فضولهای کامپیوتری

آیا ثبت‌کننده‌های کلیدزنی *(keylogger)* را اگر ببینید خواهید شناخت؟

ابربزرگراه اطلاعاتی قدیمی خوب در اصل یک خیابان دوطرفه است: ما به آن وصل می‌شویم و آن هم به ما وصل می‌شود. بنابراین، خطرات پنهان فراوانی، یعنی نرم‌افزارهای موذی و زیان‌آور، وجود دارد که باید مراقب آنها باشید. یکی از موذی‌ترین آنها **برنامهٔ ثبت‌کنندهٔ کلیدزنی** است.

قصد و غرض هرچه که باشد، ثبت‌کنندهٔ کلیدزنی را می‌توان به عنوان کسی یا چیزی تعریف کرد که کلیدزنیهای یک کاربر را می‌رباید. گاهی ثبت‌کنندهٔ کلیدزنی یک برنامه (اغلب تحت گروه **برنامه‌های جاسوسی**[1]) است که به همهٔ کلیدزنیهای یک کاربر «گوش می‌دهد» و آنها را ثبت می‌کند، بدون اطلاع صریح آن کاربر، و سپس اطلاعات کلیدزنیهای ذخیره‌شده را به شخص یا برنامه‌ای ارسال می‌کند که ثبت‌کنندهٔ کلیدزنی را از طریق اینترنت نصب کرده است.

ربودن اطلاعات کلیدزنی ممکن است به لحاظ قانونی در مواردی محدود برای دولتها مشروع باشد اما دزدها و هکرها برای سوءاستفاده و اقدامات شریرانهٔ خود دست به این کار می‌زنند. سوءشهرت ثبت کلیدزنی به چند دلیل است. دایره‌های جاسوسی از آن برای گذشتن از حفاظهای امنیتی و دست یافتن به کلمه‌های عبور و کلیدهای **رمزنگاری** (encryption) بهره می‌گیرند.

تبهکاران از ثبت‌کننده‌های کلیدزنی برای شکار کلمه‌های عبور یا اطلاعات کارتهای اعتباری استفاده می‌کنند. و حتی بعضی از همسران پارانوئید نیز وجود دارند که از این فناوری برای زیرنظر گرفتن گفتگوهای اینترنتی همسران خود بهره می‌گیرند. وقتی کامپیوتری «آلوده» می‌شود، اغلب یک **اسب تروا** را می‌توان مقصر دانست. **اسبهای تروا** برنامه‌هایی هستند که مدعی هستند که کار مفیدی را انجام می‌دهند اما در عمل یک ثبت‌کنندهٔ کلیدزنی را در زمینه نصب می‌کنند. ثبت‌کننده‌های کلیدزنی ابزاری «باهوش» هستند، چون آنها منتظر صفحهٔ وبی می‌مانند که حاوی کادرهای نام کاربری و کلمهٔ عبور است و سپس آنها پایگاه وب مزبور و هر چیزی را که کاربر در آن صفحه وارد می‌کند ثبت می‌کنند. ثبت‌کنندهٔ کلیدزنی می‌تواند در کامپیوتر شخصی یک کاربر یا بر روی یک سیستم عمومی مانند کامپیوتر یک کتابخانه نصب شود.

بعضی از ثبت‌کننده‌های کلیدزنی وقتی یک خرید اینترنتی انجام می‌دهید اطلاعات کارت اعتباری را شناسایی و ضبط می‌کنند. نظر به این که ثبت‌کننده‌های کلیدزنی می‌توانند کلمه‌های عبور یا شماره‌های حساب بانکی و کارت اعتباری را در لحظه‌ای که وارد می‌کنید بربایند، آنها پیش از آن که سیستم، کلمهٔ عبور را رمزی کند کلیدهای زده‌شده را ثبت می‌کنند. اگر کامپیوتر شما حاوی برنامهٔ جاسوسی باشد، این احتمال به خوبی وجود دارد که کامپیوترتان به یک ثبت‌کنندهٔ کلیدزنی آلوده شده باشد.

کاربران خانگی را نمی‌توان از مجموعهٔ قربانیان ثبت کلیدزنی خارج کرد. آیا فکر می‌کنید که باز نکردن پیامهای ایمیل مشکوک از افرادی که نمی‌شناسید کامپیوتر شما را سالم نگه می‌دارد؟ متأسفانه، مکانیسمهای آلوده‌سازی فراوانی وجود دارد که فقط به وسیلهٔ ایمیل یا به وسیلهٔ بازدید از پایگاههای وب بد انتقال نمی‌یابند. وصل کردن کامپیوتر به اینترنت بی‌خطر نیست. مدتی که طول می‌کشد تا یک سیستم ویندوز اکس‌پی بدون **وصله** (patch) پس از یک ارتباط با شبکه آلوده شود ۱۴ دقیقه است.

شناسایی ثبت کلیدزنی

علائم مشهود آلودگی کامپیوتر به ثبت‌کنندهٔ کلیدزنی به قرار زیرند: پدیدار شدن **نوارابزار** جدید در برنامهٔ مرورگر اینترنت، آهسته شدن سیستم، یا پدیدار شدن تصادفی آگهیهای پاپ‌آپ حتی در زمانی که اینترنت را مرور نمی‌کنید.

اکثر اوقات، بدون کمک نرم‌افزار اضافی، تشخیص این که کامپیوتر به ثبت‌کنندهٔ کلیدزنی یا برنامه‌های جاسوسی و موذی آلوده شده است

[1] spyware

دشوار است. کاربران باید دربارهٔ پایگاههای وبی که بازدید می‌کنند گوش به زنگ باشند. هرچند، حتی پایگاههای وبی که معتبر به نظر می‌رسند به دلیل بعضی از خصوصیات برنامه‌های مرورگر و حفره‌های امنیتی می‌توانند خطرناک باشند. وقتی یک download مخفی رخ بدهد و وقتی یک ثبت‌کنندهٔ کلیدزنی یا انواع دیگر برنامهٔ جاسوسی/موذی بر روی سیستم به طور مخفیانه نصب شود ممکن است کاربر کاملاً بی‌اطلاع باشد، چه کاربر متوسط باشد چه کاربر پیشرفته.

اگر به آلودگی کامپیوتر خود مظنون هستید، یک برنامهٔ خوب برای پیدا کردن ثبت‌کننده‌های کلیدزنی برنامهٔ رایگان Process Explorer است:

www.sysinternals.com/Utilities/ProcessExplorer.html

این برنامهٔ مفید **پراسسهای** (process) در حال اجرا، منابع سیستمی مورد استفاده، و هر برنامه‌ای که یک پراسس را به اجرا درآورده باشد به دقت شناسایی می‌کند. به شما کمک می‌کند که پیش از نصب Process Explorer، برنامه‌های معتبر نصب شده بر روی کامپیوتر را شناسایی کنید. اگر چیزی را در Process Explorer ببینید که خودتان آن را نصب نکرده‌اید، می‌توانید برنامه را برای پیدا کردن مکان استقرار آن ردیابی کنید تا راحت‌تر بتوانید آن را حذف کنید.

روش دیگر برای شناسایی یک ثبت‌کنندهٔ کلیدزنی (یا هر برنامهٔ موذی دیگر) بررسی **پراسسهای راه‌اندازی** (startup) در داخل ویندوز است زیرا تعداد زیادی از برنامه‌های موذی طوری طراحی می‌شوند که در زمان راه‌اندازی به اجرا دربیایند. اینجاست که برنامهٔ خدماتی رایگان Autoruns به کمک شما می‌آید:

www.sysinternals.com/utilities/Autoruns.html

پس از اجرای این برنامه، می‌توانید منوی View آن را ببینید و موارد Show مختلف را بررسی کنید. این کار به شما امکان می‌دهد که برنامه‌ها و همچنین سرویسها و Browser Objectهایی را ببینید که در زمان راه‌اندازی به اجرا درمی‌آیند.

هرگاه به اشتباه به یک پایگاه وب موذی سربزنید (معمولاً چنین پایگاهی شبیه به پایگاههای مشهور و خوشنام است)، یک ثبت‌کنندهٔ کلیدزنی به طور خودکار بدون اطلاع شما وارد کامپیوتر شما می‌شود، نصب می‌شود، و به اجرا درمی‌آید. به عنوان مثال، برنامهٔ Internet Explorer معمولاً دریافت خودکار کد قابل اجرایی مشهور به یک ActiveX control را ممکن می‌سازد. وقتی کاربران ناآگاهانه یک پایگاه وب آلوده‌ساز را بازدید کنند یک ActiveX control ممکن است روی سیستم آنها نصب شود. این عمل می‌تواند در هر پایگاهی و نه فقط پایگاههایی که سوءشهرت دارند رخ بدهد. بسیاری از این پایگاهها از اهداف جستجوهای کاربران بهره‌برداری می‌کنند، نمونه‌هایی از این نوع پایگاهها عبارتند: پایگاههای دریافت موسیقی، دریافت بازی، دریافت icon، و پایگاههای حاوی برنامه‌های مربوط به اوضاع جوی. برای پیش‌گیری از خطر، به چنین پایگاههایی سرنزنید.

دریافت پاپ‌آپ (pop-up)

پاپ‌آپها را خیلی از کاربران می‌بینند. بعضی از آنها طوری طراحی می‌شوند که اگر کاربر روی هر چیزی در آنها کلیک کند ثبت‌کنندهٔ کلیدزنی یا برنامهٔ موذی دیگر خود را وارد کامپیوتر می‌کنند. اگر آنها را دیدید بهترین کار آن است که با زدن کلید ترکیبی CTRL-ALT-DEL، برنامهٔ Task Manager را به اجرا درآورید و برنامهٔ پاپ‌آپ را به وسیلهٔ آن ببندید تا مطمئن شوید که چیزی را وارد کامپیوتر نمی‌کند. کاربران باید در مورد هر چیزی که خودشان به اجرا درنیاورده‌اند مشکوک باشند. در نتیجه، رفتارهای خارج از انتظار، مانند پاپ‌آپها، را به دقت و با هشیاری بررسی کنید و به آنچه پاپ‌آپ می‌گوید توجه نکنید. امروزه حتی بعضی از پاپ‌آپهای آلوده‌ساز ادعا می‌کنند که ویروسها و برنامه‌های جاسوسی را برای شما حذف می‌کنند.

حال که می‌دانید، چه باید کرد؟

اولین گام خوب آن است که **وصله‌های** (patch) موردنیاز پی‌سی را نصب کنید تا روزآمد شود. داشتن یک برنامهٔ خوب ضدویروس می‌تواند آسیب‌پذیری کامپیوتر را کمتر کند. یک سیستم‌عامل روزآمد نشده با وصله‌های جدید حاوی حفره‌های آسیب‌پذیر است. بسیاری از این حفره‌ها شناخته‌شده هستند و به آسانی می‌توانند مورد بهره‌برداری هکرها قرار بگیرند.

اغلب فقط بعد از شناسایی حضور یک ثبت‌کنندهٔ کلیدزنی می‌توانید کامپیوتر خود را در

برابـر آن محافظـت کنیـد. بهتـرین دفـاع در برابـر ثبت‌کننده‌های کلیدزنی سخت‌افزاری آن است که کامپیوتر خـود را بـه طـور فیزیکـی بررسـی کنیـد. پیداکردن وسیله‌ای که به کابـل صـفحه کلیـد شـما وصل شده است آسـان اسـت؛ امـا شناسـایی وقتـی دشـوار مـی‌شـود کـه ثبـت‌کننـده را در داخـل صفحه‌کلید شما جاسازی کرده باشند.

در پاسخ به تهدید امنیتـی ناشـی از ثبـت‌کننـدهٔ کلیـدزنی، بعـضی از شـرکتها نـرم‌افـزاری را بـرای جلـوگیری و شناسـایی تهدیـدهای برنامـه‌هـای جاسوسـی سـاخته‌انـد. امـا تحـت هـیچ شـرایطی، هیچ‌کدام از هزاران برنامهٔ ضدجاسوسی موجـود در اینترنت را دریافت نکنید، مگر این که آنهـا را منـابع معتبر تأیید کرده باشند. اکثر این برنامه‌هـا خودشـان در دل خود حاوی برنامـهٔ جاسوسـی هـستند. بـرای شناسایی برنامه‌های مسئله‌دار و مشکوک بـه پایگـاه وب زیر سربزنید:

spywarewarrior.com

و روی لینـــــــــــــــــــــــک Rogue/Suspect Anti-Spyware کلیک کنید.

یـک بـستهٔ خـوب، نـرم‌افـزار رایگـان Google Pack اسـت کـه برنامـهٔ ضدجاسوسـی مشهور Ad-Aware SE Personal را نیـز در خـود دارد.

www.google.com/downloads

مایکروســـــــافت نیـــــــز برنامـــــــهٔ Windows Defender را فراهم سـاخته اسـت کـه نگارش بتای ۲ آن را می‌توانید از پایگاه وب زیر بـه رایگان دریافت کنید:

www.microsoft.com/athome/security/spyware/software/default.mspx

یـک برنامـهٔ خـوب دیگـر برنامـهٔ ۳۰ دلاری Spy Sweeper است:

www.webroot.com

بهتـرین راه جلـوگیری از ورود ثبـت‌کننـدهٔ کلیدزنی پرهیز از بازدید پایگاههای وب مشکوک اسـت. در مجمـوع، اکثـر پایگاههـای وب سـالم هستند، اما برای ایـن کـه بـا اطمینـان و قـوت قلـب پایگاههـای وب را مـرور کنیـد برنامـهٔ رایگـان محصول SiteAdvisor.com را به کار بگیریـد کـه به برنامهٔ مرورگر وصل می‌شود و بـرای هـر پایگـاه وب یک امتیاز رنگی می‌دهد.□