیریم، به اطلاعات بیشتری نیاز داشتیم. این مقاله می‌تواند به شما کمک کند که وقتی دیوارهٔ آتش به پاسخ شما نیاز دارد چگونه تصمیم بگیرید.

تصمیمات مهم

بسیاری از دیواره‌های آتش امکانات بیشتری به جز Allow و Deny دارند. از لحاظ کلی، می‌توانید دستور مجاز یا غیرمجازبودن هر دستیابی شبکه (یا اینترنت) را هر بار به طور مستقل صادر کنید، یعنی دیوارهٔ آتش هربار که یک درخواست دستیابی شبکه (یا اینترنت) به اجرا درآید از شما پرسش کند. این تنظیم گاهی Ask نامیده می‌شود، که مختصر عبارت «ask each time» است.

همچنین، گزینه‌های قبول یا رد همیشگی (always)، یا دائمی (permanently) دستیابی فایل برای شبکه یا وب نیز فراهم است. با انتخاب چنین گزینه‌ای، دیوارهٔ آتش دیگر دربارهٔ آن عمل، پیام صادر نخواهد کرد. کلمه‌های «always» و «permanently» کمی گمراه‌کننده هستند، چون اگر بعداً تغییر عقیده بدهید برای تصحیح مجبورید در میان تنظیمهای دیوارهٔ آتش جستجو کنید. معمولاً در برنامه‌های کاربرپسندی چون برنامهٔ ZoneAlarm، علامت تیک سبز نمایندهٔ مجاز و علامت X قرمز نمایندهٔ غیرمجاز است:

www.zonealarm.com

[1] process؛ فایلهایی که در حافظه بار می‌شوند.

اکثر دیواره‌های آتش _ بسته به آنچه یک برنامه سعی می‌کند انجام دهد_ از شما دربارهٔ اجازه‌دادن به **پراسهایی** (process) که داده‌هایی را داخل می‌کنند یا داده‌هایی را از کامپیوتر شما خارج می‌کنند پرسشهای جداگانه‌ای می‌پرسند. در اصطلاح ZoneAlarm، دستیابی یعنی **واکشی** (fetch) داده‌ها از یک کامپیوتر متصل به وب یا شبکه، مانند واکشی از یک **خدمات‌دهندهٔ** (server) حاوی آخرین داده‌های جاسوس‌یاب برای برنامهٔ Spybot. اگر کامپیوترتان به صورت یک **خدمات‌دهنده** عمل کند اجازهٔ کپی از روی داده‌های مستقر در کامپیوتر شما را به کامپیوترهای دیگر می‌دهد؛ مثلاً به یک شبکهٔ **همتابه‌همتا** (peer-to-peer) اجازه داده می‌شود که کپی فایلهای صوتی روی دیسک سخت شما را بگیرد. می‌توانید به برنامهٔ مرورگر خود اجازه بدهید که همیشه اینترنت را دستیابی کند، اما می‌توانید به دیوارهٔ آتش بگویید که وقتی برنامهٔ مرورگر شما سعی می‌کند که به عنوان یک **خدمات‌دهنده** عمل کند (یعنی اجازهٔ کپی از روی داده‌های مستقر در کامپیوتر شما را به کامپیوترهای دیگر بدهد) بر یک اساس مورد-به-مورد بپرسد.

وقتی دیوارهٔ آتش دربارهٔ درخواست یک برنامهٔ خوشنام برای دستیابی اینترنت (یا شبکه) از شما بپرسد، تصمیم‌گیری نسبتاً آسان است، مانند iTunes در مثال ما. اما در مورد پراسهایی که آشنا به نظر نمی‌رسند چه؟ چگونه می‌توانید مطمئن شوید که Alg.exe بی‌گناه است یا گناهکار؟ Cli.exe چه کاری انجام می‌دهد؟ و آنها سعی می‌کنند با کدام کامپیوتر ارتباط برقرار کنند؟

مثالهایی که ما ذکر کردیم کاملاً بی‌آزار هستند. Cli.exe فقط به شما امکان می‌دهد که تنظیمهای گرافیک ATI را از یک **نماد** (icon) **نوارتکلیف**[2] دستیابی کنید، و Alg.exe برای اجرای ویندوز اکس‌پی ضروری است.

اگر برای اولین بار یک برنامهٔ کاربردی را به اجرا درآورده‌اید، و برنامهٔ دیوارهٔ آتش پیامی صادر کرده است، علت، به احتمال قریب به یقین در این برنامهٔ جدید است. برنامه‌های IM (پیام‌رسانی فوری)، ایمیل، مرورگر وب، و برنامه‌های خدماتی امنیتی‌ای که به طور خودکار پایگاه وب سازنده را از لحاظ **وصله‌های روزآمدساز** بررسی می‌کنند همگی مجبورند برای این عمل به **روی خط** (online) بروند. اگر به برنامهٔ خود اعتماد دارید اجازهٔ دستیابی را صادر کنید. اگر به یک پراسس اجازهٔ فعالیت بدهید، برنامهٔ دیوارهٔ آتش باز هم کانال ارتباطی آن را زیرنظر می‌گیرد و رفتارهای مشکوک را به شما اطلاع می‌دهد.

از سوی دیگر، بعضی از نرم‌افزارها به همراه خود برنامه‌های «piggyback» دارند که می‌توانند برنامهٔ تبلیغاتی یا جاسوسی باشند. برنامه‌های peer-to-peer client (خدمات‌گیرندهٔ همتا-به-همتا) و برنامه‌های بازی اینترنتی به داشتن برنامه‌های اضافی (تبلیغاتی یا جاسوسی) شهرت دارند، مانند BonziBuddy و WhenU، و در حقیقت، اگر برنامه‌های همراه آنها را حذف کنید، آنها درست کار نخواهند کرد.

حتماً نمی‌خواهید که عملی را که برنامهٔ معتبر شما می‌خواهد انجام بدهد بلوکه (مسدود) کنید. به ویژه، نمی‌خواهید که برنامه‌های جاسوسی یا تبلیغاتی را به طور دائم تأیید کنید. می‌توانید مسدودسازی یک پراسس را یک بار امتحان کنید و سپس ببینید که آیا جلوی اجرای یک برنامهٔ «خوب» را می‌گیرد یا نه. اگر نگرفت، بار بعد که پیام صادر می‌شود می‌توانید تصمیم دائم را بگیرید. هرچه تصمیمهای دائمی بیشتری دربارهٔ اجازهٔ برنامه‌ها اتخاذ کنید، به مرور کمتر با پیامهای آزاردهندهٔ دیوارهٔ آتش برخورد خواهید کرد.

پژوهش

البته، ممکن است لازم باشد که برای اتخاذ هر تصمیم کمی تحقیق کنید. بعضی از پیامهای مبهم دیواره‌های آتش سعی خواهند کرد که شما را راهنمایی کنند؛ رتبه‌بندی با کد رنگی **کم-خطر** (Low-Risk)، **متوسط-خطر** (Medium-Risk)، و **پرخطر** (High-Risk) در برنامهٔ Nvidia Firewall یکی از نمونه‌هاست. بعضی از دیواره‌های آتش، مانند دیوارهٔ آتش **نورتون** یا ZoneAlarm، برای کمک به تصمیم‌گیری، لینکهایی را به اطلاعات بیشتر دربارهٔ یک پراسس یا برنامه فراهم می‌سازند. به عنوان مثال، در یک پیام مبهم ZoneAlarm می‌توانید روی دکمهٔ More Info کلیک کنید تا صفحهٔ وبی را ظاهر کند که ممکن است در آن اطلاعات بیشتری وجود داشته باشد.

برنامهٔ Nvidia Firewall می‌تواند نام سازنده، مسیر فایل، و توصیف هر فایلی را که در پیام خود می‌آورد به شما بگوید. وقتی یک پیام مبهم صادر شد کافی است روی More Options کلیک کنید. اگر دیوارهٔ آتش شما چنین اطلاعاتی را فراهم نکرد، جستجوی نام پراسس را در ویندوز امتحان کنید. در ویندوز اکس‌پی روی Start کلیک کنید و بعد Search را انتخاب کنید. گزینهٔ All Files And Folders را انتخاب کنید و کادر Look In را روی Local Hard Drives میزان کنید. اگر هیچ نتیجه‌ای به دست نیامد، می‌توانید روی Include Hidden And System Folders کلیک کنید. (به طور پیش‌گزیده، ویندوز اکس‌پی فایلهای سیستمی را جستجو نمی‌کند.)

[2] Taskbar؛ نوارابزار پایین در صفحهٔ ویندوز

پس از آن که فایل را یافتید، مانند Alg.exe، به پوشه و پوشه‌های فرعی‌ای که این فایل در آن مستقر شده است نگاه کنید، مانند C:\Windows\System32. در اکثر موارد، یکی از آن پوشه‌ها نام برنامهٔ کاربردی‌ای را خواهد گفت که آن فایل به آن تعلق دارد. در مورد مثال ما، یک فایل ویندوز است، و باید به درخواست ارتباط آن اجازهٔ کار بدهید. با این حال، ویروسها و برنامه‌های زیان‌آور می‌توانند فایلهای خود را در پوشه‌های یک برنامهٔ کاربردی دیگر مستقر کنند، در نتیجه، باید آن فایل را روی یک پایگاه امنیتی مورد اعتماد نیز بررسی کنید، مانند پایگاههای www.processlibrary.com و www.sarc.com.

همچنین می‌توانید فایلها، برنامه‌های کاربردی، و پراسسهای مشکوک را بر روی موتور جستجوی مورد استفادهٔ خود، مانند گوگل یا یاهو، نیز بررسی کنید و توضیحاتی را بیابید که کاربران دیگر در موقع برخورد با پیامهای مبهم دیوارهای آتش در مورد پراسس مشابه درج کرده‌اند. اگر در این توضیحات، عباراتی چون «بی‌آزار بودن پراسس» را دیدید می‌توانید تردید خود را کمتر کنید و دستور اجازهٔ فعالیت را صادر کنید. اما اگر داده‌های روی کامپیوترتان بسیار اهمیت دارد باید بیشتر بررسی کنید و بعد تصمیم بگیرید.

سرانجام، برنامه‌های ضدویروس و ضدجاسوسی خود را روزآمد نگه دارید و آنها را برای حفاظت از سیستم خود فعال کنید. حتی اگر اشتباه کنید و به یک کد زیان‌آور اجازه بدهید که وارد کامپیوتر شما شود (شاید به این دلیل که زیر یک نام فایل مورد اعتماد پنهان شده است)، برنامهٔ دیوارهٔ آتش و سایر برنامه‌های امنیتی شما ممکن است جلوی فعالیت آن را به دلیل رفتارهای مشکوک بگیرند و مسئله‌ای برای داده‌هایتان به وجود نیاید.□

برگزیده مقاله‌های ماهنامه ریزپردازنده در کتاب جدید انتشارات ریزپردازنده:

● اینترنت چگونه کار می‌کند

□قیمت: ۱۷۰۰ تومان

□برای دریافت کتاب فوق مبلغ ذکرشده را به حساب جاری شماره ۲۹۱۷ بانک ملی ایران شعبه کسری (کدشعبه ۱۸۵) تهران به نام علیرضا محمدی‌فر (قابل پرداخت در کلیه شعب بانک ملی ایران) واریز کنید و اصل فیش را به همراه فرم زیر به نشانی مجله (تهران، صندوق‌پستی ۱۵۸۷۵/۶۵۹۱، مجله‌ریزپردازنده) ارسال نمایید.

□نام و نام خانوادگی: **□ تلفن:**

□نشانی:

برگزیده مقاله‌های ماهنامه ریزپردازنده در کتاب جدید انتشارات ریزپردازنده:

۵۰۰ ترفند در ویندوز XP

□قیمت: ۱۹۰۰ تومان

□برای دریافت کتاب فوق مبلغ ذکرشده را به حساب جاری شماره ۲۹۱۷ بانک ملی ایران شعبه کسری (کدشعبه ۱۸۵) تهران به نام علیرضا محمدی‌فر (قابل پرداخت در کلیه شعب بانک ملی ایران) واریز کنید و اصل فیش را به همراه فرم زیر به نشانی مجله (تهران، صندوق‌پستی ۱۵۸۷۵/۶۵۹۱، مجله‌ریزپردازنده) ارسال نمایید.

□نام و نام خانوادگی: **□ تلفن:**

□نشانی: