تهدیدهای اینترنتی

هیچ‌کس دوست ندارد که به روزهایی باز گردد که اینترنت یک آرزو در داستان‌های علمی–تخیلی بود و مردم داده‌های خود را با استفاده از دیسکت‌های فلاپی مبادله می‌کردند، اما آن دوران باستان کامپیوتری از یک لحاظ بسیار بهتر از دورانی است که در آن به سر می‌بریم: **بدافزار**. بدافزار یا **malware** کوتاه‌شدهٔ «نرم‌افزار بد» یا «malicious software» است. بدافزار به مجموعهٔ ویروس‌ها، کرم‌ها[1]، ثبت‌کننده‌های کلیدزنی[2]، و سایر برنامه‌هایی گفته می‌شود که هر کاری از دزدی اطلاعات شخصی گرفته تا خراب‌کردن کامپیوتر را انجام می‌دهند.

پیش از عصر اینترنت نیز بدافزار وجود داشت. در آن هنگام، بدافزار معمولاً باید بر روی یک دیسکت فلاپی ذخیره می‌شد، و برای ورود به یک کامپیوتر باید آن دیسکت در **دیسکت‌ران** آن کامپیوتر قرار می‌گرفت. نظر به این که در آن زمان کمتر از شبکه‌های خانگی و اداری کوچک بهره گرفته می‌شد، هنگامی که بدافزار نصب می‌شد، خسارت بدافزار فقط روی یک کامپیوتر رخ می‌داد.

اینترنت همه چیز را عوض کرد. محبوبیت و همه‌جاگیری آن سبب شد که برنامه‌سازان بدافزار نیازی به دسترسی فیزیکی کامپیوترها نداشته باشند. آنها می‌توانستند از راه دور به اهداف سوء خود برسند، و حتی میلیون‌ها کامپیوتر را هدف قرار دهند. طبق یک بررسی Panda Labs، در فصل چهارم سال ۲۰۰۸ بر روی 2.5میلیون کامپیوتر، 34.97درصد از آن کامپیوترها دست‌کم به یک بدافزار آلوده بودند.

برنامه‌سازان بدافزار برای نصب ساخته‌های خود بر روی کامپیوتر شما باید سه کار انجام دهند. اول، آنها باید تصمیم بگیرند که چه نوع برنامه‌ای را می‌خواهند نصب کنند. دوم، باید آن را بسته‌بندی کنند. و سرانجام، آنها باید آن را به شما برسانند. در این مقاله، انواع تهدیدهایی را که به هنگام ارتباط با اینترنت ممکن است با آنها بربخورید و همچنین کارهایی را که علیه آنها می‌توانید انجام دهید خواهیم گفت.

انواع بدافزار

هر برنامهٔ بدافزاری، به جز موارد نادر، یک **هدف** دارد. اگر بخواهید بهترین روش جلوگیری از ورود برنامه‌های بدافزار را بشناسید، یا آلودگی‌های موجود را پاک کنید، پیداکردن آن هدف بسیار مهم است.

● **پایش‌افزار**[3] **و تبلیغ‌افزار**[4]. این بدافزارها همان‌گونه کار می‌کنند که از نام آنها پیداست. **پایش‌افزار** یک یا چند نوع کار کامپیوتری شما را تحت نظر می‌گیرد.

بعضی از انواع پایش‌افزار، **گذرواژه‌هایی** را که شما تایپ می‌کنید می‌دزدند، و بعضی دیگر از آنها رفتار مرور اینترنتی شما را زیر نظر می‌گیرند. در مجموع، پایش‌افزار سعی می‌کند که اطلاعات شخصی و خصوصی شما را به دست بیاورد و آنها را به کسی بدهد که به طور طبیعی نباید به آن دسترسی داشته باشد.

تبلیغ‌افزار نرم‌افزاری است که تبلیغات تجاری یا غیرتجاری‌ای را بر روی کامپیوتر شما نمایش می‌دهد که به طور طبیعی به نمایش در نمی‌آیند. گاهی همراه با پایش‌افزار کار می‌کند تا آگهی‌هایی که به نمایش در می‌آیند براساس اطلاعات جمع‌آوری‌شده با پایش‌افزار مطابق سلیقه‌های فردی شما باشد.

حذف پایش‌افزار و تبلیغ‌افزار به برنامه‌های اختصاصی ضدپایش‌افزار/ ضدتبلیغ‌افزار نیاز دارد. برنامه‌های ضدویروسی که اکثر مردم با آنها آشنا هستند برای مقابله با این تهدیدها کارساز نیستند، مگر این که بخش ضدپایش‌افزار/ ضدتبلیغ‌افزار داشته باشند.

● **ثبت‌کننده‌های کلیدزنی و عکاسان صفحه‌نمایش.** آیا اگر کسی بتواند هر چیزی را که شما بر روی کامپیوتر تایپ می‌کنید ببیند وحشتناک نیست؟ این همان کاری است که برنامه‌های ثبت‌کنندهٔ

[1] worm
[2] keylogger
[3] spyware
[4] adware

کلیدزنی انجام می‌دهند. آنها هر چیزی را که شما تایپ می‌کنید ذخیره می‌کنند و از طریق اینترنت به کسی دیگر می‌دهند.

عکاسان صفحه‌نمایش[5] عمل مشابهی را انجام می‌دهند اما نتیجهٔ آنها می‌تواند بدتر باشد. این برنامه‌ها در فواصل زمانی منظم (یا برنامه‌سازی‌شده) از **دسک‌تاپ** شما عکس می‌گیرند، و به کسی دیگر امکان می‌دهند که دقیقاً ببیند که شما در طول روز به چه چیزهایی بر روی کامپیوترتان نگاه می‌کرده‌اید. بسیاری از برنامه‌های ثبت‌کنندهٔ کلیدزنی و عکاس صفحه‌نمایش به وسیلهٔ کسانی نصب می‌شوند که به کامپیوتر شما دسترسی دارند و می‌خواهند جاسوسی شما را کنند، اما تعداد بسیار زیادی از برنامه‌های ثبت‌کنندهٔ کلیدزنی در حال حاضر از راه دور نصب می‌شوند و بیشتر برای دزدی گذرواژه به کار گرفته می‌شوند.

برنامه‌های ثبت‌کنندهٔ کلیدزنی‌ای که به وسیلهٔ کسانی نصب می‌شود که به کامپیوتر شما دسترسی دارند گاهی وسایل فیزیکی‌ای هستند که به یک شکاف USB، یا بین سیم صفحه‌کلید و پورت صفحه‌کلید کامپیوتر وصل می‌شوند. اغلب اوقات، با برنامه‌های خوب ضدپایش‌افزار قابل شناسایی‌اند، اما اگر به وسیلهٔ کسی نصب شده باشند که شما او را می‌شناسید، آنها ممکن است برنامهٔ ضدپایش‌افزار شما را نیز غیرفعال کرده باشند یا برنامهٔ ثبت‌کنندهٔ کلیدزنی را در **فهرست سفید**[6] برنامهٔ ضدپایش‌افزار قرار داده باشند. **فهرست سفید** فهرستی از نرم‌افزارهاست که برنامهٔ ضدپایش‌افزار به طور خودکار آنها را نادیده می‌گیرد، در نتیجه، هر از گاهی فهرست سفید برنامهٔ ضدپایش‌افزارتان را بررسی کنید تا اطمینان یابید که هیچ مورد مشکوکی در آنجا حضور ندارد.

- **بات‌نت‌ها**[7]. یکی از بزرگ‌ترین کاربردهای بدافزار در این روزها آلوده‌سازی تعداد بسیار زیادی کامپیوتر با برنامه‌ای است که در یک زمان خاص فعال می‌شوند، یا می‌توانند از راه دور به وسیلهٔ برنامه‌ساز بدافزار راه‌اندازی شوند. این **بات‌ها** سپس برای اجرای کارهایی مانند آشفته‌کردن غیرقانونی ارتباطات یا ارسال انبوهی از درخواست‌های همزمان برای یک سایت وب و در نتیجه غیرقابل استفاده‌کردن آن (مشهور به DoS[8] یا «حملهٔ خارج از سرویس‌سازی») مورد استفاده قرار می‌گیرند.

شناسایی نرم‌افزار **بات** بسیار دشوار است چون طوری طراحی می‌شود که خودش را پنهان کند و تا زمانی که فراخوانی نشده باشد کاری انجام نمی‌دهد. بسیاری از بات‌ها را با استفاده از برنامهٔ ضدویروس و ضدپایش‌افزار می‌توان حذف کرد، اما خلاص‌شدن از شر بعضی از آنها به ابزار ویژه‌ای نیاز دارد که اختصاصاً برای آن نوع خاص از بات طراحی شده است. بسیاری از این ابزارها را سازندگان ضدویروس و ضدپایش‌افزار می‌سازند، و مایکروسافت نیز ابزار و وصله‌های تعمیرکنندهٔ گوناگونی منتشر می‌کند که هنگامی که ویندوز را روزآمد می‌کنید نصب می‌شوند.

استفاده از برنامهٔ مرورگری به جز Internet Explorer، مانند برنامهٔ Google Chrome، می‌تواند به شما کمک کند که جلوی بعضی از حمله‌های بدافزاری را بگیرید.

بدافزار مخرب

هدف بعضی از بدافزارها که تعداد آنها رو به کاهش است ایجاد آسیب بر روی کامپیوتر هدف است. این برنامه‌های صرفاً آشوب‌گر ممکن است کل دیسک‌سخت را پاک کنند، جلوی بوت‌کردن کامپیوتر را بگیرند، یا سبب شوند که ویندوز یا برنامه‌ها ضربه بخورند. گاهی طراحی آنها چنین است، و گاهی، به دلیل ضعف در برنامه‌سازی

[5] screen scraper
[6] whitelist
[7] botnet
[8] Denial-of-Service

و خارج از کنترل‌شدن آنهاست. هر کدام که باشد، نتیجه مخرب است. استفادهٔ منظم از برنامه‌های ضدویروس و ضدپایش‌افزار معمولاً جلوی بدافزار مخرب را می‌گیرد.

در گذشته، یک برنامهٔ ضدویروس خوب برای پیش‌گیری از آلودگی کامپیوتر کافی بود، اما تهدیدها به گونه‌ای فزاینده پیچیده‌تر می‌شوند.

این روزها، برای جلوگیری یا حذف‌کردن آلودگی‌ها به چند برنامهٔ ویژه نیاز دارید، چون بدافزارها به شکل‌های مختلفی بسته‌بندی می‌شوند. ما دربارهٔ روش‌های رساندن بدافزار در بخش بعدی صحبت خواهیم کرد، اما در مجموع به هیچ برنامه‌ای که به ایمیل‌ها پیوست می‌شوند نباید اطمینان کنید، در مورد سایت‌های ارائه‌دهندهٔ فایل بسیار احتیاط کنید، و ابتدا همهٔ فایل‌های دریافتی خود از اینترنت را با برنامهٔ ضدویروس یا ضدپایش‌افزارتان بررسی کنید و سپس آنها را نصب کنید.

● **ویروس.** ویروس‌های کامپیوتری به این دلیل این نام را گرفته‌اند که از جنبه‌های مختلف بسیار شبیه به ویروس‌های زیستی هستند. آنها به محض آن که با یک سیستم تماس پیدا می‌کنند آن را آلوده می‌کنند، خودشان را تکثیر می‌کنند، و سعی می‌کنند ایمیل‌ها یا سایر فایل‌هایی را که کاربران نقل و انتقال می‌دهند آلوده کنند تا بتوانند به آلوده‌سازی سیستم‌های دیگر ادامه بدهند. اکثر ویروس‌ها شناسایی شده‌اند. آنها را با استفاده از یک برنامهٔ ضدویروس روزآمدشده می‌توان متوقف یا حذف کرد.

● **کرم.** کرم‌ها از این لحاظ که خودشان را تکثیر می‌کنند شبیه به ویروس‌ها هستند، اما کرم‌ها پیش از آن که شایع بشوند، برخلاف ویروس‌های واقعی که به اجرای نوعی عمل یک کاربر نیاز دارند (مثلاً ارسال یک ایمیل)، بدون هیچ کمک خارجی می‌توانند انتشار پیدا کنند. این توانایی برای شایع‌شدن خودکار، کرم‌ها را بسیار خطرناک‌تر از ویروس‌ها کرده است، و در نتیجه، برای این که کامپیوترتان در برابر کرم‌ها ایمن باشد نرم‌افزار ضدویروس‌تان را تا جای ممکن باید روزآمد نگه دارید.

● **اسب تروا**[9]. این برنامه‌ها بسیار فریبنده هستند چون آنها به شکل برنامه‌هایی سودمند ظاهر می‌شوند اما حاوی یک بخش خطرناک پنهان هستند که بدافزار را بر روی کامپیوتر شما نصب می‌کند. به عنوان مثال، ممکن است یک بازی کامپیوتری را از اینترنت دریافت کنید که کاملاً طبیعی کار می‌کند، اما در زمینه، کامپیوتر شما را به یک برنامهٔ ناخواسته آلوده می‌کند. جلوگیری از آلودگی‌های ترویایی بسیار دشوار است چون خود کاربر چنین نرم‌افزاری را به طور دستی نصب می‌کند، که معمولاً از خطوط دفاعی‌ای چون نرم‌افزار ضدویروس و ضدپایش‌افزار عبور می‌کند. برای حذف آلودگی‌های موجود به برنامهٔ ضدویروس و ضدپایش‌افزار نیاز دارید، و گاهی برنامه‌های حذف ویژه نیز لازم است.

● **روت‌کیت**[10]. در میان همهٔ روش‌های بسته‌بندی شرح داده‌شده در این مقاله، روت‌کیت‌ها تا به حال پردردسرترین روش بوده‌اند. آنها برای نصب خودشان در مکان‌های غیرقابل‌شناسایی هوشمندانه برنامه‌سازی می‌شوند و سپس هستهٔ بنیادی ــ یا ریشه ــ سیستم‌عامل را دستیابی می‌کنند. هنگامی که کنترل آنجا را بگیرند، می‌توانند هر کاری انجام بدهند، شامل غیرفعال‌کردن نرم‌افزاری که توان شناسایی روت‌کیت را دارد، دادن کنترل از راه دور همهٔ جنبه‌های کامپیوتر به یک برنامه‌ساز داده‌ستیز، و حتی برپاکردن یک بخش اطلاعاتی اضافی برای هنگامی که به طریقی حذف یا غیرفعال می‌شود، تا بتواند به طور خودکار خودش را از نو نصب کند.

روت‌کیت‌هایی که برنامه‌سازی دقیقی دارند در برابر نرم‌افزار ضدویروس ایمن هستند و فقط با استفاده از برنامه‌های اختصاصی

[9] Trojan horse
[10] rootkit

حذف‌کنندهٔ روت‌کیت حذف می‌شوند. یک روش دیگر حذف آنها فرمت‌کردن کامل دیسک‌سخت و نصب مجدد ویندوز است.

بدافزاررسانی

حال که می‌دانید که داده‌ستیزان چه چیزی از شما می‌خواهند و معلومات کافی دربارهٔ ابزاری که آنها برای دزدی اطلاعات شما به کار می‌گیرند به دست آورده‌اید، باید ببینیم که آنها چگونه از اینترنت برای جاگذاشتن دست‌ساخته‌های خود بهره می‌گیرند و یاد بگیریم که شما چگونه می‌توانید کالای آنها را نپذیرید.

• **دریافت‌های آلوده**[11]. متداول‌ترین روش بدافزاررسانی، آلوده‌سازی فایل‌هایی که کاربران از اینترنت یا شبکه‌ها دریافت می‌کنند _ به طور عمد یا غیر عمد _ و نصب دستی آنهاست. یک روند رو به فزونی آن است که داده‌ستیزان سایت‌های وبی می‌سازند که معتبر به نظر می‌رسد و در آنها نرم‌افزار رایگان ضدبدافزار ارائه می‌کنند که در عمل یک اسب تروا‌ست که برای نصب بدافزار بر روی کامپیوتر شما طراحی شده است. براساس گزارشی با عنوان 2008 Phishing Activity Trends Report که گروه Anti-Phishing Working Group منتشر کرده است این برنامه‌های ضدبدافزار دروغین از ۲۸۵۰ مورد در جولای ۲۰۰۸ به ۹۲۸۷ مورد در دسامبر ۲۰۰۸ رسیده است. بهترین دفاع در برابر این برنامه‌ها آن است که همهٔ فایل‌های دریافتی خود را با برنامهٔ ضدویروس و ضدبدافزار معتبر بررسی کنید و هیچ‌گاه از طریق یک لینک واقع در یک ایمیل، یا از طریق سایتی که به آن اعتماد ندارید هیچ فایلی را دریافت نکنید.

•**نرم‌افزار پیگی‌-بک**[12]. یک تاکتیک متداول بدافزارها آن است که برنامه‌ای را آلوده می‌کنند که بعداً به وسیلهٔ هدف دریافت می‌شود، معمولاً از طریق سایت‌های ارائه‌دهندهٔ فایل‌های قابل اجرای بازی، کاغذدیواری، و موسیقی. هنگامی که برنامه نصب شود، بدافزار نیز با آن نصب می‌شود.

•**هرزنامه‌ها**[13] **و فریب‌نامه‌ها**[14]. بهترین روش فریب‌دادن کاربران برای نصب انواع زیان‌بار بدافزار، مانند روت‌کیت‌ها و اسب‌های تروا، از طریق ایمیل است. **هرزنامه**، یا ایمیل ناخواسته، حاوی یک لینک به برنامه‌ای است که به نظر می‌رسد برنامهٔ معتبری است، اما در عمل بدافزار در پشت نقاب آن قرار دارد.

فریب‌نامه یک گام فراتر می‌رود و یک لینک به سایت وبی دارد که به نظر می‌رسد یک سایت معتبر باشد، اما در عمل توسط داده‌ستیزان اداره می‌شود. آنها اطلاعات مهمی مانند نام کاربری، گذرواژه، و شماره کارت اعتباری را از قربانیان خود درخواست می‌کنند، و طبعاً عده‌ای فریب چنین سایتی را می‌خورند و این اطلاعات را تایپ می‌کنند. یا آنها نرم‌افزارهایی را که در اصل بدافزار هستند اما سیمای نرم‌افزارهای معتبر را دارند برای‌شان ارسال می‌کنند. در گذشته، فریب‌نامه‌ها عمدتاً به ایمیل محدود می‌شدند، اما امروزه از طریق توضیحات وبلاگ‌ها، نامه‌های انجمن‌ها، و هر مکانی بر روی وب که در آنها کاربران می‌توانند بحث کنند یا نامه بدهند نیز به کار گرفته می‌شوند.

بهترین روش‌های جلوگیری از ورود هرزنامه و فریب‌نامه استفاده از یک فیلتر هرزنامه بر روی حساب ایمیل، استفاده از مرورگری که فناوری **ضدفریب‌نامه**[15] دارد و می‌تواند به شما بگوید که سایتی که در حال بازدید از آن هستید معتبر است یا نه، و عدم کلیک‌کردن روی یک لینک در ایمیل‌ها یا وبلاگ‌ها است.

• **گروگان‌گیر مرورگر**[16]. کلیک‌کردن روی یک پنجرهٔ پاپ‌-آپ بدافزار یا دریافت نرم‌افزار آلوده می‌تواند سبب به گروگان گرفته‌شدن برنامهٔ مرورگر شود، یعنی برنامهٔ مرورگر شما طوری

[11] Infected download
[12] Piggyback software

[13] spam
[14] phishing
[15] antiphishing
[16] browser hijack

پیکربندی می‌شود که آگهی‌های تجاری ناخواسته‌ای را به نمایش درآورد، یا به سایت‌هایی برود که برای سازندهٔ بدافزار پول در می‌آورند. برنامهٔ گروگان‌گیر ممکن است **سراصفحهٔ**[17] پیش‌فرض برنامهٔ مرورگر شما را تغییر بدهد، جلوی دریافت برنامه‌های ضدویروس یا ضدپایش‌افزار را بگیرد، صدها آگهی پاپ‌آپ را به نمایش در بیاورد، و مانند آن. با استفاده از یک برنامهٔ افزودنی **مسدودکنندهٔ پاپ-آپ**[18] (که در بسیاری از برنامه‌های مرورگر جدید تعبیه شده است)، می‌توانید با این نوع تهدید مقابله کنید. یا اصلاً روی پاپ‌آپ‌ها کلیک نکنید، و هیچ نرم‌افزاری را نصب نکنید مگر این که آن را از یک منبع قابل اعتماد دریافت کرده باشید و آن را با برنامه‌های ضدویروس و ضدپایش‌افزار بررسی کرده باشید.

● **سایت‌های بهره‌گیرنده از منفذهای امنیتی**[19]. گاهی، عمل صرف بازدید از یک سایت وب به سازندگان بدافزار امکان می‌دهد که از منفذهای امنیتی در برنامهٔ مرورگر شما بهره بگیرند و بدافزار را بدون آن که شما روی چیزی کلیک کرده باشید یا به طور دستی چیزی را نصب کرده باشید در کامپیوترتان نصب کنند. روزآمدنگه‌داشتن برنامهٔ مرورگر و استفاده از مرورگرهایی به جز Internet Explorer (یک هدف محبوب نویسندگان بدافزار) می‌توانند به شما کمک کنند که جلوی این مسئله را بگیرید.

● **در پشتی**[20]. گاهی، بدافزار (معمولاً به شکل یک اسب تروا یا به شکل روت‌کیت) یک **درپشتی** مجازی برای کامپیوتر شما می‌سازد که به برنامه‌سازان بدافزار امکان می‌دهد که عمل ورود (login) به ویندوز را دور بزنند و کنترل کامل کامپیوتر شما را به دست بگیرند. در بسیاری از موارد، درهای پشتی بی‌آن که به دخالت شما نیاز باشد مستقیماً برای نصب پنهانی بدافزار در کامپیوتر شما به کار می‌روند. از شر درهای پشتی به راحتی نمی‌توان خلاص شد چون آنها ممکن است بتوانند باز و شناسایی‌نشده باقی بمانند، حتی اگر بدافزاری که آنها را ساخته است حذف شود؛ در نتیجه، فرمت‌کردن مجدد دیسک‌سخت و نصب مجدد ویندوز اغلب تنها راه است.

از خودتان محافظت کنید

داده‌ستیزان از نقاط آسیب‌پذیر برنامهٔ Internet Explorer برای حملات خود بهره می‌گیرند، چون این مرورگر پراستفاده‌ترین مرورگر دنیاست، و در نتیجه، آنها می‌توانند به تعداد بسیار زیادی قربانی دست پیدا کنند. استفاده از یک برنامهٔ مرورگر دیگر مانند **فایرفاکس**[21] یا **Google Chrome**[22] یک روش خوب برای کاستن از تعداد جاده‌هایی است که حملات از آنها آغاز می‌شوند. از هر مرورگری استفاده می‌کنید، حتماً آن را روزآمد نگه دارید، چون پیوسته نقاط آسیب‌پذیر آنها شناسایی و تعمیر می‌شود.

یک برنامهٔ ضدویروس و یک یا چند برنامهٔ ضدپایش‌افزار نصب کنید، و آنها را به همراه ویندوز همواره روزآمد نگه دارید. یک **دیوارهٔ آتش** یا **فایروال**[23]، که کل ترافیک ورودی و خروجی اینترنت را زیر نظر می‌گیرد و ترافیک مشکوک را به شما اطلاع می‌دهد یا مسدود می‌کند نیز یک وسیلهٔ مهم در لایه‌های دفاعی شماست.

گذشته از اینها، رفتارهای مرور خوب اولین خط دفاعی شماست. پیش از دریافت هر فایل از اینترنت یا کلیک‌کردن روی لینک‌هایی که نمی‌دانید شما را به کجا می‌برند خوب فکر کنید. اگر این قواعد عمومی را رعایت کنید زندگی را برای داده‌ستیزان دشوارتر خواهید کرد.

علامت‌های قرمز بدافزار

داده‌ستیزان آدم‌هایی حیله‌گر هستند، و اگر کار خود را درست انجام بدهند، شما حتی نخواهید فهمید که آنها حضور دارند. خوشبختانه تعداد کمی از آنها کار خود را خوب انجام می‌دهند، و

[17] home page
[18] pop-up blocker
[19] drive-by downloads
[20] backdoors
[21] www.mozilla.com/firefox
[22] www.google.com/chrome
[23] firewall

بسیاری از آنها چنان بی‌حیا هستند که علامت‌هایی از حضور خود را نشان می‌دهند. در نتیجه، اگر این علامت‌ها را بشناسید زودتر می‌توانید آنها را نابود کنید. اگر هر یک از علامت‌های زیر بر روی کامپیوترتان ظاهر شد، برنامهٔ ضدویروس و ضدبدافزار خود را روزآمد کنید و یک بررسی کامل را با آنها به اجرا درآورید.

• **گروگان گرفته‌شدن سراصفحه.** اگر به طور ناگهانی **سراصفحهٔ** (home page) برنامهٔ مرورگرتان تغییر کند، و شما به هنگام نصب نرم‌افزار چنین مجوزی را صادر نکرده باشید، یا به طور دستی چنین تغییری را در تنظیم‌های برنامهٔ مرورگر به وجود نیاورده باشید، معمولاً بدین معنی است که یک برنامه‌ساز بدافزار آن را به گروگان گرفته است. برنامه‌ساز بدافزار آن را طوری میزان کرده است که به سایتی برود که بدافزار بیشتری در کامپیوتر شما بار می‌کند، یا این که هر بار که صفحهٔ آنها در برنامهٔ مرورگر وب شما بار می‌شود چند سنت پول بیشتر به دست می‌آورند. اگر چنین وضعیتی به وجود آمد، یک بررسی کامل را با استفاده از برنامهٔ ضدویروس و ضدپایش‌افزار خود انجام دهید، سراصفحه را به نشانی وب مورد نظر خودتان تغییر بدهید، و برطرف‌شدن مسئله را بررسی کنید. (معمولاً تنظیم سراصفحه را در منوی Options برنامهٔ مرورگرتان می‌توانید پیدا کنید).

• **نوارابزارها و بوک‌مارک‌های ناشناس در مرورگر.** گاهی هنگامی که یک نرم‌افزار را نصب می‌کنید، از شما می‌پرسد که آیا مایلید یک **نوارابزار** (toolbar) مرورگر را نیز نصب کند یا نه (نوارابزارهای گوگل و یاهو دو نمونهٔ مشهور هستند)، اما گاهی برنامه‌سازان بدافزار نرم‌افزار خود را از طریق نصب یک نوارابزار غیرمجاز در کامپیوتر بار می‌کنند. به طور مشابه، برنامه‌سازان بدافزار گاهی از منفذهای مرورگر یا نرم‌افزار غیرقانونی برای بارکردن **بوک‌مارک‌ها** (bookmark) یا Favoriteهای غیرمجاز در برنامهٔ مرورگر شما به این امید بهره می‌گیرند که روزی شما روی آنها کلیک کنید و سایتی را بار کنید که بدافزار جدید در کامپیوترتان نصب می‌کند، یا به ازای هر بار بازدید شما چند سنتی پول را نصیب برنامه‌ساز می‌کند. پنهان‌کردن یا حذف‌کردن این نوارابزارها به ندرت کار می‌کند، چون بدافزاری که آنها را نصب کرده است احتمالاً در کامپیوتر همچنان حضور دارد و در جایی پنهان است.

• **نتایج جستجوی عجیب.** برنامهٔ مرورگر شما یک فراهم‌کنندهٔ جستجوی پیش‌فرض دارد که به هنگامی که کلماتی را در کادر Search تایپ می‌کنید به کار گرفته می‌شود. اگر این فراهم‌کننده تغییر کند (به ویژه اگر فراهم‌کنندهٔ جستجوی جدید، یک نام آشنا مانند **گوگل** یا **یاهو** نباشد)، احتمال این که برنامهٔ مرورگرتان به گروگان گرفته شده باشد بالاست.

• **ایمیل‌هایی که اطلاعات یک حساب شما را می‌پرسند.** اگر بانک شما یا مؤسسه دیگری که با آن کار می‌کنید یک ایمیل بفرستد و از شما گذرواژهٔ حساب‌تان یا اطلاعات شخصی دیگری را بپرسد که باید خودش از قبل آنها را داشته باشد، چنین ایمیلی را پاک کنید. روی هیچ‌یک از لینک‌های آن کلیک نکنید، به هیچ‌یک از شماره‌تلفن‌های آن زنگ نزنید، و هیچ پاسخی به آن ندهید، چون به احتمال زیاد یک حملهٔ فریب‌نامه‌ای است. از دفتر تلفن خود یا از شماره‌تلفن چاپ‌شده در پشت کارت اعتباری خود برای تماس با بانک یا مؤسسهٔ طرف خود بهره بگیرید و از درست یا نادرست‌بودن درخواست مطمئن شوید.

• **پاپ‌آپ‌های بی‌توقف.** پاپ‌آپ‌هایی که حتی در زمانی به نمایش در می‌آیند که شما یک **مسدودکنندهٔ پاپ‌آپ** فعال دارید، یا حتی در زمانی به نمایش در می‌آیند که برنامهٔ مرورگر شما باز نیست به این معنی هستند که بر روی کامپیوتر شما یک بدافزار یا تبلیغ‌افزار نصب شده است. در این صورت، یک بررسی کامل را با برنامه‌های ضدویروس و ضدپایش‌افزار خود انجام دهید.

• **کارنکردن برنامهٔ ضدویروس و ضدپایش‌افزار.** اگر برنامهٔ ضدویروس و ضدپایش‌افزار شما به طور ناگهانی غیرقابل دستیابی شود، یا اگر دیگر نتوانید به سایت‌های وب سازندگان آنها سر بزنید یا روزآمدکننده‌های آنها را دریافت کنید، علامت خوبی نیست. یک بدافزار در کامپیوترتان نصب شده است، و اگر نمی‌خواهید که کل

دیسک‌سخت را فرمت کنید و ویندوز را از اول نصب کنید احتمالاً به کمک یک متخصص برای حذف آن بدافزار نیاز خواهید داشت.

- **ضعیف‌شدن بازدهی کامپیوتر.** بسیاری از بدافزارها به گونه‌ای معیوب طراحی می‌شوند و ممکن است سبب آهسته‌شدن کامپیوتر، ضربه‌های سیستمی، و مسائل **بوت** شوند. بعضی از بدافزارها، مانند نرم‌افزاری که حاوی **بات‌نت** است، بخش بزرگی از **پهنای باند** ارتباط اینترنت شما را مصرف می‌کنند، در نتیجه، اگر مرور وب خیلی آهسته شود، زمان بررسی کامل کامپیوتر با یک برنامهٔ ضدویروس و ضدپایش‌افزار فرا رسیده است.□