هنگام برخورد با یک فایل ناشناخته چه باید کرد

به‌تازگی خاموش‌سازی ویندوز کامپیوتر مسئله‌دار شده است. در بسیاری از مواقع، پیش از آن که سیستم‌عامل خاموش شود، با پیامی برخورد می‌کنیم که می‌گوید:

“Ending Program ccApp . . . Please Wait.”

ccApp چیست و چگونه وارد کامپیوتر ما شده است؟ پس از تحقیقات فراوان، دریافتیم که فایل ccApp در سیستم ما، بخشی از برنامهٔ Norton AntiVirus است که به تازگی نصب کرده‌ایم. لابد شما هم مانند ما در گذشته با یک فایل ناشناخته برخورد کرده‌اید و این پرسش به ذهنتان آمده است که آیا دوست است یا دشمن. گرایش کاربران در برخورد با چنین فایلهایی معمولاً پاک‌کردن سریع آنهاست، اما اگر چنین فایلی، همچون مورد CcApp.exe ما، یک فایل ضروری برای اجرای یک برنامهٔ مجاز باشد، پاک‌کردن فایل مزبور یک اشتباه خواهد بود.

وقتی با یک فایل ناشناخته برخورد کنید، چند راه برای شناسایی آن فایل وجود دارد.

بررسی بسط فایل

اگر دربارهٔ یکی از فایلهایی که از طریق ویندوز می‌بینید _ و در نتیجه می‌توانید نام و مکان ذخیرهٔ آن فایل را ببینید _ کنجکاو باشید، اولین کاری که باید انجام دهید کلیک–راست‌کردن روی نام آن فایل و انتخاب گزینهٔ Properties از منویی است که ظاهر می‌شود. پنجرهٔ Properties چند صفحهٔ مختلف دارد که حاوی اطلاعاتی چون زمان ساخت فایل، نام شرکت سازنده، و نام برنامهٔ بازکنندهٔ آن فایل است. اطلاعات موجود در اینجا لزوماً جامع نیست، اما یک نقطهٔ شروع خوب است.

گام بعدی شما، رفتن به اینترنت و پیداکردن اطلاعاتی دربارهٔ **بسط**[1] آن فایل است، یعنی حروفی در نام فایل که بعد از نقطهٔ مربوط به نام فایل می‌آید، مانند «.DOC» در نام فایل یک سند Word.

نشانی وب دو منبع عالی برای شناسایی بسط فایل در زیر آمده است:

http://www.filext.com
http://www.wotsit.org/

این دو پایگاه وب، فهرستی الفبایی از بسطهای فایل را به همراه توضیحی دربارهٔ علت نام‌گذاری و برنامه‌هایی آورده‌اند که با آنها چنان فایلهایی ساخته یا استفاده می‌شوند.

اگر این بانکهای اطلاعاتی بسط فایل نتوانستند اطلاعاتی را برای شما فراهم کنند، برای پیداکردن اطلاعات بیشتر از یک پایگاه وب جستجوگر بهره بگیرید. چنین جستجویی ممکن است شما را به طرف یک بانک اطلاعاتی بسط فایل دیگر هدایت کند، یا شما را به سوی پایگاه وب شرکتی ببرد که سازندهٔ برنامهٔ استفاده‌کننده از آن فایل است.

پراسسها[2]

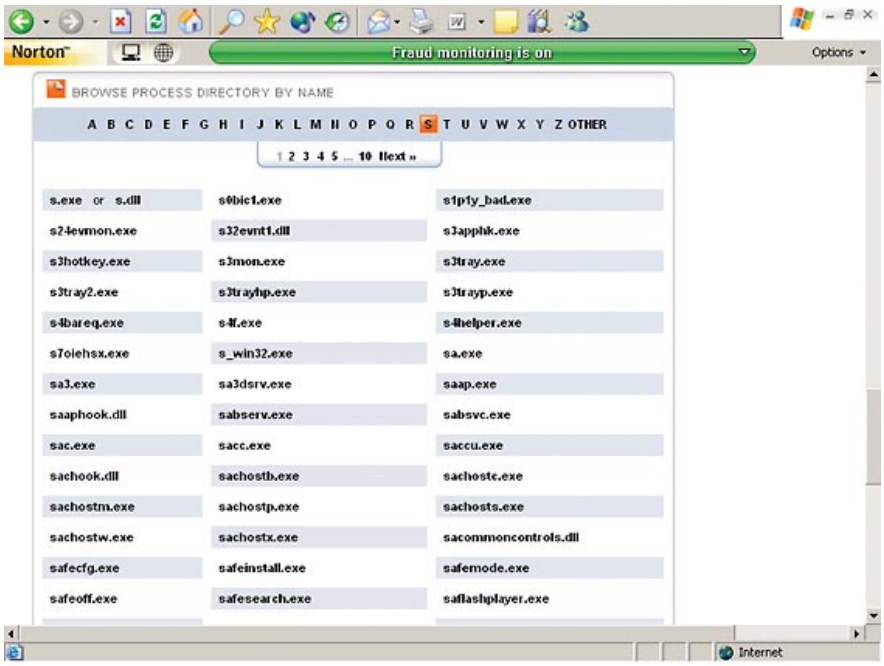
با این همه، فایلهای ناشناس با بسط «.EXE» یا یک بسط فایل قابل اجرای دیگررا جدی بگیرید. **برنامه‌های پراسسی** نیز از این نوع فایلها هستند. برنامه‌های پراسسی اکثراً در زمینهٔ سیستم شما اجرا می‌شوند. در حقیقت، وقتی دریابید که تعداد زیادی پراسس به طور همزمان در حال اجرا هستند ممکن است شگفت‌زده شوید، حتی اگر تعداد کمی برنامه باز باشد.

برای درک بهتر پراسسها، Windows Task Manager را باز کنید (کلید ترکیبی CTRL-ALT-DELETE را به طور همزمان بزنید). ابتدا، روی دکمهٔ Applications کلیک کنید. همهٔ برنامه‌ها و فایلهایی را خواهید دید که باز کرده‌اید، مانند Microsoft Word و Internet Explorer.

حال روی دکمهٔ سربرگی Processes کلیک کنید. نظر به این که فهرستی که به نمایش در می‌آید فهرست برنامه‌های در حال

[1] extension

[2] process



برای این که دریابید که یک فایل ناشناختهٔ قابل اجرا خوب، بد، یا غیرضروری است، به پایگاه وب Process Library مراجعه کنید.

اجرا بر روی کامپیوتر است، هر چیزی که در اینجا به نمایش در می‌آید یک فایل قابل اجراست. همچنین متوجه خواهید شد که تعداد پراسسهای فهرست‌شده بسیار بیشتر از تعداد **برنامه‌های کاربردی**[3] فهرست‌شده (در صفحهٔ Application) است. در حقیقت، در یک نقطه که ما Task Manager را در سیستم خود باز کردیم، صفحهٔ Application، فقط یک برنامه را فهرست کرد، اما صفحهٔ Processes حاوی ۴۷ پراسس در حال اجرا بود. همچنان که پیشتر ذکر شد، پراسسها در زمینه کار می‌کنند، شامل پراسسهایی که نمی‌خواهید در سیستم شما اجرا شوند.

متأسفانه، ویروسها، تروجاها[4]، برنامه‌های **پایش‌افزار**[5]، و آگهیها[6] نیز می‌توانند به صورت فایلهای قابل اجرا باشند، و گاهی مؤلفان آنها به آنها نامهایی چون نامهای فایلهای قانونی می‌دهند، یا وقتی به سیستم شما حمله می‌کنند نامی چون یک نام فایل قانونی می‌گیرند.

ما یک پایگاه وب آگاهی‌بخش برای یادگیری اطلاعات مختلف دربارهٔ فایلهای قابل اجرا و متمایزکردن انواع خوب، بد، و غیرضروری پیدا کردیم. پایگاه Uniblue Process Library، فایلهای قابل اجرایی را فهرست و تعریف می‌کند که بخشی قانونی از ویندوز و سایر برنامه‌ها هستند، مانند برنامه‌های **دستگاه‌ران**[7] وسایل سخت‌افزاری جانبی. این پایگاه همچنین فایلهایی را فهرست می‌کند که خطرساز هستند و نباید بر روی سیستم شما حضور داشته باشند. از این کتابخانه به رایگان می‌توانید استفاده کنید.

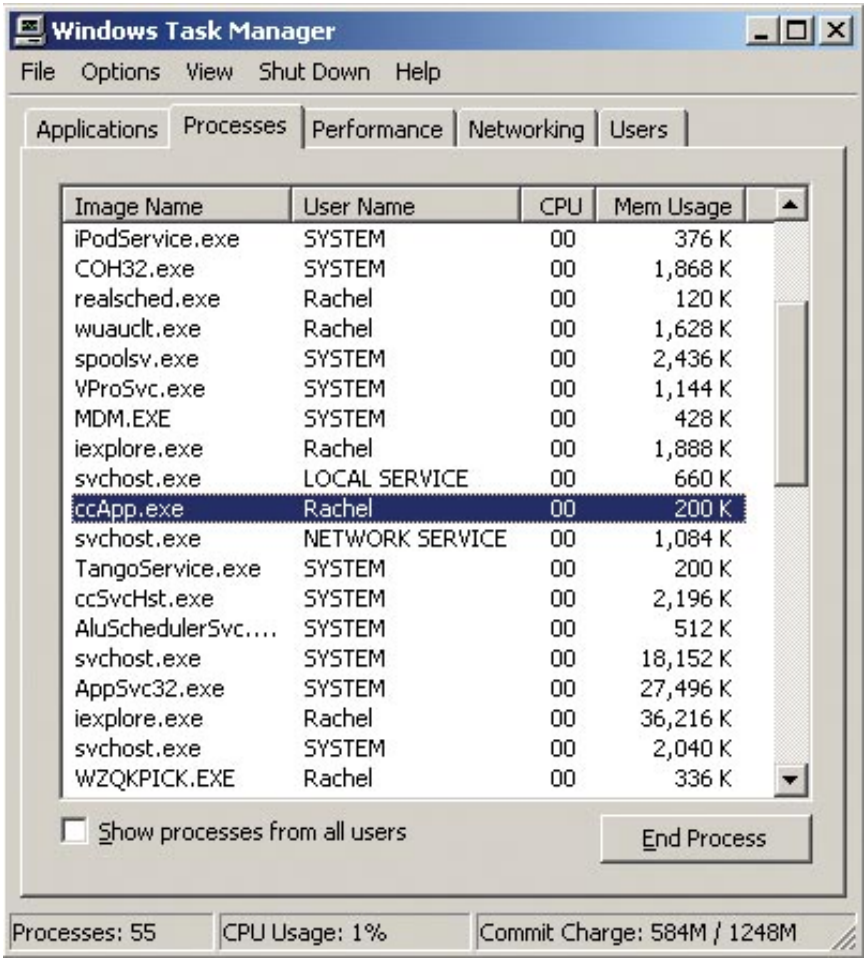
http://www.processlibrary.com/

ما در Process Library یاد گرفتیم که فایل CcApp.exe بر روی سیستم ما امکانات محافظت خودکار و بررسی ایمیل را برای برنامهٔ Norton AntiVirus فراهم می‌کند. اگر این فایل حذف شود، برنامهٔ ضدویروس نورتون درست عمل نخواهد کرد _ در حقیقت، این پایگاه به ما هشدار داد که به کار این فایل خاتمه ندهیم.

از سوی دیگر، Process Library این آگاهی را نیز به ما داد که فایلی با همین نام، پراسسی است که به یک برنامهٔ تبلیغاتی تعلق دارد. این فایل داده‌هایی دربارهٔ عادات مرور کاربر گردآوری می‌کند و این اطلاعات را به سرورهایی ارسال می‌کند که متعلق به مؤلف آن فایل هستند. افزون بر این، این فایل تولیدکنندهٔ آگهیهای پاپ–آپ نیز هست. Process Library توصیه می‌کند که این فایل را حتماً حذف کنید.

در نتیجه پرسش ما به این پرسش تبدیل می‌شود که چگونه می‌توان گفت که یک فایل قابل اجرا خوب است یا بد. یکی از پاسخها، به بخشی از سیستم شما بستگی دارد که فایل مزبور در آن عمل می‌کند. اگر در یک پوشهٔ برنامه‌ای قرار داشته باشد و متعلق به آن برنامه باشد _ مانند فایل CcApp.exe در سیستم ما _ فایل خوبی باید باشد. در نتیجه، اگر یک فایل قابل اجرا بر روی سیستم خود پیدا کنید که در مورد آن مشکوک هستید، نام آن را در پایگاه وب Process Library بررسی کنید تا آن فایل را شناسایی کند، و سپس از فرمان Search

[3] application
[4] Trojans
[5] spyware
[6] adware
[7] driver



Windows Task Manager همهٔ پراسسهای (فایلهای قابل اجرا) در حال اجرا بر روی سیستم را نمایش می‌دهد.

(روی Start و بعد Search کلیک کنید) برای تعیین مکان فایل بر روی سیستم خود بهره بگیرید. سرانجام، توصیه‌های Process Library را در مورد حفظ یا حذف فایل مسئله‌دار بخوانید.

افزون بر این، باید نام فایل مسئله‌دار را در پایگاه وب سازندهٔ برنامهٔ ضدویروس مورد استفادهٔ خود نیز بررسی کنید. پایگاههایی مانند سیمانتک و مک‌آفی، که دو سازندهٔ اصلی نرم‌افزار ضدویروس هستند، آخرین اطلاعات را دربارهٔ ویروسها، اسبهای تروا، پایش‌افزار، و برنامه‌های تبلیغاتی در صفحات وب خود جای می‌دهند:

http://www.symantec.com/

http://www.mcafee.com/

به عنوان مثال، در **سراصفحهٔ**[8] مک‌آفی، بخش Threat Center، فهرست نامهای آخرین فایلهای مسئله‌دار را نمایش می‌دهد. اگر روی نام یک فایل در آنجا کلیک کنید، اطلاعاتی چون نوع فایل، زمان کشف فایل، اثرات مخرب فایل بر روی کامپیوتر، و سطح خطر آن فایل به نمایش در می‌آید.

[8] Home page

FileAdvisor

اگر سیستم شما با یک برنامهٔ ضدویروس محافظت شده باشد که آن را همواره روزآمد نگه می‌دارید، به ندرت باید با فایلی تهدیدکننده برخورد کنید.

اما اگر به دنبال یک لایهٔ دفاعی اضافی هستید، FileAdvisor را امتحان کنید، که یک موتور جستجوگر رایگان است که می‌توانید آن را از پایگاه وب Bit9 دریافت کنید:

www.bit9.com/products/fileadvisor.php

یا مستقیماً بر روی وب از خدمات آن بهره بگیرید:

fileadvisor.bit9.com/services/search.aspx

کاتالوگ موجود در این پایگاه، نام میلیونها فایل قابل اجرا، دستگاه‌ران، و وصله را فهرست می‌کند که جزئی از برنامه‌های طراحی‌شده برای ویندوز هستند. افزون بر این، نام هزاران فایل زیان‌آور را فهرست کرده است که می‌توانند به سیستم شما ضربه بزنند. با کلیک‌کردن روی یک دکمه، می‌توانید یک نام یا Hash (رشته‌ای از اعداد گنجانده‌شده در فایل) یک فایل ناشناخته را تحویل بدهید و اطلاعات فراوانی را دربارهٔ آن فایل دریافت کنید. با FileAdvisor، همهٔ مزایای فراهم‌شده به وسیلهٔ سایر برنامه‌ها و پایگاههای وب را که پیشتر ذکر کردیم _ از یک جا دستیابی خواهید کرد.□